

# Junos® OS

---

## High Availability User Guide

Published  
2023-03-14

Juniper Networks, Inc.  
1133 Innovation Way  
Sunnyvale, California 94089  
USA  
408-745-2000  
[www.juniper.net](http://www.juniper.net)

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, 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.

*Junos® OS High Availability User Guide*

Copyright © 2023 Juniper Networks, Inc. All rights reserved.

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 | xxvi**

1

## **Overview**

**High Availability Overview | 2**

Understanding High Availability Features on Juniper Networks Routers | 2

High Availability-Related Features in Junos OS | 8

High Availability Features for EX Series Switches Overview | 9

2

## **Configuring Switching Control Board Redundancy**

**Understanding How Switching Control Board Redundancy Prevents Network Failures | 15**

Understanding Switching Control Board Redundancy | 15

**Configuring Switching Control Board Redundancy | 20**

Configuring Switching Control Board Redundancy | 20

Configuring CFEB Redundancy on the M10i Router | 20

Configuring FEB Redundancy on the M120 Router | 21

Example: Configuring FEB Redundancy on M120 Routers | 22

Configuring SFM Redundancy on M40e and M160 Routers | 24

Configuring SSB Redundancy on the M20 Router | 24

Configuring the Junos OS to Support Redundancy on Routers Having Multiple Routing Engines or Switching Boards | 25

3

## **Configuring Bidirectional Forwarding Detection (BFD)**

**Understanding How BFD Detects Network Failures | 27**

Understanding How BFD Detects Network Failures | 27

Understanding BFD | 28

Centralized BFD | 29

Distributed BFD | 29

Inline BFD | 31

Understanding BFD for Static Routes for Faster Network Failure Detection | 33

Understanding BFD for BGP | 37

Understanding BFD for OSPF | 38

Understanding BFD for IS-IS | 41

Understanding BFD for RIP | 44

Understanding Independent Micro BFD Sessions for LAG | 45

Configuration Guidelines for Micro-BFD Sessions | 46

Understanding Static Route State When BFD is in Admin Down State | 47

## Configuring BFD | 50

Configuring BFD | 50

Example: Configuring BFD for Static Routes for Faster Network Failure Detection | 51

Requirements | 51

Overview | 51

Configuration | 52

Verification | 57

Example: Configuring BFD on Internal BGP Peer Sessions | 60

Requirements | 60

Overview | 60

Configuration | 62

Verification | 68

Example: Configuring BFD for OSPF | 72

Requirements | 73

Overview | 73

Configuration | 75

Verification | 77

Example: Configuring BFD for IS-IS | 78

Requirements | 78

Overview | 79

Configuration | 79

Verification | 85

Example: Configuring BFD for RIP | 88

Requirements | 89

Overview | 89

Configuration | 91

Verification | 95

Configuring Micro BFD Sessions for LAG | 97

Example: Configuring Independent Micro BFD Sessions for LAG | 103

Requirements | 103

## 4

- Overview | 104
- Configuration | 104
- Verification | 112

- Configuring BFD for PIM | 116

- Enabling Dedicated and Real-Time BFD on SRX Devices | 118

## Configuring Routing Engine Redundancy

- Understanding How Routing Engine Redundancy Prevents Network Failures | 124

- Understanding Routing Engine Redundancy | 124

### Configuring Routing Engine Redundancy | 131

- Configuring Routing Engine Redundancy | 131

- Modifying the Default Routing Engine Primary Role | 132

- Configuring Automatic Failover to the Backup Routing Engine | 132

- Without Interruption to Packet Forwarding | 133

- On Detection of a Hard Disk Error on the Primary Routing Engine | 133

- On Detection of a Broken LCMD Connectivity Between the VM and RE | 133

- On Detection of a Loss of Keepalive Signal from the Primary Routing Engine | 133

- On Detection of the em0 Interface Failure on the Primary Routing Engine | 135

- When a Software Process Fails | 135

- Manually Switching Routing Engine Primary Role | 135

- Verifying Routing Engine Redundancy Status | 136

- Initial Routing Engine Configuration Example | 137

- Copying a Configuration File from One Routing Engine to the Other | 140

- Loading a Software Package from the Other Routing Engine | 141

## 5

## Configuring Load Balancing

- Understanding Load Balancing | 143

- Load Balancing on Aggregated Ethernet Interfaces | 143

- Load Balancing and Ethernet Link Aggregation Overview | 144

- Understanding Aggregated Ethernet Load Balancing | 144

- Stateful Load Balancing for Aggregated Ethernet Interfaces Using 5-Tuple Data | 146

- Configuring Stateful Load Balancing on Aggregated Ethernet Interfaces | 150

- Configuring Adaptive Load Balancing | 151

- Configuring Symmetrical Load Balancing on an 802.3ad Link Aggregation Group on MX Series Routers | 152

- Symmetrical Load Balancing on an 802.3ad LAG on MX Series Routers Overview | 152

Configuring Symmetric Load Balancing on an 802.3ad LAG on MX Series Routers | 153

Configuring Symmetrical Load Balancing on Trio-Based MPCs | 156

Example Configurations | 158

Configuring PIC-Level Symmetrical Hashing for Load Balancing on 802.3ad LAGs for MX Series Routers | 160

Examples: Configuring PIC-Level Symmetrical Hashing for Load Balancing on 802.3ad LAGs on MX Series Routers | 162

Example: Configuring Aggregated Ethernet Load Balancing | 165

Example: Configuring Aggregated Ethernet Load Balancing | 165

## Configuring Graceful Routing Engine Switchover (GRES)

Understanding How GRES Enables Uninterrupted Packet Forwarding During a Routing Engine Switchover | 185

Understanding Graceful Routing Switchover | 185

Understanding Graceful Routing Engine Switchover | 185

Graceful Routing Engine Switchover System Requirements | 194

### Configuring GRES | 200

Configuring Graceful Routing Engine Switchover | 200

Requirements for Routers with a Backup Router Configuration | 201

Enabling Graceful Routing Engine Switchover | 201

Configuring Graceful Routing Engine Switchover with Graceful Restart | 202

Synchronizing the Routing Engine Configuration | 202

Verifying Graceful Routing Engine Switchover Operation | 203

Configuring Graceful Routing Engine Switchover in a Virtual Chassis | 204

Preventing Graceful Routing Engine Switchover in the Case of Slow Disks | 205

Resetting Local Statistics | 206

Example: Configuring IS-IS for GRES with Graceful Restart | 206

Requirements | 207

Overview | 207

Configuration | 207

Verification | 209

### Configuring Ethernet Automatic Protection Switching for High Availability | 212

Configuring Ethernet Automatic Protection Switching | 212

Ethernet Automatic Protection Switching Overview | 212

Mapping of CCM Defects to APS Events | 216

7

Example: Configuring Protection Switching Between Psuedowires | 217

Requirements | 218

Overview and Topology | 218

Configuration | 219

## Configuring Ethernet Ring Protection Switching

Understanding Ethernet Ring Protection Switching for High Availability | 223

Understanding Ethernet Ring Protection Switching | 223

Ethernet Ring Protection Switching Overview | 223

Understanding Ethernet Ring Protection Switching Functionality | 224

Configuring Ethernet Ring Protection Switching for High Availability | 234

Configuring Ethernet Ring Protection Switching | 234

Configuring Ethernet Ring Protection Switching | 234

Example: Ethernet Ring Protection Switching Configuration on MX Routers | 235

Requirements | 236

Ethernet Ring Overview and Topology | 236

Configuring a Three-Node Ring | 237

8

## Configuring Nonstop Bridging

Understanding How Nonstop Bridging Preserves Layer 2 Protocol Information During a Routing Engine Switchover | 249

Understanding Nonstop Bridging | 249

Nonstop Bridging Concepts | 249

Understanding Nonstop Bridging on EX Series Switches | 252

Nonstop Bridging System Requirements | 252

Configuring Nonstop Bridging | 254

Configuring Nonstop Bridging | 254

Enabling Nonstop Bridging | 254

Synchronizing the Routing Engine Configuration | 255

Verifying Nonstop Bridging Operation | 255

Configuring Nonstop Bridging on Switches (CLI Procedure) | 255

Configuring Nonstop Bridging on EX Series Switches (CLI Procedure) | 257

9

## Configuring Nonstop Active Routing (NSR)

Understanding How Nonstop Active Routing Preserves Routing Protocol Information During a Routing Engine Switchover | 260

**Understanding Nonstop Active Routing | 260**

Nonstop Active Routing Concepts | 260

Understanding Nonstop Active Routing on EX Series Switches | 264

Nonstop Active Routing System Requirements | 265

**Configuring Nonstop Active Routing | 281****Configuring Nonstop Active Routing | 281**

Enabling Nonstop Active Routing | 282

Synchronizing the Routing Engine Configuration | 283

Verifying Nonstop Active Routing Operation | 283

Configuring Nonstop Active Routing on Switches | 284

Preventing Automatic Reestablishment of BGP Peer Sessions After NSR Switchovers | 285

Example: Configuring Nonstop Active Routing | 286

Resetting Local Statistics | 289

Example: Configuring Nonstop Active Routing on Switches | 290

Requirements | 290

Overview and Topology | 290

Configuration | 291

Verification | 292

Troubleshooting | 294

**Configuring Graceful Restart****Understanding How Graceful Restart Enables Uninterrupted Packet Forwarding When a Router is Restarted | 297****Understanding Graceful Restart | 297**

Graceful Restart Concepts | 298

Graceful Restart for Aggregate and Static Routes | 299

Graceful Restart and Routing Protocols | 299

Graceful Restart and MPLS-Related Protocols | 302

Understanding Restart Signaling-Based Helper Mode Support for OSPF Graceful Restart | 303

Graceful Restart and Layer 2 and Layer 3 VPNs | 304

Graceful Restart on Logical Systems | 305

Graceful Restart System Requirements | 306

**Configuring Graceful Restart | 307****Configuring Graceful Restart | 307**

Enabling Graceful Restart | 307



Configuring Graceful Restart | 308

Configuring VPN Graceful Restart | 342

- Configuring Graceful Restart Globally | 343

- Configuring Graceful Restart for the Routing Instance | 343

Configuring Logical System Graceful Restart | 344

- Enabling Graceful Restart Globally | 344

- Configuring Graceful Restart for a Routing Instance | 345

Configuring Graceful Restart for QFabric Systems | 346

- Enabling Graceful Restart | 347

- Configuring Graceful Restart Options for BGP | 348

- Configuring Graceful Restart Options for OSPF and OSPFv3 | 348

- Tracking Graceful Restart Events | 350

Example: Managing Helper Modes for OSPF Graceful Restart | 351

- Requirements | 353

- Overview | 353

- Verification | 353

Tracing Restart Signaling-Based Helper Mode Events for OSPF Graceful Restart | 354

Verifying Graceful Restart Operation | 355

- Graceful Restart Operational Mode Commands | 356

- Verifying BGP Graceful Restart | 356

- Verifying IS-IS and OSPF Graceful Restart | 357

- Verifying CCC and TCC Graceful Restart | 358

Configuring Graceful Restart for Routing Protocols | 359

- Enabling Graceful Restart | 360

- Configuring Graceful Restart Options for BGP | 361

- Using Control Plane Dependent BFD along with Graceful Restart Helper Mode | 362

- Configuring Graceful Restart Options for ES-IS | 363

- Configuring Graceful Restart Options for IS-IS | 363

- Configuring Graceful Restart Options for OSPF and OSPFv3 | 364

- Configuring Graceful Restart Options for RIP and RIPng | 366

- Configuring Graceful Restart Options for PIM Sparse Mode | 366

- Tracking Graceful Restart Events | 367

- Configuring Graceful Restart for MPLS-Related Protocols | 368

- Configuring Graceful Restart Globally | 368

- Configuring Graceful Restart Options for RSVP, CCC, and TCC | 368

## 11

Configuring Graceful Restart Options for LDP | 369

## Power Management Overview

### Understanding Power Management | 373

Understanding Power Management on EX Series Switches | 373

### Configuring Power Management | 380

Configuring Power Management | 380

Configuring the Power Priority of Line Cards (CLI Procedure) | 380

Configuring Power Supply Redundancy (CLI Procedure) | 381

### Redundant Power System Overview | 383

Understanding the EX Series Redundant Power System | 383

EX Series Redundant Power System Hardware Overview | 383

Understanding How Power Priority Is Determined and Set for Switches Connected to the EX Series Redundant Power System | 387

Determining and Setting Priority for Switches Connected to an EX Series RPS | 389

Using RPS Default Configuration | 390

Setting the EX Series RPS Priority for a Switch (CLI) | 390

## 12

## Configuring Virtual Router Redundancy Protocol (VRRP)

### Understanding How the VRRP Router Failover Mechanism Prevents Network Failures | 393

Understanding VRRP | 393

Understanding VRRP | 393

VRRP and VRRP for IPv6 Overview | 398

Understanding VRRP Between QFabric Systems | 398

Junos OS Support for VRRPv3 | 403

VRRP failover-delay Overview | 409

### Configuring VRRP | 412

Configuring VRRP | 412

Configuring Basic VRRP Support | 414

Example: Configuring VRRP for IPv4 | 419

Requirements | 419

Overview | 419

Configuring VRRP | 420

Verification | 426

Configuring VRRP and VRRP for IPv6	429
Configuring VRRP for IPv6 (CLI Procedure)	431
Example: Configuring VRRP for IPv6	433
Requirements	433
Overview	433
Configuring VRRP	434
Verification	441
Configuring VRRP Authentication (IPv4 Only)	445
Configuring VRRP Preemption and Hold Time	446
Configuring VRRP Preemption	447
Configuring the Preemption Hold Time	447
Configuring the Advertisement Interval for the VRRP Primary Router	448
Modifying the Advertisement Interval in Seconds	449
Modifying the Advertisement Interval in Milliseconds	449
Configuring the Startup Period for VRRP Operations	451
Configuring a Backup Router to Preempt the VRRP Primary Router	451
Configuring a Backup to Accept Packets Destined for the Virtual IP Address	452
Modifying the Preemption Hold-Time Value for the VRRP Primary Router	453
Configuring the Asymmetric Hold Time for VRRP Routers	454
Configuring Passive ARP Learning for Backup VRRP Routers	454
Configuring VRRP Route Tracking	455
Configuring a Logical Interface to Be Tracked for a VRRP Group	457
Configuring a Route to Be Tracked for a VRRP Group	460
Example: Configuring Multiple VRRP Owner Groups	462
Requirements	462
Overview	462
Configuration	462
Verification	471
Configuring Inheritance for a VRRP Group	471
Configuring an Interface to Accept All Packets Destined for the Virtual IP Address of a VRRP Group	472
Configuring the Silent Period to Avoid Alarms Due to Delay in Receiving VRRP Advertisement Packets	473
Enabling the Distributed Periodic Packet Management Process for VRRP	474
Improving the Convergence Time for VRRP	476
Configuring VRRP to Improve Convergence Time	477

Tracing VRRP Operations | 479

Example: Configuring VRRP for Load Sharing | 480

Requirements | 481

Overview and Topology | 481

Configuring VRRP on Both Switches | 483

Verification | 487

Troubleshooting VRRP | 489

## Performing Unified In-Service Software Upgrade (ISSU)

Getting Started with Unified ISSU and Understanding How Unified ISSU Works | 492

Understanding Unified ISSU | 492

Getting Started with Unified In-Service Software Upgrade | 492

Understanding the Unified ISSU Process | 493

Understanding the Unified ISSU Process on a Router | 494

Understanding the Unified ISSU Process on the TX Matrix Router | 498

Understanding In-Service Software Upgrade (ISSU) | 501

Understanding In-Service Software Upgrade (ISSU) in ACX5000 Series Routers | 502

Unified ISSU System Requirements | 504

Unified ISSU System Requirements | 504

Performing a Unified ISSU | 532

Performing a Unified ISSU | 532

Best Practices for Performing a Unified ISSU | 532

Example: Performing a Unified ISSU | 533

Requirements | 533

Overview | 535

Configuration | 535

Verifying Dual Routing Engines and Enabling GRES and NSR | 536

Verifying the Software Versions and Backing Up the Device Software | 539

Adjusting Timers and Changing Feature-Specific Configuration | 540

Upgrading and Rebooting Both Routing Engines Automatically | 542

Restoring Feature-Specific Configuration | 550

Upgrading Both Routing Engines and Rebooting the New Backup Routing Engine Manually | 552

Upgrading and Rebooting Only One Routing Engine | 561

Performing an In-Service Software Upgrade (ISSU) with Non-Stop Routing | 572

Preparing the Switch for Software Installation | 572

Upgrading the Software Using ISSU | 573

Performing an In-Service Software Upgrade (ISSU) in ACX5000 Series Routers | 576

Preparing the Router for Software Installation | 577

Upgrading the Software Using ISSU | 578

Verifying a Unified ISSU | 581

How to Use Unified ISSU with Enhanced Mode | 581

Unified ISSU with Enhanced Mode Overview | 582

Benefits of Unified ISSU with Enhanced Mode | 582

Prerequisites for Performing Unified ISSU with Enhanced Mode | 582

Performing Unified ISSU with Enhanced Mode | 583

Verifying a Unified ISSU | 585

Troubleshooting Unified ISSU Problems | 587

Managing and Tracing BFD Sessions During Unified ISSU Procedures | 587

**Performing an ISSR | 589**

Performing an In-Service Software Reboot | 589

## **Performing Nonstop Software Upgrade (NSSU)**

**Getting Started with NSSU and Understanding How NSSU Works | 593**

Understanding Nonstop Software Upgrade on EX Series Switches | 593

**Performing a NSSU | 603**

Performing a NSSU | 603

Configuring Line-Card Upgrade Groups for Nonstop Software Upgrade | 603

How Line-card Upgrade Groups Work with Nonstop Software Upgrade | 604

Line-card Upgrade Groups Support | 604

Configure Line-Card Upgrade Groups on an EX4650 Virtual Chassis, a QFX Series Virtual Chassis or a QFX5100 VCF | 605

Configure Line-Card Upgrade Groups on Standalone EX6200 or EX8200 Switches | 605

Configure Line-Card Upgrade Groups on an EX8200 Virtual Chassis | 606

Example: Configuring Line-Card Upgrade Groups for Nonstop Software Upgrade on EX Series Switches | 608

Requirements | 608

Overview and Topology | 608

Configuration | 610

## **Multinode High Availability**

## Overview | 613

### Multinode High Availability | 613

- Overview | 613

- How Multinode High Availability Works | 627

- Multinode High Availability Monitoring | 645

### Prepare Your Environment for Multinode High Availability Deployment | 654

### Multinode High Availability Services | 658

### IPsec VPN Support in Multinode High Availability | 664

## Multinode High Availability Configuration | 672

### Example: Configure Multinode High Availability in a Layer 3 Network | 672

- Overview | 672

- Requirements | 673

- Topology | 673

- Configuration | 676

- Verification | 703

### Example: Configure Multinode High Availability in a Default Gateway Deployment | 717

- Overview | 717

- Requirements | 717

- Topology | 718

- Configuration | 720

- Verification | 740

### Example: Configure Multinode High Availability in a Hybrid Deployment | 752

- Overview | 752

- Requirements | 753

- Topology | 753

- Configuration | 756

- Verification | 782

### Example: Configure IPsec VPN in Active-Active Multinode High Availability in a Layer 3 Network | 795

- Overview | 795

- Requirements | 796

- Topology | 796

- Configuration | 801

Verification | 857

## Hardware and Software Upgrades | 885

Software Upgrade in Multinode High Availability | 885

Insert Additional SRX5K-SPC3 in a Multinode High Availability Setup | 904

Insert SRX5K-SPC3 in a Multinode High Availability Setup | 905

## Multinode High Availability Support for vSRX | 908

Multinode High Availability Support for vSRX Instances in Public Cloud Deployments | 908

Overview | 908

Multinode High Availability in AWS | 909

Example: Configure Multinode High Availability in AWS Deployment | 912

16

## Configuration Statements and Operational Commands

### Configuration Statements: Adaptive Load Balancing | 937

adaptive | 937

### Configuration Statements: Bidirectional Forwarding Detection | 940

dedicated-ukern-cpu (BFD) | 940

realtime-ukern-thread (BFD) | 941

authentication (LAG) | 943

bfd-liveness-detection (LAG) | 945

detection-time (LAG) | 948

traceoptions (Protocols BFD) | 949

transmit-interval (LAG) | 952

### Ethernet Automatic Protection Switching | 955

clear | 955

exercise | 956

force switch | 957

lockout | 958

manual switch | 959

### Configuration Statements: Ethernet Ring Protection Switching | 961

compatibility-version | 962

control-channel | 963

data-channel | 965

dot1p-priority | 966

east-interface | 968

ethernet-ring | 970

guard-interval | 972

hold-interval (Protection Group) | 973

major-ring-name | 975

non-revertive | 976

non-vc-mode | 977

node-id | 978

propagate-tc | 979

protection-group | 981

restore-interval | 984

ring-id | 985

ring-protection-link-end | 987

ring-protection-link-owner | 988

wait-to-block-interval | 989

west-interface | 990

## **Configuration Statements: Graceful Routing Engine Switchover | 993**

graceful-switchover | 993

graceful-switchover | 994

redundancy (Graceful Switchover) | 996

## **Configuration Statements: Graceful Restart | 998**

disable | 999



disable (BGP Graceful Restart) | 1000

dont-help-shared-fate-bfd-down | 1002

graceful-restart (Enabling Globally) | 1003

graceful-restart (Multicast Snooping) | 1006

graceful-restart (Protocols BGP) | 1007

graceful-restart (Protocols OSPF) | 1009

helper-disable (Multiple Protocols) | 1012

kernel-replication | 1013

maximum-helper-recovery-time | 1015

maximum-helper-restart-time (RSVP) | 1016

maximum-neighbor-reconnect-time | 1018

maximum-neighbor-recovery-time | 1019

not-on-disk-underperform | 1021

reconnect-time | 1022

recovery-time | 1023

restart-duration | 1025

restart-time (BGP Graceful Restart) | 1027

stale-routes-time | 1029

traceoptions (Protocols) | 1030

warm-standby | 1033

## **Configuration Statements: Multinode High Availability | 1035**

activeness-probe | 1035

hardware-upgrade | 1037

high-availability (Chassis) | 1039

high-availability (security cloud) | 1042

liveness-detection (high availability) | 1043

local-id | 1046

managed-services | 1048

peer-id | 1049

monitor (Multinode High Availability) | 1051

services-redundancy-group | 1053

software-upgrade | 1058

traceoptions | 1059

virtual-ip | 1062

### **Configuration Statements: Nonstop Active Routing | 1064**

nonstop-routing | 1064

switchover-on-routing-crash | 1066

synchronize | 1067

traceoptions | 1069

### **Configuration Statements: Nonstop Bridging | 1074**

nonstop-bridging | 1074

nonstop-bridging (Ethernet Switching) | 1075

### **Configuration Statements: NSSU | 1077**

fpcs (NSSU Upgrade Groups) | 1077

member (NSSU Upgrade Groups) | 1079

nssu | 1081

upgrade-group | 1083

### **Configuration Statements: Power Management | 1085**

power-budget-priority | 1085

n-plus-n (Power Management) | 1087

psu | 1088

redundancy (Power Management) | 1089

**Configuration Statements: Redundant Power System | 1091**

member (Redundant Power System) | 1091

priority (Redundant Power System) | 1093

redundant-power-system | 1094

**Configuration Statements: Routing Engine and Switching Control Board Redundancy | 1096**

cfeb | 1097

description (Chassis Redundancy) | 1098

disk-failure-action | 1099

failover (Chassis) | 1101

failover (Chassis) | 1103

failover (System Process) | 1104

feb (Creating a Redundancy Group) | 1105

feb (Assigning a FEB to a Redundancy Group) | 1107

keepalive-time | 1108

keepalive-time | 1110

no-auto-failover | 1112

on-disk-failure (Chassis Redundancy Failover) | 1113

on-disk-failure | 1114

on-loss-of-keepalives | 1116

on-loss-of-keepalives | 1117

redundancy | 1119

redundancy-group | 1121

routing-engine (Chassis Redundancy) | 1122

sfm (Chassis Redundancy) | 1124

ssb | 1125

vcp-no-hold-time | 1127

**Configuration Statements: Unified ISSU | 1129**

no-issu-timer-negotiation | 1129

traceoptions (Protocols BFD) | 1130

**Configuration Statements: VRRP | 1134**

accept-data | 1135

advertise-interval | 1137

asymmetric-hold-time | 1139

asymmetric-hold-time | 1140

authentication-key | 1141

authentication-type | 1143

bandwidth-threshold | 1145

delegate-processing (VRRP) | 1147

failover-delay | 1148

failover-delay | 1150

fast-interval | 1151

global-advertisements-threshold | 1153

hold-time (VRRP) | 1155

hold-time | 1157

inherit-advertisement-interval | 1158

inet6-advertise-interval | 1159

inet6-advertise-interval | 1161

interface | 1162

preempt (VRRP) | 1164

preempt | 1165

priority (Protocols VRRP) | 1167

priority | 1169

priority-cost (VRRP) | 1170

priority-hold-time | 1172

route (Interfaces) | 1174

skew-timer-disable | 1175

startup-silent-period | 1177

traceoptions (Protocols VRRP) | 1178

traceoptions | 1181

track (VRRP) | 1184

version-3 | 1186

virtual-address | 1187

virtual-inet6-address | 1189

virtual-link-local-address | 1190

vrrp-group | 1192

vrrp-inet6-group | 1194

vrrp-inherit-from | 1196

## **Administration | 1198**

Upgrading Software on an EX6200 or EX8200 Standalone Switch Using Nonstop Software Upgrade (CLI Procedure) | 1198

Preparing the Switch for Software Installation | 1199

Upgrading Both Routing Engines Using NSSU | 1200

Upgrading One Routing Engine Using NSSU (EX8200 Switch Only) | 1204

Upgrading the Original Primary Routing Engine (EX8200 Switch Only) | 1207

Upgrading Software on an EX8200 Virtual Chassis Using Nonstop Software Upgrade (CLI Procedure) | 1209

Preparing the Switch for Software Installation | 1210

Upgrading the Software Using NSSU | 1211

Upgrading Software Using Nonstop Software Upgrade on EX Series Virtual Chassis and Mixed Virtual Chassis (CLI Procedure) | 1215

Preparing the Switch for Software Installation | 1215

Upgrading the Software Using NSSU | 1217

## Verification Tasks | 1220

Verifying Power Configuration and Use | 1220

## Operational Commands | 1224

clear chassis high-availability data-plane statistics | 1226

clear chassis high-availability information | 1227

clear security pki node-local certificate-request | 1229

clear security pki node-local local-certificate | 1230

clear security pki node-local key-pair | 1232

clear vrrp | 1233

request chassis high-availability failover services-redundancy-group | 1235

request chassis redundancy feb slot | 1236

request chassis routing-engine master | 1238

request chassis sfm master switch | 1246

request chassis ssb master switch | 1248

request redundant-power-system multi-backup | 1250

request security pki node-local local-certificate verify | 1252

request security pki node-local local-certificate re-enroll | 1254

request security pki node-local local-certificate load | 1255

request security pki node-local local-certificate export | 1257

request security pki node-local local-certificate enroll | 1259

request security pki node-local key-pair export | 1262

request security pki node-local generate-key-pair | 1264

request security pki sync-from-peer | 1266

request security pki node-local generate-certificate-request | 1267

request system software in-service-upgrade | 1270

request system software in-service-upgrade (MX Series 5G Universal Routing Platforms and EX9200 Switches) | **1291**

request system software nonstop-upgrade | **1314**

request system software validate in-service-upgrade | **1327**

show bgp neighbor | **1332**

show log | **1372**

show (ospf | ospf3) overview | **1379**

show chassis dedicated-ukern-cpu | **1388**

show chassis in-service-upgrade | **1389**

show chassis realtime-ukern-thread | **1395**

show chassis redundancy feb | **1396**

show chassis high-availability data-plane statistics | **1401**

show chassis high-availability information | **1406**

show chassis high-availability peer-info | **1415**

show chassis high-availability prefix-srgid-table | **1417**

show chassis high-availability services-redundancy-group | **1419**

show chassis nonstop-upgrade | **1426**

show chassis nonstop-upgrade node-group | **1429**

show chassis power-budget-statistics | **1431**

show chassis redundant-power-system | **1436**

show protection-group ethernet-ring aps | **1439**

show protection-group ethernet-ring configuration | **1445**

show protection-group ethernet-ring data-channel | **1453**

show protection-group ethernet-ring flush-info | **1457**

show protection-group ethernet-ring interface | **1459**

show protection-group ethernet-ring node-state | **1465**

show protection-group ethernet-ring statistics | **1472**

show protection-group ethernet-ring vlan | **1479**

show redundant-power-system led | **1486**

show redundant-power-system multi-backup | **1489**

show redundant-power-system network | **1490**

show redundant-power-system power-supply | **1492**

show redundant-power-system status | **1494**

show redundant-power-system upgrade | **1497**

show redundant-power-system version | **1499**

show security pki node-local local-certificate | **1501**

show security pki node-local certificate-request | **1507**

show chassis ssb | **1510**

show nonstop-routing | **1513**

show pfe ssb | **1517**

show system switchover | **1526**

show task replication | **1535**

show vrrp | **1538**

show vrrp track | **1555**

## **Troubleshooting | 1562**

Tracing Nonstop Active Routing Synchronization Events | **1562**

Troubleshooting the EX Series Redundant Power System Power On and Power Backup Issues | **1564**

The EX Series RPS Is Not Powering On | **1565**

A Switch Is Not Recognized by the RPS | **1566**

An Error Message Indicates That an RPS Power Supply is Not Supported | **1566**

The EX Series Redundant Power System Is Not Providing Power Backup to a Connected Switch | **1567**

The Wrong Switches Are Being Backed Up | **1568**

Six Switches That Do Not Require PoE Are Not All Being Backed Up | **1569**





# About This Guide

Use this guide to configure high availability features like ISSU, GRES, and BFD on a Junos OS device.

# 1

PART

## Overview

---

[High Availability Overview](#) | 2

---

## CHAPTER 1

# High Availability Overview

**IN THIS CHAPTER**

- Understanding High Availability Features on Juniper Networks Routers | 2
- High Availability-Related Features in Junos OS | 8
- High Availability Features for EX Series Switches Overview | 9

## Understanding High Availability Features on Juniper Networks Routers

**IN THIS SECTION**

- Routing Engine Redundancy | 3
- Graceful Routing Engine Switchover | 3
- Nonstop Bridging | 3
- Nonstop Active Routing | 4
- Graceful Restart | 4
- Nonstop Active Routing Versus Graceful Restart | 6
- Effects of a Routing Engine Switchover | 6
- VRRP | 6
- Unified ISSU | 7
- Interchassis Redundancy for MX Series Routers Using Virtual Chassis | 7

For Juniper Networks routing platforms running the Junos operating system (Junos OS), *high availability* refers to the hardware and software components that provide redundancy and reliability for packet-based communications. This topic provides brief overviews of the following high availability features:

## Routing Engine Redundancy

Redundant Routing Engines are two Routing Engines that are installed in the same routing platform. One functions as the primary, while the other stands by as a backup should the primary Routing Engine fail. On routing platforms with dual Routing Engines, network reconvergence takes place more quickly than on routing platforms with a single Routing Engine.

## Graceful Routing Engine Switchover

*Graceful Routing Engine switchover* (GRES) enables a routing platform with redundant Routing Engines to continue forwarding packets, even if one Routing Engine fails. Graceful Routing Engine switchover preserves interface and kernel information. Traffic is not interrupted. However, graceful Routing Engine switchover does not preserve the control plane. Neighboring routers detect that the router has experienced a restart and react to the event in a manner prescribed by individual routing protocol specifications.

**NOTE:** To preserve routing during a switchover, graceful Routing Engine switchover must be combined with either graceful restart protocol extensions or *nonstop active routing*. For more information, see *Understanding Graceful Routing Engine Switchover and Nonstop Active Routing Concepts*.

**NOTE:** In T Series routers, TX Matrix routers, and TX Matrix Plus routers, the control plane is preserved in case of GRES with NSR, and 75% of line rate worth of traffic per Packet Forwarding Engine remains uninterrupted during GRES.

## Nonstop Bridging

Nonstop bridging enables an MX Series 5G Universal Routing Platform with redundant Routing Engines to switch from a primary Routing Engine to a backup Routing Engine without losing Layer 2 Control Protocol (L2CP) information. Nonstop bridging uses the same infrastructure as graceful Routing Engine switchover to preserve interface and kernel information. However, nonstop bridging also saves L2CP information by running the Layer 2 Control Protocol process (l2cpd) on the backup Routing Engine.

**NOTE:** To use nonstop bridging, you must first enable graceful Routing Engine switchover.

Nonstop bridging is supported for the following Layer 2 control protocols:

- Spanning Tree Protocol (STP)

- Rapid Spanning Tree Protocol (RSTP)
- Multiple Spanning Tree Protocol (MSTP)
- VLAN Spanning Tree Protocol (VSTP)

For more information, see [Nonstop Bridging Concepts](#).

## Nonstop Active Routing

Nonstop active routing (NSR) enables a routing platform with redundant Routing Engines to switch from a primary Routing Engine to a backup Routing Engine without alerting peer nodes that a change has occurred. Nonstop active routing uses the same infrastructure as graceful Routing Engine switchover to preserve interface and kernel information. However, nonstop active routing also preserves routing information and protocol sessions by running the routing protocol process (rpd) on both Routing Engines. In addition, nonstop active routing preserves TCP connections maintained in the kernel.

**NOTE:** To use nonstop active routing, you must also configure graceful Routing Engine switchover.

For a list of protocols and features supported by nonstop active routing, see [Nonstop Active Routing Protocol and Feature Support](#).

For more information about nonstop active routing, see [Nonstop Active Routing Concepts](#).

## Graceful Restart

With routing protocols, any service interruption requires an affected router to recalculate adjacencies with neighboring routers, restore routing table entries, and update other protocol-specific information. An unprotected restart of a router can result in forwarding delays, route flapping, wait times stemming from protocol reconvergence, and even dropped packets. To alleviate this situation, graceful restart provides extensions to routing protocols. These protocol extensions define two roles for a router—*restarting* and *helper*. The extensions signal neighboring routers about a router undergoing a restart and prevent the neighbors from propagating the change in state to the network during a graceful restart wait interval. The main benefits of graceful restart are uninterrupted packet forwarding and temporary suppression of all routing protocol updates. Graceful restart enables a router to pass through intermediate convergence states that are hidden from the rest of the network.

When a router is running graceful restart and the router stops sending and replying to protocol liveness messages (hellos), the adjacencies assume a graceful restart and begin running a timer to monitor the restarting router. During this interval, helper routers do not process an adjacency change for the router that they assume is restarting, but continue active routing with the rest of the network. The helper

routers assume that the router can continue stateful forwarding based on the last preserved routing state during the restart.

If the router was actually restarting and is back up before the graceful timer period expires in all of the helper routers, the helper routers provide the router with the routing table, topology table, or label table (depending on the protocol), exit the graceful period, and return to normal network routing.

If the router does not complete its negotiation with helper routers before the graceful timer period expires in all of the helper routers, the helper routers process the router's change in state and send routing updates, so that convergence occurs across the network. If a helper router detects a link failure from the router, the topology change causes the helper router to exit the graceful wait period and to send routing updates, so that network convergence occurs.

To enable a router to undergo a graceful restart, you must include the `graceful-restart` statement at the global `[edit routing-options]` or `[edit routing-instances instance-name routing-options]` hierarchy level. You can, optionally, modify the global settings at the individual protocol level. When a routing session is started, a router that is configured with graceful restart must negotiate with its neighbors to support it when it undergoes a graceful restart. A neighboring router will accept the negotiation and support helper mode without requiring graceful restart to be configured on the neighboring router.

**NOTE:** A Routing Engine switchover event on a helper router that is in graceful wait state causes the router to drop the wait state and to propagate the adjacency's state change to the network.

Graceful restart is supported for the following protocols and applications:

- BGP
- ES-IS
- IS-IS
- OSPF/OSPFv3
- PIM sparse mode
- RIP/RIPng
- MPLS-related protocols, including:
  - Label Distribution Protocol (LDP)
  - Resource Reservation Protocol (RSVP)
  - Circuit cross-connect (CCC)
  - Translational cross-connect (TCC)

- Layer 2 and Layer 3 virtual private networks (VPNs)

For more information, see Graceful Restart Concepts.

## Nonstop Active Routing Versus Graceful Restart

Nonstop active routing and graceful restart are two different methods of maintaining high availability. Graceful restart requires a router restart. A router undergoing a graceful restart relies on its neighbors (or helpers) to restore its routing protocol information. The restart is the mechanism by which helpers are signaled to exit the wait interval and start providing routing information to the restarting router. For more information, see Graceful Restart Concepts.

In contrast, nonstop active routing does not involve a router restart. Both the primary and backup Routing Engines are running the routing protocol process (rpd) and exchanging updates with neighbors. When one Routing Engine fails, the router simply switches to the active Routing Engine to exchange routing information with neighbors. Because of these feature differences, nonstop routing and graceful restart are mutually exclusive. Nonstop active routing cannot be enabled when the router is configured as a graceful restarting router. If you include the graceful-restart statement at any hierarchy level and the nonstop-routing statement at the [edit routing-options] hierarchy level and try to commit the configuration, the commit request fails. For more information, see Nonstop Active Routing Concepts.

## Effects of a Routing Engine Switchover

Effects of a Routing Engine Switchover describes the effects of a Routing Engine switchover when no high availability features are enabled and when graceful Routing Engine switchover, graceful restart, and nonstop active routing features are enabled.

## VRRP

The Virtual Router Redundancy Protocol (VRRP) enables hosts on a LAN to make use of redundant routing platforms (primary and backup pairs) on the LAN, requiring only the static configuration of a single default route on the hosts.

The VRRP routing platform pairs share the IP address corresponding to the default route configured on the hosts. At any time, one of the VRRP routing platforms is the primary (active) and the others are backups. If the primary fails, one of the backup routers or switches becomes the new primary router.

VRRP has advantages in ease of administration and network throughput and reliability:

- It provides a virtual default routing platform.
- It enables traffic on the LAN to be routed without a single point of failure.
- A virtual backup router can take over a failed default router:



- Within a few seconds.
- With a minimum of VRRP traffic.
- Without any interaction with the hosts.

Devices running VRRP dynamically elect primary and backup routers. You can also force assignment of primary and backup routers using priorities from 1 through 255, with 255 being the highest priority.

In VRRP operation, the default primary router sends advertisements to backup routers at regular intervals (default 1 second). If a backup router does not receive an advertisement for a set period, the backup router with the next highest priority takes over as primary and begins forwarding packets.

As of Junos OS Release 13.2, VRRP nonstop active routing (NSR) is enabled only when you configure the nonstop-routing statement at the [edit routing-options] or [edit logical system *logical-system-name* routing-options] hierarchy level.

For more information, see Understanding VRRP.

## Unified ISSU

A unified in-service software upgrade (unified ISSU) enables you to upgrade between two different Junos OS Releases with no disruption on the control plane and with minimal disruption of traffic. Unified ISSU is only supported by dual Routing Engine platforms. In addition, graceful Routing Engine switchover (GRES) and nonstop active routing (NSR) must be enabled.

With a unified ISSU, you can eliminate network downtime, reduce operating costs, and deliver higher services levels. For more information, see Getting Started with Unified In-Service Software Upgrade.

## Interchassis Redundancy for MX Series Routers Using Virtual Chassis

*Interchassis redundancy* is a high availability feature that can span equipment located across multiple geographies to prevent network outages and protect routers against access link failures, uplink failures, and wholesale chassis failures without visibly disrupting the attached subscribers or increasing the network management burden for service providers. As more high-priority voice and video traffic is carried on the network, interchassis redundancy has become a requirement for providing stateful redundancy on broadband subscriber management equipment such as broadband services routers, broadband network gateways, and broadband remote access servers. Interchassis redundancy support enables service providers to fulfill strict service-level agreements (SLAs) and avoid unplanned network outages to better meet the needs of their customers.

To provide a stateful interchassis redundancy solution for MX Series 5G Universal Routing Platforms, you can configure a *Virtual Chassis*. A *Virtual Chassis* configuration interconnects two MX Series routers into a logical system that you can manage as a single network element. The member routers in a Virtual Chassis are designated as the *primary router* (also known as the *protocol primary*) and the *backup router*

(also known as the *protocol backup*). The member routers are interconnected by means of dedicated *Virtual Chassis ports* that you configure on Trio Modular Port Concentrator/Modular Interface Card (MPC/MIC) interfaces.

An MX Series Virtual Chassis is managed by the *Virtual Chassis Control Protocol (VCCP)*, which is a dedicated control protocol based on IS-IS. VCCP runs on the Virtual Chassis port interfaces and is responsible for building the Virtual Chassis topology, electing the Virtual Chassis primary router, and establishing the interchassis routing table to route traffic within the Virtual Chassis.

Starting with Junos OS Release 11.2, Virtual Chassis configurations are supported on MX240, MX480, and MX960 Universal Routing Platforms with Trio MPC/MIC interfaces and dual Routing Engines. In addition, graceful Routing Engine switchover (GRES) and nonstop active routing (NSR) must be enabled on both member routers in the Virtual Chassis.

## RELATED DOCUMENTATION

[High Availability-Related Features in Junos OS](#) | 8

## High Availability-Related Features in Junos OS

Related redundancy and reliability features include:

- Redundant power supplies, host modules, host subsystems, and forwarding boards. For more information, see the [Junos OS Administration Library for Routing Devices](#) and the *Junos OS Hardware Network Operations Guide*.
- Additional link-layer redundancy, including Automatic Protection Switching (APS) for SONET interfaces, Multiplex Section Protection (MSP) for SDH interfaces, and DLSw redundancy for Ethernet interfaces. For more information, see the [Junos OS Network Interfaces Library for Routing Devices](#).
- Bidirectional Forwarding Detection (BFD) works with other routing protocols to detect failures rapidly. For more information, see the [Junos OS Routing Protocols Library for Routing Devices](#).
- Redirection of Multiprotocol Label Switching (MPLS) label-switched path (LSP) traffic—Mechanisms such as link protection, node-link protection, and fast reroute recognize link and node failures, allowing MPLS LSPs to select a bypass LSP to circumvent failed links or devices. For more information, see the [MPLS Applications User Guide](#).

## RELATED DOCUMENTATION

[Understanding High Availability Features on Juniper Networks Routers](#) | 2

# High Availability Features for EX Series Switches Overview

## IN THIS SECTION

- [VRRP](#) | 9
- [Graceful Protocol Restart](#) | 10
- [Redundant Routing Engines](#) | 10
- [Virtual Chassis](#) | 11
- [Graceful Routing Engine Switchover](#) | 11
- [Link Aggregation](#) | 12
- [Nonstop Active Routing and Nonstop Bridging](#) | 12
- [Nonstop Software Upgrade](#) | 12
- [Redundant Power System](#) | 13

*High availability* refers to the hardware and software components that provide redundancy and reliability for network communications. This topic covers the following high availability features of Juniper Networks EX Series Ethernet Switches:

## VRRP

You can configure Virtual Router Redundancy Protocol (VRRP) for IP and IPv6 on most switch interfaces, including Gigabit Ethernet interfaces, high-speed Gigabit Ethernet uplink interfaces, and logical interfaces. When VRRP is configured, the switches act as virtual routing platforms. VRRP enables hosts on a LAN to make use of redundant routing platforms on that LAN without requiring more than the static configuration of a single default route on the hosts. The VRRP routing platforms share the IP address corresponding to the default route configured on the hosts. At any time, one of the VRRP routing platforms is the primary (active) and the others are backups. If the primary routing platform fails, one of the backup routing platforms becomes the new primary, providing a virtual default routing platform and enabling traffic on the LAN to be routed without relying on a single routing platform. Using VRRP, a backup switch can take over a failed default switch within a few seconds. This is done with minimum loss of VRRP traffic and without any interaction with the hosts.

## Graceful Protocol Restart

With standard implementations of routing protocols, any service interruption requires an affected switch to recalculate adjacencies with neighboring switches, restore routing table entries, and update other protocol-specific information. An unprotected restart of a switch can result in forwarding delays, route flapping, wait times stemming from protocol reconvergence, and even dropped packets. Graceful protocol restart enables a restarting switch and its neighbors to continue forwarding packets without disrupting network performance. Because neighboring switches assist in the restart (these neighbors are called helper switches), the restarting switch can quickly resume full operation without recalculating algorithms from scratch.

On the switches, graceful protocol restart can be applied to aggregate and static routes and for routing protocols (BGP, IS-IS, OSPF, and RIP).

Graceful protocol restart works similarly for the different routing protocols. The main benefits of graceful protocol restart are uninterrupted packet forwarding and temporary suppression of all routing protocol updates. Graceful protocol restart thus allows a switch to pass through intermediate convergence states that are hidden from the rest of the network. Most graceful restart implementations define two types of switches—the restarting switch and the helper switch. The restarting switch requires rapid restoration of forwarding state information so that it can resume the forwarding of network traffic. The helper switch assists the restarting switch in this process. Individual graceful restart configuration statements typically apply to either the restarting switch or the helper switch.

## Redundant Routing Engines

Redundant Routing Engines are two Routing Engines that are installed in a switch or a *Virtual Chassis*. When a switch has two Routing Engines, one functions as the primary, while the other stands by as a backup in case the primary Routing Engine fails. When a Virtual Chassis has two Routing Engines, the switch in the primary role functions as the primary Routing Engine and the switch in the backup role functions as the backup Routing Engine. Redundant Routing Engines are supported on Juniper Networks EX6200 Ethernet Switches, Juniper Networks EX8200 Ethernet Switches, and on all EX Series Virtual Chassis configurations.

The primary Routing Engine receives and transmits routing information, builds and maintains routing tables, communicates with interfaces and Packet Forwarding Engine components of the switch, and has full control over the control plane of the switch.

The backup Routing Engine stays in sync with the primary Routing Engine in terms of protocol states, forwarding tables, and so forth. If the primary becomes unavailable, the backup Routing Engine takes over the functions that the primary Routing Engine performs.

Network reconvergence takes place more quickly on switches and on Virtual Chassis with redundant Routing Engines than on switches and on Virtual Chassis with a single Routing Engine.

## Virtual Chassis

A Virtual Chassis is multiple switches connected together that operate as a single network entity. The advantages of connecting multiple switches into a Virtual Chassis include better-managed bandwidth at a network layer, simplified configuration and maintenance because multiple devices can be managed as a single device, a simplified Layer 2 network topology that minimizes or eliminates the need for loop prevention protocols such as Spanning Tree Protocol (STP), and improved fault tolerance and high availability. A Virtual Chassis improves high availability for the following reasons:

- **Dual Routing Engine support.** A Virtual Chassis automatically has two Routing Engines—the switches in the primary and backup routing-engine roles—and, therefore, provides more high availability options than standalone switches. Many high availability features, including graceful protocol restart, graceful Routing Engine switchover (GRES), nonstop software upgrade (NSSU), nonstop active routing (NSR), and nonstop bridging (NSB), are available for an EX Series Virtual Chassis that are not available on standalone EX Series switches.
- **Increased fault tolerance.** You increase your fault tolerance options when you configure your EX Series switches into a Virtual Chassis. You can, for instance, configure interfaces into a link aggregation group (LAG) with member interfaces on different member switches in the same Virtual Chassis to ensure network traffic is received by a Virtual Chassis even when a switch or physical interface in the Virtual Chassis fails.

Juniper Networks EX2200 Ethernet Switches, Juniper Networks EX3300 Ethernet Switches, Juniper Networks EX4200 Ethernet Switches, Juniper Networks EX4300 Ethernet Switches, Juniper Networks EX4500 Ethernet Switches, Juniper Networks EX4550 Ethernet Switches, or Juniper Networks EX8200 Ethernet Switches can form a Virtual Chassis. EX4200, EX4500, and EX4550 switches can be interconnected together to form a mixed Virtual Chassis.

## Graceful Routing Engine Switchover

You can configure *graceful Routing Engine switchover* (GRES) on a switch with redundant Routing Engines or on a Virtual Chassis, allowing control to switch from the primary Routing Engine to the backup Routing Engine with minimal interruption to network communications. When you configure GRES, the backup Routing Engine automatically synchronizes with the primary Routing Engine to preserve kernel state information and forwarding state. Any updates to the primary Routing Engine are replicated to the backup Routing Engine as soon as they occur. If the kernel on the primary Routing Engine stops operating, the primary Routing Engine experiences a hardware failure, or the administrator initiates a manual switchover, primary role switches to the backup Routing Engine.

When the backup Routing Engine assumes primary role in a redundant failover configuration (that is, when GRES is not enabled), the Packet Forwarding Engines initialize their state to the boot state before they connect to the new primary Routing Engine. In contrast, in a GRES configuration, the Packet Forwarding Engines do not reinitialize their state, but resynchronize their state to that of the new primary Routing Engine. The interruption to traffic is minimal.

## Link Aggregation

You can combine multiple physical Ethernet ports to form a logical point-to-point link, known as a link aggregation group (LAG) or bundle. A LAG provides more bandwidth than a single Ethernet link can provide. Additionally, link aggregation provides network redundancy by load-balancing traffic across all available links. If one of the links should fail, the system automatically load-balances traffic across all remaining links. In a Virtual Chassis, LAGs can be used to load-balance network traffic between member switches, which increases high availability by ensuring that network traffic is received by the Virtual Chassis even if a single interface fails for any reason.

The number of Ethernet interfaces you can include in a LAG and the number of LAGs you can configure on a switch depend on the switch model.

## Nonstop Active Routing and Nonstop Bridging

*Nonstop active routing* (NSR) provides high availability in a switch with redundant Routing Engines by enabling transparent switchover of the Routing Engines without requiring restart of supported Layer 3 routing protocols. Both Routing Engines are fully active in processing protocol sessions, and so each can take over for the other. The switchover is transparent to neighbor routing devices, which do not detect that a change has occurred.

Nonstop bridging (NSB) provides the same mechanism for Layer 2 protocols. NSB provides high availability in a switch with redundant Routing Engines by enabling transparent switchover of the Routing Engines without requiring restart of supported Layer 2 protocols. Both Routing Engines are fully active in processing protocol sessions, and so each can take over for the other. The switchover is transparent to neighbor switching devices, which do not detect that a change has occurred.

To use NSR or NSB, you must also configure GRES.

## Nonstop Software Upgrade

Nonstop software upgrade (NSSU) allows you to upgrade the software on a switch with dual Routing Engines or on a Virtual Chassis in an automated manner with minimal traffic disruption. NSSU takes advantage of GRES and NSR to enable upgrading the Junos OS version with no disruption to the control plane. In addition, NSSU minimizes traffic disruption by:

- Upgrading line cards one at a time in an EX6200 switch, EX8200 switch, or EX8200 Virtual Chassis, permitting traffic to continue to flow through the line cards that are not being upgraded.
- Upgrading member switches one at a time in all other Virtual Chassis, permitting traffic to continue to flow through the members that are not being upgraded.

By configuring LAGs such that the member links reside on different line cards or Virtual Chassis members, you can achieve minimal traffic disruption when performing an NSSU.

## Redundant Power System

Most Juniper Networks Ethernet Switches have a built-in capability for redundant power supplies—therefore if one power supply fails on those switches, the other power supply takes over. However, EX2200 switches and EX3300 switches have only one internal fixed power supply. If an EX2200 switch or EX3300 switch is deployed in a critical situation, we recommend that you connect a Redundant Power System (RPS) to that switch to supply backup power if the internal power supply fails. RPS is not a primary power supply—it only provides backup power to switches when the single dedicated power supply fails. An RPS operates in parallel with the single dedicated power supplies of the switches connected to it and provides all connected switches enough power to support either Power over Ethernet (PoE) or non-PoE devices. For more information about RPS, see EX Series Redundant Power System Hardware Overview.

### RELATED DOCUMENTATION

---

[Junos OS High Availability Configuration Guide](#)

---

[\*Understanding EX Series Virtual Chassis\*](#)

---

[\*EX8200 Virtual Chassis Overview\*](#)

---

[Understanding Nonstop Active Routing on EX Series Switches](#)

---

[Understanding Nonstop Software Upgrade on EX Series Switches | 593](#)

---

[EX Series Redundant Power System Hardware Guide](#)

# 2

PART

## Configuring Switching Control Board Redundancy

---

Understanding How Switching Control Board Redundancy Prevents Network Failures | 15

Configuring Switching Control Board Redundancy | 20

---



# Understanding How Switching Control Board Redundancy Prevents Network Failures

## IN THIS CHAPTER

- [Understanding Switching Control Board Redundancy | 15](#)

## Understanding Switching Control Board Redundancy

### SUMMARY

Switching control board redundancy allows your device to continue routing and switching functions if a primary control board fails.

### IN THIS SECTION

- [Redundant CFEBs on the M10i Router | 15](#)
- [Redundant FEBs on the M120 Router | 16](#)
- [Redundant SSBs on the M20 Router | 18](#)
- [Redundant SFMs on the M40e and M160 Routers | 19](#)

**NOTE:** In this section, the term *failover* refers to an automatic event, whereas *switchover* refers to either an automatic or a manual event.

### Redundant CFEBs on the M10i Router

On the M10i router, the CFEB performs the following functions:

- Route lookups—Performs route lookups using the forwarding table stored in synchronous SRAM (SSRAM).

- Management of shared memory—Uniformly allocates incoming data packets throughout the router's shared memory.
- Transfer of outgoing data packets—Passes data packets to the destination Fixed Interface Card (FIC) or *Physical Interface Card* (PIC) when the data is ready to be transmitted.
- Transfer of exception and control packets—Passes exception packets to the microprocessor on the CFEB, which processes almost all of them. The remainder are sent to the Routing Engine for further processing. Any errors originating in the Packet Forwarding Engine and detected by the CFEB are sent to the Routing Engine using system log messages.

The M10i router has two CFEBs, one that is configured to act as the primary and the other that serves as a backup in case the primary fails. You can initiate a manual switchover by issuing the request `chassis cfeb master switch` command. For more information, see the [Junos OS Administration Library for Routing Devices](#).

## Redundant FEBs on the M120 Router

The M120 router supports up to six Forwarding Engine Boards (FEBs). Flexible PIC Concentrator (FPCs), which host PICs, are separate from the FEBs, which handle packet forwarding. FPCs are located on the front of the chassis and provide power and management to PICs through the midplane. FEBs are located on the back of the chassis and receive signals from the midplane, which the FEBs process for packet forwarding. The midplane allows any FEB to carry traffic for any FPC.

To configure the mapping of FPCs to FEBs, use the `fpc-feb-connectivity` statement as described in the [Junos OS Administration Library for Routing Devices](#). You cannot specify a connection between an FPC and a FEB configured as a backup. If an FPC is not specified to connect to a FEB, the FPC is assigned automatically to the FEB with the same slot number. For example, the FPC in slot 1 is assigned to the FEB in slot 1.

You can configure one FEB as a backup for one or more FEBs by configuring a FEB redundancy group. When a FEB fails, the backup FEB can quickly take over packet forwarding. A redundancy group must contain exactly one backup FEB and can optionally contain one primary FEB and multiple other FEBs. A FEB can belong to only one group. A group can provide backup on a one-to-one basis (primary-to-backup), a many-to-one basis (two or more other-FEBs-to-backup), or a combination of both (one primary-to-backup and one or more other-FEBs-to-backup).

When you configure a primary FEB in a redundancy group, the backup FEB mirrors the exact forwarding state of the primary FEB. If switchover occurs from a primary FEB, the backup FEB does not reboot. A manual switchover from the primary FEB to the backup FEB results in less than 1 second of traffic loss. Failover from the primary FEB to the backup FEB results in less than 10 seconds of traffic loss.

If a failover occurs from the other FEB and a primary FEB is specified for the group, the backup FEB reboots so that the forwarding state from the other FEB can be downloaded to the backup FEB and forwarding can continue. Automatic failover from a FEB that is not specified as a primary FEB results in

higher packet loss. The duration of packet loss depends on the number of interfaces and on the size of the routing table, but it can be minutes.

If a failover from a FEB occurs when no primary FEB is specified in the redundancy group, the backup FEB does not reboot and the interfaces on the FPC connected to the previously active FEB remain online. The backup FEB must obtain the entire forwarding state from the Routing Engine after a switchover, and this update may take a few minutes. If you do not want the interfaces to remain online during the switchover for the other FEB, configure a primary FEB for the redundancy group.

Failover to a backup FEB occurs automatically if a FEB in a redundancy group fails. You can disable automatic failover for any redundancy group by including the `no-auto-failover` statement at the `[edit chassis redundancy feb redundancy-group group-name]` hierarchy level.

You can also initiate a manual switchover by issuing the `request chassis redundancy feb slot slot-number switch-to-backup` command, where *slot-number* is the number of the active FEB. For more information, see the [CLI Explorer](#).

The following conditions result in failover as long as the backup FEB in a redundancy group is available:

- The FEB is absent.
- The FEB experienced a hard error while coming online.
- A software failure on the FEB resulted in a crash.
- Ethernet connectivity from a FEB to a Routing Engine failed.
- A hard error on the FEB, such as a power failure, occurred.
- The FEB was disabled when the offline button for the FEB was pressed.
- The software watchdog timer on the FEB expired.
- Errors occurred on the links between all the active fabric planes and the FEB. This situation results in failover to the backup FEB if it has at least one valid fabric link.
- Errors occurred on the link between the FEB and all of the FPCs connected to it.

After a switchover occurs, a backup FEB is no longer available for the redundancy group. You can revert from the backup FEB to the previously active FEB by issuing the *operational mode command* **`request chassis redundancy feb slot slot-number revert-from-backup`**, where *slot-number* is the number of the previously active FEB. For more information, see the [CLI Explorer](#).

When you revert from the backup FEB, it becomes available again for a switchover. If the redundancy group does not have a primary FEB, the backup FEB reboots after you revert back to the previously active FEB. If the FEB to which you revert back is not a primary FEB, the backup FEB is rebooted so that it can align with the state of the primary FEB.

If you modify the configuration for an existing redundancy group so that a FEB connects to a different FPC, the FEB is rebooted unless the FEB was already connected to one or two Type 1 FPCs and the change only resulted in the FEB being connected either to one additional or one fewer Type 1 FPC. For more information about how to map a connection between an FPC and a FEB, see the [Junos OS Administration Library for Routing Devices](#). If you change the primary FEB in a redundancy group, the backup FEB is rebooted. The FEB is also rebooted if you change a backup FEB to a nonbackup FEB or change an active FEB to a backup FEB.

To view the status of configured FEB redundancy groups, issue the `show chassis redundancy feb operational` command. For more information, see the [CLI Explorer](#).

## Redundant SSBs on the M20 Router

The System and Switch Board (SSB) on the M20 router performs the following major functions:

- Shared memory management on the FPCs—The Distributed Buffer Manager ASIC on the SSB uniformly allocates incoming data packets throughout shared memory on the FPCs.
- Outgoing data cell transfer to the FPCs—A second Distributed Buffer Manager ASIC on the SSB passes data cells to the FPCs for packet reassembly when the data is ready to be transmitted.
- Route lookups—The Internet Processor ASIC on the SSB performs route lookups using the forwarding table stored in SSRAM. After performing the lookup, the Internet Processor ASIC informs the midplane of the forwarding decision, and the midplane forwards the decision to the appropriate outgoing interface.
- System component monitoring—The SSB monitors other system components for failure and alarm conditions. It collects statistics from all sensors in the system and relays them to the Routing Engine, which sets the appropriate alarm. For example, if a temperature sensor exceeds the first internally defined threshold, the Routing Engine issues a “high temp” alarm. If the sensor exceeds the second threshold, the Routing Engine initiates a system shutdown.
- Exception and control packet transfer—The Internet Processor ASIC passes exception packets to a microprocessor on the SSB, which processes almost all of them. The remaining packets are sent to the Routing Engine for further processing. Any errors that originate in the Packet Forwarding Engine and are detected by the SSB are sent to the Routing Engine using system log messages.
- FPC reset control—The SSB monitors the operation of the FPCs. If it detects errors in an FPC, the SSB attempts to reset the FPC. After three unsuccessful resets, the SSB takes the FPC offline and informs the Routing Engine. Other FPCs are unaffected, and normal system operation continues.

The M20 router holds up to two SSBs. One SSB is configured to act as the primary and the other is configured to serve as a backup in case the primary fails. You can initiate a manual switchover by issuing the `request chassis ssb master switch` command. For more information, see the [CLI Explorer](#).

## Redundant SFMs on the M40e and M160 Routers

The M40e and M160 routers have redundant Switching and Forwarding Modules (SFMs). The SFMs contain the Internet Processor II ASIC and two Distributed Buffer Manager ASICs. SFMs ensure that all traffic leaving the FPCs is handled properly. SFMs provide route lookup, filtering, and switching.

The M40e router holds up to two SFMs, one that is configured to act as the primary and the other configured to serve as a backup in case the primary fails. Removing the standby SFM has no effect on router function. If the active SFM fails or is removed from the chassis, forwarding halts until the standby SFM boots and becomes active. It takes approximately 1 minute for the new SFM to become active. Synchronizing router configuration information can take additional time, depending on the complexity of the configuration.

The M160 router holds up to four SFMs. All SFMs are active at the same time. A failure or taking an SFM offline has no effect on router function. Forwarding continues uninterrupted.

You can initiate a manual switchover by issuing the `request chassis sfm master switch` command. For more information, see the [CLI Explorer](#).

### RELATED DOCUMENTATION

[Understanding High Availability Features on Juniper Networks Routers | 2](#)

[Understanding Routing Engine Redundancy | 124](#)

[Configuring CFEB Redundancy on the M10i Router](#)

[Configuring FEB Redundancy on the M120 Router](#)

[Configuring SFM Redundancy on M40e and M160 Routers](#)

[Configuring SSB Redundancy on the M20 Router](#)

[show chassis redundancy feb | 1396](#)

[request chassis cb](#)

# Configuring Switching Control Board Redundancy

## IN THIS CHAPTER

- [Configuring Switching Control Board Redundancy | 20](#)

## Configuring Switching Control Board Redundancy

### SUMMARY

Follow the steps below to configure switching control board redundancy.

### IN THIS SECTION

- [Configuring CFEB Redundancy on the M10i Router | 20](#)
- [Configuring FEB Redundancy on the M120 Router | 21](#)
- [Example: Configuring FEB Redundancy on M120 Routers | 22](#)
- [Configuring SFM Redundancy on M40e and M160 Routers | 24](#)
- [Configuring SSB Redundancy on the M20 Router | 24](#)
- [Configuring the Junos OS to Support Redundancy on Routers Having Multiple Routing Engines or Switching Boards | 25](#)

## Configuring CFEB Redundancy on the M10i Router

The Compact Forwarding Engine Board (CFEB) on the M10i router provides route lookup, filtering, and switching on incoming data packets, and then directs outbound packets to the appropriate interface for transmission to the network. The CFEB communicates with the Routing Engine using a dedicated 100-Mbps Fast Ethernet link that transfers routing table data from the Routing Engine to the forwarding table in the integrated ASIC. The link is also used to transfer from the CFEB to the Routing Engine

routing link-state updates and other packets destined for the router that have been received through the router interfaces.

To configure a CFEB redundancy group, include the following statements at the [edit chassis redundancy] hierarchy level:

```
[edit chassis redundancy]
cfep slot-number (always | preferred);
```

**slot-number** can be 0 or 1.

**always** defines the CFEB as the sole device.

**preferred** defines a preferred CFEB.

To manually switch CFEB primary role, issue the request chassis cfep master switch command. To view CFEB status, issue the show chassis cfep command.

## SEE ALSO

[Understanding Switching Control Board Redundancy | 15](#)

## Configuring FEB Redundancy on the M120 Router

To configure a FEB redundancy group for the M120 router, include the following statements at the [edit chassis redundancy feb] hierarchy level:

```
[edit chassis redundancy feb]
redundancy-group group-name {
    description description;
    feb slot-number (backup | primary);
    no-auto-failover;
}
```

**group-name** is the unique name for the redundancy group. The maximum length is 39 alphanumeric characters.

**slot-number** is the slot number of each FEB you want to include in the redundancy group. The range is from 0 through 5. You must specify exactly one FEB as a backup FEB per redundancy group. Include the **backup** keyword when configuring the backup FEB and make sure that the FEB is not connected to an FPC.

Include the **primary** keyword to optionally specify one primary FEB per redundancy group. When the **primary** keyword is specified for a particular FEB, that FEB is configured for 1:1 redundancy. With 1:1 redundancy, the backup FEB contains the same forwarding state as the primary FEB. When no FEB in the redundancy group is configured as a primary FEB, the redundancy group is configured for  $n$ :1 redundancy. In this case, the backup FEB has no forwarding state. When a FEB fails, the forwarding state must be downloaded from the Routing Engine to the backup FEB before forwarding continues.

A combination of 1:1 and  $n$ :1 redundancy is possible when more than two FEBs are present in a group. The backup FEB contains the same forwarding state as the primary FEB, so that when the primary FEB fails, 1:1 failover is in effect. When a nonprimary FEB fails, the backup FEB must be rebooted so that the forwarding state from the nonprimary FEB is installed on the backup FEB before it can continue forwarding.

You can optionally include the `description` statement to describe a redundancy group.

Automatic failover is enabled by default. To disable automatic failover, include the `no-auto-failover` statement. If you disable automatic failover, you can perform only a manual switchover using the operational command **request chassis redundancy feb slot *slot-number* switch-to-backup**.

To view FEB status, issue the `show chassis feb` command. For more information, see the [CLI Explorer](#).

## SEE ALSO

[Understanding Switching Control Board Redundancy | 15](#)

Example: Configuring FEB Redundancy on M120 Routers

### Example: Configuring FEB Redundancy on M120 Routers

In the following configuration, two FEB redundancy groups are created:

- A FEB redundancy group named **group0** with the following properties:
  - Contains three FEBs (0 through 2).
  - Has a primary FEB (2).
  - Has a unique backup FEB (0).
  - Automatic failover is disabled.

When an active FEB in **group0** fails, automatic failover to the backup FEB does not occur. For **group0**, you can only perform a manual switchover.

- A FEB redundancy group named **group1** with the following properties:
  - Two FEBs (3 and 5). There is no primary FEB.



- A unique backup FEB (5).
- Automatic failover is enabled by default.

When **feb 3** in **group1** fails, an automatic failover occurs.

Because you must explicitly configure an FPC *not* to connect to the backup FEB, connectivity is set to none between **fpc 0** and **feb 0** and between **fpc 5** and **feb 5**.

**NOTE:** For information about the `fpc-feb-connectivity` statement, see the [Junos OS Administration Library for Routing Devices](#).

FPC to primary FEB connectivity is not explicitly configured, so by default, the software automatically assigns connectivity based on the numerical order of the FPCs.

```
[edit]
chassis {
  fpc-feb-connectivity {
    fpc 0 feb none;
    fpc 5 feb none;
  }
  redundancy feb {
    redundancy-group group0 {
      description "Interfaces to Customer X";
      feb 2 primary;
      feb 1;
      feb 0 backup;
      no-auto-failover;
    }
    redundancy-group group1 {
      feb 3;
      feb 5 backup;
    }
  }
}
```

## SEE ALSO

[Understanding Switching Control Board Redundancy | 15](#)

Configuring FEB Redundancy on the M120 Router

## Configuring SFM Redundancy on M40e and M160 Routers

By default, the Switching and Forwarding Module (SFM) in slot 0 is the primary and the SFM in slot 1 is the backup. To modify the default configuration, include the `sfm` statement at the `[edit chassis redundancy]` hierarchy level:

```
[edit chassis redundancy]
sfm slot-number (always | preferred);
```

On the M40e router, *slot-number* is 0 or 1. On the M160 router, *slot-number* is 0 through 3.

**always** defines the SFM as the sole device.

**preferred** defines a preferred SFM.

To manually switch primary role between SFMs, issue the `request chassis sfm master switch` command. To view SFM status, issue the `show chassis sfm` command. For more information, see the [CLI Explorer](#).

### SEE ALSO

[Understanding Switching Control Board Redundancy | 15](#)

## Configuring SSB Redundancy on the M20 Router

For M20 routers with two System and Switch Boards (SSBs), you can configure which SSB is the primary and which is the backup. By default, the SSB in slot 0 is the primary and the SSB in slot 1 is the backup. To modify the default configuration, include the `ssb` statement at the `[edit chassis redundancy]` hierarchy level:

```
[edit chassis redundancy]
ssb slot-number (always | preferred);
```

*slot-number* is 0 or 1.

**always** defines the SSB as the sole device.

**preferred** defines a preferred SSB.

To manually switch primary role between SSBs, issue the `request chassis ssb master switch` command.

To display SSB status information, issue the `show chassis ssb` command. The command output displays the number of times the primary role has changed, the SSB slot number, and the current state of the SSB: primary, backup, or empty. For more information, see the [CLI Explorer](#).

## SEE ALSO

[Understanding Switching Control Board Redundancy | 15](#)

## Configuring the Junos OS to Support Redundancy on Routers Having Multiple Routing Engines or Switching Boards

For routers that have multiple Routing Engines or these multiple switching control boards: Switching and Forwarding Modules (SFMs), System and Switch Boards (SSBs), Forwarding Engine Boards (FEBs), or Compact Forwarding Engine Boards (CFEBs), you can configure redundancy properties.

To configure redundancy, include the following redundancy statements at the `[edit chassis]` hierarchy level:

```

redundancy {
  cfcb slot (always | preferred);
  failover {
    on-disk-failure
    on-loss-of-keepalives;
  }
  feb {
    redundancy-group group-name {
      feb slot-number (backup | primary);
      description description;
      no-auto-failover;
    }
  }
  graceful-switchover;
  keepalive-time seconds;
  routing-engine slot-number (master | backup | disabled);
  sfm slot-number (always | preferred);
  ssb slot-number (always | preferred);
}

```

## SEE ALSO

[Understanding Routing Engine Redundancy | 124](#)

# 3

PART

## Configuring Bidirectional Forwarding Detection (BFD)

---

[Understanding How BFD Detects Network Failures](#) | 27

[Configuring BFD](#) | 50

---

# Understanding How BFD Detects Network Failures

## IN THIS CHAPTER

- [Understanding How BFD Detects Network Failures | 27](#)

## Understanding How BFD Detects Network Failures

### SUMMARY

An overview of the Bidirectional Forwarding Detection (BFD) protocol and the different types of BFD sessions.

### IN THIS SECTION

- [Understanding BFD | 28](#)
- [Centralized BFD | 29](#)
- [Distributed BFD | 29](#)
- [Inline BFD | 31](#)
- [Understanding BFD for Static Routes for Faster Network Failure Detection | 33](#)
- [Understanding BFD for BGP | 37](#)
- [Understanding BFD for OSPF | 38](#)
- [Understanding BFD for IS-IS | 41](#)
- [Understanding BFD for RIP | 44](#)
- [Understanding Independent Micro BFD Sessions for LAG | 45](#)
- [Understanding Static Route State When BFD is in Admin Down State | 47](#)

## Understanding BFD

IN THIS SECTION

- [Benefits | 28](#)
- [Types of BFD Sessions | 28](#)
- [Single-hop and Multihop BFD | 29](#)

The Bidirectional Forwarding Detection (BFD) protocol is a simple hello mechanism that detects failures in a network. A pair of routing devices exchange BFD packets. The devices send hello packets at a specified, regular interval. The device detects a neighbor failure when the routing device stops receiving a reply after a specified interval.

### Benefits

- Use BFD to check the health of your network.
- BFD works with a wide variety of network environments and topologies.
- The BFD failure detection timers have short time limits, so they provide fast failure detection.
- BFD timers are adaptive. You can adjust them to be more or less aggressive.

### Types of BFD Sessions

There are four types of BFD sessions based on the source from which BFD packets are sent to the neighbors. The different types of BFD sessions are:

Type of BFD session	Description
Centralized (or non-distributed) BFD	BFD sessions run completely on the Routing Engine.
Distributed BFD	BFD sessions run completely on the FPC CPU.
Inline BFD	BFD sessions run on the FPC software.
Hardware-assisted inline BFD	BFD sessions run on the ASIC firmware.

## Single-hop and Multihop BFD

- Single-hop BFD—Single-hop BFD in Junos OS runs in centralized mode by default. Single-hop BFD control packets use UDP port 3784.
- Multihop BFD—One desirable application of BFD is to detect connectivity to routing devices that span multiple network hops and follow unpredictable paths. This is known as a multihop session. Multihop BFD control packets use UDP port 4784.

Consider the following when using multihop BFD:

- In a multichassis link aggregation group (MC-LAG) setup, Inter-Chassis Control Protocol (ICCP) uses BFD in multihop mode. Multihop BFD runs in centralized mode in this kind of setup.
- Starting in Junos OS Release 13.3R5, Junos OS does not execute firewall filters that you apply on a loopback interface for a multihop BFD session with a delegated anchor FPC. There is an implicit filter on all ingress FPCs to forward packets to the anchor FPC. Therefore, the firewall filter on the loopback interface is not applied on these packets. If you do not want these packets to be forwarded to the anchor FPC, you can configure the `no-delegate-processing` option.

## Centralized BFD

In *centralized BFD* mode (also called *non-distributed BFD* mode), the Routing Engine handles BFD.

For both single-hop BFD and multihop BFD, run BFD in non-distributed mode by enabling `routing-options ppm no-delegate-processing` and then running the `clear bfd session` command.

You can see what mode BFD is running in as follows:

```
user@device> show ppm adjacencies detail
Protocol: BFD, Hold time: 6000, IFL-index: 65
Distributed: FALSE
BFD discriminator: 18, BFD routing table index: 0
```

## Distributed BFD

### IN THIS SECTION

- [Benefits | 30](#)
- [Configuration and Support | 30](#)

The term *distributed BFD* refers to BFD that runs on the FPC CPU. The Routing Engine creates the BFD sessions and the FPC CPU processes them.

## Benefits

The benefits of distributed BFD are mainly in the scaling and performance areas. Distributed BFD:

- Allows for the creation of a larger number of BFD sessions.
- Runs BFD sessions with a shorter transfer/receive timer interval, which can in turn be used to bring down the overall detection time.
- Separates the functionality of BFD from that of the Routing Engine.
- A BFD session can stay up during graceful restart, even with an aggressive interval. The minimum interval for Routing Engine-based BFD sessions to survive *graceful Routing Engine switchover* is 2500 ms. Distributed BFD sessions have a minimum interval of less than a second.
- Frees up the Routing Engine CPU, which improves scaling and performance for Routing Engine-based applications.
- BFD protocol packets flow even when the Routing Engine CPU is congested.

## Configuration and Support

SRX Series devices support a BFD failure detection time of 3 x 100 ms. We support this feature for a standalone SRX Series device. It is not supported for chassis clusters.

Enable distributed mode on the SRX5000 line of devices with SPC3 line cards and SRX1500, SRX4100, SRX4200, and SRX4600 devices by configuring the BFD failure detection time to a value less than 500 ms. SRX1500 devices run in dedicated mode if you've configured `set chassis dedicated-ukern-cpu`, regardless of the BFD failure detection time. You can enable distributed mode on SRX1500 devices only when dedicated mode is not enabled.

To determine if a BFD peer is running distributed BFD, run the `show bfd sessions extensive` command and look for `Remote is control-plane independent` in the command output.

For distributed BFD to work, you need to configure the lo0 interface with unit 0 and the appropriate family.

```
# set interfaces lo0 unit 0 family inet
# set interfaces lo0 unit 0 family inet6
# set interfaces lo0 unit 0 family mpls
```

This is true for the following types of BFD sessions:



- BFD over aggregated Ethernet logical interfaces, both IPv4 and IPv6
- Multihop BFD, both IPv4 and IPv6
- BFD over VLAN interfaces in EX Series switches, both IPv4 and IPv6
- Virtual Circuit Connectivity Verification (VCCV) BFD (Layer 2 circuit, Layer 3 VPN, and VPLS) (MPLS)

**NOTE:** Flapping occurs during the BFD session when the lo0 interface is not configured on PTX Series routers.

**NOTE:** Starting in Junos OS Release 13.3, the distribution of adjacency entry (the IP addresses of adjacent routers) and transmit entry (the IP address of transmitting routers) for a BFD session is asymmetric. This is because an adjacency entry that requires rules might or might not be distributed based on the redirect rule, and the distribution of transmit entries is *not* dependent on the redirect rule.

The term *redirect rule* here denotes the capability of an interface to send protocol redirect messages. See [Disabling the Transmission of Redirect Messages on an Interface](#).

## Inline BFD

### IN THIS SECTION

- [Benefits | 31](#)
- [Inline BFD | 32](#)
- [Hardware-Assisted Inline BFD | 32](#)
- [Configuration | 33](#)

We support two types of inline BFD: inline BFD and hardware-assisted inline BFD. *Inline BFD* sessions run on the FPC software. *Hardware-assisted inline BFD* sessions run on the ASIC firmware. Support depends on your device and software version.

### Benefits

- Inline BFD sessions can have keepalive intervals of less than a second, so you can detect errors in milliseconds.

- If you are running inline BFD and the Routing Engine crashes, the inline BFD sessions will continue without interruption for 15 seconds.
- Inline BFD has many of the same benefits as distributed BFD since it also separates the functionality of BFD from the Routing Engine.
- The Packet Forwarding Engine software and the ASIC firmware process the packets more quickly than the FPC CPU, so inline BFD is faster than distributed BFD.

## Inline BFD

*Inline BFD* sessions run on the FPC software. The Routing Engine creates the BFD sessions and the Packet Forwarding Engine software processes them. Starting in Junos OS Release 16.1R1, integrated routing and bridging (IRB) interfaces support inline BFD sessions.

MX Series routers only support inline BFD if the router is static and has MPCs/MICs with `enhanced-ip` configured.

QFX5110, QFX5120, QFX5200, and QFX5210 switches support 10 multihop inline BFD sessions. You can configure them with a timer of 150 x 3 milliseconds. Single-hop sessions are also supported.

## Hardware-Assisted Inline BFD

*Hardware-assisted inline BFD* sessions run on the ASIC firmware. Hardware-assisted inline BFD is a hardware implementation of the inline BFD protocol. The Routing Engine creates BFD sessions and passes them to the ASIC firmware for processing. The device uses existing paths to forward any BFD events that need to be processed by protocol processes.

Regular inline BFD is a software approach. In hardware-assisted inline BFD, the firmware handles most of the BFD protocol processing. The ASIC firmware processes the packets more quickly than the software, so hardware-assisted inline BFD is faster than regular inline BFD. We support this feature for single-hop and multihop IPv4 and IPv6 BFD sessions.

Devices support either regular inline BFD or hardware-assisted inline BFD. Starting in Junos OS Release 21.2R1, QFX5120-32C and QFX5120-48Y switches support hardware-assisted inline BFD. They support a timer of 100 x 3 milliseconds. They can run up to 128 hardware-assisted inline BFD sessions, which can be a mix of single-hop and multihop BFD sessions.

## Limitations

If the Packet Forwarding Engine process restarts or the system reboots, the BFD sessions will go down.

Hardware-assisted inline BFD:

- Does not support micro BFD.

- Is only supported on standalone devices.
- Does not support BFD authentication.
- Does not support IPv6 link local BFD sessions.
- Cannot be used with VXLAN encapsulation of BFD packets.

**NOTE:** If you have configured EVPN overlay BGP peerings, do not use hardware-assisted inline BFD. Use distributed BFD instead.

## Configuration

Devices support either regular inline BFD or hardware-assisted inline BFD. Use the `set routing-options ppm inline-processing-enable` command to enable the type of inline BFD that your device supports. To return BFD to the default mode, delete the configuration.

## SEE ALSO

Enabling Dedicated and Real-Time BFD

*Understanding EBGMP Multihop*

Understanding BFD for Static Routes for Faster Network Failure Detection

## Understanding BFD for Static Routes for Faster Network Failure Detection

The Bidirectional Forwarding Detection (BFD) protocol is a simple hello mechanism that detects failures in a network. BFD works with a wide variety of network environments and topologies. A pair of routing devices exchanges BFD packets. Hello packets are sent at a specified, regular interval. A neighbor failure is detected when the routing device stops receiving a reply after a specified interval. The BFD failure detection timers have shorter time limits than the static route failure detection mechanisms, so they provide faster detection.

The BFD failure detection timers can be adjusted to be faster or slower. The lower the BFD failure detection timer value, the faster the failure detection and vice versa. For example, the timers can adapt to a higher value if the adjacency fails (that is, the timer detects failures more slowly). Or a neighbor can negotiate a higher value for a timer than the configured value. The timers adapt to a higher value when a BFD session flap occurs more than three times in a span of 15 seconds. A back-off algorithm increases the receive (Rx) interval by two if the local BFD instance is the reason for the session flap. The transmission (Tx) interval is increased by two if the remote BFD instance is the reason for the session flap. You can use the `clear bfd adaptation` command to return BFD interval timers to their configured

values. The `clear bfd adaptation` command is hitless, meaning that the command does not affect traffic flow on the routing device.

By default, BFD is supported on single-hop static routes.

**NOTE:** On MX Series devices, multihop BFD is not supported on a static route if the static route is configured with more than one next hop. It is recommended that you avoid using multiple next hops when a multihop BFD is required for a static route.

To enable failure detection, include the `bfd-liveness-detection` statement in the static route configuration.

**NOTE:** Starting with Junos OS Release 15.1X49-D70 and Junos OS Release 17.3R1, the `bfd-liveness-detection` command includes the `description` field. The `description` is an attribute under the `bfd-liveness-detection` object and it is supported only on SRX Series devices. This field is applicable only for the static routes.

In Junos OS Release 9.1 and later, the BFD protocol is supported for IPv6 static routes. Global unicast and link-local IPv6 addresses are supported for static routes. The BFD protocol is not supported on multicast or anycast IPv6 addresses. For IPv6, the BFD protocol supports only static routes and only in Junos OS Release 9.3 and later. IPv6 for BFD is also supported for the eBGP protocol.

To configure the BFD protocol for IPv6 static routes, include the `bfd-liveness-detection` statement at the `[edit routing-options rib inet6.0 static route destination-prefix]` hierarchy level.

In Junos OS Release 8.5 and later, you can configure a hold-down interval to specify how long the BFD session must remain up before a state change notification is sent.

To specify the hold-down interval, include the `holddown-interval` statement in the BFD configuration. You can configure a number in the range from 0 through 255,000 milliseconds. The default is 0. If the BFD session goes down and then comes back up during the hold-down interval, the timer is restarted.

**NOTE:** If a single BFD session includes multiple static routes, the hold-down interval with the highest value is used.

To specify the minimum transmit and receive intervals for failure detection, include the `minimum-interval` statement in the BFD configuration.

This value represents both the minimum interval after which the local routing device transmits hello packets and the minimum interval after which the routing device expects to receive a reply from the neighbor with which it has established a BFD session. You can configure a number in the range from 1

through 255,000 milliseconds. Optionally, instead of using this statement, you can configure the minimum transmit and receive intervals separately using the **transmit-interval** **minimum-interval** and **minimum-receive-interval** statements.

**NOTE:** EX4600 switches do not support minimum interval values of less than 1 second.

**NOTE:** BFD is an intensive protocol that consumes system resources. Specifying a minimum interval for BFD of less than 100 ms for Routing Engine-based sessions and 10 ms for distributed BFD sessions can cause undesired BFD flapping.

Depending on your network environment, these additional recommendations might apply:

- For large-scale network deployments with a large number of BFD sessions, specify a minimum interval of 300 ms for Routing Engine-based sessions and 100 ms for distributed BFD sessions.
- For very large-scale network deployments with a large number of BFD sessions, contact Juniper Networks customer support for more information.
- For BFD sessions to remain up during a Routing Engine switchover event when *nonstop active routing* (NSR) is configured, specify a minimum interval of 2500 ms for Routing Engine-based sessions. For distributed BFD sessions with NSR configured, the minimum interval recommendations are unchanged and depend only on your network deployment.

To specify the minimum receive interval for failure detection, include the **minimum-receive-interval** statement in the BFD configuration. This value represents the minimum interval after which the routing device expects to receive a reply from a neighbor with which it has established a BFD session. You can configure a number in the range from 1 through 255,000 milliseconds. Optionally, instead of using this statement, you can configure the minimum receive interval using the **minimum-interval** statement at the [edit routing-options static route *destination-prefix* bfd-liveness-detection] hierarchy level.

To specify the number of hello packets not received by the neighbor that causes the originating interface to be declared down, include the **multiplier** statement in the BFD configuration. The default value is 3. You can configure a number in the range from 1 through 255.

To specify a threshold for detecting the adaptation of the detection time, include the **threshold** statement in the BFD configuration.

When the BFD session detection time adapts to a value equal to or higher than the threshold, a single trap and a system log message are sent. The detection time is based on the multiplier of the **minimum-interval** or the **minimum-receive-interval** value. The threshold must be a higher value than the multiplier for either of these configured values. For example if the **minimum-receive-interval** is 300 ms and the

**multiplier** is 3, the total detection time is 900 ms. Therefore, the detection time threshold must have a value higher than 900.

To specify the minimum transmit interval for failure detection, include the `transmit-interval minimum-interval` statement in the BFD configuration.

This value represents the minimum interval after which the local routing device transmits hello packets to the neighbor with which it has established a BFD session. You can configure a value in the range from 1 through 255,000 milliseconds. Optionally, instead of using this statement, you can configure the minimum transmit interval using the `minimum-interval` statement at the `[edit routing-options static route destination-prefix bfd-liveness-detection]` hierarchy level.

To specify the threshold for the adaptation of the transmit interval, include the `transmit-interval threshold` statement in the BFD configuration.

The threshold value must be greater than the transmit interval. When the BFD session transmit time adapts to a value greater than the threshold, a single trap and a system log message are sent. The detection time is based on the multiplier of the value for the **minimum-interval** or the `minimum-receive-interval` statement at the `[edit routing-options static route destination-prefix bfd-liveness-detection]` hierarchy level. The threshold must be a higher value than the multiplier for either of these configured values.

To specify the BFD version, include the `version` statement in the BFD configuration. The default is to have the version detected automatically.

To include an IP address for the next hop of the BFD session, include the `neighbor` statement in the BFD configuration.

**NOTE:** You must configure the `neighbor` statement if the next hop specified is an interface name. If you specify an IP address as the next hop, that address is used as the neighbor address for the BFD session.

In Junos OS Release 9.0 and later, you can configure BFD sessions not to adapt to changing network conditions. To disable BFD adaptation, include the `no-adaptation` statement in the BFD configuration.

**NOTE:** We recommend that you not disable BFD adaptation unless it is preferable *not* to have BFD adaptation in your network.

**NOTE:** If BFD is configured only on one end of a static route, the route is removed from the routing table. BFD establishes a session when BFD is configured on both ends of the static route.

BFD is not supported on ISO address families in static routes. BFD does support IS-IS.

If you configure *graceful Routing Engine switchover* (GRES) at the same time as BFD, GRES does not preserve the BFD state information during a failover.

## SEE ALSO

Enabling Dedicated and Real-Time BFD

## Understanding BFD for BGP

The Bidirectional Forwarding Detection (BFD) protocol is a simple hello mechanism that detects failures in a network. Hello packets are sent at a specified, regular interval. A neighbor failure is detected when the routing device stops receiving a reply after a specified interval. BFD works with a wide variety of network environments and topologies. The failure detection timers for BFD have shorter time limits than default failure detection mechanisms for BGP, so they provide faster detection.

**NOTE:** Configuring both BFD and graceful restart for BGP on the same device is counterproductive. When an interface goes down, BFD detects this instantly, stops traffic forwarding and the BGP session goes down whereas graceful restart forwards traffic despite the interface failure, this behavior might cause network issues. Hence we do not recommend configuring both BFD and graceful restart on the same device.

**NOTE:** EX4600 switches do not support minimum interval values of less than 1 second.

**NOTE:** QFX5110, QFX5120, QFX5200, and QFX5210 switches support multihop Bidirectional Forwarding Detection (BFD) inline keep alive support which will enable sessions to be configured at less than 1 second. Performance may vary depending on the system load. 10 inline BFD sessions are supported and can be configured with a timer of 150 x 3 milliseconds. Single-hop sessions are also supported.

The BFD failure detection timers can be adjusted to be faster or slower. The lower the BFD failure detection timer value, the faster the failure detection and vice versa. For example, the timers can adapt to a higher value if the adjacency fails (that is, the timer detects failures more slowly). Or a neighbor can negotiate a higher value for a timer than the configured value. The timers adapt to a higher value when a BFD session flap occurs more than three times in a span of 15 seconds (15000 milliseconds). A back-off

algorithm increases the receive (Rx) interval by two if the local BFD instance is the reason for the session flap. The transmission (Tx) interval is increased by two if the remote BFD instance is the reason for the session flap. You can use the `clear bfd adaptation` command to return BFD interval timers to their configured values. The `clear bfd adaptation` command is hitless, meaning that the command does not affect traffic flow on the routing device.

**NOTE:** On all SRX Series devices, high CPU utilization triggered for reasons such as CPU intensive commands and SNMP walks causes the BFD protocol to flap while processing large BGP updates. (Platform support depends on the Junos OS release in your installation.) Starting with Junos OS Release 15.1X49-D100, SRX340, SRX345, and SRX1500 devices support dedicated BFD.

Starting with Junos OS Release 15.1X49-D100, SRX300 and SRX320 devices support real-time BFD.

Starting with Junos OS Release 15.1X49-D110, SRX550M devices support dedicated BFD.

In Junos OS Release 8.3 and later, BFD is supported on internal BGP (IBGP) and multihop external BGP (EBGP) sessions as well as on single-hop EBGP sessions. In Junos OS Release 9.1 through Junos OS Release 11.1, BFD supports IPv6 interfaces in static routes only. In Junos OS Release 11.2 and later, BFD supports IPv6 interfaces with BGP.

## SEE ALSO

Enabling Dedicated and Real-Time BFD

## Understanding BFD for OSPF

The Bidirectional Forwarding Detection (BFD) protocol is a simple hello mechanism that detects failures in a network. BFD works with a wide variety of network environments and topologies. A pair of routing devices exchange BFD packets. Hello packets are sent at a specified, regular interval. A neighbor failure is detected when the routing device stops receiving a reply after a specified interval. The BFD failure detection timers have shorter time limits than the OSPF failure detection mechanisms, so they provide faster detection.

The BFD failure detection timers are adaptive and can be adjusted to be faster or slower. The lower the BFD failure detection timer value, the faster the failure detection and vice versa. For example, the timers can adapt to a higher value if the adjacency fails (that is, the timer detects failures more slowly). Or a neighbor can negotiate a higher value for a timer than the configured value. The timers adapt to a higher value when a BFD session flap occurs more than three times in a span of 15 seconds. A back-off algorithm increases the receive (Rx) interval by two if the local BFD instance is the reason for the session flap. The transmission (Tx) interval is increased by two if the remote BFD instance is the reason for the



session flap. You can use the `clear bfd adaptation` command to return BFD interval timers to their configured values. The `clear bfd adaptation` command is hitless, meaning that the command does not affect traffic flow on the routing device.

**NOTE:** EX4600 switches do not support minimum interval values of less than 1 second.

**NOTE:** BFD is supported for OSPFv3 in Junos OS Release 9.3 and later.

**NOTE:** For branch SRX Series devices, we recommend 1000 ms as the minimum keepalive time interval for BFD packets.

You can configure the following BFD protocol settings:

- **detection-time threshold**—Threshold for the adaptation of the detection time. When the BFD session detection time adapts to a value equal to or greater than the configured threshold, a single trap and a single system log message are sent.
- **full-neighbors-only**—Ability to establish BFD sessions only for OSPF neighbors with full neighbor adjacency. The default behavior is to establish BFD sessions for all OSPF neighbors. This setting is available in Junos OS Release 9.5 and later.
- **minimum-interval**—Minimum transmit and receive interval for failure detection. This setting configures both the minimum interval after which the local routing device transmits hello packets and the minimum interval after which the routing device expects to receive a reply from the neighbor with which it has established a BFD session. Both intervals are in milliseconds. You can also specify the minimum transmit and receive intervals separately using the `transmit-interval` `minimum-interval` and `minimum-receive-interval` statements.

**NOTE:** BFD is an intensive protocol that consumes system resources. Specifying a minimum interval for BFD of less than 100 ms for Routing Engine-based sessions and 10 ms for distributed BFD sessions can cause undesired BFD flapping.

Depending on your network environment, the following may apply:

- For large-scale network deployments with a large number of BFD sessions, specify a minimum interval of no less than 500 ms. An interval of 1000 ms is recommended to avoid any instability issues.

- For BFD sessions to remain up during a Routing Engine switchover event when *nonstop active routing* (NSR) is configured, specify a minimum interval of 2500 ms for Routing Engine-based sessions. Without NSR, Routing Engine-based sessions can have a minimum interval of 100 ms.
  - For distributed BFD sessions with NSR configured, the minimum interval recommendations are unchanged and depend only on your network deployment.
  - Junos OS 21.2R1 and later support distributed OSPFv3 and ISIS BFD sessions with IPv6 link local addresses on MX series routers running MPCs 1 through 9 (it is not supported on MPC 10 or MPC 11). The default for IPv6 link local BFD is inline mode.
  - BFD is not distributed prior to Junos 21.2 (because for OSPFv3, BFD is based in the Routing Engine).
  - On a single QFX5100 switch, when you add a QFX-EM-4Q expansion module, specify a minimum interval higher than 1000 ms.
- `minimum-receive-interval`—Minimum receive interval for failure detection. This setting configures the minimum receive interval, in milliseconds, after which the routing device expects to receive a hello packet from a neighbor with which it has established a BFD session. You can also specify the minimum receive interval using the `minimum-interval` statement.
  - `multiplier`—Multiplier for hello packets. This setting configures the number of hello packets that are not received by a neighbor, which causes the originating interface to be declared down. By default, three missed hello packets cause the originating interface to be declared down.
  - `no-adaptation`—Disables BFD adaptation. This setting disables BFD sessions from adapting to changing network conditions. This setting is available in Junos OS Release 9.0 and later.
- NOTE:** We recommend that you do not disable BFD adaptation unless it is preferable not to have BFD adaptation in your network.
- `transmit-interval minimum-interval`—Minimum transmit interval for failure detection. This setting configures the minimum transmit interval, in milliseconds, at which the local routing device transmits hello packets to the neighbor with which it has established a BFD session. You can also specify the minimum transmit interval using the `minimum-interval` statement.
  - `transmit-interval threshold`—Threshold for the adaptation of the BFD session transmit interval. When the transmit interval adapts to a value greater than the threshold, a single trap and a single system log message are sent. The threshold value must be greater than the minimum transmit interval. If you attempt to commit a configuration with a threshold value less than the minimum transmit interval, the routing device displays an error and does not accept the configuration.

- **version**—BFD version. This setting configures the BFD version used for detection. You can explicitly configure BFD version 1, or the routing device can automatically detect the BFD version. By default, the routing device automatically detects the BFD version automatically, which is either 0 or 1.

You can also trace BFD operations for troubleshooting purposes.

## Understanding BFD for IS-IS

The Bidirectional Forwarding Detection (BFD) protocol is a simple hello mechanism that detects failures in a network. Hello packets are sent at a specified, regular interval. A neighbor failure is detected when the routing device stops receiving a reply after a specified interval. BFD works with a wide variety of network environments and topologies. The failure detection timers for BFD have shorter time limits than the failure detection mechanisms of IS-IS, providing faster detection.

The BFD failure detection timers are adaptive and can be adjusted to be faster or slower. For example, the timers can adapt to a higher value if the adjacency fails, or a neighbor can negotiate a higher value for a timer than the configured value. The timers adapt to a higher value when a BFD session flap occurs more than three times in a span of 15 seconds. A back-off algorithm increases the receive (RX) interval by two if the local BFD instance is the reason for the session flap. The transmission (TX) interval is increased by two if the remote BFD instance is the reason for the session flap.

You can use the `clear bfd adaptation` command to return BFD interval timers to their configured values. The `clear bfd adaptation` command is hitless, meaning that the command does not affect traffic flow on the routing device.

**NOTE:** Starting with Junos OS Release 16.1R1, you can configure IS-IS BFD sessions for IPv6 by including the `bfd-liveness-detection` statement at the `[edit protocols isis interface interface-name family inet|inet6]` hierarchy level.

- For interfaces that support both IPv4 and IPv6 routing, the `bfd-liveness-detection` statement must be configured separately for each inet family.
- BFD over IPv6 link local address is currently not distributed because IS-IS uses link local addresses for forming adjacencies.
- BFD sessions over IPv6 must not have the same aggressive detection intervals as IPv4 sessions.
- BFD IPv6 sessions with detection intervals less than 2.5 seconds are currently not supported when nonstop active routing (NSR) is enabled.

**NOTE:** EX4600 switches do not support minimum interval values of less than 1 second.

To detect failures in the network, the set of statements in [Table 1 on page 42](#) are used in the configuration.

**Table 1: Configuring BFD for IS-IS**

Statement	Description
<code>bfd-liveness-detection</code>	Enable failure detection.
<code>minimum-interval milliseconds</code>	<p>Specify the minimum transmit and receive intervals for failure detection.</p> <p>This value represents the minimum interval at which the local router transmits hellos packets as well as the minimum interval at which the router expects to receive a reply from a neighbor with which it has established a BFD session. You can configure a number from 1 through 255,000 milliseconds. You can also specify the minimum transmit and receive intervals separately.</p> <p><b>NOTE:</b> BFD is an intensive protocol that consumes system resources. Specifying a minimum interval for BFD less than 100 ms for Routing Engine-based sessions and 10 ms for distributed BFD sessions can cause undesired BFD flapping.</p> <p>Depending on your network environment, these additional recommendations might apply:</p> <ul style="list-style-type: none"> <li>• For large-scale network deployments with a large number of BFD sessions, specify a minimum interval of 300 ms for Routing Engine-based sessions and 100 ms for distributed BFD sessions.</li> <li>• For very large-scale network deployments with a large number of BFD sessions, please contact Juniper Networks customer support for more information.</li> <li>• For BFD sessions to remain up during a Routing Engine switchover event when <i>nonstop active routing</i> (NSR) is configured, specify a minimum interval of 2500 ms for Routing Engine-based sessions. For distributed BFD sessions with nonstop active routing configured, the minimum interval recommendations are unchanged and depend only on your network deployment.</li> </ul>
<code>minimum-receive-interval milliseconds</code>	<p>Specify only the minimum receive interval for failure detection.</p> <p>This value represents the minimum interval at which the local router expects to receive a reply from a neighbor with which it has established a BFD session. You can configure a number from 1 through 255,000 milliseconds.</p>

**Table 1: Configuring BFD for IS-IS (Continued)**

Statement	Description
<code>multiplier number</code>	<p>Specify the number of hello packets not received by the neighbor that causes the originating interface to be declared down.</p> <p>The default is 3, and you can configure a value from 1 through 225.</p>
<code>no-adaptation</code>	<p>Disable BFD adaptation.</p> <p>In Junos OS Release 9.0 and later, you can specify that the BFD sessions not adapt to changing network conditions.</p> <p><b>NOTE:</b> We recommend that you not disable BFD adaptation unless it is preferable not to have BFD adaptation enabled in your network.</p>
<code>threshold</code>	<p>Specify the threshold for the following:</p> <ul style="list-style-type: none"> <li>Adaptation of the detection time</li> </ul> <p>When the BFD session detection time adapts to a value equal to or greater than the threshold, a single trap and a system log message are sent.</p> <ul style="list-style-type: none"> <li>Transmit interval</li> </ul> <p><b>NOTE:</b> The threshold value must be greater than the minimum transmit interval multiplied by the multiplier number.</p>
<code>transmit-interval</code> <code>minimum-interval</code>	<p>Specify the minimum transmit interval for failure detection.</p> <p>This value represents the minimum interval at which the local routing device transmits hello packets to the neighbor with which it has established a BFD session. You can configure a value from 1 through 255,000 milliseconds.</p>
<code>version</code>	<p>Specify the BFD version used for detection.</p> <p>The default is to have the version detected automatically.</p>

**NOTE:** You can trace BFD operations by including the `traceoptions` statement at the `[edit protocols bfd]` hierarchy level.

For a list of hierarchy levels at which you can include these statements, see the statement summary sections for these statements.

## SEE ALSO

Example: Configuring BFD for IS-IS

*Understanding BFD Authentication for IS-IS*

## Understanding BFD for RIP

The Bidirectional Forwarding Detection (BFD) Protocol is a simple hello mechanism that detects failures in a network. Hello packets are sent at a specified, regular interval. A neighbor failure is detected when the routing device stops receiving a reply after a specified interval. BFD works with a wide variety of network environments and topologies. BFD failure detection times are shorter than RIP detection times, providing faster reaction times to various kinds of failures in the network. Instead of waiting for the routing protocol neighbor timeout, BFD provides rapid detection of link failures. BFD timers are adaptive and can be adjusted to be more or less aggressive. For example, a timer can adapt to a higher value if the adjacency fails, or a neighbor can negotiate a higher value for a timer than the one configured. Note that the functionality of configuring BFD for RIP described in this topic is not supported in Junos OS Releases 15.1X49, 15.1X49-D30, or 15.1X49-D40.

**NOTE:** EX4600 switches do not support minimum interval values of less than 1 second.

BFD enables quick failover between a primary and a secondary routed path. The protocol tests the operational status of the interface multiple times per second. BFD provides for configuration timers and thresholds for failure detection. For example, if the minimum interval is set for 50 milliseconds and the threshold uses the default value of three missed messages, a failure is detected on an interface within 200 milliseconds of the failure.

Intervening devices (for example, an Ethernet LAN switch) hide link-layer failures from routing protocol peers, such as when two routers are connected by way of a LAN switch, where the local interface status remains up even when a physical fault happens on the remote link. Link-layer failure detection times vary, depending on the physical media and the Layer 2 encapsulation. BFD can provide fast failure detection times for all media types, encapsulations, topologies, and routing protocols.

To enable BFD for RIP, both sides of the connection must receive an update message from the peer. By default, RIP does not export any routes. Therefore, you must enable update messages to be sent by configuring an export policy for routes before a BFD session is triggered.

## Understanding Independent Micro BFD Sessions for LAG

### IN THIS SECTION

- [Configuration Guidelines for Micro-BFD Sessions | 46](#)

The Bidirectional Forwarding Detection (BFD) protocol is a simple detection protocol that quickly detects failures in the forwarding paths. To enable failure detection for aggregated Ethernet interfaces in a LAG, you can configure an independent, asynchronous-mode BFD session on every LAG member link in a LAG bundle. Instead of a single BFD session monitoring the status of the UDP port, independent micro-BFD sessions monitor the status of individual member links.

When you configure micro-BFD sessions on every member link in a LAG bundle, each individual session determines the Layer 2 and Layer 3 connectivity of each member link in a LAG.

After the individual session is established on a particular link, member links are attached to the LAG and then load balanced by either one of the following:

- Static configuration—The device control process acts as the client to the micro-BFD session.
- Link Aggregation Control Protocol (LACP)—LACP acts as the client to the micro-BFD session.

When the micro-BFD session is up, a LAG link is established and data is transmitted over that LAG link. If the micro-BFD session on a member link is down, that particular member link is removed from the load balancer, and the LAG managers stop directing traffic to that link. These micro-BFD sessions are independent of each other despite having a single client that manages the LAG interface.

Micro-BFD sessions run in the following modes:

- Distribution mode—In this mode, the Packet Forwarding Engine (PFE) sends and receives the packets at Layer 3. By default, micro-BFD sessions are distributed at Layer 3.
- Non-distribution mode—In this mode, the Routing Engine sends and receives the packets at Layer 2. You can configure the BFD session to run in this mode by including the `no-delegate-processing` statement under periodic packet management (PPM).

A pair of routing devices in a LAG exchange BFD packets at a specified, regular interval. The routing device detects a neighbor failure when it stops receiving a reply after a specified interval. This allows the quick verification of member link connectivity with or without LACP. A UDP port distinguishes BFD over LAG packets from BFD over single-hop IP packets. The Internet Assigned Numbers Authority (IANA) has allocated 6784 as the UDP destination port for micro-BFD.

## Benefits

- Failure detection for LAG—Enables failure detection between devices that are in point-to-point connections.
- Multiple BFD sessions—Enables you to configure multiple micro-BFD sessions for each member link instead of a single BFD session for the entire bundle.

## Configuration Guidelines for Micro-BFD Sessions

Consider the following guidelines as you configure individual micro-BFD sessions on an aggregated Ethernet bundle.

- This feature works only when both the devices support BFD. If BFD is configured at one end of the LAG, this feature does not work.
- Starting with Junos OS Release 13.3, IANA has allocated 01-00-5E-90-00-01 as the dedicated MAC address for micro BFD. Dedicated MAC mode is used by default for micro BFD sessions.
- In Junos OS, micro-BFD control packets are always untagged by default. For Layer 2 aggregated interfaces, the configuration must include `vlan-tagging` or `flexible-vlan-tagging` options when you configure Aggregated Ethernet with BFD. Otherwise, the system will throw an error while committing the configuration.
- When you enable micro-BFD on an aggregated Ethernet interface, the aggregated interface can receive micro-BFD packets. In Junos OS Release 19.3 and later, for MPC10E and MPC11E MPCs, you cannot apply firewall filters on the micro-BFD packets received on the aggregated Ethernet interface. For MPC1E through MPC9E, you can apply firewall filters on the micro-BFD packets received on the aggregated Ethernet interface only if the aggregated Ethernet interface is configured as an untagged interface.
- Starting with Junos OS Release 14.1, specify the neighbor in a BFD session. In releases before Junos OS Release 16.1, you must configure the loopback address of the remote destination as the neighbor address. Beginning with Junos OS Release 16.1, you can also configure this feature on MX Series routers with aggregated Ethernet interface address of the remote destination as the neighbor address.
- Beginning with Release 16.1R2, Junos OS checks and validates the configured micro-BFD local-address against the interface or loopback IP address before the configuration commit. Junos OS performs this check on both IPv4 and IPv6 micro-BFD address configurations, and if they do not match, the commit fails. The configured micro-BFD local address should match with the micro-BFD neighbour address that you have configured on the peer router.



- For the IPv6 address family, disable duplicate address detection before configuring this feature with aggregated Ethernet interface addresses. To disable duplicate address detection, include the `dad-disable` statement at the `[edit interface aex unit y family inet6]` hierarchy level.
- Starting in Junos OS 21.4R1, LACP minimum link with sync reset and microBFD configuration is supported on PTX10001-36MR, PTX10003, PTX10004, PTX10008, and PTX10016 routers.



**CAUTION:** Deactivate `bfd-liveness-detection` at the `[edit interfaces aex aggregated-ether-options]` hierarchy level or deactivate the aggregated Ethernet interface before changing the neighbor address from the loopback IP address to the aggregated Ethernet interface IP address. Modifying the local and neighbor address without deactivating `bfd-liveness-detection` or the aggregated Ethernet interface first might cause micro-BFD sessions failure.

## SEE ALSO

[authentication](#)

[bfd-liveness-detection \(LAG\) | 945](#)

[detection-time](#)

[transmit-interval](#)

## Understanding Static Route State When BFD is in Admin Down State

The Bidirectional Forwarding Detection (BFD) Admin Down state is used to bring down a BFD session administratively (applicable for normal BFD session and micro BFD session), to protect client applications from BFD configuration removal, license issues, and clearing of BFD sessions.

When BFD enters the Admin Down state, BFD notifies the new state to its peer for a failure detection time and after the time expires, the client stops transmitting packets.

For the Admin Down state to work, the peer, which receives the Admin Down state notification, must have the capability to distinguish between administratively down state and real link failure.

A BFD session moves to the Admin Down state under the following conditions:

- If BFD configuration is removed for the last client tied to a BFD session, BFD moves to Admin Down state and communicates the change to the peer, to enable the client protocols without going down.
- If BFD license is removed on the client, BFD moves to Admin Down state and communicates the change to the remote system to enable the client protocols without going down.
- When `clear bfd session` command is executed, the BFD sessions move to Admin Down state before restarting. This `clear bfd session` command also ensures that the client applications are not impacted.

Starting from Junos OS 16.1R1 release, you can set the state of static route in BFD Admin Down state by configuring one of the following commands:

- `set routing-options static static-route bfd-admin-down active`—BFD Admin Down state pulls down the static route.
- `set routing-options static static-route bfd-admin-down passive`—BFD Admin Down state does not pull down the static route.

## SEE ALSO

Understanding BFD for Static Routes for Faster Network Failure Detection

Example: Configuring BFD for Static Routes for Faster Network Failure Detection

### Release History Table

Release	Description
19.3	Starting with Junos OS Release 19.3 and later, for MPC10E and MPC11E MPCs, you cannot apply firewall filters on the MicroBFD packets received on the aggregated Ethernet Interface. For MPC1E through MPC9E, you can apply firewall filters on the MicroBFD packets received on the aggregated Ethernet Interface only if the aggregated Ethernet Interface is configured as an untagged Interface.
16.1R1	Starting in Junos OS Release 16.1R1, inline BFD sessions are supported on integrated routing and bridging (IRB) interfaces.
16.1	Beginning with Junos OS Release 16.1, you can also configure this feature on MX series routers with aggregated Ethernet interface address of the remote destination as the neighbor address.
16.1	Beginning with Release 16.1R2, Junos OS checks and validates the configured micro BFD local-address against the interface or loopback IP address before the configuration commit.
15.1X49-D70	Starting with Junos OS Release 15.1X49-D70 and Junos OS Release 17.3R1, the <code>bfd-liveness-detection</code> command includes the description field. The description is an attribute under the <b>bfd-liveness-detection</b> object and it is supported only on SRX Series devices. This field is applicable only for the static routes.
15.1X49-D100	Starting with Junos OS Release 15.1X49-D100, SRX340, SRX345, and SRX1500 devices support dedicated BFD.
15.1X49-D100	Starting with Junos OS Release 15.1X49-D100, SRX300 and SRX320 devices support real-time BFD.

15.1X49	Note that the functionality of configuring BFD for RIP described in this topic is not supported in Junos OS Releases 15.1X49, 15.1X49-D30, or 15.1X49-D40.
14.1	Starting with Junos OS Release 14.1, specify the neighbor in a BFD session. In releases prior to Junos OS Release 16.1, you must configure the loopback address of the remote destination as the neighbor address.
13.3R5	Starting in Junos OS Release 13.3R5, if you apply a firewall filter on a loopback interface for a multihop BFD session with a delegated anchor FPC, Junos OS does not execute this filter, because there is an implicit filter on all ingress FPCs to forward packets to the anchor FPC.
13.3	Starting in Junos OS Release 13.3, the distribution of adjacency entry (the IP addresses of adjacent routers) and transmit entry (the IP address of transmitting routers) for a BFD session is asymmetric.
13.3	Starting in Junos OS Release 13.3, inline BFD is supported only on static MX Series routers with MPCs/MICs that have configured enhanced-ip.
13.3	Starting with Junos OS Release 13.3, IANA has allocated 01-00-5E-90-00-01 as the dedicated MAC address for micro BFD.
11.2	In Junos OS Release 11.2 and later, BFD supports IPv6 interfaces with BGP.
9.1	In Junos OS Release 9.1 through Junos OS Release 11.1, BFD supports IPv6 interfaces in static routes only.
8.3	In Junos OS Release 8.3 and later, BFD is supported on internal BGP (IBGP) and multihop external BGP (EBGP) sessions as well as on single-hop EBGp sessions.

## CHAPTER 5

# Configuring BFD

**IN THIS CHAPTER**

- [Configuring BFD | 50](#)

## Configuring BFD

**SUMMARY**

Use the following examples to configure Bidirectional Forwarding Detection (BFD) on your device.

**IN THIS SECTION**

- [Example: Configuring BFD for Static Routes for Faster Network Failure Detection | 51](#)
- [Example: Configuring BFD on Internal BGP Peer Sessions | 60](#)
- [Example: Configuring BFD for OSPF | 72](#)
- [Example: Configuring BFD for IS-IS | 78](#)
- [Example: Configuring BFD for RIP | 88](#)
- [Configuring Micro BFD Sessions for LAG | 97](#)
- [Example: Configuring Independent Micro BFD Sessions for LAG | 103](#)
- [Configuring BFD for PIM | 116](#)
- [Enabling Dedicated and Real-Time BFD on SRX Devices | 118](#)

## Example: Configuring BFD for Static Routes for Faster Network Failure Detection

### IN THIS SECTION

- [Requirements | 51](#)
- [Overview | 51](#)
- [Configuration | 52](#)
- [Verification | 57](#)

This example shows how to configure Bidirectional Forwarding Detection (BFD) for static routes.

### Requirements

In this example, no special configuration beyond device initialization is required.

### Overview

### IN THIS SECTION

- [Topology | 52](#)

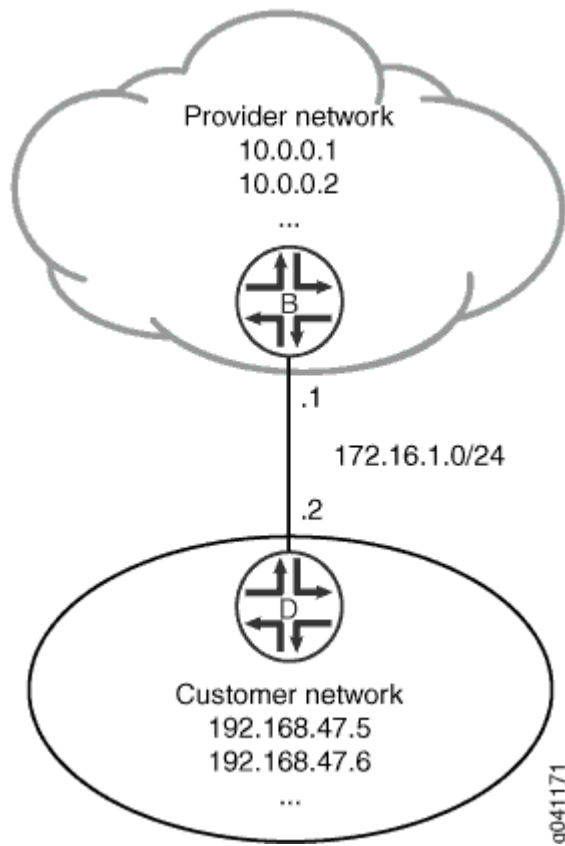
There are many practical applications for static routes. Static routing is often used at the network edge to support attachment to stub networks, which, given their single point of entry and egress, are well suited to the simplicity of a static route. In Junos OS, static routes have a global preference of 5. Static routes are activated if the specified next hop is reachable.

In this example, you configure the static route 192.168.47.0/24 from the provider network to the customer network, using the next-hop address of 172.16.1.2. You also configure a static default route of 0.0.0.0/0 from the customer network to the provider network, using a next-hop address of 172.16.1.1.

For demonstration purposes, some loopback interfaces are configured on Device B and Device D. These loopback interfaces provide addresses to ping and thus verify that the static routes are working.

[Figure 1 on page 52](#) shows the sample network.

Figure 1: Customer Routes Connected to a Service Provider



### Topology

### Configuration

#### IN THIS SECTION

- [CLI Quick Configuration | 53](#)
- [Procedure | 53](#)
- [Results | 55](#)

## CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the [edit] hierarchy level.

### Device B

```
set interfaces ge-1/2/0 unit 0 description B->D
set interfaces ge-1/2/0 unit 0 family inet address 172.16.1.1/24
set interfaces lo0 unit 57 family inet address 10.0.0.1/32
set interfaces lo0 unit 57 family inet address 10.0.0.2/32
set routing-options static route 192.168.47.0/24 next-hop 172.16.1.2
set routing-options static route 192.168.47.0/24 bfd-liveness-detection minimum-interval 1000
set routing-options static route 192.168.47.0/24 bfd-liveness-detection description Site-xxx
set protocols bfd traceoptions file bfd-trace
set protocols bfd traceoptions flag all
```

### Device D

```
set interfaces ge-1/2/0 unit 1 description D->B
set interfaces ge-1/2/0 unit 1 family inet address 172.16.1.2/24
set interfaces lo0 unit 2 family inet address 192.168.47.5/32
set interfaces lo0 unit 2 family inet address 192.168.47.6/32
set routing-options static route 0.0.0.0/0 next-hop 172.16.1.1
set routing-options static route 0.0.0.0/0 bfd-liveness-detection minimum-interval 1000
set protocols bfd traceoptions file bfd-trace
set protocols bfd traceoptions flag all
```

## Procedure

### Step-by-Step Procedure

The following example requires that you navigate various levels in the configuration hierarchy. For information about navigating the CLI, see [Using the CLI Editor in Configuration Mode](#) in the [Junos OS CLI User Guide](#).

To configure BFD for static routes:

1. On Device B, configure the interfaces.

```
[edit interfaces]
user@B# set ge-1/2/0 unit 0 description B->D
user@B# set ge-1/2/0 unit 0 family inet address 172.16.1.1/24
user@B# set lo0 unit 57 family inet address 10.0.0.1/32
user@B# set lo0 unit 57 family inet address 10.0.0.2/32
```

2. On Device B, create a static route and set the next-hop address.

```
[edit routing-options]
user@B# set static route 192.168.47.0/24 next-hop 172.16.1.2
```

3. On Device B, configure BFD for the static route.

```
[edit routing-options]
user@B# set static route 192.168.47.0/24 bfd-liveness-detection minimum-interval 1000
set routing-options static route 192.168.47.0/24 bfd-liveness-detection description Site-xxx
```

4. On Device B, configure tracing operations for BFD.

```
[edit protocols]
user@B# set bfd traceoptions file bfd-trace
user@B# set bfd traceoptions flag all
```

5. If you are done configuring Device B, commit the configuration.

```
[edit]
user@B# commit
```

6. On Device D, configure the interfaces.

```
[edit interfaces]
user@D# set ge-1/2/0 unit 1 description D->B
user@D# set ge-1/2/0 unit 1 family inet address 172.16.1.2/24
```



```
user@D# set lo0 unit 2 family inet address 192.168.47.5/32
user@D# set lo0 unit 2 family inet address 192.168.47.6/32
```

7. On Device D, create a static route and set the next-hop address.

```
[edit routing-options]
user@D# set static route 0.0.0.0/0 next-hop 172.16.1.1
```

8. On Device D, configure BFD for the static route.

```
[edit routing-options]
user@D# set static route 0.0.0.0/0 bfd-liveness-detection minimum-interval 1000
```

9. On Device D, configure tracing operations for BFD.

```
[edit protocols]
user@D# set bfd traceoptions file bfd-trace
user@D# set bfd traceoptions flag all
```

10. If you are done configuring Device D, commit the configuration.

```
[edit]
user@D# commit
```

## Results

Confirm your configuration by issuing the `show interfaces`, `show protocols`, and `show routing-options` commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

## Device B

```
user@B# show interfaces
ge-1/2/0 {
  unit 0 {
    description B->D;
    family inet {
      address 172.16.1.1/24;
```

```

    }
  }
}
lo0 {
  unit 57 {
    family inet {
      address 10.0.0.1/32;
      address 10.0.0.2/32;
    }
  }
}
}

```

```
user@D# show protocols
```

```

bfd {
  traceoptions {
    file bfd-trace;
    flag all;
  }
}

```

```
user@B# show routing-options
```

```

static {
  route 192.168.47.0/24 {
    next-hop 172.16.1.2;
    bfd-liveness-detection {
      description Site- xxx;
      minimum-interval 1000;
    }
  }
}
}

```

## Device D

```
user@D# show interfaces
```

```

ge-1/2/0 {
  unit 1 {
    description D->B;
    family inet {
      address 172.16.1.2/24;
    }
  }
}

```

```

    }
  }
}
lo0 {
  unit 2 {
    family inet {
      address 192.168.47.5/32;
      address 192.168.47.6/32;
    }
  }
}
}

```

```

user@D# show routing-options
static {
  route 0.0.0.0/0 {
    next-hop 172.16.1.1;
    bfd-liveness-detection {
      description Site - xxx;
      minimum-interval 1000;
    }
  }
}

```

## Verification

### IN THIS SECTION

- [Verifying That BFD Sessions Are Up | 57](#)
- [Viewing Detailed BFD Events | 59](#)

Confirm that the configuration is working properly.

### *Verifying That BFD Sessions Are Up*

## Purpose

Verify that the BFD sessions are up, and view details about the BFD sessions.

## Action

From operational mode, enter the `show bfd session` extensive command.

```
user@B> show bfd session extensive
```

Address	State	Interface	Detect Time	Transmit Interval	Multiplier
172.16.1.2	Up	lt-1/2/0.0	3.000	1.000	3

Client Static, description Site-xxx, TX interval 1.000, RX interval 1.000  
 Session up time 00:14:30  
 Local diagnostic None, remote diagnostic None  
 Remote state Up, version 1  
 Replicated, routing table index 172  
 Min async interval 1.000, min slow interval 1.000  
 Adaptive async TX interval 1.000, RX interval 1.000  
 Local min TX interval 1.000, minimum RX interval 1.000, multiplier 3  
 Remote min TX interval 1.000, min RX interval 1.000, multiplier 3  
 Local discriminator 2, remote discriminator 1  
 Echo mode disabled/inactive

1 sessions, 1 clients  
 Cumulative transmit rate 1.0 pps, cumulative receive rate 1.0 pps

**NOTE:** The **description Site- <xxx>** is supported only on the SRX Series devices.

If each client has more than one description field, then it displays "and more" along with the first description field.

```
user@D> show bfd session extensive
```

Address	State	Interface	Detect Time	Transmit Interval	Multiplier
172.16.1.1	Up	lt-1/2/0.1	3.000	1.000	3

Client Static, TX interval 1.000, RX interval 1.000  
 Session up time 00:14:35  
 Local diagnostic None, remote diagnostic None  
 Remote state Up, version 1  
 Replicated, routing table index 170  
 Min async interval 1.000, min slow interval 1.000  
 Adaptive async TX interval 1.000, RX interval 1.000  
 Local min TX interval 1.000, minimum RX interval 1.000, multiplier 3

```
Remote min TX interval 1.000, min RX interval 1.000, multiplier 3
Local discriminator 1, remote discriminator 2
Echo mode disabled/inactive
```

```
1 sessions, 1 clients
```

```
Cumulative transmit rate 1.0 pps, cumulative receive rate 1.0 pps
```

## Meaning

The TX interval 1.000, RX interval 1.000 output represents the setting configured with the `minimum-interval` statement. All of the other output represents the default settings for BFD. To modify the default settings, include the optional statements under the `bfd-liveness-detection` statement.

### *Viewing Detailed BFD Events*

## Purpose

View the contents of the BFD trace file to assist in troubleshooting, if needed.

## Action

From operational mode, enter the file `show /var/log/bfd-trace` command.

```
user@B> file show /var/log/bfd-trace
Nov 23 14:26:55    Data (9) len 35: (hex) 42 46 44 20 70 65 72 69 6f 64 69 63 20 78 6d 69 74 20
72
Nov 23 14:26:55 PPM Trace: BFD periodic xmit rt tbl index 172
Nov 23 14:26:55 Received Downstream TraceMsg (22) len 108:
Nov 23 14:26:55    IfIndex (3) len 4: 0
Nov 23 14:26:55    Protocol (1) len 1: BFD
Nov 23 14:26:55    Data (9) len 83: (hex) 70 70 6d 64 5f 62 66 64 5f 73 65 6e 64 6d 73 67 20 3a
20
Nov 23 14:26:55 PPM Trace: ppmd_bfd_sendmsg : socket 12 len 24, ifl 78 src 172.16.1.1 dst
172.16.1.2 errno 65
Nov 23 14:26:55 Received Downstream TraceMsg (22) len 93:
Nov 23 14:26:55    IfIndex (3) len 4: 0
Nov 23 14:26:55    Protocol (1) len 1: BFD
Nov 23 14:26:55    Data (9) len 68: (hex) 42 46 44 20 70 65 72 69 6f 64 69 63 20 78 6d 69 74 20
74
```

## Meaning

BFD messages are being written to the trace file.

## Example: Configuring BFD on Internal BGP Peer Sessions

### IN THIS SECTION

- [Requirements | 60](#)
- [Overview | 60](#)
- [Configuration | 62](#)
- [Verification | 68](#)

This example shows how to configure internal BGP (IBGP) peer sessions with the Bidirectional Forwarding Detection (BFD) protocol to detect failures in a network.

### Requirements

No special configuration beyond device initialization is required before you configure this example.

### Overview

The minimum configuration to enable BFD on IBGP sessions is to include the [bfd-liveness-detection](#) `minimum-interval` statement in the BGP configuration of all neighbors participating in the BFD session. The `minimum-interval` statement specifies the minimum transmit and receive intervals for failure detection. Specifically, this value represents the minimum interval after which the local routing device transmits hello packets as well as the minimum interval that the routing device expects to receive a reply from a neighbor with which it has established a BFD session. You can configure a value from 1 through 255,000 milliseconds.

Optionally, you can specify the minimum transmit and receive intervals separately using the `transmit-interval` `minimum-interval` and `minimum-receive-interval` statements. For information about these and other optional BFD configuration statements, see [bfd-liveness-detection](#).

**NOTE:** BFD is an intensive protocol that consumes system resources. Specifying a minimum interval for BFD less than 100 milliseconds for Routing Engine-based sessions and less than 10 milliseconds for distributed BFD sessions can cause undesired BFD flapping.

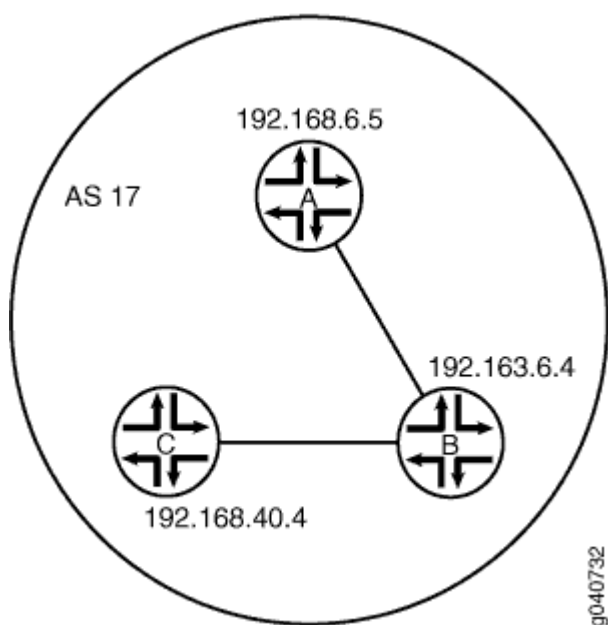
Depending on your network environment, these additional recommendations might apply:

- To prevent BFD flapping during the general Routing Engine switchover event, specify a minimum interval of 5000 milliseconds for Routing Engine-based sessions. This minimum value is required because, during the general Routing Engine switchover event, processes such as RPD, MIBD, and SNMPD utilize CPU resources for more than the specified threshold value. Hence, BFD processing and scheduling is affected because of this lack of CPU resources.
- For BFD sessions to remain up during the dual chassis cluster control link scenario, when the first control link fails, specify the minimum interval of 6000 milliseconds to prevent the LACP from flapping on the secondary node for Routing Engine-based sessions.
- For large-scale network deployments with a large number of BFD sessions, specify a minimum interval of 300 milliseconds for Routing Engine-based sessions and 100 milliseconds for distributed BFD sessions.
- For very large-scale network deployments with a large number of BFD sessions, contact Juniper Networks customer support for more information.
- For BFD sessions to remain up during a Routing Engine switchover event when nonstop active routing (NSR) is configured, specify a minimum interval of 2500 milliseconds for Routing Engine-based sessions. For distributed BFD sessions with NSR configured, the minimum interval recommendations are unchanged and depend only on your network deployment.

BFD is supported on the default routing instance (the main router), routing instances, and logical systems. This example shows BFD on logical systems.

[Figure 2 on page 62](#) shows a typical network with internal peer sessions.

Figure 2: Typical Network with IBGP Sessions



## Configuration

### IN THIS SECTION

- [CLI Quick Configuration | 62](#)
- [Configuring Device A | 64](#)

### CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the [edit] hierarchy level.

#### Device A

```
set logical-systems A interfaces lt-1/2/0 unit 1 description to-B
set logical-systems A interfaces lt-1/2/0 unit 1 encapsulation ethernet
set logical-systems A interfaces lt-1/2/0 unit 1 peer-unit 2
set logical-systems A interfaces lt-1/2/0 unit 1 family inet address 10.10.10.1/30
set logical-systems A interfaces lo0 unit 1 family inet address 192.168.6.5/32
```



```

set logical-systems A protocols bgp group internal-peers type internal
set logical-systems A protocols bgp group internal-peers traceoptions file bgp-bfd
set logical-systems A protocols bgp group internal-peers traceoptions flag bfd detail
set logical-systems A protocols bgp group internal-peers local-address 192.168.6.5
set logical-systems A protocols bgp group internal-peers export send-direct
set logical-systems A protocols bgp group internal-peers bfd-liveness-detection minimum-interval
1000
set logical-systems A protocols bgp group internal-peers neighbor 192.163.6.4
set logical-systems A protocols bgp group internal-peers neighbor 192.168.40.4
set logical-systems A protocols ospf area 0.0.0.0 interface lo0.1 passive
set logical-systems A protocols ospf area 0.0.0.0 interface lt-1/2/0.1
set logical-systems A policy-options policy-statement send-direct term 2 from protocol direct
set logical-systems A policy-options policy-statement send-direct term 2 then accept
set logical-systems A routing-options router-id 192.168.6.5
set logical-systems A routing-options autonomous-system 17

```

## Device B

```

set logical-systems B interfaces lt-1/2/0 unit 2 description to-A
set logical-systems B interfaces lt-1/2/0 unit 2 encapsulation ethernet
set logical-systems B interfaces lt-1/2/0 unit 2 peer-unit 1
set logical-systems B interfaces lt-1/2/0 unit 2 family inet address 10.10.10.2/30
set logical-systems B interfaces lt-1/2/0 unit 5 description to-C
set logical-systems B interfaces lt-1/2/0 unit 5 encapsulation ethernet
set logical-systems B interfaces lt-1/2/0 unit 5 peer-unit 6
set logical-systems B interfaces lt-1/2/0 unit 5 family inet address 10.10.10.5/30
set logical-systems B interfaces lo0 unit 2 family inet address 192.163.6.4/32
set logical-systems B protocols bgp group internal-peers type internal
set logical-systems B protocols bgp group internal-peers local-address 192.163.6.4
set logical-systems B protocols bgp group internal-peers export send-direct
set logical-systems B protocols bgp group internal-peers bfd-liveness-detection minimum-interval
1000
set logical-systems B protocols bgp group internal-peers neighbor 192.168.40.4
set logical-systems B protocols bgp group internal-peers neighbor 192.168.6.5
set logical-systems B protocols ospf area 0.0.0.0 interface lo0.2 passive
set logical-systems B protocols ospf area 0.0.0.0 interface lt-1/2/0.2
set logical-systems B protocols ospf area 0.0.0.0 interface lt-1/2/0.5
set logical-systems B policy-options policy-statement send-direct term 2 from protocol direct
set logical-systems B policy-options policy-statement send-direct term 2 then accept
set logical-systems B routing-options router-id 192.163.6.4
set logical-systems B routing-options autonomous-system 17

```

## Device C

```

set logical-systems C interfaces lt-1/2/0 unit 6 description to-B
set logical-systems C interfaces lt-1/2/0 unit 6 encapsulation ethernet
set logical-systems C interfaces lt-1/2/0 unit 6 peer-unit 5
set logical-systems C interfaces lt-1/2/0 unit 6 family inet address 10.10.10.6/30
set logical-systems C interfaces lo0 unit 3 family inet address 192.168.40.4/32
set logical-systems C protocols bgp group internal-peers type internal
set logical-systems C protocols bgp group internal-peers local-address 192.168.40.4
set logical-systems C protocols bgp group internal-peers export send-direct
set logical-systems C protocols bgp group internal-peers bfd-liveness-detection minimum-interval
1000
set logical-systems C protocols bgp group internal-peers neighbor 192.163.6.4
set logical-systems C protocols bgp group internal-peers neighbor 192.168.6.5
set logical-systems C protocols ospf area 0.0.0.0 interface lo0.3 passive
set logical-systems C protocols ospf area 0.0.0.0 interface lt-1/2/0.6
set logical-systems C policy-options policy-statement send-direct term 2 from protocol direct
set logical-systems C policy-options policy-statement send-direct term 2 then accept
set logical-systems C routing-options router-id 192.168.40.4
set logical-systems C routing-options autonomous-system 17

```

## Configuring Device A

### Step-by-Step Procedure

The following example requires that you navigate various levels in the configuration hierarchy. For information about navigating the CLI, see [Using the CLI Editor in Configuration Mode](#) in the [CLI User Guide](#).

To configure Device A:

1. Set the CLI to Logical System A.

```
user@host> set cli logical-system A
```

2. Configure the interfaces.

```

[edit interfaces lt-1/2/0 unit 1]
user@host:A# set description to-B
user@host:A# set encapsulation ethernet

```

```

user@host:A# set peer-unit 2
user@host:A# set family inet address 10.10.10.1/30
[edit interfaces lo0 unit 1]
user@host:A# set family inet address 192.168.6.5/32

```

### 3. Configure BGP.

The neighbor statements are included for both Device B and Device C, even though Device A is not directly connected to Device C.

```

[edit protocols bgp group internal-peers]
user@host:A# set type internal
user@host:A# set local-address 192.168.6.5
user@host:A# set export send-direct
user@host:A# set neighbor 192.163.6.4
user@host:A# set neighbor 192.168.40.4

```

### 4. Configure BFD.

```

[edit protocols bgp group internal-peers]
user@host:A# set bfd-liveness-detection minimum-interval 1000

```

You must configure the same minimum interval on the connecting peer.

### 5. (Optional) Configure BFD tracing.

```

[edit protocols bgp group internal-peers]
user@host:A# set traceoptions file bgp-bfd
user@host:A# set traceoptions flag bfd detail

```

### 6. Configure OSPF.

```

[edit protocols ospf area 0.0.0.0]
user@host:A# set interface lo0.1 passive
user@host:A# set interface lt-1/2/0.1

```

### 7. Configure a policy that accepts direct routes.

Other useful options for this scenario might be to accept routes learned through OSPF or local routes.

```
[edit policy-options policy-statement send-direct term 2]
user@host:A# set from protocol direct
user@host:A# set then accept
```

**8. Configure the router ID and the autonomous system (AS) number.**

```
[edit routing-options]
user@host:A# set router-id 192.168.6.5
user@host:A# set autonomous-system 17
```

**9. If you are done configuring the device, enter `commit` from configuration mode.**  
Repeat these steps to configure Device B and Device C.

## Results

From configuration mode, confirm your configuration by entering the `show interfaces`, `show policy-options`, `show protocols`, and `show routing-options` commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@host:A# show interfaces
lt-1/2/0 {
  unit 1 {
    description to-B;
    encapsulation ethernet;
    peer-unit 2;
    family inet {
      address 10.10.10.1/30;
    }
  }
}
lo0 {
  unit 1 {
    family inet {
      address 192.168.6.5/32;
    }
  }
}
```

```
    }
}
```

```
user@host:A# show policy-options
policy-statement send-direct {
    term 2 {
        from protocol direct;
        then accept;
    }
}
```

```
user@host:A# show protocols
bgp {
    group internal-peers {
        type internal;
        traceoptions {
            file bgp-bfd;
            flag bfd detail;
        }
        local-address 192.168.6.5;
        export send-direct;
        bfd-liveness-detection {
            minimum-interval 1000;
        }
        neighbor 192.163.6.4;
        neighbor 192.168.40.4;
    }
}
ospf {
    area 0.0.0.0 {
        interface lo0.1 {
            passive;
        }
        interface lt-1/2/0.1;
```

```
}
}
```

```
user@host:A# show routing-options
router-id 192.168.6.5;
autonomous-system 17;
```

## Verification

### IN THIS SECTION

- [Verifying That BFD Is Enabled | 68](#)
- [Verifying That BFD Sessions Are Up | 69](#)
- [Viewing Detailed BFD Events | 70](#)
- [Viewing Detailed BFD Events After Deactivating and Reactivating a Loopback Interface | 71](#)

Confirm that the configuration is working properly.

### *Verifying That BFD Is Enabled*

## Purpose

Verify that BFD is enabled between the IBGP peers.

## Action

From operational mode, enter the `show bgp neighbor` command. You can use the `| match bfd` filter to narrow the output.

```
user@host:A> show bgp neighbor | match bfd
Options: <BfdEnabled>
  BFD: enabled, up
  Trace file: /var/log/A/bgp-bfd size 131072 files 10
Options: <BfdEnabled>
```

```
BFD: enabled, up
Trace file: /var/log/A/bgp-bfd size 131072 files 10
```

## Meaning

The output shows that Logical System A has two neighbors with BFD enabled. When BFD is not enabled, the output displays BFD: disabled, down, and the <BfdEnabled> option is absent. If BFD is enabled and the session is down, the output displays BFD: enabled, down. The output also shows that BFD-related events are being written to a log file because trace operations are configured.

## Verifying That BFD Sessions Are Up

### Purpose

Verify that the BFD sessions are up, and view details about the BFD sessions.

### Action

From operational mode, enter the `show bfd session extensive` command.

```
user@host:A> show bfd session extensive
```

Address	State	Interface	Detect Time	Transmit Interval	Multiplier
192.163.6.4	Up		3.000	1.000	3

```
Client BGP, TX interval 1.000, RX interval 1.000
Session up time 00:54:40
Local diagnostic None, remote diagnostic None
Remote state Up, version 1
Logical system 12, routing table index 25
Min async interval 1.000, min slow interval 1.000
Adaptive async TX interval 1.000, RX interval 1.000
Local min TX interval 1.000, minimum RX interval 1.000, multiplier 3
Remote min TX interval 1.000, min RX interval 1.000, multiplier 3
Local discriminator 10, remote discriminator 9
Echo mode disabled/inactive
Multi-hop route table 25, local-address 192.168.6.5
```

Address	State	Interface	Detect Time	Transmit Interval	Multiplier
192.168.40.4	Up		3.000	1.000	3

```
Client BGP, TX interval 1.000, RX interval 1.000
```

```

Session up time 00:48:03
Local diagnostic None, remote diagnostic None
Remote state Up, version 1
Logical system 12, routing table index 25
Min async interval 1.000, min slow interval 1.000
Adaptive async TX interval 1.000, RX interval 1.000
Local min TX interval 1.000, minimum RX interval 1.000, multiplier 3
Remote min TX interval 1.000, min RX interval 1.000, multiplier 3
Local discriminator 14, remote discriminator 13
Echo mode disabled/inactive
Multi-hop route table 25, local-address 192.168.6.5

2 sessions, 2 clients
Cumulative transmit rate 2.0 pps, cumulative receive rate 2.0 pps

```

## Meaning

The TX interval 1.000, RX interval 1.000 output represents the setting configured with the `minimum-interval` statement. All of the other output represents the default settings for BFD. To modify the default settings, include the optional statements under the `bfd-liveness-detection` statement.

### *Viewing Detailed BFD Events*

## Purpose

View the contents of the BFD trace file to assist in troubleshooting, if needed.

## Action

From operational mode, enter the file `show /var/log/A/bgp-bfd` command.

```

user@host:A> file show /var/log/A/bgp-bfd
Aug 15 17:07:25 trace_on: Tracing to "/var/log/A/bgp-bfd" started
Aug 15 17:07:26.492190 bgp_peer_init: BGP peer 192.163.6.4 (Internal AS 17) local address
192.168.6.5 not found. Leaving peer idled
Aug 15 17:07:26.493176 bgp_peer_init: BGP peer 192.168.40.4 (Internal AS 17) local address
192.168.6.5 not found. Leaving peer idled
Aug 15 17:07:32.597979 task_connect: task BGP_17.192.163.6.4+179 addr 192.163.6.4+179: No route
to host
Aug 15 17:07:32.599623 bgp_connect_start: connect 192.163.6.4 (Internal AS 17): No route to host
Aug 15 17:07:36.869394 task_connect: task BGP_17.192.168.40.4+179 addr 192.168.40.4+179: No

```



```

route to host
Aug 15 17:07:36.870624 bgp_connect_start: connect 192.168.40.4 (Internal AS 17): No route to host
Aug 15 17:08:04.599220 task_connect: task BGP_17.192.163.6.4+179 addr 192.163.6.4+179: No route
to host
Aug 15 17:08:04.601135 bgp_connect_start: connect 192.163.6.4 (Internal AS 17): No route to host
Aug 15 17:08:08.869717 task_connect: task BGP_17.192.168.40.4+179 addr 192.168.40.4+179: No
route to host
Aug 15 17:08:08.869934 bgp_connect_start: connect 192.168.40.4 (Internal AS 17): No route to host
Aug 15 17:08:36.603544 advertising receiving-speaker only capabilty to neighbor 192.163.6.4
(Internal AS 17)
Aug 15 17:08:36.606726 bgp_read_message: 192.163.6.4 (Internal AS 17): 0 bytes buffered
Aug 15 17:08:36.609119 Initiated BFD session to peer 192.163.6.4 (Internal AS 17):
address=192.163.6.4 ifindex=0 ifname=(none) txivl=1000 rxivl=1000 mult=3 ver=255
Aug 15 17:08:36.734033 advertising receiving-speaker only capabilty to neighbor 192.168.40.4
(Internal AS 17)
Aug 15 17:08:36.738436 Initiated BFD session to peer 192.168.40.4 (Internal AS 17):
address=192.168.40.4 ifindex=0 ifname=(none) txivl=1000 rxivl=1000 mult=3 ver=255
Aug 15 17:08:40.537552 BFD session to peer 192.163.6.4 (Internal AS 17) up
Aug 15 17:08:40.694410 BFD session to peer 192.168.40.4 (Internal AS 17) up

```

## Meaning

Before the routes are established, the No route to host message appears in the output. After the routes are established, the last two lines show that both BFD sessions come up.

### *Viewing Detailed BFD Events After Deactivating and Reactivating a Loopback Interface*

## Purpose

Check to see what happens after bringing down a router or switch and then bringing it back up. To simulate bringing down a router or switch, deactivate the loopback interface on Logical System B.

## Action

1. From configuration mode, enter the deactivate logical-systems B interfaces lo0 unit 2 family inet command.

```

user@host:A# deactivate logical-systems B interfaces lo0 unit 2 family inet
user@host:A# commit

```

2. From operational mode, enter the file `show /var/log/A/bgp-bfd` command.

```
user@host:A> file show /var/log/A/bgp-bfd
...
Aug 15 17:20:55.995648 bgp_read_v4_message:9747: NOTIFICATION received from 192.163.6.4
(Internal AS 17): code 6 (Cease) subcode 6 (Other Configuration Change)
Aug 15 17:20:56.004508 Terminated BFD session to peer 192.163.6.4 (Internal AS 17)
Aug 15 17:21:28.007755 task_connect: task BGP_17.192.163.6.4+179 addr 192.163.6.4+179: No
route to host
Aug 15 17:21:28.008597 bgp_connect_start: connect 192.163.6.4 (Internal AS 17): No route to
host
```

3. From configuration mode, enter the activate logical-systems B interfaces `lo0` unit 2 family `inet` command.

```
user@host:A# activate logical-systems B interfaces lo0 unit 2 family inet
user@host:A# commit
```

4. From operational mode, enter the file `show /var/log/A/bgp-bfd` command.

```
user@host:A> file show /var/log/A/bgp-bfd
...
Aug 15 17:25:53.623743 advertising receiving-speaker only capability to neighbor 192.163.6.4
(Internal AS 17)
Aug 15 17:25:53.631314 Initiated BFD session to peer 192.163.6.4 (Internal AS 17):
address=192.163.6.4 ifindex=0 ifname=(none) txivl=1000 rxivl=1000 mult=3 ver=255
Aug 15 17:25:57.570932 BFD session to peer 192.163.6.4 (Internal AS 17) up
```

## SEE ALSO

[Example: Configuring BFD Authentication for BGP](#)

## Example: Configuring BFD for OSPF

### IN THIS SECTION

 [Requirements](#) | 73

- Overview | 73
- Configuration | 75
- Verification | 77

This example shows how to configure the Bidirectional Forwarding Detection (BFD) protocol for OSPF.

## Requirements

Before you begin:

- Configure the device interfaces. See the [Junos OS Network Interfaces Library for Routing Devices](#).
- Configure the router identifiers for the devices in your OSPF network. See [Example: Configuring an OSPF Router Identifier](#).
- Control OSPF designated router election. See [Example: Controlling OSPF Designated Router Election](#).
- Configure a single-area OSPF network. See [Example: Configuring a Single-Area OSPF Network](#).
- Configure a multiarea OSPF network. See [Example: Configuring a Multiarea OSPF Network](#).
- Configure a multiarea OSPF network. See [Example: Configuring a Multiarea OSPF Network](#).

## Overview

### IN THIS SECTION

- Topology | 75

An alternative to adjusting the OSPF hello interval and dead interval settings to increase route convergence is to configure BFD. The BFD protocol is a simple hello mechanism that detects failures in a network. The BFD failure detection timers have shorter timer limits than the OSPF failure detection mechanisms, thereby providing faster detection.

BFD is useful on interfaces that are unable to detect failure quickly, such as Ethernet interfaces. Other interfaces, such as SONET interfaces, already have built-in failure detection. Configuring BFD on those interfaces is unnecessary.

You configure BFD on a pair of neighboring OSPF interfaces. Unlike the OSPF hello interval and dead interval settings, you do not have to enable BFD on all interfaces in an OSPF area.

In this example, you enable failure detection by including the `bfd-liveness-detection` statement on the neighbor OSPF interface **fe-0/1/0** in area 0.0.0.0 and configure the BFD packet exchange interval to 300 milliseconds, configure 4 as the number of missed hello packets that causes the originating interface to be declared down, and configure BFD sessions only for OSPF neighbors with full neighbor adjacency by including the following settings:

- **full-neighbors-only**—In Junos OS Release 9.5 and later, configures the BFD protocol to establish BFD sessions only for OSPF neighbors with full neighbor adjacency. The default behavior is to establish BFD sessions for all OSPF neighbors.
- **minimum-interval**—Configures the minimum interval, in milliseconds, after which the local routing device transmits hello packets as well as the minimum interval after which the routing device expects to receive a reply from the neighbor with which it has established a BFD session. You can configure a number in the range from 1 through 255,000 milliseconds. You can also specify the minimum transmit and receive intervals separately using the **transmit-interval** **minimum-interval** and **minimum-receive-interval** statements.

**NOTE:** BFD is an intensive protocol that consumes system resources. Specifying a minimum interval for BFD of less than 100 ms for Routing Engine-based sessions and 10 ms for distributed BFD sessions can cause undesired BFD flapping.

Depending on your network environment, these additional recommendations might apply:

- For large-scale network deployments with a large number of BFD sessions, specify a minimum interval of no less than 500 ms. An interval of 1000 ms is recommended to avoid any instability issues.

**NOTE:**

- For the `bfdd` process, the detection time interval set is lower than 300 ms. If there is a high priority process such as `ppmd` running on the system, the CPU might spend time on the `ppmd` process rather than the `bfdd` process.
- For branch SRX Series devices, we recommend 1000 ms as the minimum keepalive time interval for BFD packets.
- For very large-scale network deployments with a large number of BFD sessions, contact Juniper Networks customer support for more information.

- For BFD sessions to remain up during a Routing Engine switchover event when nonstop active routing (NSR) is configured, specify a minimum interval of 2500 ms for Routing Engine-based sessions. For distributed BFD sessions with NSR configured, the minimum interval recommendations are unchanged and depend only on your network deployment.
- **multiplier**—Configures the number of hello packets not received by a neighbor that causes the originating interface to be declared down. By default, three missed hello packets cause the originating interface to be declared down. You can configure a value in the range from 1 through 255.

### *Topology*

### **Configuration**

#### **IN THIS SECTION**

- [Procedure | 75](#)

### *Procedure*

#### **CLI Quick Configuration**

To quickly configure the BFD protocol for OSPF, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the [edit] hierarchy level, and then enter `commit` from configuration mode.

```
[edit]
set protocols ospf area 0.0.0.0 interface fe-0/0/1 bfd-liveness-detection minimum-interval 300
set protocols ospf area 0.0.0.0 interface fe-0/0/1 bfd-liveness-detection multiplier 4
set protocols ospf area 0.0.0.0 interface fe-0/0/1 bfd-liveness-detection full-neighbors-only
```

### **Step-by-Step Procedure**

To configure the BFD protocol for OSPF on one neighboring interface:

1. Create an OSPF area.

**NOTE:** To specify OSPFv3, include the `ospf3` statement at the `[edit protocols]` hierarchy level.

```
[edit]
user@host# edit protocols ospf area 0.0.0.0
```

2. Specify the interface.

```
[edit protocols ospf area 0.0.0.0]
user@host# set interface fe-0/0/1
```

3. Specify the minimum transmit and receive intervals.

```
[edit protocols ospf area 0.0.0.0 ]
user@host# set interface fe-0/0/1 bfd-liveness-detection minimum-interval 300
```

4. Configure the number of missed hello packets that cause the originating interface to be declared down.

```
[edit protocols ospf area 0.0.0.0 ]
user@host# set interface fe-0/0/1 bfd-liveness-detection multiplier 4
```

5. Configure BFD sessions only for OSPF neighbors with full neighbor adjacency.

```
[edit protocols ospf area 0.0.0.0 ]
user@host# set interface fe-0/0/1 bfd-liveness-detection full-neighbors-only
```

6. If you are done configuring the device, commit the configuration.

```
[edit protocols ospf area 0.0.0.0 ]
user@host# commit
```

**NOTE:** Repeat this entire configuration on the other neighboring interface.

## Results

Confirm your configuration by entering the `show protocols ospf` command. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@host# show protocols ospf
area 0.0.0.0 {
  interface fe-0/0/1.0 {
    bfd-liveness-detection {
      minimum-interval 300;
      multiplier 4;
      full-neighbors-only;
    }
  }
}
```

To confirm your OSPFv3 configuration, enter the `show protocols ospf3` command.

## Verification

### IN THIS SECTION

- [Verifying the BFD Sessions | 77](#)

Confirm that the configuration is working properly.

### *Verifying the BFD Sessions*

#### Purpose

Verify that the OSPF interfaces have active BFD sessions, and that session components have been configured correctly.

#### Action

From operational mode, enter the `show bfd session detail` command.

## Meaning

The output displays information about the BFD sessions.

- The Address field displays the IP address of the neighbor.
- The Interface field displays the interface you configured for BFD.
- The State field displays the state of the neighbor and should show Full to reflect the full neighbor adjacency that you configured.
- The Transmit Interval field displays the time interval you configured to send BFD packets.
- The Multiplier field displays the multiplier you configured.

## Example: Configuring BFD for IS-IS

### IN THIS SECTION

- [Requirements | 78](#)
- [Overview | 79](#)
- [Configuration | 79](#)
- [Verification | 85](#)

This example describes how to configure the Bidirectional Forwarding Detection (BFD) protocol to detect failures in an IS-IS network.

**NOTE:** BFD is not supported with ISIS for IPV6 on QFX10000 series switches.

## Requirements

Before you begin, configure IS-IS on both routers. See [Example: Configuring IS-IS](#) for information about the required IS-IS configuration.

This example uses the following hardware and software components:

- Junos OS Release 7.3 or later
- M Series, MX Series, and T Series routers



## Overview

### IN THIS SECTION

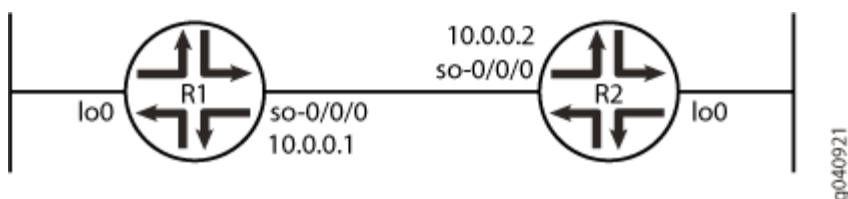
- [Topology | 79](#)

This example shows two routers connected to each other. A loopback interface is configured on each router. IS-IS and BFD protocols are configured on both routers.

### *Topology*

[Figure 3 on page 79](#) shows the sample network.

**Figure 3: Configuring BFD for IS-IS**



## Configuration

### IN THIS SECTION

- [CLI Quick Configuration | 79](#)
- [Procedure | 80](#)
- [Results | 83](#)

### *CLI Quick Configuration*

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the [edit] hierarchy level.

## Router R1

```

set protocols isis interface so-0/0/0 family inet6 bfd-liveness-detection detection-time
threshold 5
set protocols isis interface so-0/0/0 family inet6 bfd-liveness-detection minimum-interval 2
set protocols isis interface so-0/0/0 family inet6 bfd-liveness-detection minimum-receive-
interval 1
set protocols isis interface so-0/0/0 family inet6 bfd-liveness-detection no-adaptation
set protocols isis interface so-0/0/0 family inet6 bfd-liveness-detection transmit-interval
threshold 3
set protocols isis interface so-0/0/0 family inet6 bfd-liveness-detection transmit-interval
minimum-interval 1
set protocols isis interface so-0/0/0 family inet6 bfd-liveness-detection multiplier 2
set protocols isis interface so-0/0/0 family inet6 bfd-liveness-detection version automatic

```

## Router R2

```

set protocols isis interface so-0/0/0 family inet6 bfd-liveness-detection detection-time
threshold 6
set protocols isis interface so-0/0/0 family inet6 bfd-liveness-detection minimum-interval 3
set protocols isis interface so-0/0/0 family inet6 bfd-liveness-detection minimum-receive-
interval 1
set protocols isis interface so-0/0/0 family inet6 bfd-liveness-detection no-adaptation
set protocols isis interface so-0/0/0 family inet6 bfd-liveness-detection transmit-interval
threshold 4
set protocols isis interface so-0/0/0 family inet6 bfd-liveness-detection transmit-interval
minimum-interval 1
set protocols isis interface so-0/0/0 family inet6 bfd-liveness-detection multiplier 2
set protocols isis interface so-0/0/0 family inet6 bfd-liveness-detection version automatic

```

*Procedure***Step-by-Step Procedure**

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see [Using the CLI Editor in Configuration Mode](#).

**NOTE:** To simply configure BFD for IS-IS, only the `minimum-interval` statement is required. The BFD protocol selects default parameters for all the other configuration statements when you use the `bfd-liveness-detection` statement without specifying any parameters.

**NOTE:** You can change parameters at any time without stopping or restarting the existing session. BFD automatically adjusts to the new parameter value. However, no changes to BFD parameters take place until the values resynchronize with each BFD peer.

To configure BFD for IS-IS on Routers R1 and R2:

1. Enable BFD failure detection for IS-IS.

```
[edit protocols isis]
user@R1# set interface so-0/0/0 family inet6 bfd-liveness-detection
```

```
[edit protocols isis]
user@R2# set interface so-0/0/0 family inet6 bfd-liveness-detection
```

2. Configure the threshold for the adaptation of the detection time, which must be greater than the multiplier number multiplied by the minimum interval.

```
[edit protocols isis interface so-0/0/0 family inet6 bfd-liveness-detection]
user@R1# set detection-time threshold 5
```

```
[edit protocols isis interface so-0/0/0 family inet6 bfd-liveness-detection]
user@R2# set detection-time threshold 6
```

3. Configure the minimum transmit and receive intervals for failure detection.

```
[edit protocols isis interface so-0/0/0 family inet6 bfd-liveness-detection]
user@R1# set minimum-interval 2
```

```
[edit protocols isis interface so-0/0/0 family inet6 bfd-liveness-detection]
user@R2# set minimum-interval 3
```

4. Configure only the minimum receive interval for failure detection.

```
[edit protocols isis interface so-0/0/0 family inet6 bfd-liveness-detection]
user@R1# set minimum-receive-interval 1
```

```
[edit protocols isis interface so-0/0/0 family inet6 bfd-liveness-detection]
user@R2# set minimum-receive-interval 1
```

5. Disable BFD adaptation.

```
[edit protocols isis interface so-0/0/0 family inet6 bfd-liveness-detection]
user@R1# set no-adaptation
```

```
[edit protocols isis interface so-0/0/0 family inet6 bfd-liveness-detection]
user@R2# set no-adaptation
```

6. Configure the threshold for the transmit interval, which must be greater than the minimum transmit interval.

```
[edit protocols isis interface so-0/0/0 family inet6 bfd-liveness-detection]
user@R1# set transmit-interval threshold 3
```

```
[edit protocols isis interface so-0/0/0 family inet6 bfd-liveness-detection]
user@R2# set transmit-interval threshold 4
```

7. Configure the minimum transmit interval for failure detection.

```
[edit protocols isis interface so-0/0/0 family inet6 bfd-liveness-detection]
user@R1# set transmit-interval minimum-interval 1
```

```
[edit protocols isis interface so-0/0/0 family inet6 bfd-liveness-detection]
user@R2# set transmit-interval minimum-interval 1
```

8. Configure the multiplier number, which is the number of hello packets not received by the neighbor that causes the originating interface to be declared down.

```
[edit protocols isis interface so-0/0/0 family inet6 bfd-liveness-detection]
user@R1# set multiplier 2
```

```
[edit protocols isis interface so-0/0/0 family inet6 bfd-liveness-detection]
user@R2# set multiplier 2
```

9. Configure the BFD version used for detection.

The default is to have the version detected automatically.

```
[edit protocols isis interface so-0/0/0 family inet6 bfd-liveness-detection]
user@R1# set version automatic
```

```
[edit protocols isis interface so-0/0/0 family inet6 bfd-liveness-detection]
user@R2# set version automatic
```

## Results

From configuration mode, confirm your configuration by issuing the `show protocols isis interface` command. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@R1# show protocols isis interface so-0/0/0 family inet6
```

```

bfd-liveness-detection {
    version automatic;
    minimum-interval 2;
    minimum-receive-interval 1;
    multiplier 2;
    no-adaptation;
    transmit-interval {
        minimum-interval 1;
        threshold 3;
    }
    detection-time {
        threshold 5;
    }
}
...

```

user@R2# **show protocols isis interface so-0/0/0 family inet6**

```

bfd-liveness-detection {
    version automatic;
    minimum-interval 3;
    minimum-receive-interval 1;
    multiplier 2;
    no-adaptation;
    transmit-interval {
        minimum-interval 1;
        threshold 4;
    }
    detection-time {
        threshold 6;
    }
}
...

```

## Verification

### IN THIS SECTION

- [Verifying the Connection Between Routers R1 and R2 | 85](#)
- [Verifying That IS-IS Is Configured | 86](#)
- [Verifying That BFD Is configured | 87](#)

Confirm that the configuration is working properly.

### *Verifying the Connection Between Routers R1 and R2*

#### Purpose

Make sure that Routers R1 and R2 are connected to each other.

#### Action

Ping the other router to check the connectivity between the two routers as per the network topology.

```
user@R1> ping 10.0.0.2
```

```
PING 10.0.0.2 (10.0.0.2): 56 data bytes
64 bytes from 10.0.0.2: icmp_seq=0 ttl=64 time=1.367 ms
64 bytes from 10.0.0.2: icmp_seq=1 ttl=64 time=1.662 ms
64 bytes from 10.0.0.2: icmp_seq=2 ttl=64 time=1.291 ms
^C
--- 10.0.0.2 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max/stddev = 1.291/1.440/1.662/0.160 ms
```

```
user@R2> ping 10.0.0.1
```

```
PING 10.0.0.1 (10.0.0.1): 56 data bytes
64 bytes from 10.0.0.1: icmp_seq=0 ttl=64 time=1.287 ms
64 bytes from 10.0.0.1: icmp_seq=1 ttl=64 time=1.310 ms
```

```
64 bytes from 10.0.0.1: icmp_seq=2 ttl=64 time=1.289 ms
^C
--- 10.0.0.1 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max/stddev = 1.287/1.295/1.310/0.010 ms
```

## Meaning

Routers R1 and R2 are connected to each other.

## *Verifying That IS-IS Is Configured*

### Purpose

Make sure that the IS-IS instance is running on both routers.

### Action

Use the `show isis database` statement to check if the IS-IS instance is running on both routers, R1 and R2.

```
user@R1> show isis database
```

```
IS-IS level 1 link-state database:
```

LSP ID	Sequence	Checksum	Lifetime	Attributes
R1.00-00	0x4a571	0x30c5	1195	L1 L2
R2.00-00	0x4a586	0x4b7e	1195	L1 L2
R2.02-00	0x330ca1	0x3492	1196	L1 L2

3 LSPs

```
IS-IS level 2 link-state database:
```

LSP ID	Sequence	Checksum	Lifetime	Attributes
R1.00-00	0x4a856	0x5db0	1194	L1 L2
R2.00-00	0x4a89d	0x149b	1194	L1 L2
R2.02-00	0x1fb2ff	0xd302	1194	L1 L2

3 LSPs

```
user@R2> show isis database
```

```
IS-IS level 1 link-state database:
```



```

LSP ID          Sequence Checksum Lifetime Attributes
R1.00-00        0x4b707  0xcc80    1195 L1 L2
R2.00-00        0x4b71b  0xeb37    1198 L1 L2
R2.02-00        0x33c2ce 0xb52d    1198 L1 L2
  3 LSPs

```

IS-IS level 2 link-state database:

```

LSP ID          Sequence Checksum Lifetime Attributes
R1.00-00        0x4b9f2  0xee70    1192 L1 L2
R2.00-00        0x4ba41  0x9862    1197 L1 L2
R2.02-00        0x3    0x6242    1198 L1 L2
  3 LSPs

```

## Meaning

IS-IS is configured on both routers, R1 and R2.

### *Verifying That BFD Is configured*

## Purpose

Make sure that the BFD instance is running on both routers, R1 and R2.

## Action

Use the `show bfd session detail` statement to check if BFD instance is running on the routers.

```

user@R1> show bfd session detail

Address          State   Interface   Detect   Transmit
                Up      so-0/0/0    Time    Interval Multiplier
10.0.0.2         Up      so-0/0/0    2.000   1.000    2
Client ISIS R2, TX interval 0.001, RX interval 0.001
Client ISIS R1, TX interval 0.001, RX interval 0.001
Session down time 00:00:00, previous up time 00:00:15
Local diagnostic NbrSignal, remote diagnostic NbrSignal
Remote state AdminDown, version 1
Router 3, routing table index 17

```

```
1 sessions, 2 clients
Cumulative transmit rate 1.0 pps, cumulative receive rate 1.0 pps

user@R2> show bfd session detail

Address          State   Interface   Detect   Transmit
                Time    Interval    Multiplier
10.0.0.1         Up      so-0/0/0    2.000   1.000     2
Client ISIS R2, TX interval 0.001, RX interval 0.001
Session down time 00:00:00, previous up time 00:00:05
Local diagnostic NbrSignal, remote diagnostic NbrSignal
Remote state AdminDown, version 1
Router 2, routing table index 15

1 sessions, 1 clients
Cumulative transmit rate 1.0 pps, cumulative receive rate 1.0 pps
```

Meaning

BFD is configured on Routers R1 and R2 for detecting failures in the IS-IS network.

SEE ALSO

| [Understanding BFD for IS-IS](#)

Example: Configuring BFD for RIP

IN THIS SECTION

- [Requirements | 89](#)
- [Overview | 89](#)
- [Configuration | 91](#)
- [Verification | 95](#)

This example shows how to configure Bidirectional Forwarding Detection (BFD) for a RIP network.

## Requirements

No special configuration beyond device initialization is required before configuring this example.

## Overview

### IN THIS SECTION

- [Topology | 91](#)

To enable failure detection, include the `bfd-liveness-detection` statement:

```
bfd-liveness-detection {  
    detection-time {  
        threshold milliseconds;  
    }  
    minimum-interval milliseconds;  
    minimum-receive-interval milliseconds;  
    multiplier number;  
    no-adaptation;  
    transmit-interval {  
        threshold milliseconds;  
        minimum-interval milliseconds;  
    }  
    version (1 | automatic);  
}
```

Optionally, you can specify the threshold for the adaptation of the detection time by including the `threshold` statement. When the BFD session detection time adapts to a value equal to or greater than the threshold, a single trap and a system log message are sent.

To specify the minimum transmit and receive interval for failure detection, include the `minimum-interval` statement. This value represents the minimum interval at which the local routing device transmits hello packets as well as the minimum interval at which the routing device expects to receive a reply from a neighbor with which it has established a BFD session. You can configure a value in the range from 1 through 255,000 milliseconds. This examples sets a minimum interval of 600 milliseconds.

**NOTE:** BFD is an intensive protocol that consumes system resources. Specifying a minimum interval for BFD of less than 100 ms for Routing Engine-based sessions and 10 ms for distributed BFD sessions can cause undesired BFD flapping.

Depending on your network environment, these additional recommendations might apply:

- For large-scale network deployments with a large number of BFD sessions, specify a minimum interval of 300 ms for Routing Engine-based sessions and 100 ms for distributed BFD sessions.
- For very large-scale network deployments with a large number of BFD sessions, contact Juniper Networks customer support for more information.
- For BFD sessions to remain up during a Routing Engine switchover event when nonstop active routing (NSR) is configured, specify a minimum interval of 2500 ms for Routing Engine-based sessions. For distributed BFD sessions with nonstop active routing configured, the minimum interval recommendations are unchanged and depend only on your network deployment.

You can optionally specify the minimum transmit and receive intervals separately.

To specify only the minimum receive interval for failure detection, include the `minimum-receive-interval` statement. This value represents the minimum interval at which the local routing device expects to receive a reply from a neighbor with which it has established a BFD session. You can configure a value in the range from 1 through 255,00 milliseconds.

To specify only the minimum transmit interval for failure detection, include the `transmit-interval minimum-interval` statement. This value represents the minimum interval at which the local routing device transmits hello packets to the neighbor with which it has established a BFD session. You can configure a value in the range from 1 through 255,000 milliseconds.

To specify the number of hello packets not received by a neighbor that causes the originating interface to be declared down, include the `multiplier` statement. The default is 3, and you can configure a value in the range from 1 through 255.

To specify the threshold for detecting the adaptation of the transmit interval, include the `transmit-interval threshold` statement. The threshold value must be greater than the transmit interval.

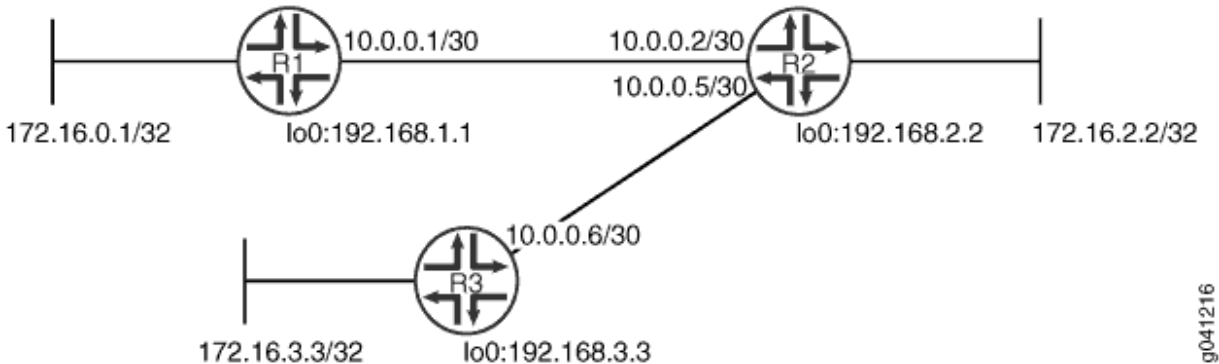
To specify the BFD version used for detection, include the `version` statement. The default is to have the version detected automatically.

You can trace BFD operations by including the `traceoptions` statement at the `[edit protocols bfd]` hierarchy level.

In Junos OS Release 9.0 and later, you can configure BFD sessions not to adapt to changing network conditions. To disable BFD adaptation, include the `no-adaptation` statement. We recommend that you not disable BFD adaptation unless it is preferable not to have BFD adaptation enabled in your network.

[Figure 4 on page 91](#) shows the topology used in this example.

**Figure 4: RIP BFD Network Topology**



"[CLI Quick Configuration](#)" on [page 91](#) shows the configuration for all of the devices in [Figure 4 on page 91](#). The section "[Step-by-Step Procedure](#)" on [page 92](#) describes the steps on Device R1.

### Topology

### Configuration

IN THIS SECTION

- [Procedure | 91](#)

### Procedure

### CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the `[edit]` hierarchy level.

## Device R1

```
set interfaces fe-1/2/0 unit 1 family inet address 10.0.0.1/30
set protocols bfd traceoptions file bfd-trace
set protocols bfd traceoptions flag all
set protocols rip group rip-group export advertise-routes-through-rip
set protocols rip group rip-group neighbor fe-1/2/0.1
set protocols rip group rip-group bfd-liveness-detection minimum-interval 600
set policy-options policy-statement advertise-routes-through-rip term 1 from protocol direct
set policy-options policy-statement advertise-routes-through-rip term 1 from protocol rip
set policy-options policy-statement advertise-routes-through-rip term 1 then accept
```

## Device R2

```
set interfaces fe-1/2/0 unit 2 family inet address 10.0.0.2/30
set interfaces fe-1/2/1 unit 5 family inet address 10.0.0.5/30
set protocols rip group rip-group export advertise-routes-through-rip
set protocols rip group rip-group neighbor fe-1/2/0.2
set protocols rip group rip-group neighbor fe-1/2/1.5
set protocols rip group rip-group bfd-liveness-detection minimum-interval 600
set policy-options policy-statement advertise-routes-through-rip term 1 from protocol direct
set policy-options policy-statement advertise-routes-through-rip term 1 from protocol rip
set policy-options policy-statement advertise-routes-through-rip term 1 then accept
```

## Device R3

```
set interfaces fe-1/2/0 unit 6 family inet address 10.0.0.6/30
set protocols rip group rip-group export advertise-routes-through-rip
set protocols rip group rip-group neighbor fe-1/2/0.6
set protocols rip group rip-group bfd-liveness-detection minimum-interval 600
set policy-options policy-statement advertise-routes-through-rip term 1 from protocol direct
set policy-options policy-statement advertise-routes-through-rip term 1 from protocol rip
set policy-options policy-statement advertise-routes-through-rip term 1 then accept
```

## Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see [Using the CLI Editor in Configuration Mode](#) in the [CLI User Guide](#).

To configure a BFD for a RIP network:

1. Configure the network interfaces.

```
[edit interfaces]
user@R1# set fe-1/2/0 unit 1 family inet address 10.0.0.1/30
```

2. Create the RIP group and add the interface.

To configure RIP in Junos OS, you must configure a group that contains the interfaces on which RIP is enabled. You do not need to enable RIP on the loopback interface.

```
[edit protocols rip group rip-group]
user@R1# set neighbor fe-1/2/0.1
```

3. Create the routing policy to advertise both direct and RIP-learned routes.

```
[edit policy-options policy-statement advertise-routes-through-rip term 1]
user@R1# set from protocol direct
user@R1# set from protocol rip
user@R1# set then accept
```

4. Apply the routing policy.

In Junos OS, you can only apply RIP export policies at the group level.

```
[edit protocols rip group rip-group]
user@R1# set export advertise-routes-through-rip
```

5. Enable BFD.

```
[edit protocols rip group rip-group]
user@R1# set bfd-liveness-detection minimum-interval 600
```

## 6. Configure tracing operations to track BFD messages.

```
[edit protocols bfd traceoptions]  
user@R1# set file bfd-trace  
user@R1# set flag all
```

## Results

From configuration mode, confirm your configuration by entering the `show interfaces`, `show protocols`, and `show policy-options` commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
user@R1# show interfaces  
fe-1/2/0 {  
  unit 1 {  
    family inet {  
      address 10.0.0.1/30;  
    }  
  }  
}
```

```
user@R1# show protocols  
bfd {  
  traceoptions {  
    file bfd-trace;  
    flag all;  
  }  
}  
rip {  
  group rip-group {  
    export advertise-routes-through-rip;  
    bfd-liveness-detection {  
      minimum-interval 600;  
    }  
    neighbor fe-1/2/0.1;
```



```
}
}
```

```
user@R1# show policy-options
policy-statement advertise-routes-through-rip {
  term 1 {
    from protocol [ direct rip ];
    then accept;
  }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

## Verification

### IN THIS SECTION

- [Verifying That the BFD Sessions Are Up | 95](#)
- [Checking the BFD Trace File | 96](#)

Confirm that the configuration is working properly.

### *Verifying That the BFD Sessions Are Up*

## Purpose

Make sure that the BFD sessions are operating.

## Action

From operational mode, enter the `show bfd session` command.

```
user@R1> show bfd session
```

Address	State	Interface	Detect Time	Transmit Interval	Multiplier
10.0.0.2	Up	fe-1/2/0.1	1.800	0.600	3

```
1 sessions, 1 clients
Cumulative transmit rate 1.7 pps, cumulative receive rate 1.7 pps
```

## Meaning

The output shows that there are no authentication failures.

## Checking the BFD Trace File

## Purpose

Use tracing operations to verify that BFD packets are being exchanged.

## Action

From operational mode, enter the `show log` command.

```
user@R1> show log bfd-trace
Feb 16 10:26:32 PPM Trace: BFD periodic xmit to 10.0.0.2 (IFL 124, rtbl 53, single-hop port)
Feb 16 10:26:32 Received Downstream TraceMsg (24) len 86:
Feb 16 10:26:32   IfIndex (3) len 4: 0
Feb 16 10:26:32   Protocol (1) len 1: BFD
Feb 16 10:26:32   Data (9) len 61: (hex) 42 46 44 20 70 61 63 6b 65 74 20 66 72 6f 6d 20 31 30
2e
Feb 16 10:26:32 PPM Trace: BFD packet from 10.0.0.1 (IFL 73, rtbl 56, ttl 255) absorbed
Feb 16 10:26:32 Received Downstream TraceMsg (24) len 60:
Feb 16 10:26:32   IfIndex (3) len 4: 0
Feb 16 10:26:32   Protocol (1) len 1: BFD
Feb 16 10:26:32   Data (9) len 35: (hex) 42 46 44 20 70 65 72 69 6f 64 69 63 20 78 6d 69 74 20
6f
...
```

## Meaning

The output shows the normal functioning of BFD.

## Configuring Micro BFD Sessions for LAG

The Bidirectional Forwarding Detection (BFD) protocol is a simple detection protocol that quickly detects failures in the forwarding paths. A link aggregation group (LAG) combines multiple links between devices that are in point-to-point connections, thereby increasing bandwidth, providing reliability, and allowing load balancing. To run a BFD session on LAG interfaces, configure an independent, asynchronous mode BFD session on every LAG member link in a LAG bundle. Instead of a single BFD session monitoring the status of the UDP port, independent micro BFD sessions monitor the status of individual member links.

**NOTE:** Starting in Junos OS Evolved Release 20.1R1, independent micro Bidirectional Forwarding Detection (BFD) sessions are enabled on a per member link basis of a Link Aggregation Group (LAG) bundle.

To enable failure detection for aggregated Ethernet interfaces:

1. Include the following statement in the configuration at the [edit interfaces *aex* aggregated-ether-options] hierarchy level:

```
bfd-liveness-detection
```

2. Configure the authentication criteria of the BFD session for LAG.

To specify the authentication criteria, include the authentication statement:

```
bfd-liveness-detection {
  authentication {
    algorithm algorithm-name;
    key-chain key-chain-name;
    loose-check;
  }
}
```

- Specify the algorithm to be used to authenticate the BFD session. You can use one of the following algorithms for authentication:
  - keyed-md5
  - keyed-sha-1
  - meticulous-keyed-md5
  - meticulous-keyed-sha-1

- simple-password
  - To configure the key chain, specify the name that is associated with the security key for the BFD session. The name you specify must match one of the key chains configured in the authentication-key-chains *key-chain* statement at the [edit security] hierarchy level.
  - Configure loose authentication checking on the BFD session. Use only for transitional periods when authentication might not be configured at both ends of the BFD session.
3. Configure BFD timers for aggregated Ethernet interfaces.

To specify the BFD timers, include the *detection-time* statement:

```
bfd-liveness-detection {
  detection-time {
    threshold milliseconds;
  }
}
```

Specify the threshold value. This is the maximum time interval for detecting a BFD neighbor. If the transmit interval is greater than this value, the device triggers a trap.

4. Configure a hold-down interval value to set the minimum time that the BFD session must remain up before a state change notification is sent to the other members in the LAG network.

To specify the hold-down interval, include the *holddown-interval* statement:

```
bfd-liveness-detection {
  holddown-interval milliseconds;
}
```

You can configure a number in the range from 0 through 255,000 milliseconds, and the default is 0. If the BFD session goes down and then comes back up during the hold-down interval, the timer is restarted.

This value represents the minimum interval at which the local routing device transmits BFD packets, as well as the minimum interval in which the routing device expects to receive a reply from a neighbor with which it has established a BFD session. You can configure a number in the range from 1 through 255,000 milliseconds. You can also specify the minimum transmit and receive intervals separately.

5. Configure the source address for the BFD session.

To specify a local address, include the `local-address` statement:

```
bfd-liveness-detection {
    local-address bfd-local-address;
}
```

The BFD local address is the loopback address of the source of the BFD session.

**NOTE:** Beginning with Junos OS Release 16.1, you can also configure this feature with the AE interface address as the local address in a micro BFD session. For the IPv6 address family, disable duplicate address detection before configuring this feature with the AE interface address. To disable duplicate address detection, include the `dad-disable` statement at the `[edit interface aex unit y family inet6]` hierarchy level.

Beginning with Release 16.1R2, Junos OS checks and validates the configured micro BFD `local-address` against the interface or loopback IP address before the configuration commit. Junos OS performs this check on both IPv4 and IPv6 micro BFD address configurations, and if they do not match, the commit fails. The configured micro-BFD `local-address` should match with the micro-BFD `neighbour-address` configured on the peer router.

6. Specify the minimum interval that indicates the time interval for transmitting and receiving data. This value represents the minimum interval at which the local routing device transmits BFD packets, as well as the minimum interval in which the routing device expects to receive a reply from a neighbor with which it has established a BFD session. You can configure a number in the range from 1 through 255,000 milliseconds. You can also specify the minimum transmit and receive intervals separately.

To specify the minimum transmit and receive intervals for failure detection, include the `minimum-interval` statement:

```
bfd-liveness-detection {
    minimum-interval milliseconds;
}
```

**NOTE:** BFD is an intensive protocol that consumes system resources. Specifying a minimum interval for BFD less than 100 ms for Routing Engine-based sessions and 10 ms for distributed BFD sessions can cause undesired BFD flapping.

Depending on your network environment, these additional recommendations might apply:

- For large-scale network deployments with a large number of BFD sessions, specify a minimum interval of 300 ms for Routing Engine-based sessions and 100 ms for distributed BFD sessions.
- For very large-scale network deployments with a large number of BFD sessions, contact Juniper Networks customer support for more information.
- For BFD sessions to remain up during a Routing Engine switchover event when nonstop active routing is configured, specify a minimum interval of 2500 ms for Routing Engine-based sessions. For distributed BFD sessions with nonstop active routing configured, the minimum interval recommendations are unchanged and depend only on your network deployment.

7. Specify only the minimum receive interval for failure detection by including the `minimum-receive-interval` statement:

```
bfd-liveness-detection {
    minimum-receive-interval milliseconds;
}
```

This value represents the minimum interval in which the local routing device expects to receive a reply from a neighbor with which it has established a BFD session. You can configure a number in the range from 1 through 255,000 milliseconds.

8. Specify the number of BFD packets that were not received by the neighbor that causes the originating interface to be declared down by including the `multiplier` statement:

```
bfd-liveness-detection {
    multiplier number;
}
```

The default value is 3. You can configure a number in the range from 1 through 255.

9. Configure the neighbor in a BFD session.

The neighbor address can be either an IPv4 or an IPv6 address.

To specify the next hop of the BFD session, include the `neighbor` statement:

```
bfd-liveness-detection {
    neighbor bfd-neighbor-address;
}
```

The BFD neighbor address is the loopback address of the remote destination of the BFD session.

**NOTE:** Beginning with Junos OS Release 16.1, you can also configure the AE interface address of the remote destination as the BFD neighbor address in a micro BFD session.

**10.** (Optional) Configure BFD sessions not to adapt to changing network conditions.

To disable BFD adaptation, include the `no-adaptation` statement:

```
bfd-liveness-detection {
    no-adaptation;
}
```

**NOTE:** We recommend that you do not disable BFD adaptation unless it is preferable not to have BFD adaptation in your network.

**11.** Specify a threshold for detecting the adaptation of the detection time by including the `threshold` statement:

```
bfd-liveness-detection {
    detection-time {
        threshold milliseconds;
    }
}
```

When the BFD session detection time adapts to a value equal to or greater than the threshold, a single trap and a system log message are sent. The detection time is based on the multiplier of the minimum-interval or the minimum-receive-interval value. The threshold must be a higher value than the multiplier for either of these configured values. For example, if the minimum-receive-interval is 300 ms and the multiplier is 3, the total detection time is 900 ms. Therefore, the detection time threshold must have a value greater than 900.

**12.** Specify only the minimum transmit interval for failure detection by including the `transmit-interval` `minimum-interval` statement:

```
bfd-liveness-detection {
    transmit-interval {
        minimum-interval milliseconds;
    }
}
```

This value represents the minimum interval at which the local routing device transmits BFD packets to the neighbor with which it has established a BFD session. You can configure a value in the range from 1 through 255,000 milliseconds.

13. Specify the transmit threshold for detecting the adaptation of the transmit interval by including the `transmit-interval threshold` statement:

```
bfd-liveness-detection {
    transmit-interval {
        threshold milliseconds;
    }
}
```

The threshold value must be greater than the transmit interval. When the BFD session detection time adapts to a value greater than the threshold, a single trap and a system log message are sent. The detection time is based on the multiplier of the minimum-interval or the minimum-receive-interval value. The threshold must be a higher value than the multiplier for either of these configured values.

14. Specify the BFD version by including the `version` statement:

```
bfd-liveness-detection {
    version (1 | automatic);
}
```

The default is to have the version detected automatically.

#### NOTE:

- The version option is not supported on the QFX Series. Starting in Junos OS Release 17.2R1, a warning will appear if you attempt to use this command.
- This feature works when both the devices support BFD. If BFD is configured at only one end of the LAG, this feature does not work.

#### SEE ALSO

[authentication](#)

[bfd-liveness-detection \(LAG\) | 945](#)

[detection-time](#)



## Example: Configuring Independent Micro BFD Sessions for LAG

### IN THIS SECTION

- [Requirements | 103](#)
- [Overview | 104](#)
- [Configuration | 104](#)
- [Verification | 112](#)

This example shows how to configure an independent micro BFD session for aggregated Ethernet interfaces.

### Requirements

This example uses the following hardware and software components:

- MX Series routers with Junos Trio chipset
- T Series routers with Type 4 FPC or Type 5 FPC

BFD for LAG is supported on the following PIC types on T-Series:

- PC-1XGE-XENPAK (Type 3 FPC),
- PD-4XGE-XFP (Type 4 FPC),
- PD-5-10XGE-SFPP (Type 4 FPC),
- 24x10GE (LAN/WAN) SFPP, 12x10GE (LAN/WAN) SFPP, 1X100GE Type 5 PICs
- PTX Series routers with 24X10GE (LAN/WAN) SFPP
- Junos OS Release 13.3 or later running on all devices

## Overview

### IN THIS SECTION

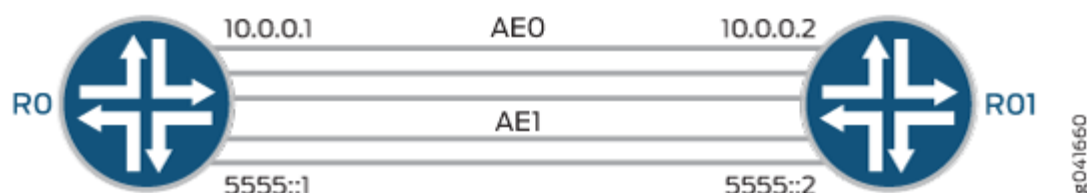
- [Topology | 104](#)

The example includes two routers that are directly connected. Configure two aggregated Ethernet interfaces, AE0 for IPv4 connectivity and AE1 for IPv6 connectivity. Configure micro BFD session on the AE0 bundle using IPv4 addresses as local and neighbor endpoints on both routers. Configure micro BFD session on the AE1 bundle using IPv6 addresses as local and neighbor endpoints on both routers. This example verifies that independent micro BFD sessions are active in the output.

### Topology

[Figure 5 on page 104](#) shows the sample topology.

**Figure 5: Configuring an Independent Micro BFD Session for LAG**



## Configuration

### IN THIS SECTION

- [CLI Quick Configuration | 105](#)
- [Configuring a Micro BFD Session for Aggregated Ethernet Interfaces | 106](#)
- [Procedure | 106](#)
- [Results | 109](#)

### CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

#### Router R0

```
set interfaces ge-1/0/1 unit 0 family inet address 20.20.20.1/30
set interfaces ge-1/0/1 unit 0 family inet6 address 3ffe::1:1/126
set interfaces xe-4/0/0 gigether-options 802.3ad ae0
set interfaces xe-4/0/1 gigether-options 802.3ad ae0
set interfaces xe-4/1/0 gigether-options 802.3ad ae1
set interfaces xe-4/1/1 gigether-options 802.3ad ae1
set interfaces lo0 unit 0 family inet address 10.255.106.107/32
set interfaces lo0 unit 0 family inet6 address 201:DB8:251::aa:aa:1/126
set interfaces ae0 aggregated-ether-options bfd-liveness-detection minimum-interval 100
set interfaces ae0 aggregated-ether-options bfd-liveness-detection neighbor 10.255.106.102
set interfaces ae0 aggregated-ether-options bfd-liveness-detection local-address 10.255.106.107
set interfaces ae0 aggregated-ether-options minimum-links 1
set interfaces ae0 aggregated-ether-options link-speed 10g
set interfaces ae0 aggregated-ether-options lacp active
set interfaces ae0 unit 0 family inet address 10.0.0.1/30
set interfaces ae1 aggregated-ether-options bfd-liveness-detection minimum-interval 100
set interfaces ae1 aggregated-ether-options bfd-liveness-detection multiplier 3
set interfaces ae1 aggregated-ether-options bfd-liveness-detection neighbor 201:DB8:251::bb:bb:1
set interfaces ae1 aggregated-ether-options bfd-liveness-detection local-address
201:DB8:251::aa:aa:1
set interfaces ae1 aggregated-ether-options minimum-links 1
set interfaces ae1 aggregated-ether-options link-speed 10g
set interfaces ae1 aggregated-ether-options lacp active
set interfaces ae1 unit 0 family inet6 address 5555::1/126
set interface ae1 unit 0 family inet6 dad-disable
set routing-options nonstop-routing
set routing-options static route 30.30.30.0/30 next-hop 10.0.0.2
set routing-options rib inet6.0 static route 3ffe::1:2/126 next-hop 5555::2
set protocols bfd traceoptions file bfd
set protocols bfd traceoptions file size 100m
set protocols bfd traceoptions file files 10
set protocols bfd traceoptions flag all
```

**Router R1**

```

set interfaces ge-1/1/8 unit 0 family inet address 30.30.30.1/30
set interfaces ge-1/1/8 unit 0 family inet6 address 3ffe::1:2/126
set interfaces xe-0/0/0 gigether-options 802.3ad ae0
set interfaces xe-0/0/1 gigether-options 802.3ad ae0
set interfaces xe-0/0/2 gigether-options 802.3ad ae1
set interfaces xe-0/0/3 gigether-options 802.3ad ae1
set interfaces lo0 unit 0 family inet address 10.255.106.102/32
set interfaces lo0 unit 0 family inet6 address 201:DB8:251::bb:bb:1/126
set interfaces ae0 aggregated-ether-options bfd-liveness-detection minimum-interval 150
set interfaces ae0 aggregated-ether-options bfd-liveness-detection multiplier 3
set interfaces ae0 aggregated-ether-options bfd-liveness-detection neighbor 10.255.106.107
set interfaces ae0 aggregated-ether-options bfd-liveness-detection local-address 10.255.106.102
set interfaces ae0 aggregated-ether-options minimum-links 1
set interfaces ae0 aggregated-ether-options link-speed 10g
set interfaces ae0 aggregated-ether-options lacp passive
set interfaces ae0 unit 0 family inet address 10.0.0.2/30
set interfaces ae1 aggregated-ether-options bfd-liveness-detection minimum-interval 200
set interfaces ae1 aggregated-ether-options bfd-liveness-detection multiplier 3
set interfaces ae1 aggregated-ether-options bfd-liveness-detection neighbor 201:DB8:251::aa:aa:1
set interfaces ae1 aggregated-ether-options bfd-liveness-detection local-address
201:DB8:251::bb:bb:1
set interfaces ae1 aggregated-ether-options minimum-links 1
set interfaces ae1 aggregated-ether-options link-speed 10g
set interfaces ae1 aggregated-ether-options lacp passive
set interfaces ae1 unit 0 family inet6 address 5555::2/126
set routing-options static route 20.20.20.0/30 next-hop 10.0.0.1
set routing-options rib inet6.0 static route 3ffe::1:1/126 next-hop 5555::1

```

***Configuring a Micro BFD Session for Aggregated Ethernet Interfaces******Procedure*****Step-by-Step Procedure**

The following example requires that you navigate various levels in the configuration hierarchy. For information about navigating the CLI, see [“Using the CLI Editor in Configuration Mode”](#) in the [CLI User Guide](#).

**NOTE:** Repeat this procedure for Router R1, modifying the appropriate interface names, addresses, and any other parameters for each router.

To configure a micro BFD session for aggregated Ethernet interfaces on Router R0:

1. Configure the physical interfaces.

```
[edit interfaces]
user@R0# set ge-1/0/1 unit 0 family inet address 20.20.20.1/30
user@R0# set ge-1/0/1 unit 0 family inet6 address 3ffe::1:1/126
user@R0# set xe-4/0/0 gigether-options 802.3ad ae0
user@R0# set xe-4/0/1 gigether-options 802.3ad ae0
user@R0# set xe-4/1/0 gigether-options 802.3ad ae1
user@R0# set xe-4/1/1 gigether-options 802.3ad ae1
```

2. Configure the loopback interface.

```
[edit interfaces]
user@R0# set lo0 unit 0 family inet address 10.255.106.107/32
user@R0# set lo0 unit 0 family inet6 address 201:DB8:251::aa:aa:1/128
```

3. Configure an IP address on the aggregated Ethernet interface ae0 with either IPv4 or IPv6 addresses, as per your network requirements.

```
[edit interfaces]
user@R0# set ae0 unit 0 family inet address 10.0.0.1/30
```

4. Set the routing option, create a static route, and set the next-hop address.

**NOTE:** You can configure either an IPv4 or IPv6 static route, depending on your network requirements.

```
[edit routing-options]
user@R0# set nonstop-routing
```

```
user@R0# set static route 30.30.30.0/30 next-hop 10.0.0.2
user@R0# set rib inet6.0 static route 3ffe::1:2/126 next-hop 5555::2
```

5. Configure the Link Aggregation Control Protocol (LACP).

```
[edit interfaces]
user@R0# set ae0 aggregated-ether-options lacp active
```

6. Configure BFD for the aggregated Ethernet interface ae0, and specify the minimum interval, local IP address, and the neighbor IP address.

```
[edit interfaces]
user@R0# set ae0 aggregated-ether-options bfd-liveness-detection minimum-interval 100
user@R0# set ae0 aggregated-ether-options bfd-liveness-detection multiplier 3
user@R0# set ae0 aggregated-ether-options bfd-liveness-detection neighbor 10.255.106.102
user@R0# set ae0 aggregated-ether-options bfd-liveness-detection local-address 10.255.106.107
user@R0# set ae0 aggregated-ether-options minimum-links 1
user@R0# set ae0 aggregated-ether-options link-speed 10g
```

7. Configure an IP address on the aggregated Ethernet interface ae1.

You can assign either IPv4 or IPv6 addresses as per your network requirements.

```
[edit interfaces]
user@R0# set ae1 unit 0 family inet6 address 5555::1/126
```

8. Configure BFD for the aggregated Ethernet interface ae1.

```
[edit interfaces]
user@R0# set ae1 aggregated-ether-options bfd-liveness-detection minimum-interval 100
user@R0# set ae1 aggregated-ether-options bfd-liveness-detection multiplier 3
user@R0# set ae1 aggregated-ether-options bfd-liveness-detection neighbor 201:DB8:251::bb:bb:1
user@R0# set ae1 aggregated-ether-options bfd-liveness-detection local-address
201:DB8:251::aa:aa:1
user@R0# set ae1 aggregated-ether-options minimum-links 1
user@R0# set ae1 aggregated-ether-options link-speed 10g
```

**NOTE:** Beginning with Junos OS Release 16.1, you can also configure this feature with the AE interface address as the local address in a micro BFD session.

Beginning with Release 16.1R2, Junos OS checks and validates the configured micro BFD local-address against the interface or loopback IP address before the configuration commit. Junos OS performs this check on both IPv4 and IPv6 micro BFD address configurations, and if they do not match, the commit fails.

## 9. Configure tracing options for BFD for troubleshooting.

```
[edit protocols]
user@R0# set bfd traceoptions file bfd
user@R0# set bfd traceoptions file size 100m
user@R0# set bfd traceoptions file files 10
user@R0# set bfd traceoptions flag all
```

### Results

From configuration mode, enter the **show interfaces**, **show protocols**, and **show routing-options** commands and confirm your configuration. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@R0> show interfaces
traceoptions {
  flag bfd-events;
}
ge-1/0/1 {
  unit 0 {
    family inet {
      address 20.20.20.1/30;
    }
    family inet6 {
      address 3ffe::1:1/126;
    }
  }
}
xe-4/0/0 {
  enable;
  gigether-options {
    802.3ad ae0;
```

```

    }
}
xe-4/0/1 {
    gigether-options {
        802.3ad ae0;
    }
}
xe-4/1/0 {
    enable;
    gigether-options {
        802.3ad ae1;
    }
}
xe-4/1/1 {
    gigether-options {
        802.3ad ae1;
    }
}
lo0 {
    unit 0 {
        family inet {
            address 10.255.106.107/32;
        }
        family inet6 {
            address 201:DB8:251::aa:aa:1/128;
        }
    }
}
ae0 {
    aggregated-ether-options {
        bfd-liveness-detection {
            minimum-interval 100;
            neighbor 10.255.106.102;
            local-address 10.255.106.107;
        }
        minimum-links 1;
        link-speed 10g;
        lacp {
            active;
        }
    }
    unit 0 {
        family inet {

```



```

        address 10.0.0.1/30;
    }
}
ae1 {
    aggregated-ether-options {
        bfd-liveness-detection {
            minimum-interval 100;
            multiplier 3;
            neighbor 201:DB8:251::bb:bb:1;
            local-address 201:DB8:251::aa:aa:1;
        }
        minimum-links 1
        link-speed 10g;
    }
    unit 0 {
        family inet6 {
            address 5555::1/126;
        }
    }
}

```

```

user@R0> show protocols
bfd {
    traceoptions {
        file bfd size 100m files 10;
        flag all;
    }
}

```

```

user@R0> show routing-options
nonstop-routing ;
rib inet6.0 {
    static {
        route 3ffe:1:2/126 {
            next-hop 5555::2;
        }
    }
}
static {

```

```

route 30.30.30.0/30 {
    next-hop 10.0.0.2;
}
}

```

If you are done configuring the device, commit the configuration.

```
user@R0# commit
```

## Verification

### IN THIS SECTION

- [Verifying That the Independent BFD Sessions Are Up | 112](#)
- [Viewing Detailed BFD Events | 114](#)

Confirm that the configuration is working properly.

### *Verifying That the Independent BFD Sessions Are Up*

## Purpose

Verify that the micro BFD sessions are up, and view details about the BFD sessions.

## Action

From operational mode, enter the show bfd session extensive command.

```

user@R0> show bfd session extensive

```

Address	State	Interface	Detect Time	Transmit Interval	Multiplier
10.255.106.102	Up	xe-4/0/0	9.000	3.000	3

```

Client LACPD, TX interval 0.100, RX interval 0.100
Session up time 4d 23:13, previous down time 00:00:06
Local diagnostic None, remote diagnostic None
Remote heard, hears us, version 1

```

Replicated

Session type: **Micro BFD**

Min async interval 0.100, min slow interval 1.000

Adaptive async TX interval 0.100, RX interval 0.100

Local min TX interval 0.100, minimum RX interval 0.100, multiplier 3

Remote min TX interval 3.000, min RX interval 3.000, multiplier 3

Local discriminator 21, remote discriminator 75

Echo mode disabled/inactive

Remote is control-plane independent

Session ID: 0x0

Address	State	Interface	Detect Time	Transmit Interval	Multiplier
10.255.106.102	Up	xe-4/0/1	9.000	3.000	3

Client LACPD, TX interval 0.100, RX interval 0.100

Session up time 4d 23:13, previous down time 00:00:07

Local diagnostic None, remote diagnostic None

Remote heard, hears us, version 1

Replicated

Session type: **Micro BFD**

Min async interval 0.100, min slow interval 1.000

Adaptive async TX interval 0.100, RX interval 0.100

Local min TX interval 0.100, minimum RX interval 0.100, multiplier 3

Remote min TX interval 3.000, min RX interval 3.000, multiplier 3

Local discriminator 19, remote discriminator 74

Echo mode disabled/inactive

Remote is control-plane independent

Session ID: 0x0

Address	State	Interface	Detect Time	Transmit Interval	Multiplier
201:DB8:251::bb:bb:1	Up	xe-4/1/1	9.000	3.000	3

Client LACPD, TX interval 0.100, RX interval 0.100

Session up time 4d 23:13

Local diagnostic None, remote diagnostic None

Remote not heard, hears us, version 1

Replicated

Session type: **Micro BFD**

Min async interval 0.100, min slow interval 1.000

Adaptive async TX interval 0.100, RX interval 0.100

Local min TX interval 1.000, minimum RX interval 0.100, multiplier 3

Remote min TX interval 3.000, min RX interval 3.000, multiplier 3

Local discriminator 17, remote discriminator 67

Echo mode disabled/inactive, no-absorb, no-refresh

Remote is control-plane independent

Session ID: 0x0

Address	State	Interface	Detect Time	Transmit Interval	Multiplier	
201:DB8:251::bb:bb:1		UP	xe-4/1/0	9.000	3.000	3

Client LACPD, TX interval 0.100, RX interval 0.100

Session up time 4d 23:13

Local diagnostic None, remote diagnostic None

Remote not heard, hears us, version 1

Replicated

Session type: **Micro BFD**

Min async interval 0.100, min slow interval 1.000

Adaptive async TX interval 0.100, RX interval 0.100

Local min TX interval 1.000, minimum RX interval 0.100, multiplier 3

Remote min TX interval 3.000, min RX interval 3.000, multiplier 3

Local discriminator 16, remote discriminator 66

Echo mode disabled/inactive, no-absorb, no-refresh

Remote is control-plane independent

Session ID: 0x0

4 sessions, 4 clients

Cumulative transmit rate 2.0 pps, cumulative receive rate 1.7 pps

## Meaning

The Micro BFD field represents the independent micro BFD sessions running on the links in a LAG. The TX interval *item*, RX interval *item* output represents the setting configured with the `minimum-interval` statement. All of the other output represents the default settings for BFD. To modify the default settings, include the optional statements under `bfd-liveness-detection` statement.

### *Viewing Detailed BFD Events*

## Purpose

View the contents of the BFD trace file to assist in troubleshooting, if required.

## Action

From operational mode, enter the **file show /var/log/bfd** command.

```
user@R0> file show /var/log/bfd
Jun  5 00:48:59   Protocol (1) len 1: BFD
Jun  5 00:48:59   Data (9) len 41: (hex) 42 46 44 20 6e 65 69 67 68 62 6f 72 20 31 30 2e 30 2e
30
Jun  5 00:48:59 PPM Trace: BFD neighbor 10.255.106.102 (IFL 349) set, 9 0
Jun  5 00:48:59 Received Downstream RcvPkt (19) len 108:
Jun  5 00:48:59   IfIndex (3) len 4: 329
Jun  5 00:48:59   Protocol (1) len 1: BFD
Jun  5 00:48:59   SrcAddr (5) len 8: 10.255.106.102
Jun  5 00:48:59   Data (9) len 24: (hex) 00 88 03 18 00 00 00 4b 00 00 00 15 00 2d c6 c0 00 2d
c6
Jun  5 00:48:59   PktError (26) len 4: 0
Jun  5 00:48:59   RtblIdx (24) len 4: 0
Jun  5 00:48:59   MultiHop (64) len 1: (hex) 00
Jun  5 00:48:59   Unknown (168) len 1: (hex) 01
Jun  5 00:48:59   Unknown (171) len 2: (hex) 02 3d
Jun  5 00:48:59   Unknown (172) len 6: (hex) 80 71 1f c7 81 c0
Jun  5 00:48:59   Authenticated (121) len 1: (hex) 01
Jun  5 00:48:59 BFD packet from 10.0.0.2 (IFL 329), len 24
Jun  5 00:48:59   Ver 0, diag 0, mult 3, len 24
Jun  5 00:48:59   Flags: IHU Fate
Jun  5 00:48:59   My discr 0x0000004b, your discr 0x00000015
Jun  5 00:48:59   Tx ivl 3000000, rx ivl 3000000, echo rx ivl 0
Jun  5 00:48:59 [THROTTLE]bfdd_rate_limit_can_accept_pkt: session 10.255.106.102 is up or
already in program thread
Jun  5 00:48:59 Replicate: marked session (discr 21) for update
```

## Meaning

BFD messages are being written to the specified trace file.

## SEE ALSO

[authentication \(LAG\) | 943](#)

[bfd-liveness-detection \(LAG\) | 945](#)

## Configuring BFD for PIM

The Bidirectional Forwarding Detection (BFD) Protocol is a simple hello mechanism that detects failures in a network. BFD works with a wide variety of network environments and topologies. A pair of routing devices exchanges BFD packets. Hello packets are sent at a specified, regular interval. A neighbor failure is detected when the routing device stops receiving a reply after a specified interval. The BFD failure detection timers have shorter time limits than the Protocol Independent Multicast (PIM) hello hold time, so they provide faster detection.

The BFD failure detection timers are adaptive and can be adjusted to be faster or slower. The lower the BFD failure detection timer value, the faster the failure detection and vice versa. For example, the timers can adapt to a higher value if the adjacency fails (that is, the timer detects failures more slowly). Or a neighbor can negotiate a higher value for a timer than the configured value. The timers adapt to a higher value when a BFD session flap occurs more than three times in a span of 15 seconds. A back-off algorithm increases the receive (Rx) interval by two if the local BFD instance is the reason for the session flap. The transmission (Tx) interval is increased by two if the remote BFD instance is the reason for the session flap. You can use the `clear bfd adaptation` command to return BFD interval timers to their configured values. The `clear bfd adaptation` command is hitless, meaning that the command does not affect traffic flow on the routing device.

You must specify the minimum transmit and minimum receive intervals to enable BFD on PIM.

To enable failure detection:

1. Configure the interface globally or in a routing instance.

This example shows the global configuration.

```
[edit protocols pim]
user@host# edit interface fe-1/0/0.0 family inet bfd-liveness-detection
```

2. Configure the minimum transmit interval.

This is the minimum interval after which the routing device transmits hello packets to a neighbor with which it has established a BFD session. Specifying an interval smaller than 300 ms can cause undesired BFD flapping.

```
[edit protocols pim interface fe-1/0/0.0 family inet bfd-liveness-detection]
user@host# set transmit-interval 350
```

3. Configure the minimum interval after which the routing device expects to receive a reply from a neighbor with which it has established a BFD session.

Specifying an interval smaller than 300 ms can cause undesired BFD flapping.

```
[edit protocols pim interface fe-1/0/0.0 family inet bfd-liveness-detection]
user@host# set minimum-receive-interval 350
```

4. (Optional) Configure other BFD settings.

As an alternative to setting the receive and transmit intervals separately, configure one interval for both.

```
[edit protocols pim interface fe-1/0/0.0 family inet bfd-liveness-detection]
user@host# set minimum-interval 350
```

5. Configure the threshold for the adaptation of the BFD session detection time.

When the detection time adapts to a value equal to or greater than the threshold, a single trap and a single system log message are sent.

```
[edit protocols pim interface fe-1/0/0.0 family inet bfd-liveness-detection]
user@host# set detection-time threshold 800
```

6. Configure the number of hello packets not received by a neighbor that causes the originating interface to be declared down.

```
[edit protocols pim interface fe-1/0/0.0 family inet bfd-liveness-detection]
user@host# set multiplier 50
```

7. Configure the BFD version.

```
[edit protocols pim interface fe-1/0/0.0 family inet bfd-liveness-detection]
user@host# set version 1
```

8. Specify that BFD sessions should not adapt to changing network conditions.

We recommend that you not disable BFD adaptation unless it is preferable not to have BFD adaptation enabled in your network.

```
[edit protocols pim interface fe-1/0/0.0 family inet bfd-liveness-detection]
user@host# set no-adaptation
```

9. Verify the configuration by checking the output of the show bfd session command.

## SEE ALSO

| *show bfd session*

## Enabling Dedicated and Real-Time BFD on SRX Devices

### IN THIS SECTION

- [Dedicated BFD | 118](#)
- [Real-Time BFD | 119](#)
- [BFD Support By SRX Platform | 119](#)

By default, SRX Series devices operate in centralized BFD mode. They also support distributed BFD, dedicated BFD, and real-time BFD.

### Dedicated BFD

Enabling dedicated BFD impacts traffic throughput as one CPU core is removed from data plane processing.

To enable dedicated BFD on the SRX100, SRX110, SRX210, SRX220, SRX240, SRX300, SRX320, SRX340, SRX345, SRX380, SRX550, SRX550M, SRX650, and SRX1500 devices:

1. Include the `dedicated-ukern-cpu` statement at the `[edit chassis]` hierarchy level and then commit the configuration.

a. `[edit]`

b. `user@host# set chassis dedicated-ukern-cpu`

`user@host# commit`

The following warning message to reboot the system displays when you commit the configuration:

```
warning: Packet processing throughput may be impacted in dedicated-ukernel-cpu mode. warning: A reboot is
required for dedicated-ukernel-cpu mode to be enabled. Please use "request system reboot" to reboot the
system. commit complete
```

2. Reboot the device to enable the configuration:

a. `user@host> request system reboot`



3. Verify that dedicated BFD is enabled.

```
user@host> show chassis dedicated-ukern-cpu
```

```
Dedicated Ukern CPU Status: Enabled
```

## Real-Time BFD

Enabling real-time BFD does not impact data plane performance. Higher priority is given to the Packet Forwarding Engine process handling BFD in distributed mode. This is suitable for scenarios where less than half of the maximum number of BFD sessions are being used. See ["this list" on page 120](#) for the maximum number of BFD sessions supported per SRX device.

**NOTE:** For more information about BFD in distributed mode, see ["Understanding How BFD Detects Network Failures" on page 27](#).

To enable real-time BFD on SRX100, SRX110, SRX210, SRX220, SRX240, SRX300, SRX320, SRX340, SRX345, SRX550, SRX550M, and SRX650 devices:

1. Include the `realtime-ukern-thread` statement at the `[edit chassis]` hierarchy level and then commit the configuration.

- a. `[edit]`

- b. `user@host# set chassis realtime-ukern-thread`

```
user@host# commit
```

The following warning message to reboot the system displays when you commit the configuration:

```
WARNING: realtime-ukern-thread is enable. Please use the command request system reboot.
```

2. Reboot the device to enable the configuration:

- a. `user@host> request system reboot`

3. Verify that real-time BFD is enabled.

```
user@host> show chassis realtime-ukern-thread
```

```
realtime Ukern thread Status: Enabled
```

## BFD Support By SRX Platform

SRX Series devices support the following maximum number of BFD sessions:

- Up to four sessions on SRX100, SRX110, SRX210, SRX220, SRX300, and SRX320 devices.
- Up to 50 sessions on SRX240, SRX340, SRX345, SRX380, SRX550, SRX550M, and SRX650 devices.
- Up to 120 sessions on SRX1500 devices.

On all SRX Series devices, high CPU utilization triggered for reasons such as CPU intensive commands and SNMP walks causes the BFD protocol to flap while processing large BGP updates. (Platform support depends on the Junos OS release in your installation.)

SRX Series devices operating in chassis cluster mode support only BFD centralized mode.

The table below shows the BFD modes supported on each SRX Series device.

**Table 2: BFD Modes Supported on SRX Series Devices**

SRX Series Device	Centralized BFD Mode	Distributed BFD	Real-Time BFD	Dedicated Core
SRX100	Default	Configuration	Configuration (Optional)	Not supported
SRX110	Default	Configuration	Configuration (Optional)	Not supported
SRX210	Default	Configuration	Configuration (Optional)	Not supported
SRX220	Default	Configuration	Configuration (Optional)	Not supported
SRX240	Default	Configuration	Configuration	Configuration (Optional)
SRX300	Default	Configuration	Configuration (Optional)	Not supported
SRX320	Default	Configuration	Configuration (Optional)	Not supported

**Table 2: BFD Modes Supported on SRX Series Devices (Continued)**

SRX Series Device	Centralized BFD Mode	Distributed BFD	Real-Time BFD	Dedicated Core
SRX340	Default	Configuration	Configuration	Configuration (Optional)
SRX345	Default	Configuration	Configuration	Configuration (Optional)
SRX380	Default	Configuration	Configuration	Configuration (Optional)
SRX550	Default	Configuration	Configuration	Configuration (Optional)
SRX550M	Default	Configuration	Configuration	Configuration (Optional)
SRX650	Default	Configuration	Configuration	Configuration (Optional)
SRX1500	BFD failure detection time > 500 ms and dedicated mode is not enabled	BFD failure detection time < 500 ms and dedicated mode is not enabled	Not supported	Configuration
SRX4100	BFD failure detection time > 500 ms	BFD failure detection time < 500 ms	Not supported	Not supported
SRX4200	BFD failure detection time > 500 ms	BFD failure detection time < 500 ms	Not supported	Not supported
SRX4600	BFD failure detection time > 500 ms	BFD failure detection time < 500 ms	Not supported	Not supported

**Table 2: BFD Modes Supported on SRX Series Devices (Continued)**

SRX Series Device	Centralized BFD Mode	Distributed BFD	Real-Time BFD	Dedicated Core
SRX5400	Default	Not supported	Not supported	Not supported
SRX5600	Default	Not supported	Not supported	Not supported
SRX5800	Default	Not supported	Not supported	Not supported
SRX5000 line of devices with SPC3 card	BFD failure detection time > 500 ms	BFD failure detection time < 500 ms	Not supported	Not supported

**SEE ALSO**

Understanding BFD for BGP

[Understanding How BFD Detects Network Failures | 27](#)

[show chassis dedicated-ukern-cpu | 1388](#)

[show chassis realtime-ukern-thread | 1395](#)

# 4

PART

## Configuring Routing Engine Redundancy

---

[Understanding How Routing Engine Redundancy Prevents Network Failures](#) | 124

[Configuring Routing Engine Redundancy](#) | 131

---

# Understanding How Routing Engine Redundancy Prevents Network Failures

## IN THIS CHAPTER

- [Understanding Routing Engine Redundancy | 124](#)

## Understanding Routing Engine Redundancy

### SUMMARY

Routing engine redundancy ensures the continued functionality of your network. If the primary Routing Engine is taken offline (either by failover or switchover), the standby Routing Engine takes over all routing functions.

### IN THIS SECTION

- [Routing Engine Redundancy Overview | 124](#)
- [Conditions That Trigger a Routing Engine Failover | 125](#)
- [Default Routing Engine Redundancy Behavior | 126](#)
- [Routing Engine Redundancy on a TX Matrix Router | 127](#)
- [Routing Engine Redundancy on a TX Matrix Plus Router | 128](#)
- [Situations That Require You to Halt Routing Engines | 129](#)

## Routing Engine Redundancy Overview

Redundant Routing Engines are two Routing Engines that are installed in the same routing platform. One functions as the primary, while the other stands by as a backup should the primary Routing Engine fail. On routing platforms with dual Routing Engines, network reconvergence takes place more quickly than on routing platforms with a single Routing Engine.

When a Routing Engine is configured as primary, it has full functionality. It receives and transmits routing information, builds and maintains routing tables, communicates with interfaces and Packet Forwarding Engine components, and has full control over the chassis. When a Routing Engine is configured to be the backup, it does not communicate with the Packet Forwarding Engine or chassis components.

**NOTE:** On devices running Junos OS Release 8.4 or later, both Routing Engines cannot be configured to be primary at the same time. This configuration causes the commit check to fail.

A failover from the primary Routing Engine to the backup Routing Engine occurs automatically when the primary Routing Engine experiences a hardware failure or when you have configured the software to support a change in primary role based on specific conditions. You can also manually switch Routing Engine primary role by issuing one of the `request chassis routing-engine` commands. In this topic, the term *failover* refers to an automatic event, whereas *switchover* refers to either an automatic or a manual event.

When a failover or a switchover occurs, the backup Routing Engine takes control of the system as the new primary Routing Engine.

- If *graceful Routing Engine switchover* is not configured, when the backup Routing Engine becomes primary, it resets the switch plane and downloads its own version of the microkernel to the Packet Forwarding Engine components. Traffic is interrupted while the Packet Forwarding Engine is reinitialized. All kernel and forwarding processes are restarted.
- If graceful Routing Engine switchover is configured, interface and kernel information is preserved. The switchover is faster because the Packet Forwarding Engines are not restarted. The new primary Routing Engine restarts the routing protocol process (`rpdd`). All hardware and interfaces are acquired by a process that is similar to a warm restart.
- If graceful Routing Engine switchover and *nonstop active routing* (NSR) are configured, traffic is not interrupted during the switchover. Interface, kernel, and routing protocol information is preserved.
- If graceful Routing Engine switchover and graceful restart are configured, traffic is not interrupted during the switchover. Interface and kernel information is preserved. Graceful restart protocol extensions quickly collect and restore routing information from the neighboring routers.

## Conditions That Trigger a Routing Engine Failover

The following events can result in an automatic change in Routing Engine primary role, depending on your configuration:

- The routing platform experiences a hardware failure. A change in Routing Engine primary role occurs if either the Routing Engine or the associated host module or subsystem is abruptly powered off. You can also configure the backup Routing Engine to take primary role if it detects a hard disk error on

the primary Routing Engine. To enable this feature, include the `failover on-disk-failure` statement at the `[edit chassis redundancy]` hierarchy level.

- The routing platform experiences a software failure, such as a kernel crash or a CPU lock. You must configure the backup Routing Engine to take primary role when it detects a loss of keepalive signal. To enable this failover method, include the `failover on-loss-of-keepalives` statement at the `[edit chassis redundancy]` hierarchy level.
- The routing platform experiences an `em0` interface failure on the primary Routing Engine. You must configure the backup Routing Engine to take primary role when it detects the `em0` interface failure. To enable this failover method, include the `on-re-to-fpc-stale` statement at the `[edit chassis redundancy failover]` hierarchy level.
- A specific software process fails. You can configure the backup Routing Engine to take primary role when one or more specified processes fail at least four times within 30 seconds. Include the `failover other-routing-engine` statement at the `[edit system processes process-name]` hierarchy level.

If any of these conditions is met, a message is logged and the backup Routing Engine attempts to take primary role. By default, an alarm is generated when the backup Routing Engine becomes active. After the backup Routing Engine takes primary role, it continues to function as primary even after the originally configured primary Routing Engine has successfully resumed operation. You must manually restore it to its previous backup status. (However, if at any time one of the Routing Engines is not present, the other Routing Engine becomes primary automatically, regardless of how redundancy is configured.)

## Default Routing Engine Redundancy Behavior

By default, Junos OS uses **re0** as the primary Routing Engine and **re1** as the backup Routing Engine. Unless otherwise specified in the configuration, **re0** always becomes primary when the acting primary Routing Engine is rebooted.

**NOTE:** A single Routing Engine in the chassis always becomes the primary Routing Engine even if it was previously the backup Routing Engine.

Perform the following steps to see how the default Routing Engine redundancy setting works:

1. Ensure that **re0** is the primary Routing Engine.
2. Manually switch the state of Routing Engine primary role by issuing the `request chassis routing-engine master switch` command from the primary Routing Engine. **re0** is now the backup Routing Engine and **re1** is the primary Routing Engine.



**NOTE:** On the next reboot of the primary Routing Engine, Junos OS returns the router to the default state because you have not configured the Routing Engines to maintain this state after a reboot.

### 3. Reboot the primary Routing Engine **re1**.

The Routing Engine boots up and reads the configuration. Because you have not specified in the configuration which Routing Engine is the primary, **re1** uses the default configuration as the backup. Now both **re0** and **re1** are in a backup state. Junos OS detects this conflict and, to prevent a no-primary state, reverts to the default configuration to direct **re0** to become primary.

## Routing Engine Redundancy on a TX Matrix Router

In a routing matrix, all primary Routing Engines in the TX Matrix router and connected T640 routers must run the same Junos OS release. Likewise, all backup Routing Engines in a routing matrix must run the same Junos OS release. When you run the same Junos OS release on all primary and backup Routing Engines in a routing matrix, a change in primary role to any backup Routing Engine in the routing matrix does not cause a change in primary role in any other chassis in the routing matrix.



**CAUTION:** (Routing matrix based on the TX Matrix or TX Matrix Plus routers only)  
Within the routing matrix, we recommend that all Routing Engines run the same Junos OS release. If you run different releases on the Routing Engines and a change in primary role occurs on any backup Routing Engine in the routing matrix based on TX Matrix router or TX Matrix Plus router, one or all routers might become logically disconnected from the TX Matrix router or the TX Matrix Plus router and cause data loss.

If the same Junos OS release is not running on all primary and backup Routing Engines in the routing matrix, the following consequences occur when the failover `on-loss-of-keepalives` statement *is* included at the `[edit chassis redundancy]` hierarchy level:

- When the failover `on-loss-of-keepalives` statement is included at the `[edit chassis redundancy]` hierarchy level and you or a host subsystem initiates a change in primary role to the backup Routing Engine in the TX Matrix router, the primary Routing Engines in the T640 routers detect a software release mismatch with the new primary Routing Engine in the TX Matrix router and switch primary role to their backup Routing Engines.
- When you manually change primary role to a backup Routing Engine in a T640 router using the `request chassis routing-engine master` command, the new primary Routing Engine in the T640 router detects a software release mismatch with the primary Routing Engine in the TX Matrix router and relinquishes primary role to the original primary Routing Engine. (Routing Engine primary role in the TX Matrix router does not switch in this case.)

- When a host subsystem initiates a change in primary role to a backup Routing Engine in a T640 router because the primary Routing Engine has failed, the T640 router is logically disconnected from the TX Matrix router. To reconnect the T640 router, initiate a change in primary role to the backup Routing Engine in the TX Matrix router, or replace the failed Routing Engine in the T640 router and switch primary role to it. The replacement Routing Engine must be running the same software release as the primary Routing Engine in the TX Matrix router.

If the same Junos OS release is not running on all primary and backup Routing Engines in the routing matrix, the following consequences occur when the `failover on-loss-of-keepalives` statement *is not* included at the `[edit chassis redundancy]` hierarchy level:

- If you initiate a change in primary role to the backup Routing Engine in the TX Matrix router, all T640 routers are logically disconnected from the TX Matrix router. To reconnect the T640 routers, switch primary role of all primary Routing Engines in the T640 routers to their backup Routing Engines.
- If you initiate a change in primary role to a backup Routing Engine in a T640 router, the T640 router is logically disconnected from the TX Matrix router. To reconnect the T640 router, switch primary role of the new primary Routing Engine in the T640 router back to the original primary Routing Engine.

## Routing Engine Redundancy on a TX Matrix Plus Router

In a routing matrix, all primary Routing Engines in the TX Matrix Plus router and the connected LCC must run the same Junos OS release. Likewise, all backup Routing Engines in a routing matrix must run the same Junos OS release. When you run the same Junos OS release on all primary and backup Routing Engines in the routing matrix, a change in primary role to any backup Routing Engine in the routing matrix does not cause a change in primary role in any other chassis in the routing matrix.



### **CAUTION:** (Routing matrix based on the TX Matrix or TX Matrix Plus routers only)

Within the routing matrix, we recommend that all Routing Engines run the same Junos OS release. If you run different releases on the Routing Engines and a change in primary role occurs on any backup Routing Engine in the routing matrix based on a TX Matrix router or a TX Matrix Plus router, one or all routers might become logically disconnected from the TX Matrix router or the TX Matrix Plus router and cause data loss.

If the same Junos OS release is not running on all primary and backup Routing Engines in the routing matrix, the following scenarios occur when the `failover on-loss-of-keepalives` statement *is* included at the `[edit chassis redundancy]` hierarchy level:

- When the `failover on-loss-of-keepalives` statement is included at the `[edit chassis redundancy]` hierarchy level and you or a host subsystem initiates a change in primary role to the backup Routing Engine in the TX Matrix Plus router, the primary Routing Engines in the connected LCC detect a software

release mismatch with the new primary Routing Engine in the TX Matrix Plus router and switch primary role to their backup Routing Engines.

- When you manually change primary role to a backup Routing Engine in a connected LCC by using the `request chassis routing-engine master` command, the new primary Routing Engine in the connected LCC detects a software release mismatch with the primary Routing Engine in the TX Matrix Plus router and relinquishes primary role to the original primary Routing Engine. (Routing Engine primary role in the TX Matrix Plus router does not switch in this case.)
- When a host subsystem initiates a change in primary role to a backup Routing Engine in a connected LCC because the primary Routing Engine has failed, the connected LCC is logically disconnected from the TX Matrix Plus router. To reconnect the connected LCC, initiate a change in primary role to the backup Routing Engine in the TX Matrix Plus router, or replace the failed Routing Engine in the connected LCC and switch primary role to it. The replacement Routing Engine must be running the same software release as the primary Routing Engine in the TX Matrix Plus router.

If the same Junos OS release is not running on all primary and backup Routing Engines in the routing matrix, the following scenarios occur when the `failover on-loss-of-keepalives` statement *is not* included at the `[edit chassis redundancy]` hierarchy level:

- If you initiate a change in primary role to the backup Routing Engine in the TX Matrix Plus router, all connected LCCs are logically disconnected from the TX Matrix Plus router. To reconnect the connected LCC, switch primary role of all primary Routing Engines in the connected LCC to their backup Routing Engines.
- If you initiate a change in primary role to a backup Routing Engine in a connected LCC, the connected LCC is logically disconnected from the TX Matrix Plus router. To reconnect the connected LCC, switch primary role of the new primary Routing Engine in the connected LCC back to the original primary Routing Engine.

## Situations That Require You to Halt Routing Engines

Before you shut the power off to a routing platform that has two Routing Engines or before you remove the primary Routing Engine, you must first halt the backup Routing Engine and then halt the primary Routing Engine. Otherwise, you might need to reinstall Junos OS. You can use the `request system halt both-routing-engines` command on the primary Routing Engine, which first shuts down the primary Routing Engine and then shuts down the backup Routing Engine. To shut down only the backup Routing Engine, issue the `request system halt` command on the backup Routing Engine.

If you halt the primary Routing Engine and do not power it off or remove it, the backup Routing Engine remains inactive unless you have configured it to become the primary when it detects a loss of keepalive signal from the primary Routing Engine.

**NOTE:** To restart the router, you must log in to the console port (rather than the Ethernet management port) of the Routing Engine. When you log in to the console port of the primary Routing Engine, the system automatically reboots. After you log in to the console port of the backup Routing Engine, press Enter to reboot it.

**NOTE:** If you have upgraded the backup Routing Engine, first reboot it and then reboot the primary Routing Engine.

## RELATED DOCUMENTATION

---

[Understanding High Availability Features on Juniper Networks Routers | 2](#)

---

[Understanding Switching Control Board Redundancy | 15](#)

---

[Configuring Routing Engine Redundancy | 131](#)

# Configuring Routing Engine Redundancy

## IN THIS CHAPTER

- [Configuring Routing Engine Redundancy | 131](#)

## Configuring Routing Engine Redundancy

### SUMMARY

Follow the steps and examples below to configure routing engine redundancy.

### IN THIS SECTION

- [Modifying the Default Routing Engine Primary Role | 132](#)
- [Configuring Automatic Failover to the Backup Routing Engine | 132](#)
- [Manually Switching Routing Engine Primary Role | 135](#)
- [Verifying Routing Engine Redundancy Status | 136](#)
- [Initial Routing Engine Configuration Example | 137](#)
- [Copying a Configuration File from One Routing Engine to the Other | 140](#)
- [Loading a Software Package from the Other Routing Engine | 141](#)

**NOTE:** To complete the tasks in the following sections, **re0** and **re1** configuration groups must be defined. For more information about configuration groups, see the [Junos OS CLI User Guide](#).

## Modifying the Default Routing Engine Primary Role

For routers with two Routing Engines, you can configure which Routing Engine is the primary and which is the backup. By default, the Routing Engine in slot 0 is the primary (**re0**) and the one in slot 1 is the backup (**re1**).

**NOTE:** In systems with two Routing Engines, both Routing Engines cannot be configured to be primary at the same time. This configuration causes the commit check to fail.

To modify the default configuration, include the `routing-engine` statement at the `[edit chassis redundancy]` hierarchy level:

```
[edit chassis redundancy]
routing-engine slot-number (master | backup | disabled);
```

**slot-number** can be 0 or 1. To configure the Routing Engine to be the primary, specify the **master** option. To configure it to be the backup, specify the **backup** option. To disable a Routing Engine, specify the **disabled** option.

**NOTE:** To switch between the primary and the backup Routing Engines, see ["Manually Switching Routing Engine Primary Role" on page 135](#).

## Configuring Automatic Failover to the Backup Routing Engine

### IN THIS SECTION

- [Without Interruption to Packet Forwarding | 133](#)
- [On Detection of a Hard Disk Error on the Primary Routing Engine | 133](#)
- [On Detection of a Broken LCMD Connectivity Between the VM and RE | 133](#)
- [On Detection of a Loss of Keepalive Signal from the Primary Routing Engine | 133](#)
- [On Detection of the em0 Interface Failure on the Primary Routing Engine | 135](#)
- [When a Software Process Fails | 135](#)

The following sections describe how to configure automatic failover to the backup Routing Engine when certain failures occur on the primary Routing Engine.

## Without Interruption to Packet Forwarding

For routers with two Routing Engines, you can configure graceful Routing Engine switchover (GRES). When graceful switchover is configured, socket reconnection occurs seamlessly without interruption to packet forwarding. For information about how to configure graceful Routing Engine switchover, see ["Configuring Graceful Routing Engine Switchover" on page 200](#).

## On Detection of a Hard Disk Error on the Primary Routing Engine

After you configure a backup Routing Engine, you can direct it to take primary role automatically if it detects a hard disk error from the primary Routing Engine. To enable this feature, include the `on-disk-failure` statement at the `[edit chassis redundancy failover]` hierarchy level.

```
[edit chassis redundancy failover]
on-disk-failure;
```

## On Detection of a Broken LCMD Connectivity Between the VM and RE

Set the following configuration that will result in an automatic RE switchover when the LCMD connectivity between VM and RE is broken. To enable this feature, include the `on-loss-of-vm-host-connection` statement at the `[edit chassis redundancy failover]` hierarchy level.

```
[edit chassis redundancy failover]
on-loss-of-vm-host-connection;
```

If the LCMD process is crashing on the primary, the system will switchover after one minute provided the backup RE LCMD connection is stable. The system will not switchover under the following conditions: if the backup RE LCMD connection is unstable or if the current primary just gained primary role. When the primary has just gained primary role, the switchover happens only after four minutes.

## On Detection of a Loss of Keepalive Signal from the Primary Routing Engine

After you configure a backup Routing Engine, you can direct it to take primary role automatically if it detects a loss of keepalive signal from the primary Routing Engine.

To enable failover on receiving a loss of keepalive signal, include the `on-loss-of-keepalives` statement at the `[edit chassis redundancy failover]` hierarchy level:

```
[edit chassis redundancy failover]
on-loss-of-keepalives;
```

When graceful Routing Engine switchover is not configured, by default, failover occurs after 300 seconds (5 minutes). You can configure a shorter or longer time interval.

**NOTE:** The keepalive time period is reset to 360 seconds when the primary Routing Engine has been manually rebooted or halted.

To change the keepalive time period, include the `keepalive-time` statement at the `[edit chassis redundancy]` hierarchy level:

```
[edit chassis redundancy]
keepalive-time seconds;
```

The range for **keepalive-time** is 2 through 10,000 seconds.

The following example describes the sequence of events if you configure the backup Routing Engine to detect a loss of keepalive signal in the primary Routing Engine:

1. Manually configure a **keepalive-time** of 25 seconds.
2. After the Packet Forwarding Engine connection to the primary Routing Engine is lost and the keepalive timer expires, packet forwarding is interrupted.
3. After 25 seconds of keepalive loss, a message is logged, and the backup Routing Engine attempts to take primary role. An alarm is generated when the backup Routing Engine becomes active, and the display is updated with the current status of the Routing Engine.
4. After the backup Routing Engine takes primary role, it continues to function as primary.

**NOTE:** When graceful Routing Engine switchover is configured, the keepalive signal is automatically enabled and the failover time is set to 2 seconds (4 seconds on M20 routers). You cannot manually reset the keepalive time.



**NOTE:** When you halt or reboot the primary Routing Engine, Junos OS resets the keepalive time to 360 seconds, and the backup Routing Engine does not take over primary role until the 360-second keepalive time period expires.

A former primary Routing Engine becomes a backup Routing Engine if it returns to service after a failover to the backup Routing Engine. To restore primary status to the former primary Routing Engine, you can use the **request chassis routing-engine master switch** operational mode command.

If at any time one of the Routing Engines is not present, the remaining Routing Engine becomes primary automatically, regardless of how redundancy is configured.

### On Detection of the em0 Interface Failure on the Primary Routing Engine

After you configure a backup Routing Engine, you instruct it to take primary role automatically if the em0 interface fails on the primary Routing Engine. To enable this feature, include the `on-re-to-fpc-stale` statement at the `[edit chassis redundancy failover]` hierarchy level.

```
[edit chassis redundancy failover]
on-re-to-fpc-stale;
```

### When a Software Process Fails

To configure automatic switchover to the backup Routing Engine if a software process fails, include the `failover other-routing-engine` statement at the `[edit system processes process-name]` hierarchy level:

```
[edit system processes process-name]
failover other-routing-engine;
```

***process-name*** is one of the valid process names. If this statement is configured for a process, and that process fails four times within 30 seconds, the router reboots from the other Routing Engine. Another statement available at the `[edit system processes]` hierarchy level is **failover alternate-media**. For information about the alternate media option, see the [Junos OS Administration Library for Routing Devices](#).

### Manually Switching Routing Engine Primary Role

To manually switch Routing Engine primary role, use one of the following commands:

- On the backup Routing Engine, request that the backup Routing Engine take primary role by issuing the request chassis routing-engine master acquire command.
- On the primary Routing Engine, request that the backup Routing Engine take primary role by using the request chassis routing-engine master release command.
- On either Routing Engine, switch primary role by issuing the request chassis routing-engine master switch command.

## Verifying Routing Engine Redundancy Status

A separate log file is provided for redundancy logging at `/var/log/mastership`. To view the log, use the file `show /var/log/mastership` command. [Table 3 on page 136](#) lists the primary role log event codes and descriptions.

**Table 3: Routing Engine Primary Role Log**

Event Code	Description
E_NULL = 0	The event is a null event.
E_CFG_M	The Routing Engine is configured as primary.
E_CFG_B	The Routing Engine is configured as backup.
E_CFG_D	The Routing Engine is configured as disabled.
E_MAXTRY	The maximum number of tries to acquire or release primary role was exceeded.
E_REQ_C	A claim primary role request was sent.
E_ACK_C	A claim primary role acknowledgement was received.
E_NAK_C	A claim primary role request was not acknowledged.
E_REQ_Y	Confirmation of primary role is requested.
E_ACK_Y	Primary Role is acknowledged.

**Table 3: Routing Engine Primary Role Log (Continued)**

Event Code	Description
E_NAK_Y	Primary Role is not acknowledged.
E_REQ_G	A release primary role request was sent by a Routing Engine.
E_ACK_G	The Routing Engine acknowledged release of primary role.
E_CMD_A	The command <b>request chassis routing-engine master acquire</b> was issued from the backup Routing Engine.
E_CMD_F	The command <b>request chassis routing-engine master acquire force</b> was issued from the backup Routing Engine.
E_CMD_R	The command <b>request chassis routing-engine master release</b> was issued from the primary Routing Engine.
E_CMD_S	The command request <b>chassis routing-engine master switch</b> was issued from a Routing Engine.
E_NO_ORE	No other Routing Engine is detected.
E_TMOUT	A request timed out.
E_NO_IPC	Routing Engine connection was lost.
E_ORE_M	Other Routing Engine state was changed to primary.
E_ORE_B	Other Routing Engine state was changed to backup.
E_ORE_D	Other Routing Engine state was changed to disabled.

## Initial Routing Engine Configuration Example

You can use configuration groups to ensure that the correct IP addresses are used for each Routing Engine and to maintain a single configuration file for both Routing Engines.

The following example defines configuration groups **re0** and **re1** with separate IP addresses. These well-known configuration group names take effect only on the appropriate Routing Engine.

```
groups {
  re0 {
    system {
      host-name my-re0;
    }
    interfaces {
      fxp0 {
        description "10/100 Management interface";
        unit 0 {
          family inet {
            address 10.255.2.40/24;
          }
        }
      }
    }
  }
  re1 {
    system {
      host-name my-re1;
    }
    interfaces {
      fxp0 {
        description "10/100 Management interface";
        unit 0 {
          family inet {
            address 10.255.2.41/24;
          }
        }
      }
    }
  }
}
```

You can assign an additional IP address to the management Ethernet interface (**fxp0** in this example) on both Routing Engines. The assigned address uses the **master-only** keyword and is identical for both Routing Engines, ensuring that the IP address for the primary Routing Engine can be accessed at any time. The address is active only on the primary Routing Engine's management Ethernet interface. During a Routing Engine switchover, the address moves over to the new primary Routing Engine.

For example, on **re0**, the configuration is:

```
[edit groups re0 interfaces fxp0]

unit 0 {
    family inet {
        address 10.17.40.131/25 {
            master-only;
        }
        address 10.17.40.132/25;
    }
}
```

On **re1**, the configuration is:

```
[edit groups re1 interfaces fxp0]

unit 0 {
    family inet {
        address 10.17.40.131/25 {
            master-only;
        }
        address 10.17.40.133/25;
    }
}
```

For more information about the initial configuration of dual Routing Engines, see the [Junos OS Software Installation and Upgrade Guide](#). For more information about assigning an additional IP address to the management Ethernet interface with the **master-only** keyword on both Routing Engines, see the [Junos OS CLI User Guide](#).

## SEE ALSO

[Understanding Routing Engine Redundancy | 124](#)

[Understanding Switching Control Board Redundancy | 15](#)

## Copying a Configuration File from One Routing Engine to the Other

You can use either the console port or the management Ethernet port to establish connectivity between the two Routing Engines. You can then copy or use FTP to transfer the configuration from the primary to the backup, and load the file and commit it in the normal way.

To connect to the other Routing Engine using the management Ethernet port, issue the following command:

```
user@host> request routing-engine login (other-routing-engine | re0 | re1)
```

On a TX Matrix router, to make connections to the other Routing Engine using the management Ethernet port, issue the following command:

```
user@host> request routing-engine login (backup | lcc number | master | other-routing-engine | re0 | re1)
```

For more information about the `request routing-engine login` command, see the [CLI Explorer](#).

To copy a configuration file from one Routing Engine to the other, issue the `file copy` command:

```
user@host> file copy source destination
```

In this case, ***source*** is the name of the configuration file. These files are stored in the directory `/config`. The active configuration is `/config/juniper.conf`, and older configurations are in `/config/juniper.conf {1...9}`. The ***destination*** is a file on the other Routing Engine.

The following example copies a configuration file from Routing Engine 0 to Routing Engine 1:

```
user@host> file copy /config/juniper.conf re1:/var/tmp/copied-juniper.conf
```

The following example copies a configuration file from Routing Engine 0 to Routing Engine 1 on a TX Matrix router:

```
user@host> file copy /config/juniper.conf scc-re1:/var/tmp/copied-juniper.conf
```

To load the configuration file, enter the `load replace` command at the `[edit]` hierarchy level:

```
user@host> load replace /var/tmp/copied-juniper.conf
```



**CAUTION:** Make sure you change any IP addresses specified in the management Ethernet interface configuration on Routing Engine 0 to addresses appropriate for Routing Engine 1.

## SEE ALSO

[Understanding Routing Engine Redundancy | 124](#)

[Understanding Switching Control Board Redundancy | 15](#)

Loading a Software Package from the Other Routing Engine

## Loading a Software Package from the Other Routing Engine

You can load a package from the other Routing Engine onto the local Routing Engine using the existing `request system software add package-name` command:

```
user@host> request system software add re(0|1):/filename
```

In the **re** portion of the URL, specify the number of the other Routing Engine. In the ***filename*** portion of the URL, specify the path to the package. Packages are typically in the directory `/var/sw/pkg`.

## SEE ALSO

[Understanding Routing Engine Redundancy | 124](#)

[Understanding Switching Control Board Redundancy | 15](#)

Copying a Configuration File from One Routing Engine to the Other

## RELATED DOCUMENTATION

[Understanding Routing Engine Redundancy | 124](#)

[Understanding Switching Control Board Redundancy | 15](#)

# 5

PART

## Configuring Load Balancing

---

[Understanding Load Balancing](#) | 143

---



# Understanding Load Balancing

## IN THIS CHAPTER

- [Load Balancing on Aggregated Ethernet Interfaces | 143](#)

## Load Balancing on Aggregated Ethernet Interfaces

### SUMMARY

Load balancing on aggregated ethernet interfaces reduces network congestion by dividing traffic among multiple interfaces.

### IN THIS SECTION

- [Load Balancing and Ethernet Link Aggregation Overview | 144](#)
- [Understanding Aggregated Ethernet Load Balancing | 144](#)
- [Stateful Load Balancing for Aggregated Ethernet Interfaces Using 5-Tuple Data | 146](#)
- [Configuring Stateful Load Balancing on Aggregated Ethernet Interfaces | 150](#)
- [Configuring Adaptive Load Balancing | 151](#)
- [Configuring Symmetrical Load Balancing on an 802.3ad Link Aggregation Group on MX Series Routers | 152](#)
- [Configuring PIC-Level Symmetrical Hashing for Load Balancing on 802.3ad LAGs for MX Series Routers | 160](#)
- [Examples: Configuring PIC-Level Symmetrical Hashing for Load Balancing on 802.3ad LAGs on MX Series Routers | 162](#)
- [Example: Configuring Aggregated Ethernet Load Balancing | 165](#)

When you bundle several physical aggregated Ethernet Interfaces to form a single logical interface, it is called link aggregation. Link aggregation increases bandwidth, provides graceful degradation as failure occurs, increases availability and provides load-balancing capabilities. Load balancing enables the device to divide incoming and outgoing traffic along multiple interfaces to reduce congestion in the network. This topic describes load balancing and how to configure load balancing on your device.

## Load Balancing and Ethernet Link Aggregation Overview

You can create a link aggregation group (LAG) for a group of Ethernet ports. Layer 2 bridging traffic is load balanced across the member links of this group, making the configuration attractive for congestion concerns as well as for redundancy. You can configure up to 128 LAG bundles on M Series, and T Series routers, and 480 LAG bundles on MX Series routers and EX9200 switches. Each LAG bundle contains up to 16 links. (Platform support depends on the Junos OS release in your installation.)

By default, the hash key mechanism to load-balance frames across LAG interfaces is based on Layer 2 fields (such as frame source and destination address) and Layer 3 fields as well as the input *logical interface* (unit). The default LAG algorithm is optimized for Layer 2 switching. Starting with Junos OS Release 10.1, you can also configure the load balancing hash key for Layer 2 traffic to use fields in the Layer 3 and Layer 4 headers using the *payload* statement. However, note that the load-balancing behavior is platform-specific and based on appropriate hash-key configurations.

For more information, see [Configuring Load Balancing on a LAG Link](#). In a Layer 2 switch, one link is overutilized and other links are underutilized.

## Understanding Aggregated Ethernet Load Balancing

The link aggregation feature is used to bundle several physical aggregated Ethernet interfaces to form one logical interface. One or more links are aggregated to form a virtual link or link aggregation group (LAG). The MAC client treats this virtual link as if it were a single link. Link aggregation increases bandwidth, provides graceful degradation as failure occurs, and increases availability.

In addition to these benefits, an aggregated Ethernet bundle is enhanced to provide load-balancing capabilities that ensure that the link utilization among the member links of the aggregated Ethernet bundle are fully and efficiently utilized.

The load-balancing feature allows a device to divide incoming and outgoing traffic along multiple paths or interfaces in order to reduce congestion in the network. Load balancing improves the utilization of various network paths and provides more effective network bandwidth.

Typically, the applications that use load balancing include:

- Aggregated Interfaces (Layer 2)

Aggregated Interfaces (also called AE for aggregated Ethernet, and AS for aggregated SONET) are a Layer 2 mechanism for load-balancing across multiple interfaces between two devices. Because this is a Layer 2 load-balancing mechanism, all of the individual component links must be between the

same two devices on each end. Junos OS supports a non-signaled (static) configuration for Ethernet and SONET, as well as the 802.3ad standardized LACP protocol for negotiation over Ethernet links.

- Equal-Cost Multipath (ECMP) (Layer 3)

By default, when there are multiple equal-cost paths to the same destination for the active route, Junos OS uses a hash algorithm to choose one of the next-hop addresses to install in the forwarding table. Whenever the set of next hops for a destination changes in any way, the next-hop address is rechosen using the hash algorithm. There is also an option that allows multiple next-hop addresses to be installed in the forwarding table, known as per-packet load balancing.

ECMP load balancing can be:

- Across BGP paths (BGP multipath)
- Within a BGP path, across multiple LSPs

In complex Ethernet topologies, traffic imbalances occur due to increased traffic flow, and load balancing becomes challenging for some of the following reasons:

- Incorrect load balancing by aggregate next hops
- Incorrect packet hash computation
- Insufficient variance in the packet flow
- Incorrect pattern selection

As a result of traffic imbalance, the load is not well distributed causing congestion in certain links, whereas some other links are not efficiently utilized.

To overcome these challenges, Junos OS provides the following solutions for resolving the genuine traffic imbalance on aggregated Ethernet bundles (IEEE 802.3ad).

- Adaptive Load Balancing

Adaptive load balancing uses a feedback mechanism to correct a genuine traffic imbalance. To correct the imbalance weights, the bandwidth and packet stream of links are adapted to achieve efficient traffic distribution across the links in an AE bundle.

To configure adaptive load balancing, include the adaptive statement at the [edit interfaces *aex* aggregated-ether-options load-balance] hierarchy level.

**NOTE:** Adaptive load balancing is not supported if the VLAN ID is configured on the aggregated Ethernet interface. This limitation affects the PTX Series Packet Transport Routers and QFX10000 switches only.

To configure the tolerance value as a percentage, include the `tolerance` optional keyword at the `[edit interfaces aex aggregated-ether-options load-balance adaptive]` hierarchy level.

To configure adaptive load balancing based on packets per second (instead of the default bits per second setting), include the `pps` optional keyword at the `[edit interfaces aex aggregated-ether-options load-balance adaptive]` hierarchy level.

To configure the scan interval for the hash value based on the sample rate for the last two seconds, include the `scan-interval` optional keyword at the `[edit interfaces aex aggregated-ether-options load-balance adaptive]` hierarchy level.

**NOTE:** The `pps` and `scan-interval` optional keywords are supported on PTX Series Packet Transport Routers only.

- Per-Packet Random Spray Load Balancing

When the adaptive load-balancing option fails, per-packet random spray load balancing serves as a last resort. It ensures that the members of an AE bundle are equally loaded without taking bandwidth into consideration. Per packet causes packet reordering and hence is recommended only if the applications absorb reordering. Per-packet random spray eliminates traffic imbalance that occurs as a result of software errors, except for packet hash.

To configure per-packet random spray load balancing, include the `per-packet` statement at the `[edit interfaces aex aggregated-ether-options load-balance]` hierarchy level.

The aggregated Ethernet load-balancing solutions are mutually exclusive. When more than one of the load-balancing solutions is configured, the solution that is configured last overrides the previously configured one. You can verify the load-balancing solution being used by issuing the `show interfaces aex aggregated-ether-options load-balance` command.

## SEE ALSO

| *show interfaces (Aggregated Ethernet)*

## Stateful Load Balancing for Aggregated Ethernet Interfaces Using 5-Tuple Data

### IN THIS SECTION

- [Guidelines for Configuring Stateful Load Balancing for Aggregated Ethernet Interfaces or LAG Bundles | 149](#)

When multiple flows are transmitted out of an aggregated Ethernet (ae) interface, the flows must be distributed across the different member links evenly to enable an effective and optimal load-balancing behavior. To obtain a streamlined and robust method of load-balancing, the member link of the aggregated Ethernet interface bundle that is selected each time for load balancing plays a significant part. In Junos OS releases earlier than Release 13.2R1, on MX Series routers with Trio-based FPCs (MPCs), the selection of a member link of the ae interface bundle or the next-hop (or unilist of next-hops) for equal-cost multipath (ECMP) links is performed using a balanced mode next-hop selection methodology and an unbalanced mode of member link or next-hop selection methodology. The balanced mode of link selection uses 'n' bits in a precomputed hash value if it needs to select one of  $2^n$  ( $2$  raised to the power of  $n$ ) next-hop in the unilist. The unbalanced mode of member-link or next-hop selection uses 8 bits in a precomputed hash to select an entry in a selector table, which is randomly done with the member link IDs of the link aggregation group (LAG) or ae bundle.

The term balanced versus unbalanced indicates whether a selector table is used for load balancing mechanism or not. The LAG bundle uses the unbalanced mode (selector table balancing) to balance the traffic across member links. When the traffic flows are minimal, the following problems might occur with the unbalanced mode: The link selection logic utilizes only subset bits of the precomputed hash. Regardless of the efficiency of the hashing algorithm, it is only the compressed representation of a flow. Because the inter-flow variance is very low, the resultant hashes and the subset that are computed do not provide the necessary variability to effectively utilize all the LAG member links. An excessive amount of random nature exists in the hash computation and also in the selector table. As a result, the deviation from being an optimal load-balancing technique for each child link that is selected is higher when the number of flows is lower.

The deviation per child link is defined as

$$V_i = ((C_i - (M/N))) / N$$

where

- $V_i$  denotes the deviation for that child link 'i'.
- $i$  denotes the child link member/index.
- $C_i$  represents the packets transmitted for that child link 'i'.
- $M$  signifies the total packets transmitted on that LAG bundle.
- $N$  denotes the number of child links in that LAG.

Because of these drawbacks, for smaller number of flows, or flows with less inter-flow variance, the link utilization is skewed, and a high probability of a few child links not being utilized entirely exists. Starting with Junos OS Release 13.2R1, the capability to perform uniform load balancing and also perform rebalancing is introduced on MX Series routers with MPCs, except MPC3Es and MPC4Es. Rebalancing is not supported when load-balancing is skewed or distorted owing to a change in the number of flows.

The mechanism to record and retain states for the flows and distribute the traffic load accordingly is added. As a result, for  $m$  number of flows, they are distributed among  $n$  member links of a LAG bundle or among the unicast of next-hops in an ECMP link. This method of splitting the load among member links is called *stateful load balancing* and it uses 5-tuple information (source and destination addresses, protocol, source and destination ports). Such a method can be mapped directly to the flows, or to a precompute hash based on certain fields in the flow. As a result, the deviation observed on each child link is reduced.

This mechanism works efficiently only for minimal number of flows (less than thousands of flows, approximately). For a larger number of flows (between 1000 and 10,000 flows), we recommend that distributed Trio-based load-balancing mechanism is used.

Consider a sample scenario in which ' $n$ ' links in the LAG are identified with link IDs of 0 through  $n-1$ . A hash table or a flow table is used to record the flows as and when they show up. The hashing key is constructed using the fields that uniquely identify a flow. The result of the lookup identifies the `link_id` that the flow is currently using. For each packet, the flow table based on the flow identifier is examined. If a match is found, it denotes a packet that belongs to a flow that is previously processed or detected. The link ID is associated with the flow. If a match is not found, it is the first packet that belongs to the flow. The link ID is used to select the link and the flow is inserted into the flow table.

To enable per-flow load balancing based on hash values, include the `per-flow` statement at the `[edit interfaces aeX unit logical-unit-number forwarding-options load-balance-stateful]` hierarchy level. By default, Junos OS uses a hashing method based only on the destination address to elect a forwarding next hop when multiple equal-cost paths are available. All Packet Forwarding Engine slots are assigned the same hash value by default. To configure the load-balancing algorithm to dynamically rebalance the LAG using existing parameters, include the `rebalance interval` statement at the `[edit interfaces aeX unit logical-unit-number forwarding-options load-balance-stateful]` hierarchy level. This parameter periodically load balances traffic by providing a synchronized rebalance switchover across all the ingress Packet Forwarding Engines (PFEs) over a rebalance interval. You can specify the interval as a value in the range of 1 through 1000 flows per minute. To configure the load type, include the `load-type (low | medium | high)` statement at the `[edit interfaces aeX unit logical-unit-number forwarding-options load-balance-stateful]` hierarchy level.

The `stateful per-flow` option enables the load-balancing capability on AE bundles. The `rebalance` option clears the load balance state at specified intervals. The `load` option informs the Packet Forwarding Engine regarding the appropriate memory pattern to be used. If the number of flows that flow on this aggregated Ethernet interface is less (between 1 and 100 flows), then the `low` keyword can be used. Similarly for relatively higher flows (between 100 and 1000 flows), the `medium` keyword can be used and the `large` keyword can be used for the maximum flows (between 1000 and 10,000 flows). The approximate number of flows for effective load-balancing for each keyword is a derivative.

The `clear interfaces aeX unit logical-unit-number forwarding-options load-balance state` command clears the load balance state at the hardware level and enables rebalancing from the cleaned up, empty state. This clear state is triggered only when you use this command. The `clear interfaces aggregate forwarding-options`

load-balance state command clears all the aggregate Ethernet interface load balancing states and re-creates them newly.

### **Guidelines for Configuring Stateful Load Balancing for Aggregated Ethernet Interfaces or LAG Bundles**

Keep the following points in mind while configuring stateful load-balancing for aggregated Ethernet interfaces:

- When a child link is removed or added, a new aggregate selector is selected and traffic flows onto the new selector. Because the selector is empty, flows are filled in the selector. This behavior causes redistribution of flows because the old state is lost. This is the existing behavior without enabling stateful per-flow load-balancing.
- Stateful per-flow load-balancing functions on AE interfaces if the incoming traffic reaches the MPC1E, MPC2E, MPC3E-3D, MPC5E, and MPC6E line cards. Any other type of line card does not trigger this functionality. Appropriate CLI errors are displayed if the MPCs do not support this capability.

With the ingress line card as MPC and the egress line card as MPC or DPC, this feature works properly. Stateful load-balancing is not supported if the ingress line card is a DPC and the egress line card is a DPC or an MPC.

- This capability is not supported for multicast traffic (native/flood).
- Enabling the rebalance option or clearing the load balance state can cause packet reordering for active flows because different sets of links can be selected for traffic flows.
- Although the feature performance is high, it consumes significant amount of line card memory. Approximately, 4000 logical interfaces or 16 aggregated Ethernet logical interfaces can have this feature enabled on supported MPCs. However, when the Packet Forwarding Engine hardware memory is low, depending upon the available memory, it falls back to the default load balancing mechanism. A system logging message is generated in such a situation and sent to the Routing Engine. A restriction on the number of AE interfaces that support stateful load-balancing does not exist; the limit is determined by the line cards.
- If the traffic flows become aged frequently, then the device needs to remove or refresh the load balancing states. As a result, you must configure rebalancing or run the clear command at periodic intervals for proper load-balancing. Otherwise, traffic skewing can occur. When a child link goes down or comes up, the load balancing behavior does not undergo changes on existing flows. This condition is to avoid packet reordering. New flows pick up the child link that come up. If you observe load distribution to be not very effective, you can clear the load-balancing states or use rebalancing functionality to cause an automatic clearance of the hardware states. When you configure the rebalancing facility, traffic flows can get redirected to different links, which can cause packet reordering.

## Configuring Stateful Load Balancing on Aggregated Ethernet Interfaces

The mechanism to record and retain states for the flows and distribute the traffic load accordingly is added. As a result, for m number of flows, they are distributed among n member links of a LAG bundle or among the unilist of next-hops in an ECMP link. This method of splitting the load among member links is called *stateful load balancing* and it uses 5-tuple information (source and destination addresses, protocol, source and destination ports). Such a method can be mapped directly to the flows, or to a precompute hash based on certain fields in the flow. As a result, the deviation observed on each child link is reduced.

To configure stateful load balancing on ae interface bundles:

1. Specify that you want to configure an aggregated Ethernet interface.

```
[edit]
user@R2# set interfaces aeX unit logical-unit-number
```

2. Specify that you want to configure stateful load-balancing.

```
[edit interfaces aeX unit logical-unit-number]
user@R2# edit forwarding-options load-balance-stateful
```

3. Enable the mechanism to perform an even, effective distribution of traffic flows across member links of an aggregated Ethernet interface (ae) bundle on MX Series routers with MPCs, except MPC3Es and MPC4Es.

```
[edit interfaces aeX unit logical-unit-number load-balance-stateful]
user@R2# set per-flow
```

4. Configure periodic rebalancing of traffic flows of an aggregated Ethernet bundle by clearing the load balance state at a specified interval.

```
[edit interfaces aeX unit logical-unit-number load-balance-stateful]
user@R2# set rebalance interval
```



5. Define the load-balancing type to inform the Packet Forwarding Engine regarding the appropriate memory pattern to be used for traffic flows. The approximate number of flows for effective load-balancing for each keyword is a derivative.

```
[edit interfaces aeX unit logical-unit-number load-balance-stateful]
user@R2# set load-type (low | medium | large)
```

6. Configure the address family and IP address for the ae interface.

```
[edit interfaces aeX unit logical-unit-number]]
user@R2# set family family-name address address
```

## Configuring Adaptive Load Balancing

This topic describes how to configure adaptive load balancing. Adaptive load balancing maintains efficient utilization of member link bandwidth for an aggregated Ethernet (AE) bundle. Adaptive load balancing uses a feedback mechanism to correct traffic load imbalance by adjusting the bandwidth and packet streams on links within an AE bundle.

Before you begin:

- Configure a set of interfaces with a protocol family and IP address. These interfaces can make up the membership for the AE bundle.
- Create an AE bundle by configuring a set of router interfaces as aggregated Ethernet and with a specific AE group identifier.

To configure adaptive load balancing for an AE bundles:

1. Enable adaptive load balancing on the AE bundle:

```
[edit interfaces ae-x aggregated-ether-options load-balance]
user@router# set adaptive
```

2. Configure the scan interval value for adaptive load balancing on the AE bundle. The scan interval value determines the length of the traffic scan by multiplying the integer value with a 30-second time period:

```
[edit interfaces ae-x aggregated-ether-options load-balance adaptive]
user@router# set scan-interval multiplier
```

3. Configure the tolerance percentage value. The tolerance value determines the allowed deviation in the traffic rates among the members of the AE bundle before the router triggers an adaptive load balancing update:

```
[edit interfaces ae-x aggregated-ether-options load-balance adaptive]
user@router# set tolerance percentage
```

4. (Optional) Enable packet-per-second-based adaptive load balancing on the AE bundle:

```
[edit interfaces ae-x aggregated-ether-options load-balance adaptive]
user@router# set pps
```

## SEE ALSO

[adaptive](#) | [937](#)

## Configuring Symmetrical Load Balancing on an 802.3ad Link Aggregation Group on MX Series Routers

### IN THIS SECTION

- [Symmetrical Load Balancing on an 802.3ad LAG on MX Series Routers Overview](#) | [152](#)
- [Configuring Symmetric Load Balancing on an 802.3ad LAG on MX Series Routers](#) | [153](#)
- [Configuring Symmetrical Load Balancing on Trio-Based MPCs](#) | [156](#)
- [Example Configurations](#) | [158](#)

### Symmetrical Load Balancing on an 802.3ad LAG on MX Series Routers Overview

MX Series routers with Aggregated Ethernet PICs support symmetrical load balancing on an 802.3ad LAG. This feature is significant when two MX Series routers are connected transparently through deep packet inspection (DPI) devices over an LAG bundle. DPI devices keep track of flows and require information of a given flow in both forward and reverse directions. Without symmetrical load balancing on an 802.3ad LAG, the DPIs could misunderstand the flow, leading to traffic disruptions. By using this feature, a given flow of traffic (duplex) is ensured for the same devices in both directions.

Symmetrical load balancing on an 802.3ad LAG utilizes a mechanism of interchanging the source and destination addresses for a hash computation of fields, such as source address and destination address. The result of a hash computed on these fields is used to choose the link of the LAG. The hash-computation for the forward and reverse flow must be identical. This is achieved by swapping source fields with destination fields for the reverse flow. The swapped operation is referred to as *complement hash computation* or symmetric-hash complement and the regular (or unswapped) operation as *symmetric-hash computation* or symmetric-hash. The swappable fields are MAC address, IP address, and port.

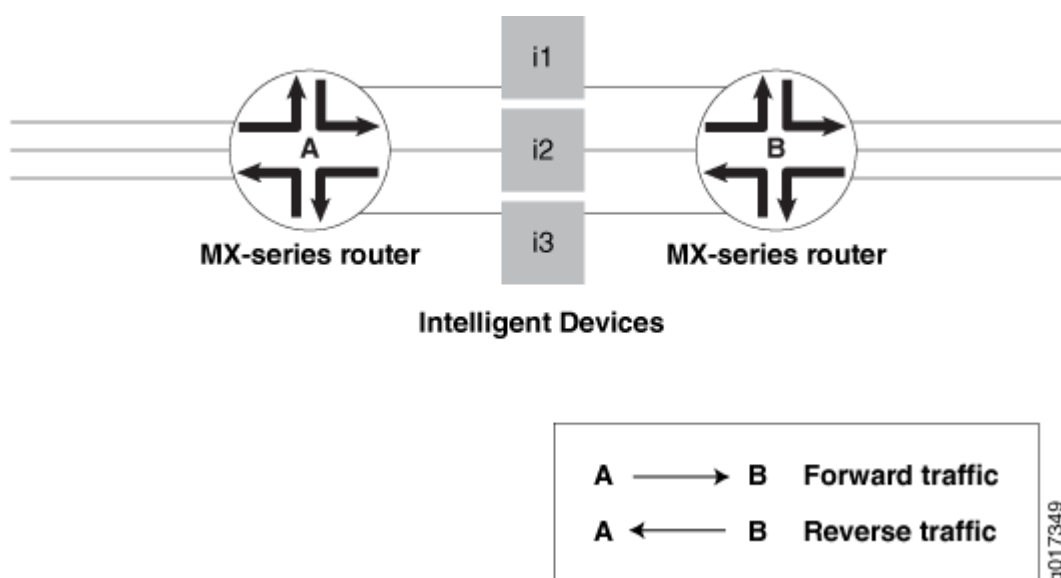
### Configuring Symmetric Load Balancing on an 802.3ad LAG on MX Series Routers

You can specify whether symmetric hash or complement hash is done for load-balancing traffic. To configure symmetric hash, use the `symmetric-hash` statement at the [edit forwarding-options hash-key family inet] hierarchy level. To configure symmetric hash complement, use the `symmetric-hash complement` statement and option at the [edit forwarding-options hash-key family inet] hierarchy level.

These operations can also be performed at the PIC level by specifying a *hash key*. To configure a hash key at the PIC level, use the `symmetric-hash` or `symmetric-hash complement` statement at the [edit chassis hash-key family inet] and [edit chassis hash-key family multiservice] hierarchy levels.

Consider the example in [Figure 6 on page 153](#).

Figure 6: Symmetric Load Balancing on an 802.3ad LAG on MX Series Routers



Router A is configured with symmetric hash and Router B is configured with symmetric hash complement. Thus, for a given flow  $fx$ , post hash computation is from Router A to Router B through i2. The reverse traffic for the same flow  $fx$  is from Router B to Router A through the same i2 device as its

hashing (done after swapping source and destination fields) and returns the same link index; since it is performed on the interchanged source and destination addresses.

However, the link chosen may or may not correspond to what was attached to the DPI. In other words, the hashing result should point to the same links that are connected, so that the traffic flows through the same DPI devices in both directions. To make sure this happens, you need to also configure the counterpart ports (ports that are connected to same DPI-iN) with the identical link index. This is done when configuring a child-link into the LAG bundle. This ensures that the link chosen for a given hash result is always the same on either router.

Note that any two links connected to each other should have the same link index and these link indices must be unique in a given bundle.

**NOTE:** The following restrictions apply when configuring symmetric load balancing on an 802.3ad LAG on MX Series routers:

- The Packet Forwarding Engine (PFE) can be configured to hash the traffic in either symmetric or complement mode. A single PFE complex cannot work simultaneously in both operational modes and such a configuration can yield undesirable results.
- The per-PFE setting overrides the chassis-wide setting only for the family configured. For the other families, the PFE complex still inherits the chassis-wide setting (when configured) or the default setting.
- This feature supports VPLS, INET, and bridged traffic only.
- This feature cannot work in tandem with the per-flow-hash-seed load-balancing option. It requires that all the PFE complexes configured in complementary fashion share the same seed. A change in the seed between two counterpart PFE complexes may yield undesired results.

For additional information, see the [Junos OS VPNs Library for Routing Devices](#) and the [Junos OS Administration Library for Routing Devices](#).

### Example Configuration Statements

To configure 802.3ad LAG parameters at the bundle level:

```
[edit interfaces]
g(x)e-fpc/pic/port {
  gigether-options {
    802.3ad {
      bundle;
      link-index number;
    }
  }
}
```

```

    }
}

```

where the link-index *number* ranges from 0 through 15.

You can check the link index configured above using the `show interfaces` command:

```

[edit forwarding-options hash-key]
family inet {
    layer-3;
    layer-4;
    symmetric-hash {
        [complement;]
    }
}
family multiservice {
    source-mac;
    destination-mac;
    payload {
        ip {
            layer-3 {
                source-ip-only | destination-ip-only;
            }
            layer-4;
        }
    }
    symmetric-hash {
        [complement;]
    }
}
}

```

For load-balancing Layer 2 traffic based on Layer 3 fields, you can configure 802.3ad LAG parameters at a per PIC level. These configuration options are available under the chassis hierarchy as follows:

```

[edit chassis]
fpc X {
    pic Y {
        .
        .
        .
        hash-key {
            family inet {

```

```

        layer-3;
        layer-4;
        symmetric-hash {
            [complement;]
        }
    }
    family multiservice {
        source-mac;
        destination-mac;
        payload {
            ip {
                layer-3 {
                    source-ip-only | destination-ip-only;
                }
                layer-4;
            }
        }
        symmetric-hash {
            [complement;]
        }
    }
}
.
.
.
}
}

```

### Configuring Symmetrical Load Balancing on Trio-Based MPCs

With some configuration differences, symmetrical load-balancing over an 802.3ad link aggregation group is supported on MX Series routers with Trio-based MPCs.

To achieve symmetrical load-balancing on Trio-Based MPCs, the following needs to be done:

- Compute a Symmetrical Hash

Both routers must compute the same hash value from the flow in the forward and reverse directions. On Trio-based platforms, the calculated hash value is independent of the direction of the flow, and hence is always symmetric in nature. For this reason, no specific configuration is needed to compute a symmetric hash value on Trio-based platforms.

However, it should be noted that the fields used to configure the hash should have identical include and exclude settings on both ends of the LAG.

- Configure Link Indexes

To allow both routers to choose the same link using the same hash value, the links within the LAG must be configured with the same link index on both routers. This can be achieved with the `link-index` statement.

- Enable Symmetric Load Balancing

To configure symmetric load balancing on Trio-based MPCs, include the `symmetric` statement at the `[edit forwarding-options enhanced-hash-key]` hierarchy level. This statement is applicable to Trio-based platforms only.

The `symmetric` statement can be used with any protocol family and enables symmetric load-balancing for all aggregated Ethernet bundles on the router. The statement needs to be enabled at both ends of the LAG. This statement is disabled by default.

- Achieve Symmetry for Bridged and Routed Traffic

In some deployments, the LAG bundle on which symmetry is desired is traversed by Layer 2 bridged traffic in the upstream direction and by IPv4 routed traffic in the downstream direction. In such cases, the computed hash is different in each direction because the Ethernet MAC addresses are taken into account for bridged packets. To overcome this, you can exclude source and destination MAC addresses from the enhanced-hash-key computation.

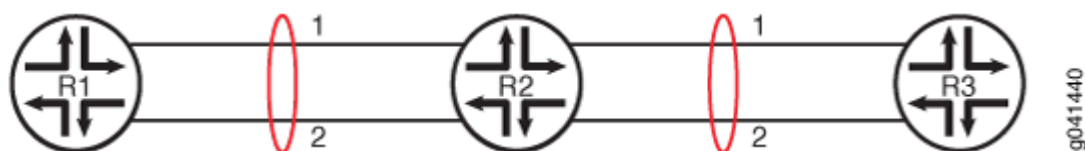
To exclude source and destination MAC addresses from the enhanced-hash-key computation, include the `no-mac-addresses` statement at the `[edit forwarding-options enhanced-hash-key family multiservice]` hierarchy level. This statement is disabled by default.

When symmetrical load balancing is enabled on Trio-based MPCs, keep in mind the following caveats:

- Traffic polarization is a phenomenon that occurs when using topologies that distribute traffic by using hashing of the same type. When routers are cascaded, traffic polarization can occur, and this can lead to unequal traffic distribution.

Traffic polarization occurs when LAGs are configured on cascaded routers. For example, in [Figure 7 on page 158](#), if a certain flow uses Link 1 of the aggregated Ethernet bundle between Device R1 and Device R2, the flow also uses Link 1 of the aggregated Ethernet bundle between Device R2 and Device R3.

**Figure 7: Traffic Polarization on Cascaded Routers When Symmetrical Load Balancing is Enabled on Trio-based MPCs**



This is unlike having a random link selection algorithm, where a flow might use Link 1 of the aggregated Ethernet bundle between Device R1 and Device R2, and Link 2 of the aggregated Ethernet bundle between Device R2 and Device R3.

- Symmetric load balancing is not applicable to per-prefix load-balancing where the hash is computed based on the route prefix.
- Symmetric load balancing is not applicable to MPLS or VPLS traffic, because in these scenarios the labels are not the same in both directions.

### Example Configurations

#### IN THIS SECTION

- [Example Configurations of Chassis Wide Settings | 158](#)
- [Example Configurations of Per-Packet-Forwarding-Engine Settings | 159](#)

### *Example Configurations of Chassis Wide Settings*

#### Router A

```
user@host> show configuration forwarding-options hash-key
family multiservice {
  payload {
    ip {
      layer-3;
    }
  }
  symmetric hash;
}
```



**Router B**

```

user@host> show configuration forwarding-options hash-key
family multiservice {
    payload {
        ip {
            layer-3;
        }
    }
    symmetric-hash {
        complement;
    }
}

```

***Example Configurations of Per-Packet-Forwarding-Engine Settings*****Router A**

```

user@host> show configuration chassis fpc 2 pic 2 hash-key
family multiservice {
    payload {
        ip {
            layer-3;
        }
    }
    symmetric hash;
}

```

**Router B**

```

user@host> show configuration chassis fpc 2 pic 3 hash-key
family multiservice {
    payload {
        ip {
            layer-3;
        }
    }
    symmetric-hash {
        complement;
    }
}

```

```
}
}
```

## RELATED DOCUMENTATION

[Junos OS VPNs Library for Routing Devices](#)

[Junos OS Administration Library for Routing Devices](#)

### Configuring PIC-Level Symmetrical Hashing for Load Balancing on 802.3ad LAGs for MX Series Routers

Symmetrical hashing for load balancing on an 802.3ad Link Aggregation Group (LAG) is useful when two MX Series routers (for example, Router A and Router B) are connected transparently through Deep Packet Inspection (DPI) devices over a LAG bundle. The DPI devices keep track of traffic flows in both the forward and reverse directions.

If symmetrical hashing is configured, the reverse flow of traffic is also directed through the same child link on the LAG and is bound to flow through the same DPI device. This enables proper accounting on the DPI of the traffic in both the forward and reverse flows.

If symmetrical hashing is not configured, a different child link on the LAG might be chosen for the reverse flow of traffic through a different DPI device. This results in incomplete information about the forward and reverse flows of traffic on the DPI device leading to incomplete accounting of the traffic by the DPI device.

Symmetrical hashing is computed based on fields like source address and destination address. You can configure symmetrical hashing both at the chassis level and the PIC level for load balancing based on Layer 2, Layer 3, and Layer 4 data unit fields for family inet (IPv4 protocol family) and multiservice (switch or bridge) traffic. Symmetrical hashing configured at the chassis level is applicable to the entire router, and is inherited by all its PICs and Packet Forwarding Engines. Configuring PIC-level symmetrical hashing provides you more granularity at the Packet Forwarding Engine level.

For the two routers connected through the DPI devices over a LAG bundle, you can configure **symmetric-hash** on one router and **symmetric-hash complement** on the remote-end router or vice-versa.

To configure symmetrical hashing at the chassis level, include the **symmetric-hash** or the **symmetric-hash complement** statements at the [edit forwarding-options hash-key family] hierarchy level. For information about configuring symmetrical hashing at the chassis level and configuring the link index, see the [Junos OS Network Interfaces Library for Routing Devices](#) and the [Junos OS VPNs Library for Routing Devices](#).

**NOTE:** On MX Series DPCs, configuring symmetrical hashing at the PIC level refers to configuring symmetrical hashing at the Packet Forwarding Engine level.

To configure symmetrical hashing at the PIC level on the inbound traffic interface (where traffic enters the router), include the **symmetric-hash** or `symmetric-hash complement` statement at the `[edit chassis fpc slot-number pic pic-number hash-key]` hierarchy level:

```
[edit chassis fpc slot-number pic pic-number hash-key]
family multiservice {
  source-mac;
  destination-mac;
  payload {
    ip {
      layer-3 (source-ip-only | destination-ip-only);
      layer-4;
    }
  }
  symmetric-hash {
    complement;
  }
}
```

```
family inet {
  layer-3;
  layer-4;
  symmetric-hash {
    complement;
  }
}
```

**NOTE:**

- PIC-level symmetrical hashing overrides the chassis-level symmetrical hashing configured at the `[edit chassis forwarding-options hash-key]` hierarchy level.

- Symmetrical hashing for load balancing on 802.3ad Link Aggregation Groups is currently supported for the VPLS, INET and bridged traffic only.
- Hash key configuration on a PIC or Packet Forwarding Engine can be either in the “symmetric hash” or the “symmetric hash complement” mode, but not both at the same time.

## SEE ALSO

*family*

*hash-key*

*inet*

*multiservice*

*payload*

*symmetric-hash*

## Examples: Configuring PIC-Level Symmetrical Hashing for Load Balancing on 802.3ad LAGs on MX Series Routers

### IN THIS SECTION

- [Configuring Symmetrical Hashing for family multiservice on Both Routers | 163](#)
- [Configuring Symmetrical Hashing for family inet on Both Routers | 164](#)
- [Configuring Symmetrical Hashing for family inet and family multiservice on the Two Routers | 164](#)

**NOTE:** These examples are applicable only to the DPCs Supported on MX240, MX480, and MX960 Routers. For the list of DPCs supported, see *DPCs Supported on MX240, MX480, and MX960 Routers* in the Related Documentation section.

The following examples show how to configure symmetrical hashing at the PIC level for load balancing on MX Series routers:

## Configuring Symmetrical Hashing for family multiservice on Both Routers

On the inbound traffic interface where traffic enters Router A, include the `symmetric-hash` statement at the `[edit chassis fpc slot-number pic pic-number hash-key family multiservice]` hierarchy level:

```
[edit chassis fpc 2 pic 2 hash-key]
family multiservice {
  source-mac;
  destination-mac;
  payload {
    ip {
      layer-3;
      layer-4;
    }
  }
  symmetric-hash;
}
```

On the inbound traffic interface where traffic enters Router B, include the `symmetric-hash complement` statement at the `[edit chassis fpc slot-number pic pic-number hash-key family multiservice]` hierarchy level:

```
[edit chassis fpc 0 pic 3 hash-key]
family multiservice {
  source-mac;
  destination-mac;
  payload {
    ip {
      layer-3;
      layer-4;
    }
  }
  symmetric-hash {
    complement;
  }
}
```

## Configuring Symmetrical Hashing for family inet on Both Routers

On the inbound traffic interface where traffic enters Router A, include the `symmetric-hash` statement at the `[edit chassis fpc slot-number pic pic-number hash-key family inet]` hierarchy level:

```
[edit chassis fpc 0 pic 1 hash-key]
family inet {
    layer-3;
    layer-4;
    symmetric-hash;
}
```

On the inbound traffic interface where traffic enters Router B, include the `symmetric-hash complement` statement at the `[edit chassis fpc slot-number pic pic-number hash-key family inet]` hierarchy level:

```
[edit chassis fpc 1 pic 2 hash-key]
family inet {
    layer-3;
    layer-4;
    symmetric-hash {
        complement;
    }
}
```

## Configuring Symmetrical Hashing for family inet and family multiservice on the Two Routers

On the inbound traffic interface where traffic enters Router A, include the `symmetric-hash` statement at the `[edit chassis fpc slot-number pic pic-number hash-key family multiservice]` hierarchy level:

```
[edit chassis fpc 1 pic 0 hash-key]
family multiservice {
    payload {
        ip {
            layer-3;
            layer-4;
        }
    }
    symmetric-hash;
}
```

On the inbound traffic interface where traffic enters Router B, include the `symmetric-hash complement` statement at the `[edit chassis fpc slot-number pic pic-number hash-key family inet]` hierarchy level:

```
[edit chassis fpc 0 pic 3 hash-key]
family inet {
    layer-3;
    layer-4;
    symmetric-hash {
        complement;
    }
}
```

## SEE ALSO

[DPCs Supported on MX240, MX480, and MX960 Routers](#)

## Example: Configuring Aggregated Ethernet Load Balancing

### IN THIS SECTION

- [Example: Configuring Aggregated Ethernet Load Balancing | 165](#)

## Example: Configuring Aggregated Ethernet Load Balancing

### IN THIS SECTION

- [Requirements | 166](#)
- [Overview | 166](#)
- [Configuration | 168](#)
- [Verification | 181](#)

This example shows how to configure aggregated Ethernet load balancing.

## Requirements

This example uses the following hardware and software components:

- Three MX Series routers with MIC and MPC interfaces or three PTX Series Packet Transport Routers with PIC and FPC interfaces
- Junos OS Release 13.3 or later running on all devices

## Overview

### IN THIS SECTION

- [Topology | 168](#)

Load balancing is required on the forwarding plane when there are multiple paths or interfaces available to the next hop router, and it is best if the incoming traffic is load balanced across all available paths for better link utilization.

Aggregated Ethernet bundle is a typical application that uses load balancing to balance traffic flows across the member links of the bundle (IEEE 802.3ad).

Starting with Junos OS Release 13.3, aggregated Ethernet load balancing is enhanced to provide two solutions for resolving genuine traffic imbalance on aggregated Ethernet bundles on MICs or MPCs of MX Series routers. Starting with Junos OS Release 14.1, aggregated Ethernet load balancing is enhanced to provide two solutions for resolving genuine traffic imbalance on aggregated Ethernet bundles on PICs or FPCs of PTX Series Packet Transport Routers.

The aggregated Ethernet load-balancing solutions are:

- **Adaptive**—Adaptive load balancing is used in scenarios where flow-based hashing is not sufficient to achieve a uniform load distribution. This load-balancing solution implements a real-time feedback and control mechanism to monitor and manage imbalances in network load.

The adaptive load-balancing solution corrects the traffic flow imbalance by modifying the selector entries, and periodically scanning the link utilization on each member link of the AE bundle to detect any deviations. When a deviation is detected, an adjustment event is triggered and fewer flows are mapped to the affected member link. As a result, the offered bandwidth of that member link goes down. This causes a continuous feedback loop, which over a period of time ensures that the same amount of byte rate is offered to all the member links, thus providing efficient traffic distribution across each member link in the AE bundle.

To configure adaptive load balancing, include the `adaptive` statement at the `[edit interfaces aex aggregated-ether-options load-balance]` hierarchy level.



**NOTE:** Adaptive load balancing is not supported if the VLAN ID is configured on the aggregated Ethernet interface. This limitation affects the PTX Series Packet Transport Routers only.

The `pps` option enables load balancing based on the packets-per-second rate. The default setting is bits-per-second load balancing.

The `scan-interval` value configures the length of time for scanning as a multiple of 30 seconds.

The `tolerance` value is the limit to the variance in the packet traffic flow to the aggregated Ethernet links in the bundle. You can specify a maximum of 100-percent variance. When the `tolerance` attribute is not configured, a default value of 20 percent is enabled for adaptive load balancing. A smaller tolerance value balances better bandwidth, but takes a longer convergence time.

**NOTE:** The `pps` and `scan-interval` optional keywords are supported on PTX Series Packet Transport Routers only.

- **Per-packet random spray**—When the adaptive load-balancing solution fails, per-packet random spray acts as a last resort. The per-packet random spray load-balancing solution helps to address traffic imbalance by randomly spraying the packets to the aggregate next hops. This ensures that all the member links of the AE bundle are equally loaded, resulting in packet reordering.

In addition, per-packet random spray identifies the ingress Packet Forwarding Engine that caused the traffic imbalance and eliminates traffic imbalance that occurs as a result of software errors, except for packet hash.

To configure per-packet random spray load balancing, include the `per-packet` statement at the `[edit interfaces aex aggregated-ether-options load-balance]` hierarchy level.

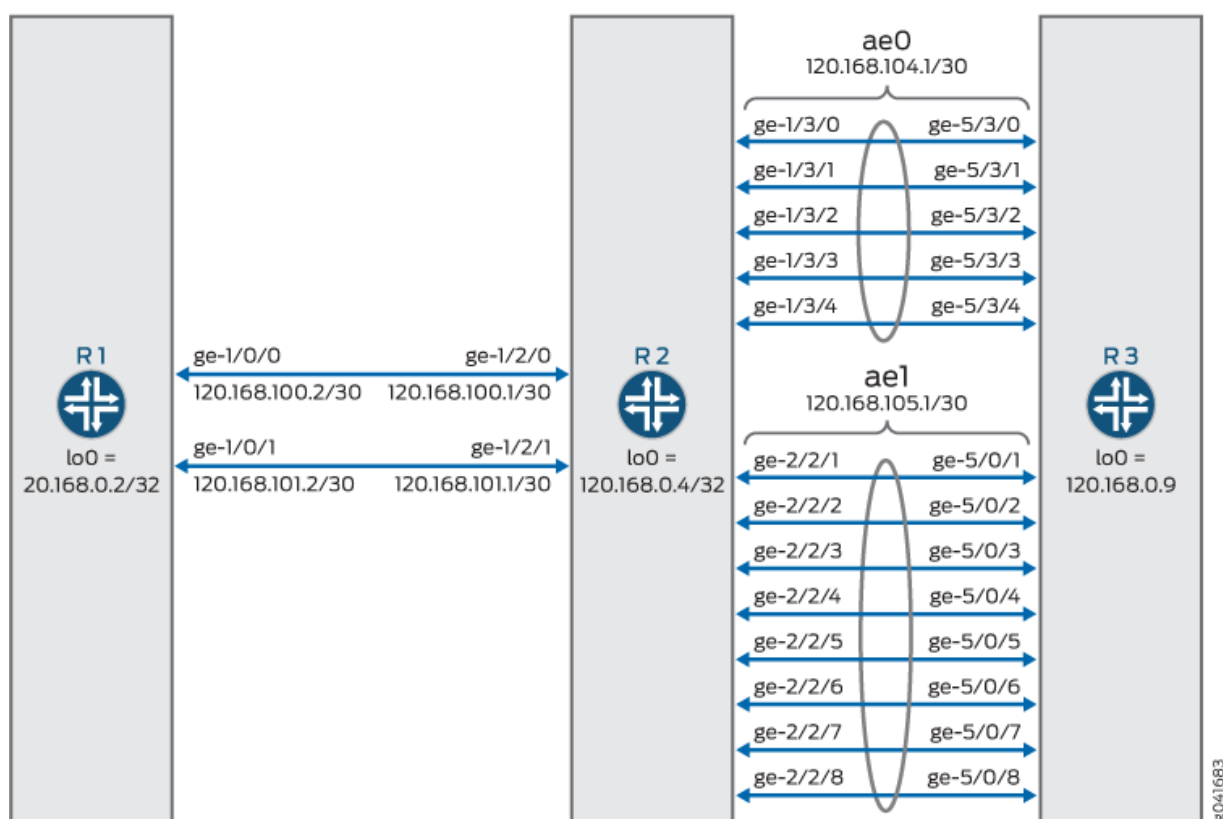
**NOTE:** The Per-Packet option for load balancing is not supported on the PTX Series Packet Transport Routers.

The aggregated Ethernet load-balancing solutions are mutually exclusive. When more than one of the load-balancing solutions is configured, the solution that is configured last overrides the previously configured one. You can verify the load-balancing solution being implemented by issuing the `show interfaces aex aggregated-ether-options load-balance` command.

## Topology

In this topology, two aggregated Ethernet bundles - ae0 and ae1 - are configured on the links between the R2 and R3 routers.

Figure 8: Aggregated Ethernet Load Balancing



## Configuration

### IN THIS SECTION

- [CLI Quick Configuration | 169](#)
- [Configuring Adaptive Load Balancing | 174](#)
- [Results | 177](#)

### CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the [edit] hierarchy level.

R1

```
set chassis aggregated-devices ethernet device-count 12
set interfaces xe-0/0/0 unit 0 family inet address 120.168.1.1/30
set interfaces xe-0/0/0 unit 0 family iso
set interfaces xe-0/0/0 unit 0 family mpls
set interfaces xe-0/0/1 unit 0 family inet address 120.168.2.1/30
set interfaces xe-0/0/1 unit 0 family iso
set interfaces xe-0/0/1 unit 0 family mpls
set interfaces ge-1/0/0 unit 0 family inet address 120.168.100.2/30
set interfaces ge-1/0/0 unit 0 family iso
set interfaces ge-1/0/0 unit 0 family mpls
set interfaces ge-1/0/1 unit 0 family inet address 120.168.101.2/30
set interfaces ge-1/0/1 unit 0 family iso
set interfaces ge-1/0/1 unit 0 family mpls
set interfaces lo0 unit 0 family inet address 120.168.0.2/32
set interfaces lo0 unit 0 family iso address 49.0001.1201.6800.0002.00
set routing-options router-id 120.168.0.2
set routing-options autonomous-system 55
set protocols rsvp interface ge-1/0/0.0
set protocols rsvp interface ge-1/0/1.0
set protocols mpls label-switched-path videl-to-sweets to 120.168.0.9
set protocols mpls label-switched-path v-2-s-601 to 60.0.1.0
set protocols mpls label-switched-path v-2-s-601 primary v-2-s-601-primary hop-limit 5
set protocols mpls label-switched-path v-2-s-602 to 60.0.2.0
set protocols mpls label-switched-path v-2-s-602 primary v-2-s-602-primary hop-limit 5
set protocols mpls label-switched-path v-2-s-603 to 60.0.3.0
set protocols mpls label-switched-path v-2-s-604 to 60.0.4.0
set protocols mpls path v-2-s-601-primary 120.168.100.1 strict
set protocols mpls path v-2-s-601-primary 120.168.104.2 strict
set protocols mpls path v-2-s-602-primary 120.168.101.1 strict
set protocols mpls path v-2-s-602-primary 120.168.105.2 strict
set protocols mpls interface ge-1/0/0.0
set protocols mpls interface ge-1/0/1.0
set protocols bgp group pe-routers type internal
set protocols bgp group pe-routers local-address 120.168.0.2
```

```

set protocols bgp group pe-routers family inet unicast
set protocols bgp group pe-routers family inet-vpn unicast
set protocols bgp group pe-routers neighbor 120.168.0.9
set protocols isis traffic-engineering family inet shortcuts
set protocols isis level 1 disable
set protocols isis interface ge-1/0/0.0
set protocols isis interface ge-1/0/1.0
set protocols isis interface lo0.0
set policy-options policy-statement nhs then next-hop self
set policy-options policy-statement vpn-m5-export term 1 from protocol bgp
set policy-options policy-statement vpn-m5-export term 1 from protocol direct
set policy-options policy-statement vpn-m5-export term 1 then community add vpn-m5-target
set policy-options policy-statement vpn-m5-export term 1 then accept
set policy-options policy-statement vpn-m5-export term 2 then reject
set policy-options policy-statement vpn-m5-import term 1 from protocol bgp
set policy-options policy-statement vpn-m5-import term 1 from community vpn-m5-target
set policy-options policy-statement vpn-m5-import term 1 then accept
set policy-options policy-statement vpn-m5-import term 2 then reject
set policy-options community vpn-m5-target members target:55:100
set routing-instances vpn-m5 instance-type vrf
set routing-instances vpn-m5 interface xe-0/0/0.0
set routing-instances vpn-m5 interface xe-0/0/1.0
set routing-instances vpn-m5 route-distinguisher 120.168.0.2:1
set routing-instances vpn-m5 vrf-import vpn-m5-import
set routing-instances vpn-m5 vrf-export vpn-m5-export
set routing-instances vpn-m5 protocols bgp group ce type external
set routing-instances vpn-m5 protocols bgp group ce peer-as 100
set routing-instances vpn-m5 protocols bgp group ce as-override
set routing-instances vpn-m5 protocols bgp group ce neighbor 120.168.1.2
set routing-instances vpn-m5 protocols bgp group ce neighbor 120.168.2.2
set routing-instances vpn-m5 protocols ospf domain-id 1.0.0.0
set routing-instances vpn-m5 protocols ospf export vpn-m5-import
set routing-instances vpn-m5 protocols ospf area 0.0.0.0 interface xe-0/0/1.0
set routing-instances vpn-m5 protocols ospf area 0.0.0.0 interface xe-0/0/0.0

```

## R2

```

set chassis aggregated-devices ethernet device-count 5
set interfaces ge-1/2/0 unit 0 family inet address 120.168.100.1/30
set interfaces ge-1/2/0 unit 0 family iso
set interfaces ge-1/2/0 unit 0 family mpls
set interfaces ge-1/2/1 unit 0 family inet address 120.168.101.1/30

```

```

set interfaces ge-1/2/1 unit 0 family iso
set interfaces ge-1/2/1 unit 0 family mpls
set interfaces ge-1/3/0 gigether-options 802.3ad ae0
set interfaces ge-1/3/1 gigether-options 802.3ad ae0
set interfaces ge-1/3/2 gigether-options 802.3ad ae0
set interfaces ge-1/3/3 gigether-options 802.3ad ae0
set interfaces ge-1/3/4 gigether-options 802.3ad ae0
set interfaces ge-2/2/1 gigether-options 802.3ad ae1
set interfaces ge-2/2/2 gigether-options 802.3ad ae1
set interfaces ge-2/2/3 gigether-options 802.3ad ae1
set interfaces ge-2/2/4 gigether-options 802.3ad ae1
set interfaces ge-2/2/5 gigether-options 802.3ad ae1
set interfaces ge-2/2/6 gigether-options 802.3ad ae1
set interfaces ge-2/2/7 gigether-options 802.3ad ae1
set interfaces ge-2/2/8 gigether-options 802.3ad ae1
set interfaces ae0 aggregated-ether-options load-balance adaptive tolerance 10
set interfaces ae0 aggregated-ether-options link-speed 1g
set interfaces ae0 aggregated-ether-options lacp active
set interfaces ae0 unit 0 family inet address 120.168.104.1/30
set interfaces ae0 unit 0 family iso
set interfaces ae0 unit 0 family mpls
set interfaces ae1 aggregated-ether-options load-balance adaptive tolerance 10
set interfaces ae1 aggregated-ether-options link-speed 1g
set interfaces ae1 aggregated-ether-options lacp active
set interfaces ae1 unit 0 family inet address 120.168.105.1/30
set interfaces ae1 unit 0 family iso
set interfaces ae1 unit 0 family mpls
set interfaces lo0 unit 0 family inet address 120.168.0.4/32
set interfaces lo0 unit 0 family iso address 49.0001.1201.6800.0004.00
set accounting-options selective-aggregate-interface-stats disable
set protocols rsvp interface ge-1/2/0.0
set protocols rsvp interface ge-1/2/1.0
set protocols rsvp interface ae0.0
set protocols rsvp interface ae1.0
set protocols mpls interface ge-1/2/0.0
set protocols mpls interface ge-1/2/1.0
set protocols mpls interface ae0.0
set protocols mpls interface ae1.0
set protocols isis traffic-engineering family inet shortcuts
set protocols isis level 1 disable
set protocols isis interface ge-1/2/0.0
set protocols isis interface ge-1/2/1.0
set protocols isis interface ae0.0

```

```
set protocols isis interface ae1.0
set protocols isis interface lo0.0
```

### R3

```
set chassis aggregated-devices ethernet device-count 5
set interfaces xe-4/0/0 unit 0 family inet address 120.168.9.1/30
set interfaces xe-4/0/0 unit 0 family mpls
set interfaces xe-4/0/1 unit 0 family inet address 120.168.10.1/30
set interfaces xe-4/0/1 unit 0 family mpls
set interfaces ge-5/0/1 gigether-options 802.3ad ae1
set interfaces ge-5/0/2 gigether-options 802.3ad ae1
set interfaces ge-5/0/3 gigether-options 802.3ad ae1
set interfaces ge-5/0/4 gigether-options 802.3ad ae1
set interfaces ge-5/0/5 gigether-options 802.3ad ae1
set interfaces ge-5/0/6 gigether-options 802.3ad ae1
set interfaces ge-5/0/7 gigether-options 802.3ad ae1
set interfaces ge-5/0/8 gigether-options 802.3ad ae1
set interfaces ge-5/3/0 gigether-options 802.3ad ae0
set interfaces ge-5/3/1 gigether-options 802.3ad ae0
set interfaces ge-5/3/2 gigether-options 802.3ad ae0
set interfaces ge-5/3/3 gigether-options 802.3ad ae0
set interfaces ge-5/3/4 gigether-options 802.3ad ae0
set interfaces ae0 aggregated-ether-options link-speed 1g
set interfaces ae0 aggregated-ether-options lacp active
set interfaces ae0 unit 0 family inet address 120.168.104.2/30
set interfaces ae0 unit 0 family iso
set interfaces ae0 unit 0 family mpls
set interfaces ae1 aggregated-ether-options link-speed 1g
set interfaces ae1 aggregated-ether-options lacp active
set interfaces ae1 unit 0 family inet address 120.168.105.2/30
set interfaces ae1 unit 0 family iso
set interfaces ae1 unit 0 family mpls
set interfaces lo0 unit 0 family inet address 120.168.0.9/32
set interfaces lo0 unit 0 family iso address 49.0001.1201.6800.0009.00
set routing-options router-id 120.168.0.9
set routing-options autonomous-system 55
set protocols rsvp interface xe-4/0/0.0
set protocols rsvp interface xe-4/0/1.0
set protocols rsvp interface ae0.0
set protocols rsvp interface ae1.0
set protocols mpls label-switched-path to-videl to 120.168.0.2
```

```

set protocols mpls interface xe-4/0/0.0
set protocols mpls interface xe-4/0/1.0
set protocols mpls interface ae0.0
set protocols mpls interface ae1.0
set protocols bgp group pe-routers type internal
set protocols bgp group pe-routers local-address 120.168.0.9
set protocols bgp group pe-routers family inet unicast
set protocols bgp group pe-routers family inet-vpn unicast
set protocols bgp group pe-routers neighbor 120.168.0.2
set protocols isis traffic-engineering family inet shortcuts
set protocols isis level 1 disable
set protocols isis interface ae0.0
set protocols isis interface ae1.0
set protocols isis interface lo0.0
set policy-options policy-statement nhs then next-hop self
set policy-options policy-statement vpn-m5-export term 1 from protocol bgp
set policy-options policy-statement vpn-m5-export term 1 from protocol direct
set policy-options policy-statement vpn-m5-export term 1 then community add vpn-m5-target
set policy-options policy-statement vpn-m5-export term 1 then accept
set policy-options policy-statement vpn-m5-export term 2 then reject
set policy-options policy-statement vpn-m5-import term 1 from protocol bgp
set policy-options policy-statement vpn-m5-import term 1 from protocol direct
set policy-options policy-statement vpn-m5-import term 1 from community vpn-m5-target
set policy-options policy-statement vpn-m5-import term 1 then accept
set policy-options policy-statement vpn-m5-import term 2 then reject
set policy-options community vpn-m5-target members target:55:100
set routing-instances vpn-m5 instance-type vrf
set routing-instances vpn-m5 interface xe-4/0/0.0
set routing-instances vpn-m5 interface xe-4/0/1.0
set routing-instances vpn-m5 route-distinguisher 120.168.0.9:1
set routing-instances vpn-m5 vrf-import vpn-m5-import
set routing-instances vpn-m5 vrf-export vpn-m5-export
set routing-instances vpn-m5 protocols bgp group ce type external
set routing-instances vpn-m5 protocols bgp group ce peer-as 100
set routing-instances vpn-m5 protocols bgp group ce as-override
set routing-instances vpn-m5 protocols bgp group ce neighbor 120.168.9.2
set routing-instances vpn-m5 protocols bgp group ce neighbor 120.168.10.2
set routing-instances vpn-m5 protocols ospf domain-id 1.0.0.0
set routing-instances vpn-m5 protocols ospf export vpn-m5-import
set routing-instances vpn-m5 protocols ospf area 0.0.0.0 interface xe-4/0/0.0
set routing-instances vpn-m5 protocols ospf area 0.0.0.0 interface xe-4/0/1.0

```

## Configuring Adaptive Load Balancing

### Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see [Using the CLI Editor in Configuration Mode](#).

To configure the R2 router:

**NOTE:** Repeat this procedure for the other routers, after modifying the appropriate interface names, addresses, and any other parameters for each router.

1. Specify the number of aggregated Ethernet interfaces to be created.

```
[edit chassis]
user@R2# set aggregated-devices ethernet device-count 5
```

2. Configure the Gigabit Ethernet interface link connecting R2 to R1.

```
[edit interfaces]
user@R2# set ge-1/2/0 unit 0 family inet address 120.168.100.1/30
user@R2# set ge-1/2/0 unit 0 family iso
user@R2# set ge-1/2/0 unit 0 family mpls
user@R2# set ge-1/2/1 unit 0 family inet address 120.168.101.1/30
user@R2# set ge-1/2/1 unit 0 family iso
user@R2# set ge-1/2/1 unit 0 family mpls
user@R2# set lo0 unit 0 family inet address 120.168.0.4/32
user@R2# set lo0 unit 0 family iso address 49.0001.1201.6800.0004.00
```

3. Configure the five member links of the ae0 aggregated Ethernet bundle.

```
[edit interfaces]
user@R2# set ge-1/3/0 gigether-options 802.3ad ae0
user@R2# set ge-1/3/1 gigether-options 802.3ad ae0
user@R2# set ge-1/3/2 gigether-options 802.3ad ae0
user@R2# set ge-1/3/3 gigether-options 802.3ad ae0
user@R2# set ge-1/3/4 gigether-options 802.3ad ae0
```



4. Configure the eight member links of the ae1 aggregated Ethernet bundle.

```
[edit interfaces]
user@R2# set ge-2/2/1 gigether-options 802.3ad ae1
user@R2# set ge-2/2/2 gigether-options 802.3ad ae1
user@R2# set ge-2/2/3 gigether-options 802.3ad ae1
user@R2# set ge-2/2/4 gigether-options 802.3ad ae1
user@R2# set ge-2/2/5 gigether-options 802.3ad ae1
user@R2# set ge-2/2/6 gigether-options 802.3ad ae1
user@R2# set ge-2/2/7 gigether-options 802.3ad ae1
user@R2# set ge-2/2/8 gigether-options 802.3ad ae1
```

5. Enable aggregate Ethernet load balancing on ae0 of R2.

```
[edit interfaces]
user@R2# set ae0 aggregated-ether-options load-balance adaptive tolerance 10
```

6. Configure the link speed for the ae0 aggregated Ethernet bundle.

```
[edit interfaces]
user@R2# set ae0 aggregated-ether-options link-speed 1g
```

7. Configure LACP on the ae0 aggregated Ethernet bundle.

```
[edit interfaces]
user@R2# set ae0 aggregated-ether-options lacp active
```

8. Configure the interface parameters for the ae0 aggregated Ethernet bundle.

```
[edit interfaces]
user@R2# set ae0 unit 0 family inet address 120.168.104.1/30
user@R2# set ae0 unit 0 family iso
user@R2# set ae0 unit 0 family mpls
```

9. Enable aggregate Ethernet load balancing on ae1 of R2.

```
[edit interfaces]
user@R2# set ae1 aggregated-ether-options load-balance adaptive tolerance 10
```

10. Configure the link speed for the ae1 aggregated Ethernet bundle.

```
[edit interfaces]
user@R2# set ae1 aggregated-ether-options link-speed 1g
```

11. Configure LACP on the ae1 aggregated Ethernet bundle.

```
[edit interfaces]
user@R2# set ae1 aggregated-ether-options lacp active
```

12. Configure the interface parameters for the ae1 aggregated Ethernet bundle.

```
[edit interfaces]
user@R2# set ae1 unit 0 family inet address 120.168.105.1/30
user@R2# set ae1 unit 0 family iso
user@R2# set ae1 unit 0 family mpls
```

13. Disable selective aggregate Ethernet statistics.

```
[edit accounting-options]
user@R2# set selective-aggregate-interface-stats disable
```

14. Configure RSVP on all the interfaces of R2 and on the AE bundles.

```
[edit protocols]
user@R2# set rsvp interface ge-1/2/0.0
user@R2# set rsvp interface ge-1/2/1.0
user@R2# set rsvp interface ae0.0
user@R2# set rsvp interface ae1.0
```

15. Configure MPLS on all the interfaces of R2 and on the AE bundles.

```
[edit protocols]
user@R2# set mpls interface ge-1/2/0.0
user@R2# set mpls interface ge-1/2/1.0
user@R2# set mpls interface ae0.0
user@R2# set mpls interface ae1.0
```

16. Configure IS-IS on all the interfaces of R2 and on the AE bundles.

```
[edit protocols]
user@R2# set isis traffic-engineering family inet shortcuts
user@R2# set isis level 1 disable
user@R2# set isis interface ge-1/2/0.0
user@R2# set isis interface ge-1/2/1.0
user@R2# set isis interface ae0.0
user@R2# set isis interface ae1.0
user@R2# set isis interface lo0.0
```

## Results

From configuration mode, confirm your configuration by entering the `show chassis`, `show interfaces`, `show accounting-options`, and `show protocols` commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@R2# show chassis
aggregated-devices {
  ethernet {
    device-count 5;
  }
}
```

```
user@R2# show interfaces
ge-1/2/0 {
  unit 0 {
    family inet {
      address 120.168.100.1/30;
    }
  }
}
```

```

        family iso;
        family mpls;
    }
}
ge-1/2/1 {
    unit 0 {
        family inet {
            address 120.168.101.1/30;
        }
        family iso;
        family mpls;
    }
}
ge-1/3/0 {
    gigether-options {
        802.3ad ae0;
    }
}
ge-1/3/1 {
    gigether-options {
        802.3ad ae0;
    }
}
ge-1/3/2 {
    gigether-options {
        802.3ad ae0;
    }
}
ge-1/3/3 {
    gigether-options {
        802.3ad ae0;
    }
}
ge-1/3/4 {
    gigether-options {
        802.3ad ae0;
    }
}
ge-2/2/1 {
    gigether-options {
        802.3ad ae1;
    }
}
}

```

```
ge-2/2/2 {
    gigether-options {
        802.3ad ae1;
    }
}
ge-2/2/3 {
    gigether-options {
        802.3ad ae1;
    }
}
ge-2/2/4 {
    gigether-options {
        802.3ad ae1;
    }
}
ge-2/2/5 {
    gigether-options {
        802.3ad ae1;
    }
}
ge-2/2/6 {
    gigether-options {
        802.3ad ae1;
    }
}
ge-2/2/7 {
    gigether-options {
        802.3ad ae1;
    }
}
ge-2/2/8 {
    gigether-options {
        802.3ad ae1;
    }
}
ae0 {
    aggregated-ether-options {
        load-balance {
            adaptive tolerance 10;
        }
        link-speed 1g;
        lacp {
            active;
        }
    }
}
```

```

    }
}
unit 0 {
    family inet {
        address 120.168.104.1/30;
    }
    family iso;
    family mpls;
}
}
ae1 {
    aggregated-ether-options {
        load-balance {
            adaptive tolerance 10;
        }
        link-speed 1g;
        lacp {
            active;
        }
    }
}
unit 0 {
    family inet {
        address 120.168.105.1/30;
    }
    family iso;
    family mpls;
}
}
lo0 {
    unit 0 {
        family inet {
            address 120.168.0.4/32;
        }
        family iso {
            address 49.0001.1201.6800.0004.00;
        }
    }
}

```

```
}
}
```

```
user@R2# show accounting-options
selective-aggregate-interface-stats disable;
```

```
user@R2# show protocols
rsvp {
    interface ge-1/2/0.0;
    interface ge-1/2/1.0;
    interface ae0.0;
    interface ae1.0;
}
mpls {
    interface ge-1/2/0.0;
    interface ge-1/2/1.0;
    interface ae0.0;
    interface ae1.0;
}
isis {
    traffic-engineering {
        family inet {
            shortcuts;
        }
    }
    level 1 disable;
    interface ge-1/2/0.0;
    interface ge-1/2/1.0;
    interface ae0.0;
    interface ae1.0;
    interface lo0.0;
}
```

## Verification

### IN THIS SECTION

- [Verifying Adaptive Load Balancing on ae0 | 182](#)

Confirm that the configuration is working properly.

### ***Verifying Adaptive Load Balancing on ae0***

#### **Purpose**

Verify that packets received on the ae0 aggregated Ethernet bundle are load-balanced among the five member links.

#### **Action**

From operational mode, run the `show interfaces ae0 extensive` command.

```
user@R2> show interfaces ae0 extensive
Logical interface ae0.0 (Index 325) (SNMP ifIndex 917) (Generation 134)
Flags: SNMP-Traps 0x4004000 Encapsulation: ENET2
Statistics          Packets          pps          Bytes          bps
Bundle:
  Input :           848761             9      81247024       7616
  Output: 166067308909    3503173 126900990064983 21423804256
Adaptive Statistics:
  Adaptive Adjusts:         264
  Adaptive Scans  :       27682
  Adaptive Updates:         10
Link:
  ge-1/3/0.0
    Input :           290888             5      29454436       3072
    Output: 33183442699    704569 25358563587277 4306031760
  ge-1/3/1.0
    Input :           162703             1      14806325        992
    Output: 33248375409    705446 25406995966732 4315342152
  ge-1/3/2.0
    Input :           127448             1      12130566        992
    Output: 33184552729    697572 25354827700261 4267192376
  ge-1/3/3.0
    Input :           121044             1      11481262       1280
    Output: 33245875402    697716 25405953405192 4265750584
  ge-1/3/4.0
    Input :           146678             1      13374435       1280
    Output: 33205071207    697870 25374651121458 4269487384
```



## Meaning

The member links of the ae0 aggregated Ethernet bundle are fully utilized with adaptive load balancing.

### Release History Table

Release	Description
14.1	Starting with Junos OS Release 14.1, aggregated Ethernet load balancing is enhanced to provide two solutions for resolving genuine traffic imbalance on aggregated Ethernet bundles on PICs or FPCs of PTX Series Packet Transport Routers.
13.3	Starting with Junos OS Release 13.3, aggregated Ethernet load balancing is enhanced to provide two solutions for resolving genuine traffic imbalance on aggregated Ethernet bundles on MICs or MPCs of MX Series routers.
13.2R1	Starting with Junos OS Release 13.2R1, the capability to perform uniform load balancing and also perform rebalancing is introduced on MX Series routers with MPCs, except MPC3Es and MPC4Es.
10.1	Starting with Junos OS Release 10.1, you can also configure the load balancing hash key for Layer 2 traffic to use fields in the Layer 3 and Layer 4 headers using the <code>payload</code> statement.



# Configuring Graceful Routing Engine Switchover (GRES)

---

Understanding How GRES Enables Uninterrupted Packet Forwarding During a  
Routing Engine Switchover | 185

Configuring GRES | 200

Configuring Ethernet Automatic Protection Switching for High Availability | 212

---

# Understanding How GRES Enables Uninterrupted Packet Forwarding During a Routing Engine Switchover

## IN THIS CHAPTER

- [Understanding Graceful Routing Switchover | 185](#)

## Understanding Graceful Routing Switchover

### IN THIS SECTION

- [Understanding Graceful Routing Engine Switchover | 185](#)
- [Graceful Routing Engine Switchover System Requirements | 194](#)

## Understanding Graceful Routing Engine Switchover

### IN THIS SECTION

- [Graceful Routing Engine Switchover Concepts | 186](#)
- [Effects of a Routing Engine Switchover | 191](#)
- [Graceful Routing Engine Switchover on Aggregated Services interfaces | 193](#)

This topic contains the following sections:

## Graceful Routing Engine Switchover Concepts

The *graceful Routing Engine switchover* (GRES) feature in Junos OS and Junos OS Evolved enables a router with redundant Routing Engines to continue forwarding packets, even if one Routing Engine fails. GRES preserves interface and kernel information. Traffic is not interrupted. However, GRES does not preserve the control plane.

**NOTE:** On PTX10004, PTX10008, and PTX10016 platforms running Junos OS Evolved, GRES is enabled by default and cannot be disabled.

**NOTE:** On T Series routers, TX Matrix routers, and TX Matrix Plus routers, the control plane is preserved in case of GRES with nonstop active routing (NSR), and nearly 75 percent of line rate worth of traffic per Packet Forwarding Engine remains uninterrupted during GRES.

Neighboring routers detect that the router has experienced a restart and react to the event in a manner prescribed by individual routing protocol specifications.

To preserve routing during a switchover, GRES must be combined with either:

- Graceful restart protocol extensions
- *Nonstop active routing* (NSR)

Any updates to the primary Routing Engine are replicated to the backup Routing Engine as soon as they occur.

**NOTE:** Because of its synchronization requirements and logic, NSR/GRES performance is limited by the slowest Routing Engine in the system.

Primary Role switches to the backup Routing Engine if:

- The primary Routing Engine kernel stops operating.
- The primary Routing Engine experiences a hardware failure.
- The administrator initiates a manual switchover.

**NOTE:** To quickly restore or to preserve routing protocol state information during a switchover, GRES must be combined with either graceful restart or nonstop active routing, respectively. For

more information about graceful restart, see Graceful Restart Concepts. For more information about nonstop active routing, see Nonstop Active Routing Concepts.

If the backup Routing Engine does not receive a keepalive from the primary Routing Engine after 2 seconds (4 seconds on M20 routers), it determines that the primary Routing Engine has failed; and assumes primary role.

The Packet Forwarding Engine:

- Seamlessly disconnects from the old primary Routing Engine
- Reconnects to the new primary Routing Engine
- Does not reboot
- Does not interrupt traffic

The new primary Routing Engine and the Packet Forwarding Engine then become synchronized. If the new primary Routing Engine detects that the Packet Forwarding Engine state is not up to date, it resends state update messages.

**NOTE:** Starting with Junos OS Release 12.2, if adjacencies between the restarting router and the neighboring peer 'helper' routers time out, graceful restart protocol extensions are unable to notify the peer 'helper' routers about the impending restart. Graceful restart can then stop and cause interruptions in traffic.

To ensure that these adjacencies are maintained, change the `hold-time` for IS-IS protocols from the default of 27 seconds to a value higher than 40 seconds.

**NOTE:** Successive Routing Engine switchover events must be a minimum of 240 seconds (4 minutes) apart after both Routing Engines have come up.

If the router or switch displays a warning message similar to Standby Routing Engine is not ready for graceful switchover. Packet Forwarding Engines that are not ready for graceful switchover might be reset, do not attempt switchover. If you choose to proceed with switchover, only the Packet Forwarding Engines that were not ready for graceful switchover are reset. None of the FPCs should spontaneously restart. We recommend that you wait until the warning no longer appears and then proceed with the switchover.

**NOTE:** Starting from Junos OS Release 14.2, when you perform GRES on MX Series routers, you must execute the `clear synchronous-ethernet wait-to-restore operational mode` command on the new primary Routing Engine to clear the wait-to-restore timer on it. This is because the `clear synchronous-ethernet wait-to-restore operational mode` command clears the wait-to-restore timer only on the local Routing Engine.

**NOTE:** In a routing matrix with TX Matrix Plus router with 3D SIBs, for successive Routing Engine switchover, events must be a minimum of 900 seconds (15 minutes) apart after both Routing Engines have come up.

GRES must be performed on one line-card chassis (LCC) (of a TX Matrix router with 3D SIBs) at a time to avoid synchronization issues.

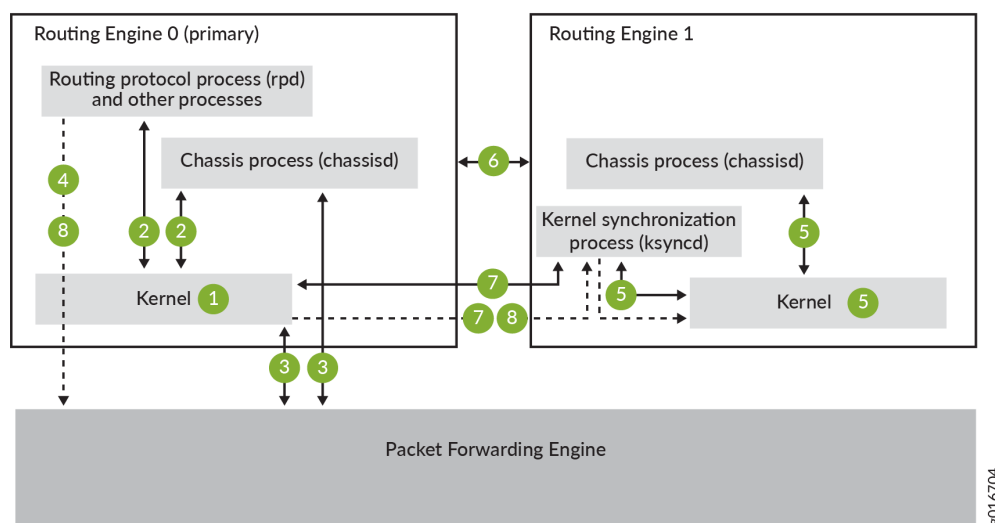
**NOTE:**

- We do *not* recommend performing a commit operation on the backup Routing Engine when GRES is enabled on the router or switch.
- We do *not* recommend enabling GRES on the backup Routing Engine in *any* scenario.

**NOTE:** On QFX10000 switches, we strongly recommend that you configure the `nsr-phantom-holdtime seconds` statement at the `[edit routing-options]` hierarchy level when nonstop routing is enabled with GRES. Doing so helps to prevent traffic loss. When you configure this statement, phantom IP addresses remain in the kernel during a switchover until the specified hold-time interval expires. After the interval expires, these routes are added to the appropriate routing tables. In an Ethernet VPN (EVPN)/VXLAN environment, we recommend that you specify a hold-time value of 300 seconds (5 minutes).

Figure 9 on page 189 shows the system architecture of graceful Routing Engine switchover and the process a routing platform follows to prepare for a switchover.

Figure 9: Preparing for a Graceful Routing Engine Switchover



**NOTE:** Check GRES readiness by executing both:

- The request chassis routing-engine master switch check command from the primary Routing Engine
- The show system switchover command from the Backup Routing Engine

The switchover preparation process for GRES is as follows:

1. The primary Routing Engine starts.
2. The routing platform processes (such as the chassis process [chassisd]) start.
3. The Packet Forwarding Engine starts and connects to the primary Routing Engine.
4. All state information is updated in the system.
5. The backup Routing Engine starts.
6. The system determines whether GRES has been enabled.
7. The kernel synchronization process (ksyncd) synchronizes the backup Routing Engine with the primary Routing Engine.
8. After ksyncd completes the synchronization, all state information and the forwarding table are updated.

Figure 10 on page 190 shows the effects of a switchover on the routing (or switching )platform.





**NOTE:** During GRES on T Series and M320 routers during GRES, the Switch Interface Boards (SIBs) are taken offline and restarted one by one. This is done to provide the Switch Processor Mezzanine Board (SPMB) that manages the SIB enough time to populate state information for its associated SIB. However, on a fully populated chassis where all FPCs are sending traffic at full line rate, there might be momentary packet loss during the switchover.

**NOTE:** When GRES is configured and the `restart chassis-control` command is executed on a TX Matrix Plus router with 3D SIBs, you cannot ascertain which Routing Engine becomes the primary. This is because the `chassisd` process restarts with the execution of the `restart chassis-control` command. The `chassisd` process is responsible for maintaining and retaining primary role and when it is restarted, the new `chassisd` is processed based on the router or switch load. As a result, any one of the Routing Engines is made the primary.

### Effects of a Routing Engine Switchover

Table 4 on page 192 describes the effects of a Routing Engine switchover when different features are enabled:

- No high availability features
- Graceful Routing Engine switchover
- Graceful restart
- Nonstop active routing

**Table 4: Effects of a Routing Engine Switchover**

Feature	Benefits	Considerations
Dual Routing Engines only (no features enabled)	<ul style="list-style-type: none"> <li>When the switchover to the new primary Routing Engine is complete, routing convergence takes place and traffic is resumed.</li> </ul>	<ul style="list-style-type: none"> <li>All physical interfaces are taken offline.</li> <li>Packet Forwarding Engines restart.</li> <li>The backup Routing Engine restarts the routing protocol process (rpd).</li> <li>All hardware and interfaces are discovered by the new primary Routing Engine.</li> <li>The switchover takes several minutes.</li> <li>All of the router's adjacencies are aware of the physical (interface alarms) and routing (topology) changes.</li> </ul>
GRES enabled	<ul style="list-style-type: none"> <li>During the switchover, interface and kernel information is preserved.</li> <li>The switchover is faster because the Packet Forwarding Engines are not restarted.</li> </ul>	<ul style="list-style-type: none"> <li>The new primary Routing Engine restarts the routing protocol process (rpd).</li> <li>All hardware and interfaces are acquired by a process that is similar to a warm restart.</li> <li>All adjacencies are aware of the router's change in state.</li> </ul>
GRES <i>and</i> NSR enabled	<ul style="list-style-type: none"> <li>Traffic is not interrupted during the switchover.</li> <li>Interface and kernel information are preserved.</li> </ul>	<ul style="list-style-type: none"> <li>Unsupported protocols must be refreshed using the normal recovery mechanisms inherent in each protocol.</li> </ul>

**Table 4: Effects of a Routing Engine Switchover (*Continued*)**

Feature	Benefits	Considerations
GRES <i>and</i> graceful restart enabled	<ul style="list-style-type: none"> <li>Traffic is not interrupted during the switchover.</li> <li>Interface and kernel information are preserved.</li> <li>Graceful restart protocol extensions quickly collect and restore routing information from the neighboring routers.</li> </ul>	<ul style="list-style-type: none"> <li>Neighbors are required to support graceful restart, and a wait interval is required.</li> <li>The routing protocol process (rpd) restarts.</li> <li>For certain protocols, a significant change in the network can cause graceful restart to stop.</li> <li>Starting with Junos OS Release 12.2, if adjacencies between the restarting router and the neighboring peer 'helper' routers time out, graceful restart can stop and cause interruptions in traffic.</li> </ul>

### Graceful Routing Engine Switchover on Aggregated Services interfaces

If a graceful Routing Engine switchover (GRES) is triggered by an operational mode command, the state of aggregated services interfaces (ASIs) are not preserved. For example:

```
request interface <switchover | revert> asi-interface
```

However, if GRES is triggered by a CLI commit or FPC restart or crash, the backup Routing Engine updates the ASI state. For example:

```
set interface si-x/y/z disable
commit
```

Or:

```
request chassis fpc restart
```

**SEE ALSO**

[Understanding High Availability Features on Juniper Networks Routers | 2](#)

Graceful Routing Engine Switchover System Requirements

[Configuring Graceful Routing Engine Switchover | 200](#)

Configuring Graceful Routing Engine Switchover in a Virtual Chassis

Configuring Graceful Routing Engine Switchover in a Virtual Chassis

Requirements for Routers with a Backup Router Configuration

Example: Configuring IS-IS for GRES with Graceful Restart

**Graceful Routing Engine Switchover System Requirements****IN THIS SECTION**

- [Graceful Routing Engine Switchover Platform Support | 194](#)
- [Graceful Routing Engine Switchover Feature Support | 195](#)
- [Graceful Routing Engine Switchover DPC Support | 197](#)
- [Graceful Routing Engine Switchover and Subscriber Access | 197](#)
- [Graceful Routing Engine Switchover PIC Support | 197](#)

Graceful Routing Engine switchover is supported on all routing (or switching) platforms that contain dual Routing Engines. All Routing Engines configured for graceful Routing Engine switchover must run the same Junos OS release. Hardware and software support for graceful Routing Engine switchover is described in the following sections:

**Graceful Routing Engine Switchover Platform Support**

To enable graceful Routing Engine switchover, your system must meet these minimum requirements:

- M20 and M40e routers—Junos OS Release 5.7 or later
- M10i router—Junos OS Release 6.1 or later
- M320 router—Junos OS Release 6.2 or later
- T320 router, T640 router, and TX Matrix router—Junos OS Release 7.0 or later
- M120 router—Junos OS Release 8.2 or later

- MX960 router—Junos OS Release 8.3 or later
- MX480 router—Junos OS Release 8.4 or later (8.4R2 recommended)
- MX240 router—Junos OS Release 9.0 or later
- PTX5000 router—Junos OS Release 12.1X48 or later
- Standalone T1600 router—Junos OS Release 8.5 or later
- Standalone T4000 router—Junos OS Release 12.1R2 or later
- TX Matrix Plus router—Junos OS Release 9.6 or later
- TX Matrix Plus router with 3D SIBs—Junos Release 13.1 or later
- EX Series switches with dual Routing Engines or in a Virtual Chassis — Junos OS Release 9.2 or later for EX Series switches
- QFX Series switches in a Virtual Chassis —Junos OS Release 13.2 or later for the QFX Series
- EX Series or QFX Series switches in a Virtual Chassis Fabric —Junos OS Release 13.2X51-D20 or later for the EX Series and QFX Series switches

For more information about support for graceful Routing Engine switchover, see the sections that follow.

### Graceful Routing Engine Switchover Feature Support

Graceful Routing Engine switchover supports most Junos OS features in Release 5.7 and later. Particular Junos OS features require specific versions of Junos OS. See [Table 5 on page 195](#).

**Table 5: Graceful Routing Engine Switchover Feature Support**

Application	Junos OS Release
Aggregated Ethernet interfaces with Link Aggregation Control Protocol (LACP) and aggregated SONET interfaces	6.2
Asynchronous Transfer Mode (ATM) virtual circuits (VCs)	6.2
Logical systems	6.3
<b>NOTE:</b> In Junos OS Release 9.3 and later, the logical router feature is renamed to logical system.	

**Table 5: Graceful Routing Engine Switchover Feature Support (Continued)**

Application	Junos OS Release
Multicast	6.4 (7.0 for TX Matrix router)
Multilink Point-to-Point Protocol (MLPPP) and Multilink Frame Relay (MLFR)	7.0
Automatic Protection Switching (APS)—The current active interface (either the designated working or the designated protect interface) remains the active interface during a Routing Engine switchover.	7.4
Point-to-multipoint Multiprotocol Label Switching MPLS LSPs (transit only)	7.4
Compressed Real-Time Transport Protocol (CRTP)	7.6
Virtual private LAN service (VPLS)	8.2
Ethernet Operation, Administration, and Management (OAM) as defined by IEEE 802.3ah	8.5
Extended DHCP relay agent	8.5
Ethernet OAM as defined by IEEE 802.1ag	9.0
Packet Gateway Control Protocol (PGCP) process (pgcpd) on Multiservices 500 PICs on T640 routers.	9.0
Subscriber access	9.4
Layer 2 Circuit and LDP-based VPLS pseudowire redundant configuration	9.6

The following constraints apply to graceful Routing Engine switchover feature support:

- When graceful Routing Engine switchover and aggregated Ethernet interfaces are configured in the same system, the aggregated Ethernet interfaces must not be configured for fast-polling LACP. When fast polling is configured, the LACP polls time out at the remote end during the Routing Engine

primary-role switchover. When LACP polling times out, the aggregated link and interface are disabled. The Routing Engine primary role change is fast enough that standard and slow LACP polling do not time out during the procedure. However, note that this restriction does not apply to MX Series Routers that are running Junos OS Release 9.4 or later and have distributed periodic packet management (PPM) enabled—which is the default configuration—on them. In such cases, you can configure graceful Routing Engine switchover and have aggregated Ethernet interfaces configured for fast-polling LACP on the same device.

**NOTE:** MACSec sessions will flap upon Graceful Routing Engine switchover.

Starting with Junos OS Release 13.2, when a graceful Routing Engine switchover occurs, the VRRP state does not change. VRRP is supported by graceful Routing Engine switchover only in the case that PPM delegation is enabled (which the default).

### Graceful Routing Engine Switchover DPC Support

Graceful Routing Engine switchover supports all Dense Port Concentrators (DPCs) on the MX Series 5G Universal Routing Platforms running the appropriate version of Junos OS as shown in ["Graceful Routing Engine Switchover Platform Support" on page 194](#). For more information about DPCs, see the *MX Series DPC Guide*.

### Graceful Routing Engine Switchover and Subscriber Access

Graceful Routing Engine switchover currently supports most of the features directly associated with dynamic DHCP and dynamic PPPoE subscriber access. Graceful Routing Engine switchover also supports the unified in-service software upgrade (ISSU) for the DHCP access model and the PPPoE access model used by subscriber access.

**NOTE:** When graceful Routing Engine switchover is enabled for subscriber management, all Routing Engines in the router must have the same amount of DRAM for stable operation.

### Graceful Routing Engine Switchover PIC Support

Graceful Routing Engine switchover is supported on most PICs, except for the services PICs listed in this section. The PIC must be on a supported routing platform running the appropriate version of Junos OS. For information about FPC types, FPC/PIC compatibility, and the initial Junos OS Release in which an FPC supported a particular PIC, see the PIC guide for your router platform.

The following constraints apply to graceful Routing Engine switchover support for services PICs:

- You can include the `graceful-switchover` statement at the `[edit chassis redundancy]` hierarchy level on a router with Adaptive Services, Multiservices, and Tunnel Services PICs configured on it and successfully commit the configuration. However, all services on these PICs—except the Layer 2 service packages and extension-provider and SDK applications on Multiservices PICs—are reset during a switchover.
- Graceful Routing Engine switchover is not supported on any Monitoring Services PICs or Multilink Services PICs. If you include the `graceful-switchover` statement at the `[edit chassis redundancy]` hierarchy level on a router with either of these PIC types configured on it and issue the `commit` command, the commit fails.
- Graceful Routing Engine switchover is not supported on Multiservices 400 PICs configured for monitoring services applications. If you include the `graceful-switchover` statement, the commit fails.

**NOTE:** When an unsupported PIC is online, you cannot enable graceful Routing Engine switchover. If graceful Routing Engine switchover is already enabled, an unsupported PIC cannot come online.

## SEE ALSO

[Understanding High Availability Features on Juniper Networks Routers | 2](#)

[Understanding Graceful Routing Engine Switchover](#)

[Configuring Graceful Routing Engine Switchover | 200](#)

[Configuring Graceful Routing Engine Switchover in a Virtual Chassis](#)

[Requirements for Routers with a Backup Router Configuration](#)

## Release History Table

Release	Description
14.2	Starting from Junos OS Release 14.2, when you perform GRES on MX Series routers, you must execute the <code>clear synchronous-ethernet wait-to-restore</code> operational mode command on the new primary Routing Engine to clear the wait-to-restore timer on it.
13.2	Starting with Junos OS Release 13.2, when a graceful Routing Engine switchover occurs, the VRRP state does not change.
12.2	Starting with Junos OS Release 12.2, if adjacencies between the restarting router and the neighboring peer 'helper' routers time out, graceful restart protocol extensions are unable to notify the peer 'helper' routers about the impending restart.



12.2

Starting with Junos OS Release 12.2, if adjacencies between the restarting router and the neighboring peer 'helper' routers time out, graceful restart can stop and cause interruptions in traffic.

---

# Configuring GRES

## IN THIS CHAPTER

- [Configuring Graceful Routing Engine Switchover | 200](#)

## Configuring Graceful Routing Engine Switchover

### SUMMARY

Learn how to configure Graceful Routing Engine Switchover (GRES) with the following steps and examples.

### IN THIS SECTION

- [Requirements for Routers with a Backup Router Configuration | 201](#)
- [Enabling Graceful Routing Engine Switchover | 201](#)
- [Configuring Graceful Routing Engine Switchover with Graceful Restart | 202](#)
- [Synchronizing the Routing Engine Configuration | 202](#)
- [Verifying Graceful Routing Engine Switchover Operation | 203](#)
- [Configuring Graceful Routing Engine Switchover in a Virtual Chassis | 204](#)
- [Preventing Graceful Routing Engine Switchover in the Case of Slow Disks | 205](#)
- [Resetting Local Statistics | 206](#)
- [Example: Configuring IS-IS for GRES with Graceful Restart | 206](#)

## Requirements for Routers with a Backup Router Configuration

If your Routing Engine configuration includes a `backup-router` statement or an `inet6-backup-router` statement, you can also use the `destination` statement to specify a subnet address or multiple subnet addresses for the backup router. Include destination subnets for the backup Routing Engine at the `[edit system (backup-router | inet6-backup-router) address]` hierarchy level. This requirement also applies to any T640 router connected to a TX Matrix router that includes a **backup-router** or `inet6-backup-router` statement.

**NOTE:** If you have a backup router configuration in which multiple static routes point to a gateway from the management Ethernet interface, you must configure prefixes that are more specific than the static routes or include the **retain** flag at the `[edit routing-options static route]` hierarchy level.

For example, if you configure the static route `172.16.0.0/12` from the management Ethernet interface for management purposes, you must specify the backup router configuration as follows:

```
backup-router 172.29.201.62 destination [172.16.0.0/13 172.16.128.0/13]
```

## SEE ALSO

Understanding Graceful Routing Engine Switchover  
Graceful Routing Engine Switchover System Requirements

## Enabling Graceful Routing Engine Switchover

By default, graceful Routing Engine switchover (GRES) is disabled. To configure GRES, include the `graceful-switchover` statement at the `[edit chassis redundancy]` hierarchy level.

```
[edit chassis redundancy]
graceful-switchover;
```

When you enable GRES, the command-line interface (CLI) indicates which Routing Engine you are using. For example:

```
{master} [edit]
user@host#
```

To disable GRES, delete the `graceful-switchover` statement from the `[edit chassis redundancy]` hierarchy level.

## Configuring Graceful Routing Engine Switchover with Graceful Restart

When using GRES with Graceful Restart, if adjacencies between the Routing Engine and the neighboring peer 'helper' routers time out, graceful restart protocol extensions are unable to notify the peer 'helper' routers about the impending restart. Graceful restart can then stop and cause interruptions in traffic.

To ensure that these adjacencies are kept, change the *hold-time* for IS-IS protocols from the default of 27 seconds to a value higher than 40 seconds.

## Synchronizing the Routing Engine Configuration

**NOTE:** A newly inserted backup Routing Engine automatically synchronizes its configuration with the primary Routing Engine configuration.

When you configure GRES, you can bring the backup Routing Engine online after the primary Routing Engine is already running. There is no requirement to start the two Routing Engines simultaneously.

Only when you enable the graceful Routing Engine switchover, you can copy the running Junos OS version of the primary Routing Engine to the backup Routing Engine.

**NOTE:** If the system is in ISSU state, you cannot copy the running Junos OS version of the primary Router Engine.

Starting in Junos OS release 14.1, you can enable automatic synchronization of the primary Routing Engine configuration with the backup Routing Engine by including the events `CHASSISD_SNMP_TRAP7` statement at the `[edit event-options policy policy-name]` hierarchy level.

`CHASSISD_SNMP_TRAP7` is a system event logging message that the chassis process (chassisd) generates a Simple Network Management Protocol (SNMP) trap with the seven indicated argument-value pairs. An example of an event script to trigger automatic synchronization of primary to the backup Routing Engine is as follows:

```
[edit event-options]
policy UPGRADE-BACKUPRE {
  events CHASSISD_SNMP_TRAP7;
  attributes-match {
    CHASSISD_SNMP_TRAP7.value5 matches "Routing Engine";
    CHASSISD_SNMP_TRAP7.trap matches "Fru Online";
```

```

CHASSISD_SNMP_TRAP7.argument5 matches jnxFruName;
}
then {
event-script auto-image-upgrade.slax {
arguments {
trap "${$.trap}";
value5 "${$.value5}";
argument5 "${$.argument5}";
}
}
}
}
event-script {
file auto-image-upgrade.slax;
}

```

After receiving this event, the event policy on the primary Router Engine is triggered and the image available in the */var/sw/pkg* path is pushed to the backup Router Engine upgrade. During script execution, the image is copied to the backup Routing Engine's */var/sw/pkg* path.

**NOTE:** If the image is not available in the */var/sw/pkg* path, the script is terminated with an appropriate syslog message.

If the Routing Engine is running at the Junos OS Release 13.2 or later, the Junos automation scripts is synchronized automatically.

After the primary Router Engine is rebooted, the event script available at the */usr/libexec/scripts/event/auto-image-upgrade.slax* must be copied to the */var/db/scripts/event* path.

**NOTE:** For MX Series routers using enhanced subscriber management, the new backup Routing Engine (the former primary Routing Engine) will reboot when a graceful Routing Engine switchover is performed. This cold restart resynchronizes the backup Routing Engine state with that of the new primary Routing Engine, preventing discrepancies in state that might have occurred during the switchover.

## Verifying Graceful Routing Engine Switchover Operation

To verify whether GRES is enabled on the backup Routing Engine, issue the `show system switchover` command. When the output of the command indicates that the **Graceful switchover** field is set to **On**,

GRES is operational. The status of the kernel database and configuration database synchronization between Routing Engines is also provided. For example:

```
Graceful switchover: On
Configuration database: Ready
Kernel database: Ready
Peer state: Steady state
```

**NOTE:** You must issue the `show system switchover` command on the backup Routing Engine. This command is not supported on the primary Routing Engine.

For more information about the `show system switchover` command, see the [CLI Explorer](#).

## Configuring Graceful Routing Engine Switchover in a Virtual Chassis

In a Virtual Chassis, one member switch is assigned the primary role and has the primary Routing Engine. Another member switch is assigned the backup role and has the backup Routing Engine. Graceful Routing Engine switchover (GRES) enables the primary and backup Routing Engines in a Virtual Chassis configuration to switch from the primary to backup without interruption to packet forwarding as a hitless failover solution. When you configure graceful Routing Engine switchover, the backup Routing Engine automatically synchronizes with the primary Routing Engine to preserve kernel state information and the forwarding state.

To set up the Virtual Chassis configuration to use graceful Routing Engine switchover (GRES):

1. Set up a minimum of two switches in a Virtual Chassis configuration with primary-role priority of 255:

```
[edit]
user@switch# set virtual-chassis member 0 mastership-priority 255

[edit]
user@switch# set virtual-chassis member 1 mastership-priority 255
```

2. Set up graceful Routing Engine switchover:

```
[edit]
user@switch# set chassis redundancy graceful-switchover
```

Commit the configuration.

**NOTE:** We recommend that you use the `commit synchronize` command to save any configuration changes that you make to a multimember Virtual Chassis.

## SEE ALSO

*Example: Configuring an EX4200 Virtual Chassis with a Primary and Backup in a Single Wiring Closet*

[High Availability Features for EX Series Switches Overview](#)

*Understanding EX Series Virtual Chassis*

*Understanding QFX Series Virtual Chassis*

## Preventing Graceful Routing Engine Switchover in the Case of Slow Disks

Unexpected slow disk access can happen for various reasons—a faulty or bad sector, for example—causing a hold up of the normal operation of processes such as the routing process (rpd). Eventually, the router's performance will be impacted. Under these circumstances, it may take longer for the typical failover mechanism to be triggered.

Juniper Networks has introduced a disk monitoring daemon to solve this dilemma. The daemon detects slow disk access and initiates failover. Failover can minimize the traffic impact and ease the load on the original primary Routing Engine for its backlog clean up.

However, there are instances when you might not want failover to occur. You might commit a large set of changes or even minor changes that might lead to a series of updates on the routing topology. Such activity could lead to extensive disk access delay and, therefore, trigger failover. For expected disk access delays like this, where you do not want to trigger failover, you can choose to not have failover occur by setting the `chassis redundancy failover not-on-disk-underperform` configuration command. Another way is to disable the disk monitoring daemon completely by setting the `system processes gstatd disable` command.

To prevent failovers in the case of slow disks in the Routing Engine:

- Set the option for preventing gstatd from initiating failovers in response to slow disks at the `[edit chassis redundancy failover]` hierarchy level.

[edit]

```
user@host# set chassis redundancy failover not-on-disk-underperform
```

## SEE ALSO

[not-on-disk-underperform](#) | 1021

Understanding Graceful Routing Engine Switchover

## Resetting Local Statistics

When you enable graceful Routing Engine switchover, the primary Routing Engine configuration is copied and loaded to the backup Routing Engine. User files, accounting information, and trace options information are not replicated to the backup Routing Engine.

When a graceful Routing Engine switchover occurs, local statistics such as process statistics and networking statistics are displayed as a cumulative value from the time the process first came online. Because processes on the primary Routing Engine can start at different times from the processes on the backup Routing Engine, the statistics on the two Routing Engines for the same process might differ. After a graceful Routing Engine switchover, we recommend that you issue the **clear interface statistics** (*interface-name* | **all**) command to reset the cumulative values for local statistics. Forwarding statistics are not affected by graceful Routing Engine switchover.

For information about how to use the **clear** command to clear statistics and protocol database information, see the [CLI Explorer](#).

**NOTE:** The **clear firewall** command cannot be used to clear the Routing Engine filter counters on a backup Routing Engine that is enabled for graceful Routing Engine switchover.

## SEE ALSO

Understanding Graceful Routing Engine Switchover

[Configuring Graceful Routing Engine Switchover](#) | 200

## Example: Configuring IS-IS for GRES with Graceful Restart

## IN THIS SECTION

- [Requirements](#) | 207
- [Overview](#) | 207
- [Configuration](#) | 207
- [Verification](#) | 209



This example shows how to configure the Routing Engine's graceful restart protocol extensions using the intermediate system to intermediate system (IS-IS) interior gateway protocol (IGP) to successfully enable graceful Routing Engine switchover (GRES) with graceful restart.

## Requirements

GRES prevents interruptions in network traffic if the primary Routing Engine fails when combined with either:

- Graceful restart
- Nonstop active routing (NSR)

Before you follow the directions here to configure graceful restart, be sure you have enabled GRES, which is disabled by default. See ["Configuring Graceful Routing Engine Switchover" on page 200](#) for more information.

## Overview

If adjacencies between the Routing Engine and the neighboring peer 'helper' routers time out, graceful restart protocol extensions are unable to notify the peer 'helper' routers about the impending restart. Graceful restart can then stop and cause interruptions in traffic.

To ensure that these adjacencies are kept, change the hold-time for IS-IS protocols from the default of 27 seconds to a value higher than 40 seconds.

If your system uses the open shortest pathway first (OSPF) protocol instead of IS-IS, see [Example: Configuring OSPF Timers](#) for configuration information.

## Configuration

### IN THIS SECTION

- [CLI Quick Configuration | 208](#)
- [Configuring the IS-IS Protocol Hold Time for Graceful Restart | 208](#)
- [Results | 209](#)

### *CLI Quick Configuration*

To quickly configure the hold-time, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the different hierarchy levels shown.

Each interface must be set individually, with a value for each level that the routing device operates on. The minimum recommended value of 41 seconds is used in this example, your system may require a higher value based on size and traffic.

Level 1 and level 2 can be set to different values.

#### **[edit protocols]**

```
set protocols isis interface ge-1/2/0 level 1 hold-time 41
set protocols isis interface ge-1/2/0 level 2 hold-time 41
```

#### **[edit logical-systems logical-system-name]**

```
set protocols isis interface ge-1/2/0 level 1 hold-time 41
set protocols isis interface ge-1/2/0 level 2 hold-time 41
```

#### **[edit logical-systems logical-system-name routing-instances routing-instance-name]**

```
set protocols isis interface ge-1/2/0 level 1 hold-time 41
set protocols isis interface ge-1/2/0 level 2 hold-time 41
```

#### **[edit routing-instances routing-instance-name]**

```
set protocols isis interface ge-1/2/0 level 1 hold-time 41
set protocols isis interface ge-1/2/0 level 2 hold-time 41
```

### *Configuring the IS-IS Protocol Hold Time for Graceful Restart*

#### **Step-by-Step Procedure**

To configure the IS-IS hold-time for graceful restart:

1. Locate or set the interfaces.

```
set protocols isis interface interface-name
```

2. Set the network level and the hold-time in seconds for that level.

```
set protocols isis interface interface-name level 1 hold-time 41
```

3. If the routing device functions on more than one level, set the value for the other level.

```
set protocols isis interface interface-name level 2 hold-time 41
```

4. If you are done configuring the routing device, commit the configuration.

**NOTE:** Repeat the entire configuration on all routing devices in a shared network.

## Results

## Verification

### IN THIS SECTION

- [Verifying the IS-IS Protocol Hold Time for Graceful Restart | 209](#)

## *Verifying the IS-IS Protocol Hold Time for Graceful Restart*

## Purpose

Verify that the IS-IS protocol hold-time is set to 41 seconds or greater to ensure that graceful restart is enabled.

Action

Confirm your configuration by entering the `show isis adjacency brief` command from operational mode. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

Meaning

A high enough IS-IS protocol hold-time value allows your system configuration to restart and ensures that even if a Routing Engine fails, traffic continues.

SEE ALSO

Understanding Graceful Routing Engine Switchover
<a href="#">Configuring Graceful Routing Engine Switchover   200</a>
<i>Example: Configuring IS-IS</i>
<i>Example: Configuring OSPF Timers</i>
<i>interface</i>
<i>level</i>
<i>hold-time</i>

Release History Table

Release	Description
14.1	Starting in Junos OS release 14.1, you can enable automatic synchronization of the primary Routing Engine configuration with the backup Routing Engine by including the events CHASSISD_SNMP_TRAP7 statement at the [edit event-options policy <i>policy-name</i> ] hierarchy level.

RELATED DOCUMENTATION

Understanding Graceful Routing Engine Switchover
Graceful Routing Engine Switchover System Requirements
Requirements for Routers with a Backup Router Configuration
Resetting Local Statistics
<a href="#">graceful-switchover   993</a>
<a href="#">graceful-switchover   994</a>
Example: Configuring IS-IS for GRES with Graceful Restart

| *hold-time*

## CHAPTER 11

# Configuring Ethernet Automatic Protection Switching for High Availability

**IN THIS CHAPTER**

- [Configuring Ethernet Automatic Protection Switching | 212](#)

## Configuring Ethernet Automatic Protection Switching

**SUMMARY**

Learn how to configure Ethernet automatic protection switching (APS) for high availability.

**IN THIS SECTION**

- [Ethernet Automatic Protection Switching Overview | 212](#)
- [Mapping of CCM Defects to APS Events | 216](#)
- [Example: Configuring Protection Switching Between Psuedowires | 217](#)

## Ethernet Automatic Protection Switching Overview

**IN THIS SECTION**

- [Unidirectional and Bidirectional Switching | 213](#)
- [Selective and Merging Selectors | 213](#)
- [Revertive and Nonrevertive Switching | 214](#)
- [Protection Switching Between VPWS Pseudowires | 214](#)
- [CLI Configuration Statements | 215](#)

Ethernet automatic protection switching (APS) is a linear protection scheme designed to protect VLAN based Ethernet networks.

With Ethernet APS, a protected domain is configured with two paths, a working path and a protection path. Both working and protection paths can be monitored using an Operations Administration Management (OAM) protocol like Connectivity Fault Management (CFM). Normally, traffic is carried on the working path (that is, the working path is the active path), and the protection path is disabled. If the working path fails, its protection status is marked as degraded (DG) and APS switches the traffic to the protection path, then the protection path becomes the active path.

APS uses two modes of operation, linear 1+1 protection switching architecture and linear 1:1 protection switching architecture. The linear 1+1 protection switching architecture operates with either unidirectional or bidirectional switching. The linear 1:1 protection switching architecture operates with bidirectional switching.

In the linear 1+1 protection switching architecture, the normal traffic is copied and fed to both working and protection paths with a permanent bridge at the source of the protected domain. The traffic on the working and protection transport entities is transmitted simultaneously to the sink of the protected domain, where a selection between the working and protection transport entities is made.

In the linear 1:1 protection switching architecture, the normal traffic is transported on either the working path or on the protection path using a selector bridge at the source of the protection domain. The selector at the sink of the protected domain selects the entity that carries the normal traffic.

### **Unidirectional and Bidirectional Switching**

Unidirectional switching utilizes fully independent selectors at each end of the protected domain. Bidirectional switching attempts to configure the two end points with the same bridge and selector settings, even for a unidirectional failure. Unidirectional switching can protect two unidirectional failures in opposite directions on different entities.

### **Selective and Merging Selectors**

In the linear 1:1 protection switching architecture, where traffic is sent only on the active path, there are two different ways in which the egress direction (the direction out of the protected segment) data forwarding can act: selective selectors and merging selectors. A selective selector forwards only traffic that is received from both the paths regardless of which one is currently active. In other words, with a merging selector the selection of the currently active path only affects the ingress direction. Merging selectors minimize the traffic loss during a protection switch, but they do not guarantee the delivery of the data packets in order.

## Revertive and Nonrevertive Switching

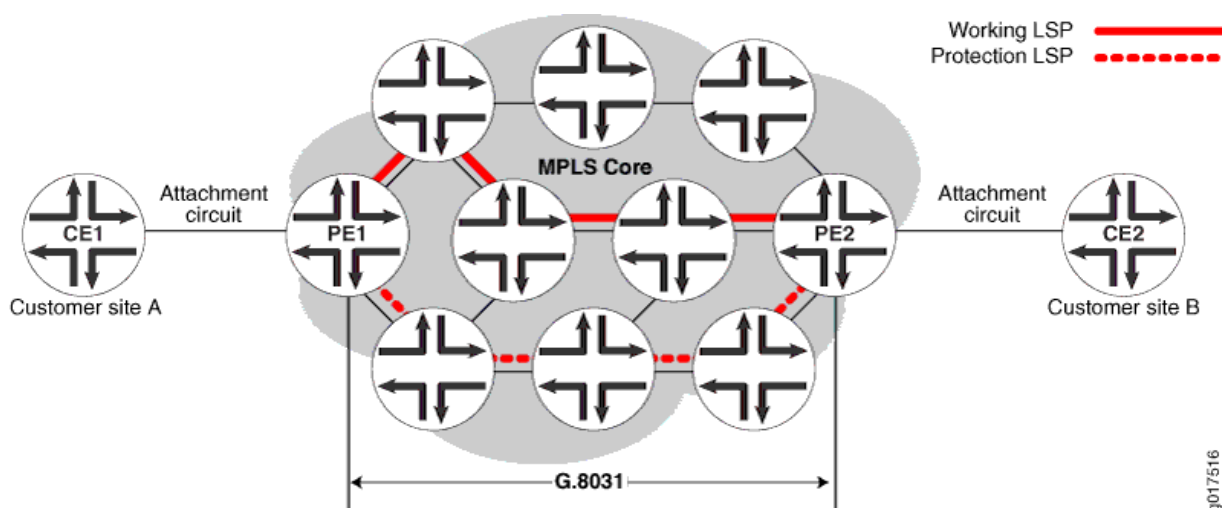
For revertive switching, traffic is restored to the working path after the conditions causing the switch have cleared.

For nonrevertive switching, traffic is allowed to remain on the protection path even after the conditions causing the switch have cleared.

**NOTE:** The configuration on both the provider edge (PE) routers have to be either in revertive mode or non-revertive mode.

## Protection Switching Between VPWS Pseudowires

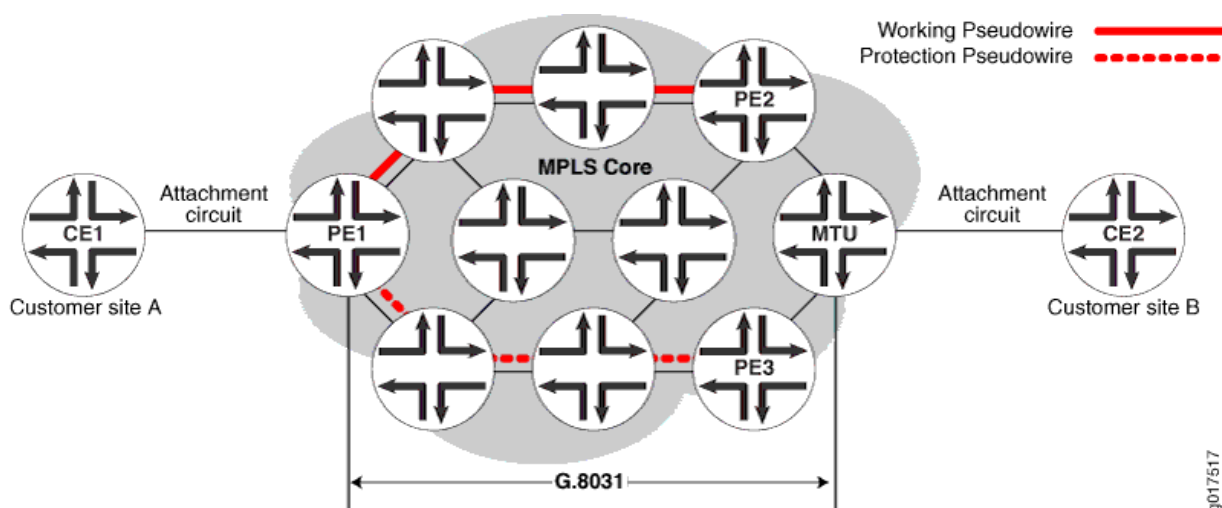
Figure 11: Connections Terminating on Single PE



In the scenario diagrammed in [Figure 11 on page 214](#), a *Virtual Private Wire Service (VPWS)* is provisioned between customer sites A and B using a single pseudowire (layer 2 circuit) in the core network, and two Multiprotocol Label Switching (MPLS) Label Switched Paths (LSPs) are provisioned, one for the working path and the other one for the protection path. CFM CCM will be used to monitor the status of each LSP. Provider edge routers PE1 and PE2 run G.8031 Ethernet APS to select one of the LSPs as the active path. Once the active path is elected at the source end of the protection group, PE1 forwards to traffic from site A to the elected active path. At the sink end of the protection group, PE2 implements a merging selector, meaning it forwards the traffic coming from both the LSPs to the customer site B.



Figure 12: Connections Terminating on a Different PE



In the scenario represented in [Figure 12 on page 215](#), a VPWS is provisioned between customer sites A and B using two pseudowires (layer 2 circuit) in the core network, one for the working path and the other for the protection path. CFM CCM will be used to monitor the status of each pseudowire.

Provider edge router PE1 and MTU run G.8031 Ethernet APS to select one of the pseudowires as the active path. Once the active path is elected at the source end of the protection group, PE1 forwards the traffic from site A to the elected active path. At the sink end of the protection group, MTU implements a merging selector, meaning it forwards the traffic coming from both the pseudowires to customer site B.

### CLI Configuration Statements

```
[edit protocols protection-group]
ethernet-aps profile{
  protocol g8031;
  revert-time seconds;
  hold-time 0-10000ms;
  local-request lockout;
}
```

**revert-time-** By default, protection logic restores the use of the working path once it recovers. The revert-time statement specifies how much time should elapse before the path for data should be switched from Protection to Working once recovery for Working has occurred. A revert-time of zero indicates no reversion. It will default to 300 sec (5 minutes) if not configured.

**hold-time-** Once a failure is detected, APS waits until this timer expires before initiating the protection switch. The range of the hold-time timer is 0 to 10,000 milliseconds. It will default to zero if not configured.

local-request- Configuring this value to lockout or force-switch will trigger lockout or force-switch operation on the protection groups using this profile.

## SEE ALSO

Mapping of CCM Defects to APS Events

Example: Configuring Protection Switching Between Psuedowires

## Mapping of CCM Defects to APS Events

The continuity check message (CCM) engine marks the status of working and protected transport entities as either Down, Degraded, or Up.

**Down**—The monitored path is declared down if any of the following Multiple End Point (MEP) defects occur:

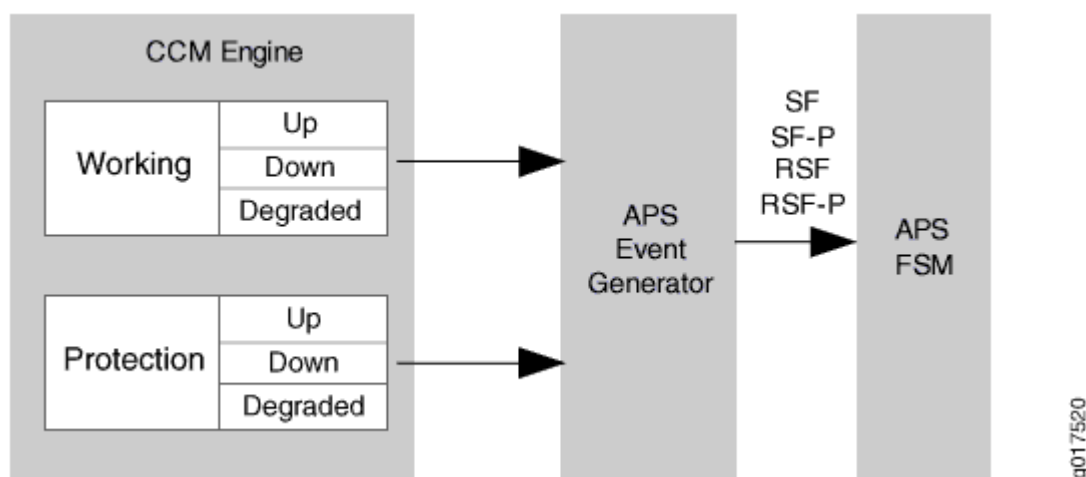
- Interface down
- CCM expiry
- RDI indicating signal failure

**Degraded**—The monitored path is declared degraded if any of the following MEP defects occur:

- FRR on
- FRR-ACK on

**Up**—The monitored path is declared up in the absence of any of the above events.

Figure 13: Understanding APS Events



As show in [Figure 13 on page 217](#), the APS event generator generates the following APS events based on the status of the working and protection paths:

- SF—Signal failure on working path
- RSF—Working path recovers from signal failure
- SF-P—Signal failure on protection path
- RSF-P—Protection path recovers from signal failure

## SEE ALSO

Ethernet Automatic Protection Switching Overview

Example: Configuring Protection Switching Between Psuedowires

## Example: Configuring Protection Switching Between Psuedowires

### IN THIS SECTION

- [Requirements | 218](#)
- [Overview and Topology | 218](#)
- [Configuration | 219](#)

## Requirements

This example uses the following hardware and software components:

- Junos OS Release 11.2 or later
- 2 MX Series PE routers

## Overview and Topology

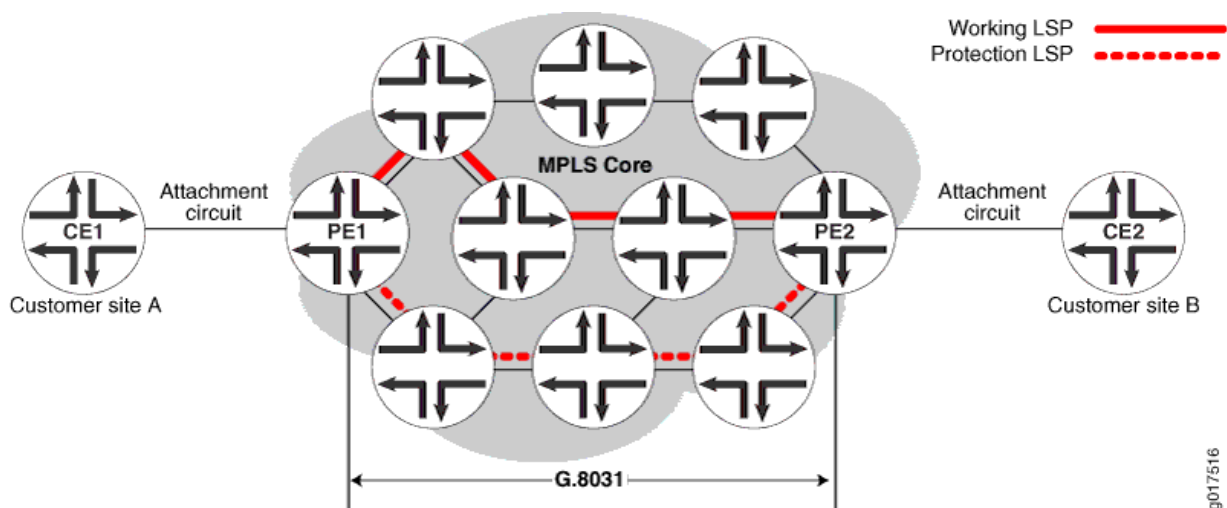
### IN THIS SECTION

- [Topology | 218](#)

The physical topology of the protection switching between psuedowires example is shown in [Figure 14 on page 218](#).

### Topology

Figure 14: Topology of a Network Using VPWS Psuedowires



The following definitions describe the meaning of the device abbreviations used in [Figure 14 on page 218](#).

- Customer edge (CE) device—A device at the customer site that provides access to the service provider's VPN over a data link to one or more provider edge (PE) routers.

- Provider edge (PE) device—A device, or set of devices, at the edge of the provider network that presents the provider's view of the customer site.

## Configuration

### IN THIS SECTION

- [Procedure | 219](#)

## Procedure

### Step-by-Step Procedure

To configure protection switching between pseudowires, perform these tasks:

1. Configure automatic protection switching.

```
protocols {
  protection-group {
    ethernet-aps {
      profile-1 {
        protocol g8031;
        hold-time 1000s;
        revert-time 5m;
      }
    }
  }
}
```

2. Configure the connectivity fault management.

```
ethernet {
  oam {
    connectivity-fault-management {
      maintenance-domain md1 {
        level 5;
      }
    }
  }
}
```

### 3. Configure the continuity check message for the working path.

```

maintenance-association W {
    protect maintenance-association P {
        aps-profile profile-1;
    }
    continuity-check {
        interval 1s;
    }
    mep 100 {
        interface ge-1/0/0.0 working;
        direction down;
        auto-discovery;
    }
}

```

### 4. Configure the continuity check message for the protection path.

```

maintenance-association P {
    continuity-check {
        interval 1s;
    }
    mep 100 {
        interface ge-1/0/0.0 protect;
        direction down;
        auto-discovery;
    }
}

```

## Results

Check the results of the configuration:

```

protocols {
    protection-group {
        ethernet-aps {
            profile-1 {
                protocol g8031;
                hold-time 1000s;
                revert-time 5m;
            }
        }
    }
}

```

```

    }
  }
}
ethernet {
  oam {
    connectivity-fault-management {
      maintenance-domain md1 {
        level 5;
        maintenance-association W {
          protect maintenance-association P {
            aps-profile profile-1;
          }
          continuity-check {
            interval 1s;
          }
          mep 100 {
            interface ge-1/0/0.0 working;
            direction down;
            auto-discovery;
          }
        }
        maintenance-association P {
          continuity-check {
            interval 1s;
          }
          mep 100 {
            interface ge-1/0/0.0 protect;
            direction down;
            auto-discovery;
          }
        }
      }
    }
  }
}

```

## SEE ALSO

Ethernet Automatic Protection Switching Overview

Mapping of CCM Defects to APS Events

# 7

PART

## Configuring Ethernet Ring Protection Switching

---

[Understanding Ethernet Ring Protection Switching for High Availability | 223](#)

[Configuring Ethernet Ring Protection Switching for High Availability | 234](#)

---



# Understanding Ethernet Ring Protection Switching for High Availability

## IN THIS CHAPTER

- [Understanding Ethernet Ring Protection Switching | 223](#)

## Understanding Ethernet Ring Protection Switching

### SUMMARY

Ethernet ring protection switching (ERPS) helps to prevent fatal loops from disrupting a network. ERPS is similar to spanning-tree protocols, but ERPS is more efficient because it is customized for ring topologies.

### IN THIS SECTION

- [Ethernet Ring Protection Switching Overview | 223](#)
- [Understanding Ethernet Ring Protection Switching Functionality | 224](#)

## Ethernet Ring Protection Switching Overview

*Ethernet ring protection switching* (ERPS) helps achieve high reliability and network stability. Links in the ring will never form loops that fatally affect the network operation and services availability. The basic idea of an Ethernet ring is to use one specific link to protect the whole ring. This special link is called a *ring protection link (RPL)*. If no failure happens in other links of the ring, the RPL blocks the traffic and is not used. The RPL is controlled by a special node called an *RPL owner*. There is only one RPL owner in a ring. The RPL owner is responsible for blocking traffic over the RPL. Under ring failure conditions, the RPL owner is responsible for unblocking traffic over the RPL. A ring failure results in protection switching of the RPL traffic. An automatic protection switching (APS) protocol is used to coordinate the protection actions over the ring. Protection switching blocks traffic on the failed link and unblocks the traffic on the RPL. When the failure clears, revertive protection switching blocks traffic over the RPL and unblocks traffic on the link on which the failure is cleared.

**NOTE:** ERPS on AE interfaces is not supported on ACX Series routers except on ACX5000 and ACX7100 Series routers.

The following standards provide detailed information on Ethernet ring protection switching:

- ITU-T Recommendation G.8032/Y.1344 version 1 and 2, *Ethernet Ring protection switching*. G.8032v1 supports a single ring topology and G.8032v2 supports multiple rings and ladder topology.

All devices with Ethernet ring protection switching support G.8032v1. MX Series and ACX Series routers also support G.8032v2.

- ITU-T Y.1731, *OAM functions and mechanisms for Ethernet-based networks*

For additional information on configuring Ethernet ring protection switching on EX Series switches, see [Example: Configuring Ethernet Ring Protection Switching on EX Series Switches](#).

For additional information on configuring Ethernet ring protection switching on MX Series routers, see the *Layer 2 Configuration Guide* for a complete example of Ethernet rings and information about STP loop avoidance and prevention.

## SEE ALSO

Understanding Ethernet Ring Protection Switching Functionality

Configuring Ethernet Ring Protection Switching

Example: Ethernet Ring Protection Switching Configuration on MX Routers

[Example: Configuring Ethernet Ring Protection Switching on EX Series Switches](#)

[Ethernet Interfaces User Guide for Routing Devices](#)

## Understanding Ethernet Ring Protection Switching Functionality

### IN THIS SECTION

- [Acronyms | 225](#)
- [Ring Nodes | 226](#)
- [Ring Node States | 226](#)
- [Default Logging of Basic State Transitions on EX Series Switches | 227](#)
- [Logical Ring | 227](#)

- FDB Flush | 227
- Traffic Blocking and Forwarding | 228
- RPL Neighbor Node | 228
- RAPS Message Blocking and Forwarding | 228
- Dedicated Signaling Control Channel | 230
- RAPS Message Termination | 230
- Revertive and Non-revertive Modes | 230
- Multiple Rings | 231
- Node ID | 231
- Ring ID | 231
- Bridge Domains with the Ring Port (MX Series Routers Only) | 231
- Wait-to-Block Timer | 231
- Adding and Removing a Node | 232

## Acronyms

The following acronyms are used in the discussion about Ethernet ring protection switching (ERPS):

- MA—Maintenance association
- MEP—Maintenance association end point
- OAM—Operations, administration, and management (Ethernet ring protection switching uses connectivity fault management daemon)
- FDB—MAC forwarding database
- STP—Spanning Tree Protocol
- RAPS—Ring automatic protection switching
- WTB—Wait to block. Note that WTB is always disabled on EX2300 and EX3400 switches because it is not supported in ERPSv1. Any configuration you make to the WTB setting on EX2300 and EX3400 switches has no effect. The output from the CLI command 'show protection-group ethernet-ring node-state detail' lists a WTB setting but that setting has no effect on EX2300 and EX3400 switches.
- WTR—Wait to restore. Note that on EX2300 and EX3400 switches only, the WTR configuration must be 5-12 minutes.

- RPL—Ring protection link

## Ring Nodes

Multiple nodes are used to form a ring. There are two different node types:

- Normal node—The node has no special role on the ring.
- RPL owner node—The node owns the RPL and blocks or unblocks traffic over the RPL.

## Ring Node States

The following are the different states for each node of a specific ring:

- init—Not a participant of a specific ring.
- idle—No failure on the ring; the node is performing normally. For a normal node, traffic is unblocked on both ring ports. For the RPL owner or RPL neighbor, traffic is blocked on the ring port that connects to the RPL and unblocked on the other ring port.
- protection—A failure occurred on the ring. For a normal node, traffic is blocked on the ring port that connects to the failing link and unblocked on working ring ports. For the RPL owner, traffic is unblocked on both ring ports if they connect to non-failure links.
- pending—The node is recovering from failure or its state after a `clear` command is used to remove the previous manual command. When a protection group is configured, the node enters the pending state. When a node is in pending state, the WTR or WTB timer will be running. All nodes are in pending state till WTR or WTB timer expiry.
- force switch—A force switch is issued. When a force switch is issued on a node in the ring all nodes in the ring will move into the force switch state.

**NOTE:** EX2300 and EX3400 switches do not support force switch.

- manual switch—A manual switch is issued. When a manual switch is issued on a node in the ring all nodes in the ring will move into the manual switch state.

**NOTE:** EX2300 and EX3400 switches do not support manual switch.

There can be only one RPL owner for each ring. The user configuration must guarantee this, because the APS protocol cannot check this.

## Default Logging of Basic State Transitions on EX Series Switches

Starting with Junos OS Release 14.1X53-D15, EX Series switches automatically log basic state transitions for the ERPS protocol. Starting with Junos OS Release 18.2R1, EX2300 and EX3400 switches automatically log basic state transitions for the ERPS protocol. No configuration is required to initiate this logging. Basic state transitions include ERPS interface transitions from up to down, and down to up; and ERPS state transitions from idle to protection, and protection to idle.

The basic state transitions are logged in a single file named **erp-default**, which resides in the **/var/log** directory of the switch. The maximum size of this file is 15 MB.

Default logging for ERPS can capture initial ERPS interface and state transitions, which can help you troubleshoot issues that occur early in the ERPS protocol startup process. However, if more robust logging is needed, you can enable traceoptions for ERPS by entering the **traceoptions** statement in the **[edit protocols protection-group]** hierarchy.

Be aware that for ERPS, only default logging or traceoptions can be active at a time on the switch. That is, default logging for ERPS is automatically enabled and if you enable traceoptions for ERPS, the switch automatically disables default logging. Conversely, if you disable traceoptions for ERPS, the switch automatically enables default logging.

## Logical Ring

You can define multiple logical-ring instances on the same physical ring. The logical ring feature currently supports only the physical ring, which means that two adjacent nodes of a ring must be physically connected and the ring must operate on the physical interface, not the VLAN. Multiple ring instances are usually defined with trunk mode ring interfaces.

## FDB Flush

When ring protection switching occurs, normally an *FDB flush* is executed. The Ethernet ring control module uses the same mechanism as the STP to trigger the FDB flush. The Ethernet ring control module controls the ring port physical interface's default STP index to execute the FDB flush.

**NOTE:** Optimized flushing is not supported on EX2300 and EX3400 switches.

Starting with Junos OS Release 14.2, the FDB flush depends on the RAPS messages received on the both the ports of the ring node.

## Traffic Blocking and Forwarding

Ethernet ring control uses the same mechanism as the STP to control forwarding or discarding of user traffic. The Ethernet ring control module sets the ring port physical interface default STP index state to forwarding or discarding in order to control user traffic.

## RPL Neighbor Node

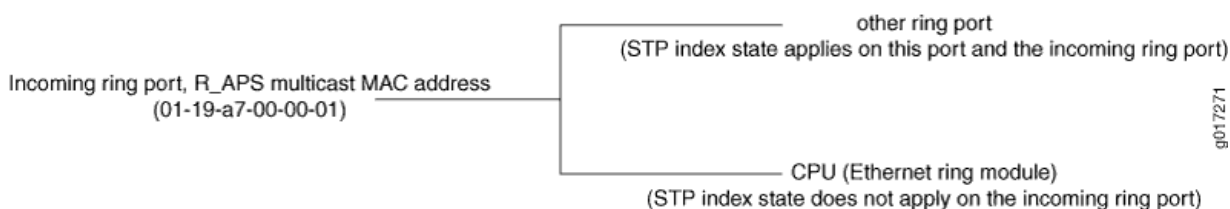
Starting with Junos OS Release 14.2, ring protection link neighbor nodes are supported. An RPL neighbor node is adjacent to the RPL and is not the RPL owner. If a node is configured with one interface as the protection-link-end and no protection-link-owner is present in its configuration, the node is an RPL neighbor node.

**NOTE:** RPL neighbor node is not supported on EX2300 and EX3400 switches.

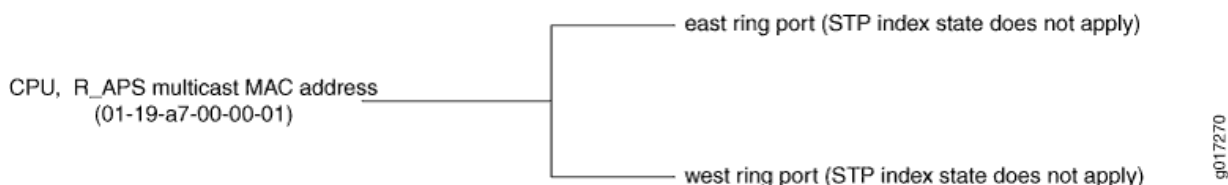
## RAPS Message Blocking and Forwarding

The router or switch treats the ring automatic protection switching (RAPS) message the same as it treats user traffic for forwarding RAPS messages between two ring ports. The ring port physical interface default STP index state also controls forwarding RAPS messages between the two ring ports. Other than forwarding RAPS messages between the two ring ports, as shown in [Figure 15 on page 228](#), the system also needs to forward the RAPS message between the CPU (Ethernet ring control module) and the ring port. This type of forwarding does not depend on the ring port physical interfaces' STP index state. The RAPS message is always sent by the router or switch through the ring ports, as shown in [Figure 16 on page 229](#). A RAPS message received from a discarding ring port is sent to the Ethernet ring control module, but is not sent to the other ring port.

**Figure 15: Protocol Packets from the Network to the Router**



### Figure 16: Protocol Packets from the Router or Switch to the Network



Juniper Networks switches and Juniper Networks routers use different methods to achieve these routes.

The switches use forwarding database entries to direct the RAPS messages. The forwarding database entry (keyed by the RAPS multicast address and VLAN) has a composite next hop associated with it—the composite next hop associates the two ring interfaces with the forwarding database entry and uses the split horizon feature to prevent sending the packet out on the interface that it is received on. This is an example of the forwarding database entry relating to the RAPS multicast MAC (a result of the `show ethernet-switching table detail` command):

```
VLAN: v1, Tag: 101, MAC: 01:19:a7:00:00:01, Interface: ERP
Interfaces:                ge-0/0/9.0, ge-0/0/3.0
Type: Static
Action: Mirror
Nextthop index: 1333
```

The routers use an implicit filter to achieve ERP routes. Each implicit filter binds to a bridge domain. Therefore, the east ring port control channel and the west ring port control channel of a particular ring instance must be configured to the same bridge domain. For each ring port control channel, a filter term is generated to control RAPS message forwarding. The filter number is the same as the number of bridge domains that contain the ring control channels. If a bridge domain contains control channels from multiple rings, the filter related to this bridge domain will have multiple terms and each term will relate to a control channel. The filter has command parts and control-channel related parts, as follows:

- Common terms:

- term 1: if [Ethernet type is not OAM Ethernet type (0x8902)]  
] { accept packet }
- term 2: if [source MAC address belongs to this bridge]  
{ drop packet, our packet loop through the ring and come back to home}

- term 3: if [destination is the RAPS PDU multicast address(0x01,0x19,0xa7,0x00,0x00,0x01)] AND[ring port STP status is DISCARDING]  
{ send to CPU }

- Control channel related terms:

- if [destination is the RAPS PDU multicast address(0x01,0x19,0xa7,0x00,0x00,0x01)] AND[ring port STP status is FORWARDING] AND [Incoming interface IFL equal to control channel IFL]  
{ send packet to CPU and send to the other ring port }  
default term: accept packet.

### Dedicated Signaling Control Channel

For each ring port, a dedicated signaling control channel with a dedicated VLAN ID must be configured. In Ethernet ring configuration, only this control *logical interface* is configured and the underlying physical interface is the physical ring port. Each ring requires that two control physical interfaces be configured. These two logical interfaces must be configured in a bridge domain for routers (or the same VLAN for switches) in order to forward RAPS protocol data units (PDUs) between the two ring control physical interfaces. If the router control channel logical interface is not a trunk port, only control logical interfaces will be configured in ring port configuration. If this router control channel logical interface is a trunk port, in addition to the control channel logical interfaces, a dedicated VLAN ID must be configured for routers. For switches, always specify either a VLAN name or VLAN ID for all links.

### RAPS Message Termination

The RAPS message starts from the originating node, travels through the entire ring, and terminates in the originating node unless a failure is present in the ring. The originating node must drop the RAPS message if the source MAC address in the RAPS message belongs to itself. The source MAC address is the node's node ID.

### Revertive and Non-revertive Modes

In revertive operation, once the condition causing a switch has cleared, traffic is blocked on the RPL and restored to the working transport entity. In nonrevertive operation, traffic is allowed to use the RPL if it has not failed, even after a switch condition has cleared.

**NOTE:** Non-revertive mode is not supported on EX2300 and EX3400 switches.



## Multiple Rings

The Ethernet ring control module supports multiple rings in each node (two logical interfaces are part of each ring). The ring control module also supports the interconnection of multiple rings. Interconnection of two rings means that two rings might share the same link or share the same node. Ring interconnection is supported only using non-virtual-channel mode. Ring interconnection using virtual channel mode is not supported.

**NOTE:** Interconnection of multiple rings is not supported on EX2300 and EX3400 switches.

## Node ID

For each node in the ring, a unique *node ID* identifies each node. The node ID is the node's MAC address.

For routers only, you can configure this node ID when configuring the ring on the node or automatically select an ID like STP does. In most cases, you will not configure this and the router will select a node ID, like STP does. It should be the manufacturing MAC address. The ring node ID should not be changed, even if you change the manufacturing MAC address. Any MAC address can be used if you make sure each node in the ring has a different node ID. The node ID on switches is selected automatically and is not configurable.

## Ring ID

The ring ID is used to determine the value of the last octet of the MAC destination address field of the RAPS protocol data units (PDUs) generated by the ERP control process. The ring ID is also used to discard any RAPS PDU, received by this ERP control process with a non-matching ring ID. Ring ID values 1 through 239 are supported.

## Bridge Domains with the Ring Port (MX Series Routers Only)

On the routers, the protection group is seen as an abstract logical port that can be configured to any bridge domain. Therefore, if you configure one ring port or its logical interface in a bridge domain, you must configure the other related ring port or its logical interface to the same bridge domain. The bridge domain that includes the ring port acts as any other bridge domain and supports the IRB Layer 3 interface.

## Wait-to-Block Timer

The RPL owner node uses a delay timer before initiating an RPL block in revertive mode of operation or before reverting to IDLE state after clearing manual commands. The Wait-to-Block (WTB) timer is used

when clearing `force switch` and `manual switch` commands. As multiple `force switch` commands are allowed to coexist in an Ethernet ring, the WTB timer ensures that clearing of a single `force switch` command does not trigger the re-blocking of the RPL. When clearing a `manual switch` command, the WTB timer prevents the formation of a closed loop due to a possible timing anomaly where the RPL Owner Node receives an outdated remote `manual switch` request during the recovery process.

When recovering from a `manual switch` command, the delay timer must be long enough to receive any latent remote `force switch`, signal failure, or `manual switch` commands. This delay timer is called the WTB timer and is defined to be 5 seconds longer than the guard timer. This delay timer is activated on the RPL Owner Node. When the WTB timer expires, the RPL Owner Node initiates the reversion process by transmitting an RAPS (NR, RB) message. The WTB timer is deactivated when any higher-priority request preempts it.

**NOTE:** The Wait To Block Timer (WTB) is always disabled on EX2300 and EX3400 switches because it is not supported in ERPSv1. Any configuration you make to the WTB setting has no effect. The output from the CLI command 'show protection-group ethernet-ring node-state detail' lists a WTB setting but that setting has no effect.

## Adding and Removing a Node

Starting with Junos OS Release 14.2, you can add or remove a node between two nodes in an Ethernet ring. Nodes are added or removed using the `force switch` command.

**NOTE:** EX2300 and EX3400 switches do not support `force switch`.

## SEE ALSO

Ethernet Ring Protection Switching Overview

Configuring Ethernet Ring Protection Switching

Example: Ethernet Ring Protection Switching Configuration on MX Routers

*Example: Configuring Ethernet Ring Protection Switching on EX Series Switches*

[Configuring Ethernet Ring Protection Switching on Switches \(CLI Procedure\)](#)

**Release History Table**

Release	Description
18.2R1	Starting with Junos OS Release 18.2R1, EX2300 and EX3400 switches automatically log basic state transitions for the ERPS protocol.
14.2	Starting with Junos OS Release 14.2, the FDB flush depends on the RAPS messages received on the both the ports of the ring node.
14.2	Starting with Junos OS Release 14.2, ring protection link neighbor nodes are supported.
14.2	Starting with Junos OS Release 14.2, you can add or remove a node between two nodes in an Ethernet ring.
14.1X53-D15	Starting with Junos OS Release 14.1X53-D15, EX Series switches automatically log basic state transitions for the ERPS protocol.

## CHAPTER 13

# Configuring Ethernet Ring Protection Switching for High Availability

**IN THIS CHAPTER**

- [Configuring Ethernet Ring Protection Switching | 234](#)

## Configuring Ethernet Ring Protection Switching

**SUMMARY**

Follow the steps below to configure Ethernet ring protection switching (ERPS) on your device.

**IN THIS SECTION**

- [Configuring Ethernet Ring Protection Switching | 234](#)
- [Example: Ethernet Ring Protection Switching Configuration on MX Routers | 235](#)

## Configuring Ethernet Ring Protection Switching

The inheritance model follows:

```
[edit protocols]
protection-group {
  ethernet-ring ring-name (
    node-id mac-address;
    ring-protection-link-owner;
    east-interface {
      control-channel channel-name {
        ring-protection-link-end;
      }
    }
    west-interface {
```

```

        node-id mac-address;
        control-channel channel-name {
            ring-protection-link-end;
        }
        data-channel {
            vlan number;
        }
        guard-interval number;
        restore-interval number;
    }
}

```

For each ring, a protection group must be configured. There may be several rings in each node, so there should be multiple protection groups corresponding to the related Ethernet rings.

Three interval parameters (restore-interval, guard-interval, and hold-interval) can be configured at the protection group level. These configurations are global configurations and apply to all Ethernet rings if the Ethernet ring doesn't have a more specific configuration for these values. If no parameter is configured at the protection group level, the global configuration of this parameter uses the default value.

## SEE ALSO

Ethernet Ring Protection Switching Overview

Understanding Ethernet Ring Protection Switching Functionality

Example: Ethernet Ring Protection Switching Configuration on MX Routers

*Example: Configuring Ethernet Ring Protection Switching on EX Series Switches*

[Ethernet Interfaces User Guide for Routing Devices](#)

## Example: Ethernet Ring Protection Switching Configuration on MX Routers

### IN THIS SECTION

- [Requirements | 236](#)
- [Ethernet Ring Overview and Topology | 236](#)
- [Configuring a Three-Node Ring | 237](#)

This example describes how to configure Ethernet ring protection switching on an MX Series router:

## Requirements

This example uses the following hardware and software components:

- Router node 1 running Junos OS with two Gigabit Ethernet interfaces.
- Router node 2 running Junos OS with two Gigabit Ethernet interfaces.
- Router node 3 running Junos OS with two Gigabit Ethernet interfaces.

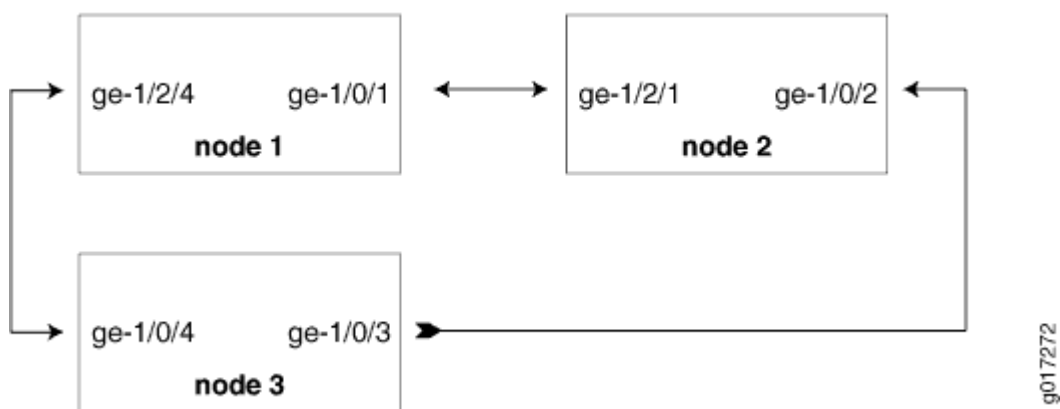
## Ethernet Ring Overview and Topology

### IN THIS SECTION

- [Topology | 236](#)

This section describes a configuration example for a three-node ring. The ring topology is shown in [Figure 17 on page 236](#).

**Figure 17: Example of a Three-Node Ring Topology**



### Topology

The configuration in this section is only for the RAPS channel. The bridge domain for user traffic is the same as the normal bridge domain. The only exception is if a bridge domain includes a ring port, then it must also include the other ring port of the same ring.

## Configuring a Three-Node Ring

### IN THIS SECTION

- [Configuring Ethernet Ring Protection Switching on a Three-Node Ring | 237](#)

To configure Ethernet Ring Protection Switching on a three-node ring, perform these tasks:

### *Configuring Ethernet Ring Protection Switching on a Three-Node Ring*

#### Step-by-Step Procedure

##### 1. Configuring Node 1

```
interfaces {
    ge-1/0/1 {
        vlan-tagging;
        encapsulation flexible-ethernet-services;
        unit 1 {
            encapsulation vlan-bridge;
            vlan-id 100;
        }
    }
    ge-1/2/4 {
        vlan-tagging;
        encapsulation flexible-ethernet-services;
        unit 1 {
            encapsulation vlan-bridge;
            vlan-id 100;
        }
    }
}
bridge-domains {
    bd1 {
        domain-type bridge;
        interface ge-1/2/4.1;
        interface ge-1/0/1.1;
    }
}
```

```

}
protocols {
    protection-group {
        ethernet-ring pg101 {
            node-id 00:01:01:00:00:01;
            ring-protection-link-owner;
            east-interface {
                control-channel ge-1/0/1.1;
                ring-protection-link-end;
            }
            west-interface {
                control-channel ge-1/2/4.1;
            }
        }
    }
}

protocols {
    oam {
        ethernet {
            connectivity-fault-management {
                action-profile rmep-defaults {
                    default-action {
                        interface-down;
                    }
                }

                maintenance-domain d1 {
                    level 0;
                    maintenance-association 100 {
                        mep 1 {
                            interface ge-1/0/1;
                            remote-mep 2 {
                                action-profile rmep-defaults;
                            }
                        }
                    }
                }

                maintenance-domain d2 {
                    level 0;
                    maintenance-association 100 {
                        mep 1 {
                            interface ge-1/2/4;
                            remote-mep 2 {

```





```

protection-group {
    ethernet-ring pg102 {
        east-interface {
            control-channel ge-1/0/2.1;
        }
        west-interface {
            control-channel ge-1/2/1.1;
        }
    }
}

protocols {
    oam {
        ethernet {
            connectivity-fault-management {
                action-profile rmep-defaults {
                    default-action {
                        interface-down;
                    }
                }
            }
            maintenance-domain d1 {
                level 0;
                maintenance-association 100 {
                    mep 2 {
                        interface ge-1/2/1;
                        remote-mep 1 {
                            action-profile rmep-defaults;
                        }
                    }
                }
            }
            maintenance-domain d3 {
                level 0;
                maintenance-association 100 {
                    mep 1 {
                        interface ge-1/0/2;
                        remote-mep 2 {
                            action-profile rmep-defaults;
                        }
                    }
                }
            }
        }
    }
}

```

```

    }
  }
}
}

```

### 3. Configuring Node 3

```

interfaces {
  ge-1/0/4 {
    vlan-tagging;
    encapsulation flexible-ethernet-services;
    unit 1 {
      encapsulation vlan-bridge;
      vlan-id 100;
    }
  }

  ge-1/0/3 {
    vlan-tagging;
    encapsulation flexible-ethernet-services;
    unit 1 {
      encapsulation vlan-bridge;
      vlan-id 100;
    }
  }
}

bridge-domains {
  bd1 {
    domain-type bridge;
    interface ge-1/0/4.1;
    interface ge-1/0/3.1;
  }
}

protocols {
  protection-group {
    ethernet-ring pg103 {
      east-interface {
        control-channel ge-1/0/3.1;

```

```

    }
    west-interface {
        control-channel ge-1/0/4.1;
    }
}
}

protocols {
    oam {
        ethernet {
            connectivity-fault-management {
                action-profile rmep-defaults {
                    default-action {
                        interface-down;
                    }
                }
                maintenance-domain d2 {
                    level 0;
                    maintenance-association 100 {
                        mep 2 {
                            interface ge-1/0/4;
                            remote-mep 1 {
                                action-profile rmep-defaults;
                            }
                        }
                    }
                }
                maintenance-domain d3 {
                    level 0;
                    maintenance-association 100 {
                        mep 2 {
                            interface ge-1/0/3;
                            remote-mep 1 {
                                action-profile rmep-defaults;
                            }
                        }
                    }
                }
            }
        }
    }
}

```

```

    }
}

```

## Examples: Ethernet RPS Output

This section provides output examples based on the configuration shown in ["Example: Ethernet Ring Protection Switching Configuration on MX Routers" on page 235](#). The show commands used in these examples can help verify configuration and correct operation.

### Normal Situation—RPL Owner Node

If the ring has no failure, the show command will have the following output for Node 1:

```
user@node1> show protection-group ethernet-ring aps
```

Ethernet Ring Name	Request/state	No Flush	Ring Protection Link Blocked
pg101	NR	No	Yes

Originator	Remote Node ID
Yes	

```
user@node1> show protection-group ethernet-ring interface
```

Ethernet ring port parameters for protection group pg101

Interface	Control Channel	Forward State	Ring Protection Link End
ge-1/0/1	ge-1/0/1.1	discarding	Yes
ge-1/2/4	ge-1/2/4.1	forwarding	No

Signal Failure	Admin State
Clear	IFF ready
Clear	IFF ready

```
user@node1> show protection-group ethernet-ring node-state
```

Ethernet ring	APS State	Event	Ring Protection Link Owner
pg101	idle	NR-RB	Yes

Restore Timer	Quard Timer	Operation state
disabled	disabled	operational

```
user@node1> show protection-group ethernet-ring statistics group-name pg101
```

Ethernet Ring statistics for PG pg101

```

RAPS sent                : 1
RAPS received            : 0
Local SF happened:       : 0
Remote SF happened:       : 0
NR event happened:        : 0
NR-RB event happened:     : 1

```

### Normal Situation—Other Nodes

For Node 2 and Node 3, the outputs should be the same:

```

user@node2> show protection-group ethernet-ring aps
Ethernet Ring Name Request/state No Flush Ring Protection Link Blocked
pg102              NR           No      Yes

Originator Remote Node ID
No          00:01:01:00:00:01

user@node2> show protection-group ethernet-ring interface
Ethernet ring port parameters for protection group pg102

Interface Control Channel Forward State Ring Protection Link End
ge-1/2/1   ge-1/2/1.1         forwarding No
ge-1/0/2   ge-1/0/2.1         forwarding No

Signal Failure Admin State
Clear       IFF ready
Clear       IFF ready

user@node2> show protection-group ethernet-ring node-state
Ethernet ring APS State Event Ring Protection Link Owner
pg102         idle      NR-RB No

Restore Timer Guard Timer Operation state
disabled      disabled operational

user@node2> show protection-group ethernet-ring statistics group-name pg102
Ethernet Ring statistics for PG pg101
RAPS sent                : 0
RAPS received            : 1
Local SF happened:       : 0
Remote SF happened:      : 0

```

```
NR event happened:           : 0
NR-RB event happened:        : 1
```

### Failure Situation—RPL Owner Node

If the ring has a link failure between Node 2 and Node 3, the `show` command will have the following outputs for Node 1:

```
user@node1> show protection-group ethernet-ring aps
Ethernet Ring Name Request/state No Flush Ring Protection Link Blocked
pg101              SF           NO      No

Originator Remote Node ID
No          00:01:02:00:00:01

user@node1> show protection-group ethernet-ring interface
Ethernet ring port parameters for protection group pg101

Interface Control Channel Forward State Ring Protection Link End
ge-1/0/1   ge-1/0/1.1         forwarding Yes
ge-1/2/4   ge-1/2/4.1         forwarding No

Signal Failure Admin State
Clear       IFF ready
Clear       IFF ready

user@node1> show protection-group ethernet-ring node-state
Ethernet ring APS State Event Ring Protection Link Owner
pg101         protected SF Yes

Restore Timer Quard Timer Operation state
disabled      disabled operational

user@node1> show protection-group ethernet-ring statistics group-name pg101
Ethernet Ring statistics for PG pg101
RAPS sent           : 1
RAPS received       : 1
Local SF happened:   : 0
Remote SF happened:  : 1
NR event happened:   : 0
NR-RB event happened: : 1
```

## Failure Situation—Other Nodes

For Node 2 and Node 3, the outputs should be the same:

```

user@node2> show protection-group ethernet-ring aps
Ethernet Ring Name Request/state No Flush Ring Protection Link Blocked
pg102              SF           No      No

Originator Remote Node ID
Yes         00:00:00:00:00:00

user@node2> show protection-group ethernet-ring interface
Ethernet ring port parameters for protection group pg102

Interface Control Channel Forward State Ring Protection Link End
ge-1/2/1   ge-1/2/1.1      forwarding No
ge-1/0/2   ge-1/0/2.1      discarding No

Signal Failure Admin State
Clear         IFF ready
set           IFF ready

user@node2> show protection-group ethernet-ring node-state
Ethernet ring APS State Event Ring Protection Link Owner
pg102         idle      NR-RB No

Restore Timer Quard Timer Operation state
disabled      disabled operational

user@node2> show protection-group ethernet-ring statistics group-name pg102
Ethernet Ring statistics for PG pg101
RAPS sent : 1
RAPS received : 1
Local SF happened: : 1
Remote SF happened: : 0
NR event happened: : 0
NR-RB event happened: : 1

```

## SEE ALSO

Ethernet Ring Protection Switching Overview



Understanding Ethernet Ring Protection Switching Functionality

---

Configuring Ethernet Ring Protection Switching

---

[Ethernet Interfaces User Guide for Routing Devices](#)

# 8

PART

## Configuring Nonstop Bridging

---

Understanding How Nonstop Bridging Preserves Layer 2 Protocol Information  
During a Routing Engine Switchover | 249

Configuring Nonstop Bridging | 254

---

# Understanding How Nonstop Bridging Preserves Layer 2 Protocol Information During a Routing Engine Switchover

## IN THIS CHAPTER

- [Understanding Nonstop Bridging | 249](#)

## Understanding Nonstop Bridging

### SUMMARY

Nonstop bridging (NSB) helps preserve interface and kernel information on Routing Engine switchover, and synchronizes all protocol information for NSB-supported Layer 2 protocols between the primary and backup Routing Engines.

### IN THIS SECTION

- [Nonstop Bridging Concepts | 249](#)
- [Understanding Nonstop Bridging on EX Series Switches | 252](#)
- [Nonstop Bridging System Requirements | 252](#)

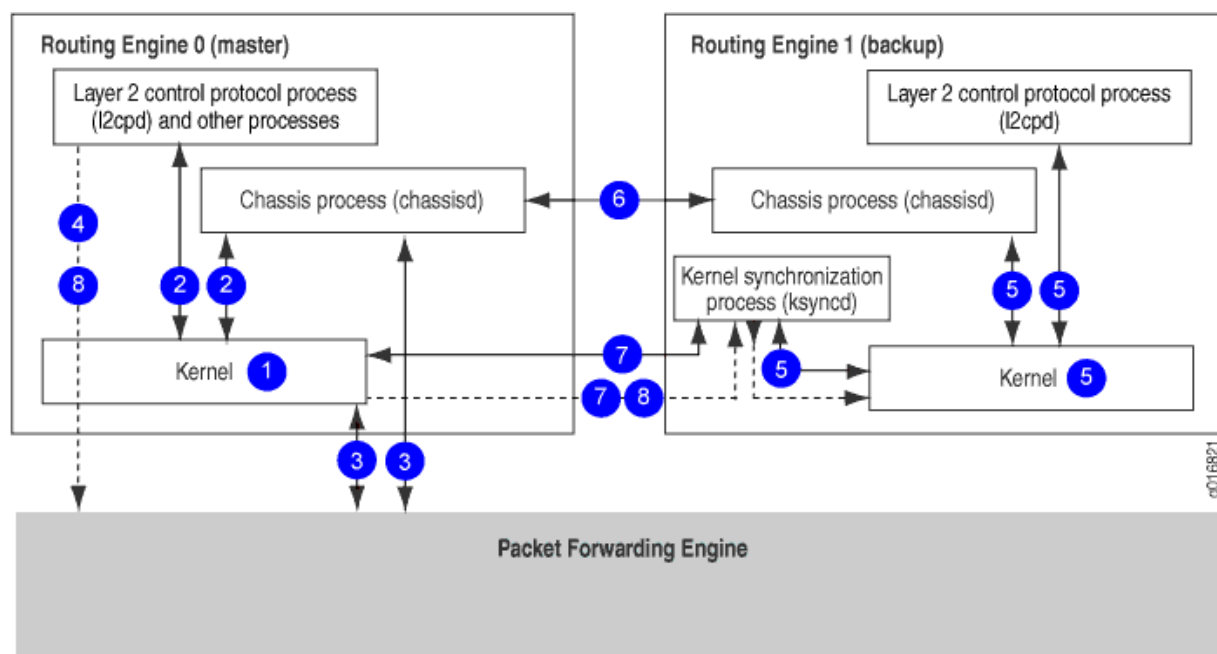
## Nonstop Bridging Concepts

Nonstop bridging uses the same infrastructure as *graceful Routing Engine switchover* (GRES) to preserve interface and kernel information. However, nonstop bridging also saves Layer 2 Control Protocol (L2CP) information by running the Layer 2 Control Protocol process (l2cpd) on the backup Routing Engine.

**NOTE:** To use nonstop bridging, you must first enable graceful Routing Engine switchover on your routing (or switching) platform. For more information about graceful Routing Engine switchover, see [Understanding Graceful Routing Engine Switchover](#).

Figure 18 on page 250 shows the system architecture of nonstop bridging and the process a routing (or switching) platform follows to prepare for a switchover.

**Figure 18: Nonstop Bridging Switchover Preparation Process**

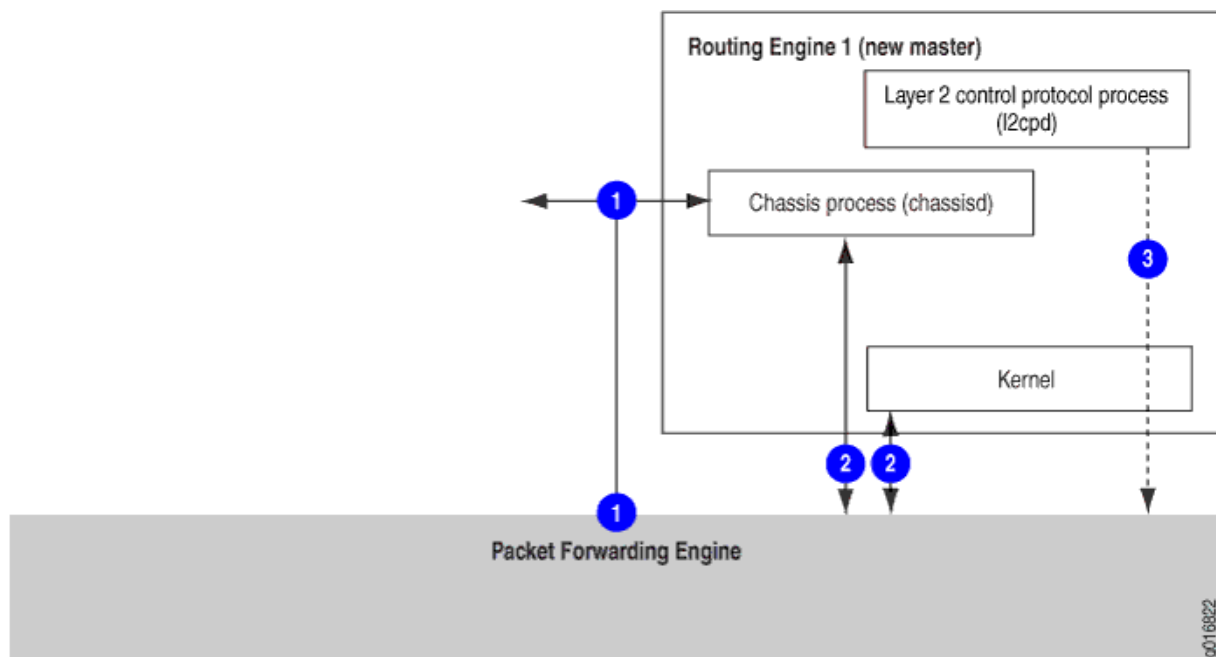


The switchover preparation process for nonstop bridging follows these steps:

1. The primary Routing Engine starts.
2. The routing platform processes on the primary Routing Engine (such as the chassis process [chassisd] and the Layer 2 Control Protocol process [l2cpd]) start.
3. The Packet Forwarding Engine starts and connects to the primary Routing Engine.
4. All state information is updated in the system.
5. The backup Routing Engine starts, including the chassis process (chassisd) and the Layer 2 Control Protocol process (l2cpd).
6. The system determines whether graceful Routing Engine switchover and nonstop bridging have been enabled.
7. The kernel synchronization process (ksyncd) synchronizes the backup Routing Engine with the primary Routing Engine.
8. For supported protocols, state information is updated directly between the l2cpds on the primary and backup Routing Engines.

Figure 19 on page 251 shows the effects of a switchover on the routing platform.

**Figure 19: Nonstop Bridging During a Switchover**



The switchover process follows these steps:

1. When keepalives from the primary Routing Engine are lost, the system switches over gracefully to the backup Routing Engine.
2. The Packet Forwarding Engine connects to the backup Routing Engine, which becomes the new primary. Because the Layer 2 Control Protocol process (l2cpd) and chassis process (chassisd) are already running, these processes do not need to restart.
3. State information learned from the point of the switchover is updated in the system. Forwarding and bridging are continued during the switchover, resulting in minimal packet loss.

## SEE ALSO

[Understanding High Availability Features on Juniper Networks Routers | 2](#)

Nonstop Bridging System Requirements

[Configuring Nonstop Bridging | 254](#)

Configuring Nonstop Bridging on Switches (CLI Procedure)

## Understanding Nonstop Bridging on EX Series Switches

You can configure nonstop bridging (NSB) to provide resilience for Layer 2 protocol sessions on a Juniper Networks EX Series Ethernet Switch or on an EX Series *Virtual Chassis* with redundant Routing Engines.

NSB operates by synchronizing all protocol information for NSB-supported Layer 2 protocols between the primary and backup Routing Engines. If the switch has a Routing Engine switchover, the NSB-supported Layer 2 protocol sessions remain active because all session information is already synchronized to the backup Routing Engine. Traffic disruption for the NSB-supported Layer 2 protocol is minimal or nonexistent as a result of the switchover. The Routing Engine switchover is transparent to neighbor devices, which do not detect any changes related to the NSB-supported Layer 2 protocol sessions on the switch.

For a list of the EX Series switches and Layer 2 protocols that support NSB, see [EX Series Switch Software Features Overview](#) and [EX Series Virtual Chassis Software Features Overview](#).

**NOTE:** Nonstop bridging provides a transparent switchover mechanism only for Layer 2 protocol sessions. *Nonstop active routing* (NSR) provides a similar mechanism for Layer 3 protocol sessions. See [Understanding Nonstop Active Routing on EX Series Switches](#).

### SEE ALSO

Configuring Nonstop Bridging on EX Series Switches (CLI Procedure)  
 Configuring Nonstop Bridging on Switches (CLI Procedure)

## Nonstop Bridging System Requirements

### IN THIS SECTION

- [Platform Support | 253](#)
- [Protocol Support | 253](#)

This topic contains the following sections:

## Platform Support

Nonstop bridging is supported on MX Series 5G Universal Routing Platforms. Your system must be running Junos OS Release 8.4 or later.

Nonstop bridging is supported on EX Series switches with redundant Routing Engines in a Virtual Chassis or in a Virtual Chassis Fabric.

Nonstop bridging is supported on QFX Series switches in a Virtual Chassis or in a Virtual Chassis Fabric.

For a list of the EX Series switches and Layer 2 protocols that support nonstop bridging, see [EX Series Switch Software Features Overview](#).

**NOTE:** All Routing Engines configured for nonstop bridging must be running the same Junos OS release.

## Protocol Support

Nonstop bridging is supported for the following Layer 2 control protocols:

- Spanning Tree Protocol (STP)
- Rapid Spanning Tree Protocol (RSTP)
- Multiple Spanning Tree Protocol (MSTP)
- VLAN Spanning Tree Protocol (VSTP)

## SEE ALSO

Nonstop Bridging Concepts

[Configuring Nonstop Bridging | 254](#)

Configuring Nonstop Bridging on Switches (CLI Procedure)

## CHAPTER 15

# Configuring Nonstop Bridging

**IN THIS CHAPTER**

- [Configuring Nonstop Bridging | 254](#)

## Configuring Nonstop Bridging

**SUMMARY**

You can configure nonstop bridging by following the steps below.

**IN THIS SECTION**

- [Enabling Nonstop Bridging | 254](#)
- [Synchronizing the Routing Engine Configuration | 255](#)
- [Verifying Nonstop Bridging Operation | 255](#)
- [Configuring Nonstop Bridging on Switches \(CLI Procedure\) | 255](#)
- [Configuring Nonstop Bridging on EX Series Switches \(CLI Procedure\) | 257](#)

### Enabling Nonstop Bridging

Nonstop bridging requires you to configure graceful Routing Engine switchover (GRES). To enable graceful Routing Engine switchover, include the `graceful-switchover` statement at the `[edit chassis redundancy]` hierarchy level:

```
[edit chassis redundancy]  
graceful-switchover;
```



By default, nonstop bridging is disabled. To enable nonstop bridging, include the `nonstop-bridging` statement at the `[edit protocols layer2-control]` hierarchy level:

```
[edit protocols layer2-control]  
nonstop-bridging;
```

To disable nonstop active routing, remove the `nonstop-bridging` statement from the `[edit protocols layer2-control]` hierarchy level.

## Synchronizing the Routing Engine Configuration

When you configure nonstop bridging, you must also include the `commit synchronize` statement at the `[edit system]` hierarchy level so that, by default, when you issue the `commit` command, the configuration changes are synchronized on both Routing Engines. If you issue the `commit synchronize` command at the `[edit]` hierarchy level on the backup Routing Engine, the Junos OS displays a warning and commits the candidate configuration.

**NOTE:** A newly inserted backup Routing Engine automatically synchronizes its configuration with the primary Routing Engine configuration.

When you configure nonstop bridging, you can bring the backup Routing Engine online after the primary Routing Engine is already running. There is no requirement to start the two Routing Engines simultaneously.

## Verifying Nonstop Bridging Operation

When you enable nonstop bridging, you can issue Layer 2 Control Protocol-related operational mode commands on the backup Routing Engine. However, the output of the commands might not match the output of the same commands issued on the primary Routing Engine.

## Configuring Nonstop Bridging on Switches (CLI Procedure)

**NOTE:** This task uses switches with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, see [Configuring Nonstop Bridging on EX Series Switches \(CLI Procedure\)](#). For ELS details, see [Using the Enhanced Layer 2 Software CLI](#).

You can configure nonstop bridging (NSB) to provide resilience for Layer 2 protocol sessions on a Juniper Networks EX Series switch with multiple Routing Engines or an EX Series or QFX Series switch in a Virtual Chassis or Virtual Chassis Fabric configuration. Limited support for NSB is also provided on QFX5100 and EX4600 standalone switches, but NSB is enabled *only* during an ISSU.

NSB operates by synchronizing all protocol information for NSB-supported Layer 2 protocols between the primary and backup Routing Engines. If the switch has a Routing Engine switchover, the NSB-supported Layer 2 protocol sessions remain active because they are already synchronized on the backup Routing Engine. The Routing Engine switchover is transparent to neighbor devices, which do not detect any changes related to the Layer 2 protocol sessions. The neighboring devices and other devices on the network do not, therefore, have to resynchronize their Layer 2 protocol states to respond to the downtime on the switch—a process that adds network overhead and risks disrupting network performance—when a Routing Engine switchover occurs when NSB is enabled.

**NOTE:** If you are using a QFX5100 or EX4600 standalone switch and you want to use ISSU, configure Graceful Routing Engine switchover (GRES), NSB and nonstop active routing (NSR). You must configure NSB, GRES, and NSR in order to run ISSU. However, GRES, NSB and NSR are enabled *only* during the upgrade. During an ISSU, the Junos OS runs in two separate virtual machines (VMs)—one VM is in the primary role acting as the primary Routing Engine, and the other VM is in the backup role acting as the backup Routing Engine. The Junos OS is upgraded on the backup VM. After a successful software upgrade, the backup VM then becomes the primary VM, and the original primary VM is no longer needed and is shut down.

To configure NSB:

1. Enable graceful Routing Engine switchover (GRES):

```
[edit chassis redundancy]
user@switch# set graceful-switchover
```

2. Enable NSB:

```
[edit protocols layer2-control]
user@switch# set nonstop-bridging
```

3. Synchronize configuration changes between the Routing Engines:

```
[edit system]
user@switch# set commit synchronize
```

If you try to commit a configuration that includes NSB without including the `commit synchronize` statement, the commit fails.

**NOTE:** There is no requirement to start the two Routing Engines simultaneously. If the backup Routing Engine is not up when you use the `commit synchronize` statement, the candidate configuration is committed in the primary Routing Engine. When the backup Routing Engine comes online, its configuration is automatically synchronized with that of the primary.

**BEST PRACTICE:** After a graceful Routing Engine switchover, we recommend that you issue the `clear interface statistics (interface-name | all)` command to reset the cumulative values for local statistics on the new primary Routing Engine.

## SEE ALSO

Performing an In-Service Software Upgrade (ISSU) with Non-Stop Routing

Understanding Nonstop Bridging on EX Series Switches

Nonstop Bridging Concepts

Understanding In-Service Software Upgrade (ISSU)

## Configuring Nonstop Bridging on EX Series Switches (CLI Procedure)

**NOTE:** This task uses Junos OS for EX Series switches that do not support the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that supports ELS, see [Configuring Nonstop Bridging on Switches \(CLI Procedure\)](#).

You can configure nonstop bridging (NSB) to provide resilience for Layer 2 protocol sessions on an EX Series switch with redundant Routing Engines.

Nonstop bridging operates by synchronizing all protocol information for NSB-supported Layer 2 protocols between the primary and backup Routing Engines. If the switch has a Routing Engine switchover, the NSB-supported Layer 2 protocol sessions remain active because they are already synchronized on the backup Routing Engine. The Routing Engine switchover is transparent to neighbor devices, which do not detect any changes related to the Layer 2 protocol sessions on the switch.

To configure nonstop bridging:

1. Enable graceful Routing Engine switchover (GRES):

```
[edit chassis redundancy]
user@switch# set graceful-switchover
```

2. Configure the switch to always synchronize configuration changes between the Routing Engines:

```
[edit system]
user@switch# set commit synchronize
```

If you try to commit a configuration in which nonstop bridging is configured but synchronization of configuration changes is not configured, the configuration is not committed.

3. Enable nonstop bridging:

```
[edit ethernet-switching-options]
user@switch# set nonstop-bridging
```

**NOTE:** There is no requirement to start both Routing Engines simultaneously. If the backup Routing Engine is not up when you commit the configuration, the candidate configuration is committed in the primary Routing Engine. When the backup Routing Engine comes online, the configuration is automatically synchronized.

## SEE ALSO

*Example: Faster Convergence and Improved Network Stability with RSTP on EX Series Switches*

Understanding Nonstop Bridging on EX Series Switches

## RELATED DOCUMENTATION

Nonstop Bridging Concepts

Nonstop Bridging System Requirements

[nonstop-bridging](#) | 1074

Configuring Nonstop Bridging on EX Series Switches (CLI Procedure)

# 9

PART

## Configuring Nonstop Active Routing (NSR)

---

Understanding How Nonstop Active Routing Preserves Routing Protocol  
Information During a Routing Engine Switchover | 260

Configuring Nonstop Active Routing | 281

---

# Understanding How Nonstop Active Routing Preserves Routing Protocol Information During a Routing Engine Switchover

## IN THIS CHAPTER

- [Understanding Nonstop Active Routing | 260](#)

## Understanding Nonstop Active Routing

### SUMMARY

Nonstop active routing (NSR) enables the transparent switchover of the Routing Engines in the event that one of the Routing Engines goes down.

### IN THIS SECTION

- [Nonstop Active Routing Concepts | 260](#)
- [Understanding Nonstop Active Routing on EX Series Switches | 264](#)
- [Nonstop Active Routing System Requirements | 265](#)

## Nonstop Active Routing Concepts

*Nonstop active routing* (NSR) uses the same infrastructure as *graceful Routing Engine switchover* (GRES) to preserve interface and kernel information. However, NSR also saves routing protocol information by running the routing protocol process (rpd) on the backup Routing Engine. By saving this additional information, NSR is self-contained and does not rely on helper routers (or switches) to assist the routing platform in restoring routing protocol information. NSR is advantageous in networks in which neighbor routers (or switches) do not support graceful restart protocol extensions. As a result of this enhanced functionality, NSR is a natural replacement for graceful restart.

Starting with Junos OS Release 15.1R1, if you have NSR configured, it is never valid to issue the restart routing command in any form on the NSR primary Routing Engine. Doing so results in a loss of protocol adjacencies and neighbors and a drop in traffic.

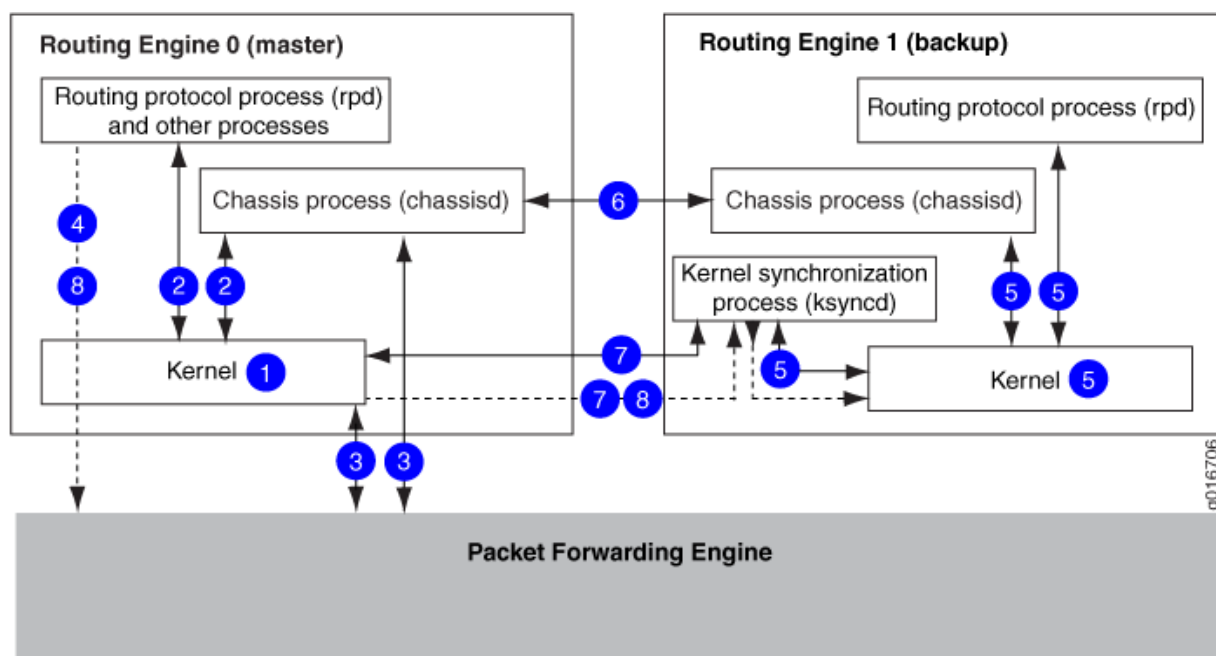
**NOTE:** To use NSR, you must first enable GRES on your routing (or switching) platform. For more information about GRES, see Understanding Graceful Routing Engine Switchover.

**NOTE:** If NSR is enabled, certain system log (syslog) messages are sent from the backup Routing Engine if the configured syslog host is reachable through the fxp0 interface.

**NOTE:** NSR is not supported during the Routing Engine reboot process on MX Series devices with the Next-Generation Routing Engine (NG-RE) installed. NSR will still work during the Routing Engine switchover process.

Figure 20 on page 261 shows the system architecture of nonstop active routing and the process a routing (or switching) platform follows to prepare for a switchover.

**Figure 20: Nonstop Active Routing Switchover Preparation Process**



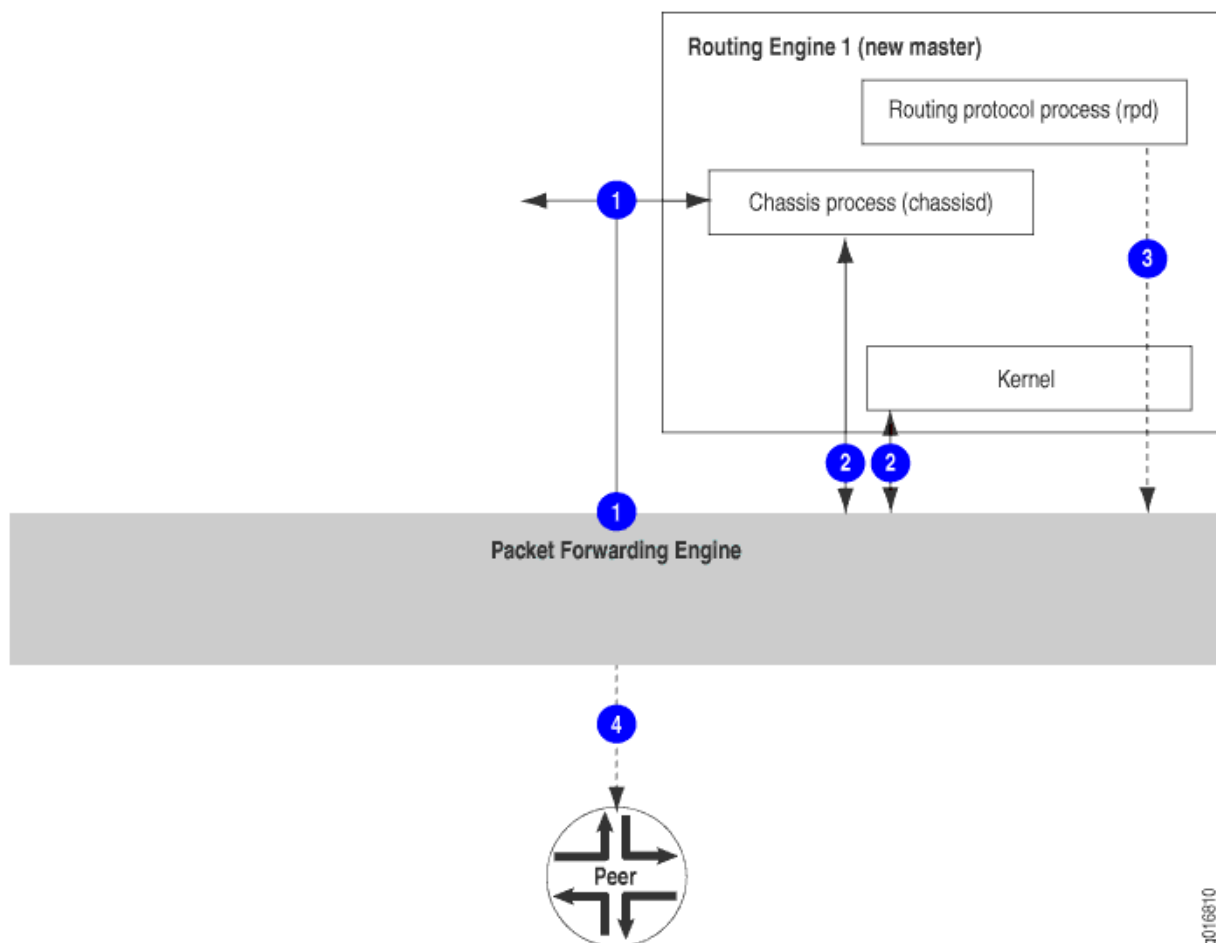
The switchover preparation process for NSR comprises the following steps:

1. The primary Routing Engine starts.
2. The routing (or switching) platform processes on the primary Routing Engine (such as the chassis process [chassisd] and the routing protocol process [rpd]) start.
3. The Packet Forwarding Engine starts and connects to the primary Routing Engine.
4. All state information is updated in the system.
5. The backup Routing Engine starts, including the chassis process (chassisd) and the routing protocol process (rpd).
6. The system determines whether GRES and NSR have been enabled.
7. The kernel synchronization process (ksyncd) synchronizes the backup Routing Engine with the primary Routing Engine.
8. For supported protocols, state information is updated directly between the routing protocol processes on the primary and backup Routing Engines.

[Figure 21 on page 263](#) shows the effects of a switchover on the routing platform.



Figure 21: Nonstop Active Routing During a Switchover



The switchover process comprises the following steps:

1. When keepalives from the primary Routing Engine are lost, the system switches over gracefully to the backup Routing Engine.
2. The Packet Forwarding Engine connects to the backup Routing Engine, which becomes the new primary. Because the routing protocol process (rpd) and chassis process (chassisd) are already running, these processes do not need to restart.
3. State information learned from the point of the switchover is updated in the system. Forwarding and routing are continued during the switchover, resulting in minimal packet loss.
4. Peer routers (or switches) continue to interact with the routing platform as if no change had occurred. Routing adjacencies and session state relying on underlying routing information are preserved and not reset.



**CAUTION:** We recommend that you do not restart the routing protocol process (rpd) on primary Routing Engine after enabling NSR, as it disrupts the protocol adjacency/peering sessions, resulting in traffic loss.

## SEE ALSO

[Understanding High Availability Features on Juniper Networks Routers | 2](#)

Nonstop Active Routing System Requirements

[Configuring Nonstop Active Routing | 281](#)

Configuring Nonstop Active Routing on Switches

## Understanding Nonstop Active Routing on EX Series Switches

You can configure *nonstop active routing* (NSR) on an EX Series switch with redundant Routing Engines or on an EX Series *Virtual Chassis* to enable the transparent switchover of the Routing Engines in the event that one of the Routing Engines goes down.

Nonstop active routing provides high availability for Routing Engines by enabling transparent switchover of the Routing Engines without requiring restart of supported routing protocols. Both Routing Engines are fully active in processing protocol sessions, and so each can take over for the other. The switchover is transparent to neighbor routing devices, which do not detect that a change has occurred.

Enable nonstop active routing when neighbor routing devices are not configured to support graceful restart of protocols or when you want to ensure graceful restart of protocols for which graceful restart is not supported—such as PIM.

You do not need to start the two Routing Engines simultaneously to synchronize them for nonstop active routing. If both Routing Engines are not present or not up when you issue a `commit synchronize` statement, the candidate configuration is committed in the primary Routing Engine and when the backup Routing Engine is inserted or comes online, its configuration is automatically synchronized with that of the primary.

Nonstop active routing uses the same infrastructure as *graceful Routing Engine switchover* (GRES) to preserve interface and kernel information. However, nonstop active routing also saves routing protocol information by running the routing protocol process (**rpd**) on the backup Routing Engine. By saving this additional information, nonstop active routing does not rely on other routing devices to assist in restoring routing protocol information.

**NOTE:** After a graceful Routing Engine switchover, we recommend that you issue the `clear interface statistics` (*interface-name* | all) command to reset the cumulative values for local statistics on the new primary Routing Engine.

If you suspect a problem with the synchronization of Routing Engines when nonstop active routing is enabled, you can gather troubleshooting information using trace options. For example, if certain protocols lose connectivity with neighbors after a graceful Routing Engine switchover with NSR enabled, you can use trace options to help isolate the problem. See ["Tracing Nonstop Active Routing Synchronization Events" on page 1562](#).

**NOTE:** Graceful restart and nonstop active routing are mutually exclusive. You will receive an error message upon commit if both are configured.

**NOTE:** Nonstop active routing provides a transparent switchover mechanism only for Layer 3 protocol sessions. Nonstop bridging (NSB) provides a similar mechanism for Layer 2 protocol sessions. See [Understanding Nonstop Bridging on EX Series Switches](#).

## SEE ALSO

Configuring Nonstop Active Routing on Switches

Example: Configuring Nonstop Active Routing on Switches

## Nonstop Active Routing System Requirements

### IN THIS SECTION

- [Nonstop Active Routing Platform and Switching Platform Support | 266](#)
- [Nonstop Active Routing Protocol and Feature Support | 268](#)
- [Nonstop Active Routing BFD Support | 272](#)
- [Nonstop Active Routing BGP Support | 273](#)
- [Nonstop Active Routing Layer 2 Circuit and VPLS Support | 274](#)
- [Nonstop Active Routing PIM Support | 275](#)

- [Nonstop Active Routing MSDP Support | 277](#)
- [Nonstop Active Routing Support for RSVP-TE LSPs | 278](#)

This section contains the following topics:

**Nonstop Active Routing Platform and Switching Platform Support**

[Table 6 on page 266](#) lists the platforms that support nonstop active routing (NSR).

**Table 6: Nonstop Active Routing Platform Support**

Platform	Junos OS Release
M10i router	8.4 or later
M20 router	8.4 or later
M40e router	8.4 or later
M120 router	9.0 or later
M320 router	8.4 or later
MX Series routers	9.0 or later

Table 6: Nonstop Active Routing Platform Support *(Continued)*

Platform	Junos OS Release
PTX Series Packet Transport Routers  <b>NOTE:</b> Nonstop active routing (NSR) switchover on PTX series is supported only for the following MPLS and VPN protocols and applications using chained composite next hops: <ul style="list-style-type: none"> <li>• Labeled BGP</li> <li>• Layer 2 VPNs excluding Layer 2 interworking (Layer 2 switching)</li> <li>• Layer 3 VPNs</li> <li>• LDP</li> <li>• RSVP</li> </ul>	12.1R4 or later
T320 router, T640 router, and TX Matrix router	8.4 or later
Standalone T1600 router	8.5 or later
Standalone T4000 router	12.1R2 or later
TX Plus Matrix router	10.0 or later
TX Plus Matrix router with 3D SIBs	13.1 or later
EX Series switch with dual Routing Engines or in a Virtual Chassis	10.4 or later for EX Series switches
EX Series or QFX Series switches in a Virtual Chassis Fabric	13.2X51-D20 or later for the EX Series and QFX Series switches

**NOTE:** All Routing Engines configured for nonstop active routing must be running the same Junos OS release.

## Nonstop Active Routing Protocol and Feature Support

Table 7 on page 268 lists the protocols that are supported by nonstop active routing.

**Table 7: Nonstop Active Routing Protocol and Feature Support**

Protocol	Junos OS Release
Aggregated Ethernet interfaces with Link Aggregation Control Protocol (LACP)	9.4 or later
Bidirectional Forwarding Detection (BFD)  For more information, see <a href="#">"Nonstop Active Routing BFD Support" on page 272</a> .	8.5 or later
BGP  For more information, see <a href="#">"Nonstop Active Routing BGP Support" on page 273</a> .	8.4 or later
EVPN <ul style="list-style-type: none"> <li>• EVPN with ingress replication for BUM traffic</li> <li>• EVPN-ETREE</li> <li>• EVPN-VPWS</li> <li>• EVPN -VXLAN</li> <li>• PBB-EVPN</li> <li>• EVPN with P2MP mLDP replication for BUM traffic</li> </ul> For more information, please see <a href="#">NSR and Unified ISSU Support for EVPN</a> .	16.2R1 or later (for EVPN with ingress replication for BUM traffic )  17.2R1 or later (for (EVPN-ETREE, EVPN-VPWS, EVPN-VXLAN, and PBB-EVPN)  18.2R1 or later (for EVPN with P2MP mLDP replication for BUM traffic)
Labeled BGP (PTX Series Packet Transport Routers: only)	12.1R4 or later
IS-IS	8.4 or later
LDP	8.4 or later

Table 7: Nonstop Active Routing Protocol and Feature Support *(Continued)*

Protocol	Junos OS Release
LDP-based virtual private LAN service (VPLS)	9.3 or later
LDP OAM (operation, administration, and management) features	9.6 or later
LDP (PTX Series Packet Transport Routers only)  Nonstop active routing support for LDP includes: <ul style="list-style-type: none"> <li>• LDP unicast transit LSPs</li> <li>• LDP egress LSPs for labeled internal BGP (IBGP) and external BGP (EBGP)</li> <li>• LDP over RSVP transit LSPs</li> <li>• LDP transit LSPs with indexed next hops</li> <li>• LDP transit LSPs with unequal cost load balancing</li> <li>• LDP Point-to-Multipoint LSPs</li> <li>• LDP ingress LSPs</li> </ul>	12.3R4 or later  (for LDP Point-to-Multipoint LSPs) 13.3R1 or later  (for LDP ingress LSPs) 13.3R1 or later
Layer 2 circuits	(on LDP-based VPLS) 9.2 or later  (on RSVP-TE LSP) 11.1 or later
Layer 2 VPNs	9.1 or later
Layer 2 VPNs (PTX Series Packet Transport Routers only)  <b>NOTE:</b> Nonstop active routing is not supported for Layer 2 interworking (Layer 2 stitching).	12.1R4 or later

**Table 7: Nonstop Active Routing Protocol and Feature Support** *(Continued)*

Protocol	Junos OS Release
Layer 3 VPNs (see the first Note after this table for restrictions)  Nonstop active routing support for Layer 3 VPNs include: <ul style="list-style-type: none"> <li>• IPv4 labeled-unicast (ingress or egress)</li> <li>• IPv4-vpn unicast (ingress or egress)</li> <li>• IPv6 labeled-unicast (ingress or egress)</li> <li>• IPv6-vpn unicast (ingress or egress)</li> </ul>	9.2 or later
Layer 3 VPNs (PTX Series Packet Transport Routers only)	12.1R4 or later
Logical System support (Nonstop active routing support for logical systems to preserve interface and kernel information).	13.3R1 or later
Multicast Source Discovery Protocol (MSDP)  For more information, see <a href="#">"Nonstop Active Routing MSDP Support" on page 277</a> .	12.1 or later
OSPF/OSPFv3	8.4 or later
Protocol Independent Multicast (PIM)  For more information, see <a href="#">"Nonstop Active Routing PIM Support" on page 275</a> .	(for IPv4) 9.3 or later  (for IPv6) 10.4 or later
RIP and RIP next generation (RIPng)	9.0 or later



Table 7: Nonstop Active Routing Protocol and Feature Support *(Continued)*

Protocol	Junos OS Release
<p>RSVP (PTX Series Packet Transport Routers only)</p> <p>Nonstop active routing support for RSVP includes:</p> <ul style="list-style-type: none"> <li>• Point-to-Multipoint LSPs <ul style="list-style-type: none"> <li>• RSVP Point-to-Multipoint ingress, transit, and egress LSPs using existing non-chained next hop.</li> <li>• RSVP Point-to-Multipoint transit LSPs using composite next hops for Point-to-Multipoint label routes.</li> </ul> </li> <li>• Point-to-Point LSPs <ul style="list-style-type: none"> <li>• RSVP Point-to-Point ingress, transit, and egress LSPs using non-chained next hops.</li> <li>• RSVP Point-to-Point transit LSPs using chained composite next hops.</li> </ul> </li> </ul>	12.1R4 or later
<p>RSVP-TE LSP</p> <p>For more information, see <a href="#">"Nonstop Active Routing Support for RSVP-TE LSPs" on page 278.</a></p>	9.5 or later
VPLS	<p>(LDP-based) 9.1 or later</p> <p>(RSVP-TE-based) 11.2 or later</p>
VRRP	13.2 or later
VRRP	13.2 or later

**NOTE:** Layer 3 VPN support does not include dynamic GRE tunnels, multicast VPNs, or BGP flow routes.

**NOTE:** If you configure a protocol that is not supported by nonstop active routing, the protocol operates as usual. When a switchover occurs, the state information for the unsupported protocol is not preserved and must be refreshed using the normal recovery mechanisms inherent in the protocol.

**NOTE:** On routers that have logical systems configured on them, NSR is only supported in the main instance.

**NOTE:** Starting with Junos OS Release 13.3R5, on EX9214 switches, the VRRP primary state might change during graceful Routing Engine switchover, even when nonstop active routing is enabled.

### Nonstop Active Routing BFD Support

Nonstop active routing supports the Bidirectional Forwarding Detection (BFD) protocol, which uses the topology discovered by routing protocols to monitor neighbors. The BFD protocol is a simple hello mechanism that detects failures in a network. Because BFD is streamlined to be efficient at fast liveness detection, when it is used in conjunction with routing protocols, routing recovery times are improved. With nonstop active routing enabled, BFD session states are not restarted when a Routing Engine switchover occurs.

**NOTE:** BFD session states are saved only for clients using aggregate or static routes or for BGP, IS-IS, OSPF/OSPFv3, PIM, or RSVP.

When a BFD session is distributed to the Packet Forwarding Engine, BFD packets continue to be sent during a Routing Engine switchover. If nondistributed BFD sessions are to be kept alive during a switchover, you must ensure that the session failure detection time is greater than the Routing Engine switchover time. The following BFD sessions are not distributed to the Packet Forwarding Engine: multihop sessions, tunnel-encapsulated sessions, and sessions over integrated routing and bridging (IRB) interfaces.

**NOTE:** BFD is an intensive protocol that consumes system resources. Specifying a minimum interval for BFD less than 100 ms for Routing Engine-based sessions and 10 ms for distributed

BFD sessions can cause undesired BFD flapping. The `minimum-interval` configuration statement is a BFD liveness detection parameter.

Depending on your network environment, these additional recommendations might apply:

- For large-scale network deployments with a large number of BFD sessions, specify a minimum interval of 300 ms for Routing Engine-based sessions, and 100 ms for distributed BFD sessions.
- For very large-scale network deployments with a large number of BFD sessions, contact Juniper Networks customer support for more information.
- For BFD sessions to remain up during a Routing Engine switchover event when nonstop active routing is configured, specify a minimum interval of 2.5 seconds for Routing Engine-based sessions. For distributed BFD sessions with nonstop active routing configured, the minimum interval recommendations are unchanged and depend only on your network deployment.

## Nonstop Active Routing BGP Support

Nonstop active routing BGP support is subject to the following conditions:

- You must include the `path-selection external-router-ID` statement at the `[edit protocols bgp]` hierarchy level to ensure consistent path selection between the primary and backup Routing Engines during and after the nonstop active routing switchover.
- Starting with Junos OS Release 14.1, you must include the `advertise-from-main-vpn-tables` statement at the `[edit protocols bgp]` hierarchy level to prevent BGP sessions from going down when route reflector (RR) or autonomous system border router (ASBR) functionality is enabled or disabled on a routing device that has VPN address families configured.
- BGP session uptime and downtime statistics are not synchronized between the primary and backup Routing Engines during Nonstop Active Routing and ISSU. The backup Routing Engine maintains its own session uptime based on the time when the backup first becomes aware of the established sessions. For example, if the backup Routing Engine is rebooted (or if you run `restart routing` on the backup Routing Engine), the backup's uptime is a short duration, because the backup has just learned about the established sessions. If the backup is operating when the BGP sessions first come up on the primary, the uptime on the primary and the uptime on the backup are almost the same duration. After a Routing Engine switchover, the new primary continues from the time left on the backup Routing Engine.
- If the BGP peer in the primary Routing Engine has negotiated address-family capabilities that are not supported for nonstop active routing, then the corresponding BGP neighbor state on the backup

Routing Engine shows as idle. On switchover, the BGP session is reestablished from the new primary Routing Engine.

Only the following address families are supported for nonstop active routing.

**NOTE:** Address families are supported only on the main instance of BGP. Only unicast is supported on VRF instances.

- inet labeled-unicast
- inet-mdt
- inet multicast
- inet-mvpn
- inet unicast
- inet-vpn unicast
- inet6 labeled-unicast
- inet6 multicast
- inet6-mvpn
- inet6 unicast
- inet6-vpn unicast
- iso-vpn
- l2vpn signaling
- route-target
- BGP route dampening does not work on the backup Routing Engine when nonstop active routing is enabled.

### Nonstop Active Routing Layer 2 Circuit and VPLS Support

Nonstop active routing supports Layer 2 circuit and VPLS on both LDP-based and RSVP-TE-based networks. Nonstop active routing support enables the backup Routing Engine to track the label advertised by Layer 2 circuit and VPLS on the primary Routing Engine, and to use the same label after the Routing Engine switchover.

in Junos OS Release 9.6 and later, nonstop active routing support is extended to the Layer 2 circuit and LDP-based VPLS pseudowire redundant configurations.

### Nonstop Active Routing PIM Support

Nonstop active routing supports Protocol Independent Multicast (PIM) with stateful replication on backup Routing Engines. State information replicated on the backup Routing Engine includes information about neighbor relationships, join and prune events, rendezvous point (RP) sets, synchronization between routes and next hops, multicast session states, and the forwarding state between the two Routing Engines.

**NOTE:** Nonstop active routing for PIM is supported for IPv4 on Junos OS Release 9.3 and later, and for IPv6 on Junos OS Release 10.4 and later. Starting with Release 11.1, Junos OS also supports nonstop active routing for PIM on devices that have both IPv4 and IPv6 configured on them.

To configure nonstop active routing for PIM, include the same statements in the configuration as for other protocols: the `nonstop-routing` statement at the `[edit routing-options]` hierarchy level and the `graceful-switchover` statement at the `[edit chassis redundancy]` hierarchy level. To trace PIM nonstop active routing events, include the `flag nsr-synchronization` statement at the `[edit protocols pim traceoptions]` hierarchy level.

**NOTE:** The `clear pim join`, `clear pim register`, and `clear pim statistics operational mode` commands are not supported on the backup Routing Engine when nonstop active routing is enabled.

Nonstop active routing support varies for different PIM features. The features fall into the following three categories: supported features, unsupported features, and incompatible features.

#### Supported features:

- Auto-RP

**NOTE:** Nonstop active routing PIM support on IPv6 does not support auto-RP because IPv6 does not support auto-RP.

- Bootstrap router (BSR)
- Static RPs
- Embedded RP on non-RP IPv6 routers

- Local RP

**NOTE:** RP set information synchronization is supported for local RP and BSR (on IPv4 and IPv6), autoRP (on IPv4), and embedded RP (on IPv6).

- BFD
- Dense mode
- Sparse mode
- Source-specific multicast (SSM)
- Draft Rosen multicast VPNs (MVPNs)
- Anycast RP (anycast RP set information synchronization and anycast RP register state synchronization on IPv4 and IPv6 configurations)
- Flow maps
- Unified ISSU
- Policy features such as neighbor policy, bootstrap router export and import policies, scope policy, flow maps, and reverse path forwarding (RPF) check policies
- Upstream assert synchronization
- PIM join load balancing

Starting with Release 12.2, Junos OS extends the nonstop active routing PIM support to draft Rosen MVPNs. Nonstop active routing PIM support for draft Rosen MVPNs enables nonstop active routing-enabled devices to preserve draft Rosen MPVN-related information—such as default and data multicast distribution tree (MDT) states—across switchovers. In releases earlier than 12.2, nonstop active routing PIM configuration was incompatible with draft Rosen MVPN configuration.

The backup Routing Engine sets up the default MDT based on the configuration and the information it receives from the primary Routing Engine, and keeps updating the default MDT state information.

However, for data MDTs, the backup Routing Engine relies on the primary Routing Engine to provide updates when data MDTs are created, updated, or deleted. The backup Routing Engine neither monitors data MDT flow rates nor triggers a data MDT switchover based on variations in flow rates. Similarly, the backup Routing Engine does not maintain the data MDT delay timer or timeout timer. It does not send MDT join TLV packets for the data MDTs until it takes over as the primary Routing Engine. After the switchover, the new primary Routing Engine starts sending MDT join TLV packets for each data MDT, and also resets the data MDT timers. Note that the expiration time for the timers might vary from the original values on the previous primary Routing Engine.

Starting with Release 12.3, Junos OS extends the Protocol Independent Multicast (PIM) nonstop active routing support to IGMP-only interfaces.

In Junos OS releases earlier than 12.3, the PIM joins created on IGMP-only interfaces were not replicated on the backup Routing Engine. Thus, the corresponding multicast routes were marked as pruned (meaning discarded) on the backup Routing Engine. Because of this limitation, after a switchover, the new primary Routing Engine had to wait for the IGMP module to come up and start receiving reports to create PIM joins and to install multicast routes. This caused traffic loss until the multicast joins and routes were reinstated.

However, in Junos OS Release 12.3 and later, the multicast joins on the IGMP-only interfaces are mapped to PIM states, and these states are replicated on the backup Routing Engine. If the corresponding PIM states are available on the backup, the multicast routes are marked as forwarding on the backup Routing Engine. This enables uninterrupted traffic flow after a switchover. This enhancement covers IGMPv2, IGMPv3, MLDv1, and MLDv2 reports and leaves.

**Unsupported features:** You can configure the following PIM features on a router along with nonstop active routing, but they function as if nonstop active routing is not enabled. In other words, during Routing Engine switchover and other outages, their state information is not preserved, and traffic loss is to be expected.

- Internet Group Management Protocol (IGMP) exclude mode
- IGMP snooping

Nonstop active routing is not supported for next-generation MVPNs with PIM provider tunnels. The commit operation fails if the configuration includes both nonstop active routing and next-generation MVPNs with PIM provider tunnels.

Junos OS provides a configuration statement that disables nonstop active routing for PIM only, so that you can activate incompatible PIM features and continue to use nonstop active routing for the other protocols on the router. Before activating an incompatible PIM feature, include the `nonstop-routing disable` statement at the `[edit protocols pim]` hierarchy level. Note that in this case, nonstop active routing is disabled for all PIM features, not just incompatible features.

### Nonstop Active Routing MSDP Support

Starting with Release 12.1, Junos OS extends nonstop active routing support to the Multicast Source Discovery Protocol (MSDP).

Nonstop active routing support for MSDP preserves the following MSDP-related information across the switchover:

- MSDP configuration and peer information
- MSDP peer socket information

- Source-active and related information

However, note that the following restrictions or limitations apply to nonstop active routing MSDP support:

- Because the backup Routing Engine learns the active source information by processing the source-active messages from the network, synchronizing of source active information between the primary and backup Routing Engines might take up to 60 seconds. So, no planned switchover is allowed within 60 seconds of the initial replication of the sockets.
- Similarly, Junos OS does not support two planned switchovers within 240 seconds of each other.

Junos OS enables you to trace MSDP nonstop active routing events by including the flag `nsr-synchronization` statement at the `[edit protocols mdp traceoptions]` hierarchy level.

### Nonstop Active Routing Support for RSVP-TE LSPs

Junos OS extends nonstop active routing support to label-switching routers (LSRs) and Layer 2 Circuits that are part of an RSVP-TE LSP. Nonstop active routing support on LSRs ensures that the primary to backup Routing Engine switchover on an LSR remains transparent to the network neighbors and that the LSP information remains unaltered during and after the switchover.

You can use the `show rsvp version` command to view the nonstop active routing mode and state on an LSR. Similarly, you can use the `show mpls lsp` and `show rsvp session` commands on the backup Routing Engine to view the state recreated on the backup Routing Engine.

The Junos OS nonstop active routing feature is also supported on RSVP point-to-multipoint LSPs. Nonstop active routing support for RSVP point-to-multipoint egress and transit LSPs was added in Junos OS Release 11.4, and for ingress LSPs in Release 12.1. During the switchover, the LSP comes up on the backup Routing Engine that shares and synchronizes the state information with the primary Routing Engine before and after the switchover. Nonstop active routing support for point-to-multipoint transit and egress LSPs ensures that the switchover remains transparent to the network neighbors, and preserves the LSP information across the switchover.

Starting with Release 14.1R1, Junos OS extends nonstop active routing support to the next-generation multicast VPNs (MVPNs).

The `show rsvp session detail` command enables you to check the point-to-multipoint LSP remerge state information (P2MP LSP re-merge; possible values are `head`, `member`, and `none`).

Starting with Release 14.1R1, Junos OS extends nonstop active routing support for point-to-multipoint LSPs used by VPLS and MVPN.

However, Junos OS does not support nonstop active routing for the following features:

- Generalized Multiprotocol Label Switching (GMPLS) and LSP hierarchy



- Interdomain or loose-hop expansion LSPs
- BFD liveness detection
- Starting with Junos OS Release 14.2, Setup protection

Nonstop active routing support for RSVP-TE LSPs is subject to the following limitations and restrictions:

- Detour LSPs are not maintained across a switchover and so, detour LSPs might fail to come back online after the switchover.
- Control plane statistics corresponding to the `show rsvp statistics` and `show rsvp interface detail | extensive` commands are not maintained across Routing Engine switchovers.
- Statistics from the backup Routing Engine are not reported for `show mpls lsp statistics` and `monitor mpls label-switched-path` commands. However, if a switchover occurs, the backup Routing Engine, after taking over as the primary, starts reporting statistics. Note that the `clear statistics` command issued on the old primary Routing Engine does not have any effect on the new primary Routing Engine, which reports statistics, including any uncleared statistics.
- State timeouts might take additional time during nonstop active routing switchover. For example, if a switchover occurs after a neighbor has missed sending two hello messages to the primary, the new primary Routing Engine waits for another three hello periods before timing out the neighbor.
- On the RSVP ingress router, if you configure auto-bandwidth functionality, the bandwidth adjustment timers are set in the new primary after the switchover. This causes a one-time increase in the length of time required for the bandwidth adjustment after the switchover occurs.
- Backup LSPs —LSPs that are established between the point of local repair (PLR) and the merge point after a node or link failure—are not preserved during a Routing Engine switchover.
- When nonstop active routing is enabled, graceful restart is not supported. However, graceful restart helper mode is supported.

## SEE ALSO

Nonstop Active Routing Concepts

[Configuring Nonstop Active Routing | 281](#)

Configuring Nonstop Active Routing on Switches

Example: Configuring Nonstop Active Routing on Switches

### Release History Table

Release	Description
15.1R1	Starting with Junos OS Release 15.1R1, if you have NSR configured, it is never valid to issue the restart routing command in any form on the NSR primary Routing Engine.
14.2	Starting with Junos OS Release 14.2, Setup protection
14.1	Starting with Junos OS Release 14.1, you must include the <a href="#">advertise-from-main-vpn-tables</a> statement at the [edit protocols bgp] hierarchy level to prevent BGP sessions from going down when route reflector (RR) or autonomous system border router (ASBR) functionality is enabled or disabled on a routing device that has VPN address families configured.
14.1	Starting with Release 14.1R1, Junos OS extends nonstop active routing support to the next-generation multicast VPNs (MVPNs).
14.1	Starting with Release 14.1R1, Junos OS extends nonstop active routing support for point-to-multipoint LSPs used by VPLS and MVPN.
13.3R5	Starting with Junos OS Release 13.3R5, on EX9214 switches, the VRRP primary state might change during graceful Routing Engine switchover, even when nonstop active routing is enabled.
12.3	Starting with Junos OS Release 12.3, because of its synchronization requirements and logic, NSR or GRES performance is limited by the slowest Routing Engine in the system.

# Configuring Nonstop Active Routing

## IN THIS CHAPTER

- [Configuring Nonstop Active Routing | 281](#)

## Configuring Nonstop Active Routing

### SUMMARY

Configure nonstop active routing on your device with the following steps and examples.

### IN THIS SECTION

- [Enabling Nonstop Active Routing | 282](#)
- [Synchronizing the Routing Engine Configuration | 283](#)
- [Verifying Nonstop Active Routing Operation | 283](#)
- [Configuring Nonstop Active Routing on Switches | 284](#)
- [Preventing Automatic Reestablishment of BGP Peer Sessions After NSR Switchovers | 285](#)
- [Example: Configuring Nonstop Active Routing | 286](#)
- [Resetting Local Statistics | 289](#)
- [Example: Configuring Nonstop Active Routing on Switches | 290](#)

## Enabling Nonstop Active Routing

Nonstop active routing (NSR) requires you to configure graceful Routing Engine switchover (GRES). To enable graceful Routing Engine switchover, include the `graceful-switchover` statement at the `[edit chassis redundancy]` hierarchy level:

```
[edit chassis redundancy]
graceful-switchover;
```

By default, nonstop active routing is disabled. To enable nonstop active routing, include the `nonstop-routing` statement at the `[edit routing-options]` hierarchy level:

```
[edit routing-options]
nonstop-routing;
```

To disable nonstop active routing, remove the `nonstop-routing` statement from the `[edit routing-options]` hierarchy level.

**NOTE:** When you enable nonstop active routing, you cannot enable automatic route distinguishers for multicast VPN routing instances. Automatic route distinguishers are enabled by configuring the `route-distinguisher-id` statement at the `[edit routing-instances instance-name]` hierarchy level; for more information, see the [Junos OS VPNs Library for Routing Devices](#).

If the routing protocol process (rpd) on the NSR primary Routing Engine crashes, the primary Routing Engine simply restarts rpd (with no Routing Engine switchover), which impacts routing protocol adjacencies and neighbors and results in traffic loss. To prevent this negative impact on traffic flow, configure the `switchover-on-routing-crash` statement at the `[edit system]` hierarchy level. This configuration forces an NSR Routing Engine switchover if rpd on the primary Routing Engine crashes.

```
[edit system]
user@host# set switchover-on-routing-crash
```

To enable the routing platform to switch over to the backup Routing Engine when the routing protocol process (rpd) fails rapidly three times in succession, include the `other-routing-engine` statement at the `[edit system processes routing failover]` hierarchy level.

For more information about the `other-routing-engine` statement, see the [Junos OS Administration Library for Routing Devices](#).

## Synchronizing the Routing Engine Configuration

When you configure nonstop active routing, you must also include the `commit synchronize` statement at the `[edit system]` hierarchy level so that configuration changes are synchronized on both Routing Engines:

```
[edit system]commit synchronize;
```

If you try to commit the nonstop active routing configuration without including the `commit synchronize` statement, the commit fails.

If you configure the `commit synchronize` statement at the `[edit system]` hierarchy level and issue a commit in the primary Routing Engine, the primary configuration is automatically synchronized with the backup.

However, if the backup Routing Engine is down when you issue the commit, the Junos OS displays a warning and commits the candidate configuration in the primary Routing Engine. When the backup Routing Engine comes up, its configuration will automatically be synchronized with the primary.

**NOTE:** A newly inserted backup Routing Engine automatically synchronizes its configuration with the primary Routing Engine configuration.

When you configure nonstop active routing, you can bring the backup Routing Engine online after the primary Routing Engine is already running. There is no requirement to start the two Routing Engines simultaneously.



**CAUTION:** We recommend that you do not restart Routing Protocol Process (rpd) on primary Routing Engine after enabling nonstop active routing, as it disrupts the protocol adjacency/peering sessions, resulting in traffic loss.

## Verifying Nonstop Active Routing Operation

To see whether or not nonstop active routing is enabled, issue the `show task replication` command. For BGP nonstop active routing, you must also issue the `show bgp replication` command.



**CAUTION:** If BGP is configured, before attempting nonstop active routing switchover, check the output of `show bgp replication` to confirm that BGP routing table synchronization has completed on the backup Routing Engine. The complete status in the output of `show task replication` only indicates that the socket replication has completed and the BGP synchronization is in progress. To determine whether BGP synchronization is complete, you must check the `Protocol state` and `Synchronization state` fields in the output of `show bgp replication` on the primary Routing Engine. The `Protocol state` must be

idle and the Synchronization state must be complete. If you perform NSR switchover before the BGP synchronization has completed, the BGP session might flap.

For more information about these commands, see the [CLI Explorer](#).

When you enable nonstop active routing or graceful Routing Engine switchover and issue routing-related operational mode commands on the backup Routing Engine (such as `show route`, `show bgp neighbor`, `show ospf database`, and so on), the output might not match the output of the same commands issued on the primary Routing Engine. For example, it is normal for the routing table on the backup Routing Engine to contain persistent phantom routes that are not present in the routing table on the primary Routing Engine.

To display BFD state replication status, issue the `show bfd session` command. The replicated flag appears in the output for this command when a BFD session has been replicated to the backup Routing Engine. For more information, see the [CLI Explorer](#).

## Configuring Nonstop Active Routing on Switches

Nonstop active routing (NSR) provides a mechanism for transparent switchover of the Routing Engines without necessitating restart of supported routing protocols. Both Routing Engines are fully active in processing protocol sessions, and so each can take over for the other. The switchover is transparent to neighbors.

You can configure NSR on an on a Juniper Networks EX Series switch with multiple Routing Engines or an EX Series or QFX Series switch in a Virtual Chassis or Virtual Chassis Fabric configuration.

To configure nonstop active routing:

1. Enable graceful Routing Engine switchover (GRES):

```
[edit chassis redundancy]
user@switch# set graceful-switchover
```

2. Enable nonstop active routing (by default, nonstop active routing is disabled):

```
[edit routing-options]
user@switch# set nonstop-routing
```

3. Synchronize configuration changes between the Routing Engines:

```
[edit system]
user@switch# set commit synchronize
```

If you try to commit the nonstop active routing configuration without including the `commit synchronize` statement, the commit fails.

4.

**NOTE:** There is no requirement to start the two Routing Engines simultaneously. If the backup Routing Engine is not up when you issue the `commit synchronize` command, the candidate configuration is committed in the primary Routing Engine. When the backup Routing Engine is inserted or comes online, its configuration is automatically synchronized with that of the primary.

**BEST PRACTICE:** After a graceful Routing Engine switchover, we recommend that you issue the `clear interface statistics (interface-name | all)` command to reset the cumulative values for local statistics on the new primary Routing Engine.

To disable nonstop active routing:

```
[edit routing-options]
user@switch# delete nonstop-routing
```

## SEE ALSO

Example: Configuring Nonstop Active Routing on Switches

[Tracing Nonstop Active Routing Synchronization Events | 1562](#)

Understanding Nonstop Active Routing on EX Series Switches

Nonstop Active Routing Concepts

## Preventing Automatic Reestablishment of BGP Peer Sessions After NSR Switchovers

It is useful to prevent a BGP peer session from automatically being reestablished after a nonstop active routing (NSR) switchover when you have applied routing policies configured in the dynamic database. When NSR is enabled, the dynamic database is not synchronized with the backup Routing Engine. Therefore, when a switchover occurs, import and export policies configured in the dynamic database might no longer be available. For more information about configuring dynamic routing policies, see the [Routing Policies, Firewall Filters, and Traffic Policers User Guide](#).

**NOTE:** The BGP established timers are not maintained across switchovers.

You can configure the routing device not to reestablish a BGP peer session after an NSR switchover either for a specified period or until you manually reestablish the session. Include the `idle-after-switch-over` statement at the `[edit protocols bgp]` hierarchy level:

```
idle-after-switch-over (forever | seconds);
```

For a list of hierarchy levels at which you can configure this statement, see the configuration statement summary for this statement.

For **seconds**, specify a value from 1 through 4294967295. The BGP peer session is not reestablished until after the specified period. If you specify the **forever** option, the BGP peer session is not reestablished until you issue the `clear bgp neighbor` command.

### Example: Configuring Nonstop Active Routing

The following example enables graceful Routing Engine switchover, nonstop active routing, and nonstop active routing trace options for BGP, IS-IS, and OSPF.

```
[edit]
system commit {
    synchronize;
}
chassis {
    redundancy {
        graceful-switchover; # This enables graceful Routing Engine switchover on
# the routing platform.
    }
}
interfaces {
    so-0/0/0 {
        unit 0 {
            family inet {
                address 10.0.1.1/30;
            }
            family iso;
        }
    }
    so-0/0/1 {
```



```

    unit 0 {
        family inet {
            address 10.1.1.1/30;
        }
        family iso;
    }
}
so-0/0/2 {
    unit 0 {
        family inet {
            address 10.2.1.1/30;
        }
        family iso;
    }
}
so-0/0/3 {
    unit 0 {
        family inet {
            address 10.3.1.1/30;
        }
        family iso;
    }
}
lo0 {
    unit 0 {
        family inet {
            address 192.168.2.1/32;
        }
        family iso {
            address 49.0004.1921.6800.2001.00;
        }
    }
}
}
routing-options {
    nonstop-routing; # This enables nonstop active routing on the routing platform.
    router-id 192.168.2.1;
    autonomous-system 65432;
}
protocols {
    bgp {
        traceoptions {
            flag nsr-synchronization detail; # This logs nonstop active routing

```

```

# events for BGP.
}
advertise-from-main-vpn-tables;
local-address 192.168.2.1;
group external-group {
    type external;
    export BGP_export;
    neighbor 192.168.1.1 {
        family inet {
            unicast;
        }
        peer-as 65103;
    }
}
group internal-group {
    type internal;
    neighbor 192.168.10.1;
    neighbor 192.168.11.1;
    neighbor 192.168.12.1;
}
}
isis {
    traceoptions {
        flag nsr-synchronization detail; # This logs nonstop active routing events
# for IS-IS.
    }
    interface all;
    interface fxp0.0 {
        disable;
    }
    interface lo0.0 {
        passive;
    }
}
ospf {
    traceoptions {
        flag nsr-synchronization detail; # This logs nonstop active routing events
# for OSPF.
    }
    area 0.0.0.0 {
        interface all;
        interface fxp0.0 {
            disable;

```

```

    }
    interface lo0.0 {
        passive;
    }
}
}
}
policy-options {
    policy-statement BGP_export {
        term direct {
            from {
                protocol direct;
            }
            then accept;
        }
        term final {
            then reject;
        }
    }
}
}

```

## SEE ALSO

[Configuring Nonstop Active Routing | 281](#)

[Tracing Nonstop Active Routing Synchronization Events | 1562](#)

## Resetting Local Statistics

After a graceful Routing Engine switchover, we recommend that you issue the `clear interface statistics` (*interface-name* | all) command to reset the cumulative values for local statistics on the new primary Routing Engine.

## SEE ALSO

[Configuring Nonstop Active Routing | 281](#)

[Tracing Nonstop Active Routing Synchronization Events | 1562](#)

## Example: Configuring Nonstop Active Routing on Switches

### IN THIS SECTION

- [Requirements | 290](#)
- [Overview and Topology | 290](#)
- [Configuration | 291](#)
- [Verification | 292](#)
- [Troubleshooting | 294](#)

Nonstop active routing (NSR) provides high availability for Routing Engines by enabling transparent switchover of the Routing Engines without necessitating restart of supported routing protocols. Both Routing Engines are fully active in processing protocol sessions, and so each can take over for the other. The switchover is transparent to neighbors.

This example describes how to configure nonstop active routing on switches with multiple Routing Engines or on an EX Series or a QFX series switch in a Virtual Chassis or Virtual Chassis Fabric configuration.

### Requirements

This example uses the following hardware and software components:

- An EX Series with multiple Routing Engines or on an EX Series or a QFX series switch in a Virtual Chassis or Virtual Chassis Fabric configuration
- Junos OS Release 10.4 or later for EX Series switches
- Junos OS Release 13.2X51-D20 or later for QFX Series switches

### Overview and Topology

Configure nonstop active routing on any EX Series with multiple Routing Engines or on an EX Series or a QFX series switch in a Virtual Chassis or Virtual Chassis Fabric configuration. Nonstop active routing is advantageous in networks where neighbor routing devices do not support graceful restart protocol extensions.

The topology used in this example consists of an EX8200 switch with redundant Routing Engines connected to neighbor routing devices that are not configured to support graceful restart of protocols.

## Configuration

### IN THIS SECTION

- [CLI Quick Configuration | 291](#)
- [Procedure | 291](#)
- [Results | 292](#)

### *CLI Quick Configuration*

To quickly configure nonstop active routing, copy the following commands and paste them into the switch terminal window:

```
[edit]  
set chassis redundancy graceful-switchover  
set routing-options nonstop-routing  
set system commit synchronize
```

### *Procedure*

#### Step-by-Step Procedure

To configure nonstop active routing on a switch:

1. Enable graceful Routing Engine switchover (GRES):

```
[edit chassis redundancy]  
user@switch# set graceful-switchover
```

2. Enable nonstop active routing (by default, nonstop active routing is disabled):

```
[edit routing-options]  
user@switch# set nonstop-routing
```

### 3. Synchronize configuration changes between the Routing Engines:

```
[edit system]
user@switch# set commit synchronize
```

If you try to commit the nonstop active routing configuration without including the `commit synchronize` statement, the commit fails.

**NOTE:** If the backup Routing Engine is down when you issue the commit, a warning is displayed and the candidate configuration is committed in the primary Routing Engine. When the backup Routing Engine comes up, its configuration is automatically synchronized with that of the primary. If you subsequently insert or bring up a backup Routing Engine, it automatically synchronizes its configuration with the primary Routing Engine configuration.

### Results

Check the results of the configuration:

```
[edit]
user@switch# show
chassis {
  redundancy {
    graceful-switchover;
  }
}
routing-options {
  nonstop-routing;
}
system {
  commit synchronize;
}
```

### Verification

#### IN THIS SECTION

- [Verifying That Nonstop Active Routing Is Working Correctly on the Switch | 293](#)

To confirm that the configuration is working properly, perform these tasks:

### *Verifying That Nonstop Active Routing Is Working Correctly on the Switch*

#### **Purpose**

Verify that nonstop active routing is enabled.

#### **Action**

Issue the `show task replication` command:

```
user@switch# show task replication
Stateful Replication: Enabled
RE mode: Master

Protocol           Synchronization Status
OSPF                Complete
RIP                 Complete
PIM                 Complete
RSVP                Complete
```

#### **Meaning**

This output shows that nonstop active routing (Stateful Replication) is enabled on primary routing engine. If nonstop routing is not enabled, instead of the output shown above:

- On the backup routing engine the following error message is displayed: “error: the routing subsystem is not running.”
- On the primary routing engine, the following output is displayed if nonstop routing is not enabled:

```
Stateful Replication: Disabled
RE mode: Master
```

Troubleshooting

IN THIS SECTION

- [Investigating Problems with Synchronization of Routing Engines When NSR Is Enabled | 294](#)

To troubleshoot nonstop active routing, perform these tasks:

*Investigating Problems with Synchronization of Routing Engines When NSR Is Enabled*

**Problem**

A protocol loses connectivity with neighbors after a graceful Routing Engine switchover (GRES) occurs with nonstop active routing (NSR) enabled.

**Solution**

Use trace options to help isolate the problem and gather troubleshooting information. Using the information gathered from trace options, you can confirm or eliminate the synchronization of the Routing Engines as the cause of the loss of connectivity for the protocol. See "[Tracing Nonstop Active Routing Synchronization Events](#)" on page 1562.

**SEE ALSO**

Configuring Nonstop Active Routing on Switches
<a href="#">Tracing Nonstop Active Routing Synchronization Events   1562</a>
Understanding Nonstop Active Routing on EX Series Switches
Nonstop Active Routing Concepts

**RELATED DOCUMENTATION**

Nonstop Active Routing Concepts
Nonstop Active Routing System Requirements
<a href="#">Tracing Nonstop Active Routing Synchronization Events   1562</a>
Resetting Local Statistics



Example: Configuring Nonstop Active Routing

---

[nonstop-routing](#) | **1064**

# 10

PART

## Configuring Graceful Restart

---

Understanding How Graceful Restart Enables Uninterrupted Packet Forwarding  
When a Router is Restarted | 297

Configuring Graceful Restart | 307

---

# Understanding How Graceful Restart Enables Uninterrupted Packet Forwarding When a Router is Restarted

## IN THIS CHAPTER

- [Understanding Graceful Restart | 297](#)

## Understanding Graceful Restart

### SUMMARY

Graceful restart allows for uninterrupted packet forwarding and temporary suppression of all routing protocol updates during the restart process.

### IN THIS SECTION

- [Graceful Restart Concepts | 298](#)
- [Graceful Restart for Aggregate and Static Routes | 299](#)
- [Graceful Restart and Routing Protocols | 299](#)
- [Graceful Restart and MPLS-Related Protocols | 302](#)
- [Understanding Restart Signaling-Based Helper Mode Support for OSPF Graceful Restart | 303](#)
- [Graceful Restart and Layer 2 and Layer 3 VPNs | 304](#)
- [Graceful Restart on Logical Systems | 305](#)
- [Graceful Restart System Requirements | 306](#)

# Graceful Restart Concepts

With routing protocols, any service interruption requires that an affected router recalculate adjacencies with neighboring routers, restore routing table entries, and update other protocol-specific information. An unprotected restart of a router can result in forwarding delays, route flapping, wait times stemming from protocol reconvergence, and even dropped packets. The main benefits of graceful restart are uninterrupted packet forwarding and temporary suppression of all routing protocol updates. Graceful restart enables a router to pass through intermediate convergence states that are hidden from the rest of the network.

Three main types of graceful restart are available on Juniper Networks routing platforms:

- Graceful restart for aggregate and static routes and for routing protocols—Provides protection for aggregate and static routes and for Border Gateway Protocol (BGP), End System-to-Intermediate System (ES-IS), Intermediate System-to-Intermediate System (IS-IS), Open Shortest Path First (OSPF), Routing Information Protocol (RIP), next-generation RIP (RIPng), and Protocol Independent Multicast (PIM) sparse mode routing protocols.
- Graceful restart for MPLS-related protocols—Provides protection for Label Distribution Protocol (LDP), Resource Reservation Protocol (RSVP), circuit cross-connect (CCC), and translational cross-connect (TCC). (Not supported on OCX Series switches.)
- Graceful restart for virtual private networks (VPNs)—Provides protection for Layer 2 and Layer 3 VPNs.

Graceful restart works similarly for routing protocols and MPLS protocols and combines components of these protocol types to enable graceful restart in VPNs. The main benefits of graceful restart are uninterrupted packet forwarding and temporary suppression of all routing protocol updates. Graceful restart thus enables a router to pass through intermediate convergence states that are hidden from the rest of the network.

Most graceful restart implementations define two types of routers—the restarting router and the helper router. The restarting router requires rapid restoration of forwarding state information so it can resume the forwarding of network traffic. The helper router assists the restarting router in this process. Graceful restart configuration statements typically affect either the restarting router or the helper router.

## SEE ALSO

[Understanding High Availability Features on Juniper Networks Routers | 2](#)

Graceful Restart System Requirements

Graceful Restart for Aggregate and Static Routes

Graceful Restart and Routing Protocols

Graceful Restart and MPLS-Related Protocols

Graceful Restart and Layer 2 and Layer 3 VPNs
Graceful Restart on Logical Systems
Configuring Graceful Restart
Configuring Graceful Restart for QFabric Systems

## Graceful Restart for Aggregate and Static Routes

When you include the `graceful-restart` statement at the `[edit routing-options]` hierarchy level, any static routes or aggregated routes that have been configured are protected. Because no helper router assists in the restart, these routes are retained in the forwarding table while the router restarts (rather than being discarded or refreshed).

### SEE ALSO

Graceful Restart Concepts
Graceful Restart System Requirements
Enabling Graceful Restart
Verifying Graceful Restart Operation
Configuring Graceful Restart

## Graceful Restart and Routing Protocols

### IN THIS SECTION

- [BGP | 299](#)
- [IS-IS | 300](#)
- [OSPF and OSPFv3 | 300](#)
- [PIM Sparse Mode | 301](#)
- [RIP and RIPng | 301](#)

This section covers the following topics:

### BGP

When a router enabled for BGP graceful restart restarts, it retains BGP peer routes in its forwarding table and marks them as stale. However, it continues to forward traffic to other peers (or receiving

peers) during the restart. To reestablish sessions, the restarting router sets the “restart state” bit in the BGP OPEN message and sends it to all participating peers. The receiving peers reply to the restarting router with messages containing end-of-routing-table markers. When the restarting router or switch receives all replies from the receiving peers, the restarting router performs route selection, the forwarding table is updated, and the routes previously marked as stale are discarded. At this point, all BGP sessions are reestablished and the restarting peer can receive and process BGP messages as usual.

While the restarting router does its processing, the receiving peers also temporarily retain routing information. When a receiving peer detects a TCP transport reset, it retains the routes received and marks the routes as stale. After the session is reestablished with the restarting router or switch, the stale routes are replaced with updated route information.

## IS-IS

Normally, IS-IS routers move neighbor adjacencies to the down state when changes occur. However, a router enabled for IS-IS graceful restart sends out Hello messages with the Restart Request (RR) bit set in a restart type length value (TLV) message. This indicates to neighboring routers that a graceful restart is in progress and to leave the IS-IS adjacency intact. The neighboring routers must interpret and implement restart signaling themselves. Besides maintaining the adjacency, the neighbors send complete sequence number PDUs (CSNPs) to the restarting router and flood their entire database.

The restarting router never floods any of its own link-state PDUs (LSPs), including pseudonode LSPs, to IS-IS neighbors while undergoing graceful restart. This enables neighbors to reestablish their adjacencies without transitioning to the down state and enables the restarting router to reinitiate a smooth database synchronization.

## OSPF and OSPFv3

When a router enabled for OSPF graceful restart restarts, it retains routes learned before the restart in its forwarding table. The router does not allow new OSPF link-state advertisements (LSAs) to update the routing table. This router continues to forward traffic to other OSPF neighbors (or helper routers), and sends only a limited number of LSAs during the restart period. To reestablish OSPF adjacencies with neighbors, the restarting router must send a grace LSA to all neighbors. In response, the helper routers enter helper mode and send an acknowledgement back to the restarting router. If there are no topology changes, the helper routers continue to advertise LSAs as if the restarting router had remained in continuous OSPF operation.

When the restarting router receives replies from all the helper routers, the restarting router selects routes, updates the forwarding table, and discards the old routes. At this point, full OSPF adjacencies are reestablished and the restarting router receives and processes OSPF LSAs as usual. When the helper routers no longer receive grace LSAs from the restarting router or the topology of the network changes, the helper routers also resume normal operation.

**NOTE:** For more information about the standard helper mode implementation, see RFC 3623, *Graceful OSPF Restart*.

Starting with Release 11.3, Junos OS supports the restart signaling-based helper mode for OSPF graceful restart configurations. The helper modes, both standard and restart signaling-based, are enabled by default. In restart signaling-based helper mode implementations, the restarting router relays the restart status to its neighbors only after the restart is complete. When the restart is complete, the restarting router sends hello messages to its helper routers with the **restart signal (RS)** bit set in the hello packet header. When a helper router receives a hello packet with the **RS** bit set in the header, the helper router returns a hello message to the restarting router. The reply hello message from the helper router contains the **ResyncState** flag and the **ResyncTimeout** timer that enable the restarting router to keep track of the helper routers that are syncing up with it. When all helpers complete the synchronization, the restarting router exits the restart mode.

**NOTE:**

For more information about restart signaling-based graceful restart helper mode implementation, see RFC 4811, *OSPF Out-of-Band Link State Database (LSDB) Resynchronization*, RFC 4812, *OSPF Restart Signaling*, and RFC 4813, *OSPF Link-Local Signaling*.

Restart signaling-based graceful restart helper mode is not supported for OSPFv3 configurations.

## PIM Sparse Mode

PIM sparse mode uses a mechanism called a *generation identifier* to indicate the need for graceful restart. Generation identifiers are included by default in PIM hello messages. An initial generation identifier is created by each PIM neighbor to establish device capabilities. When one of the PIM neighbors restarts, it sends a new generation identifier to its neighbors. All neighbors that support graceful restart and are connected by point-to-point links assist by sending multicast updates to the restarting neighbor.

The restart phase completes when either the PIM state becomes stable or when the restart interval timer expires. If the neighbors do not support graceful restart or connect to each other using multipoint interfaces, the restarting router uses the restart interval timer to define the restart period.

## RIP and RIPng

When a router enabled for RIP graceful restart restarts, routes that have been configured are protected. Because no helper router assists in the restart, these routes are retained in the forwarding table while the router restarts (rather than being discarded or refreshed).

## SEE ALSO

Graceful Restart Concepts
Graceful Restart System Requirements
<a href="#">Configuring Graceful Restart for Routing Protocols   359</a>
Verifying Graceful Restart Operation
Configuring Graceful Restart
Example: Configuring IS-IS for GRES with Graceful Restart

## Graceful Restart and MPLS-Related Protocols

### IN THIS SECTION

- [LDP | 302](#)
- [RSVP | 303](#)
- [CCC and TCC | 303](#)

This section contains the following topics:

### LDP

LDP graceful restart enables a router whose LDP control plane is undergoing a restart to continue to forward traffic while recovering its state from neighboring routers. It also enables a router on which helper mode is enabled to assist a neighboring router that is attempting to restart LDP.

During session initialization, a router advertises its ability to perform LDP graceful restart or to take advantage of a neighbor performing LDP graceful restart by sending the graceful restart TLV. This TLV contains two fields relevant to LDP graceful restart: the reconnect time and the recovery time. The values of the reconnect and recovery times indicate the graceful restart capabilities supported by the router.

The default reconnect time is configured in Junos OS as 60 seconds and is user-configurable. The reconnect time is how long the helper router waits for the restarting router to establish a connection. If the connection is not established within the reconnect interval, graceful restart for the LDP session is terminated. The default maximum reconnect time is 120 seconds and is user-configurable. The maximum reconnect time is the maximum value that a helper router accepts from its restarting neighbor.

When a router discovers that a neighboring router is restarting, it waits until the end of the recovery time before attempting to reconnect. The recovery time is the length of time a router waits for LDP to



restart gracefully. The recovery time period begins when an initialization message is sent or received. This time period is also typically the length of time that a neighboring router maintains its information about the restarting router, so it can continue to forward traffic.

You can configure LDP graceful restart both in the master instance for the LDP protocol and for a specific routing instance. You can disable graceful restart at the global level for all protocols, at the protocol level for LDP only, and for a specific routing instance only.

## RSVP

RSVP graceful restart enables a router undergoing a restart to inform its adjacent neighbors of its condition. The restarting router requests a grace period from the neighbor or peer, which can then cooperate with the restarting router. The restarting router can still forward MPLS traffic during the restart period; convergence in the network is not disrupted. The restart is not visible to the rest of the network, and the restarting router is not removed from the network topology. RSVP graceful restart can be enabled on both transit routers and ingress routers. It is available for both point-to-point LSPs and point-to-multipoint LSPs.

## CCC and TCC

CCC and TCC graceful restart enables Layer 2 connections between customer edge (CE) routers to restart gracefully. These Layer 2 connections are configured with the **remote-interface-switch** or `lsp-switch` statements. Because these CCC and TCC connections have an implicit dependency on RSVP LSPs, graceful restart for CCC and TCC uses the RSVP graceful restart capabilities.

RSVP graceful restart must be enabled on the provider edge (PE) routers and provider (P) routers to enable graceful restart for CCC and TCC. Also, because RSVP is used as the signaling protocol for signaling label information, the neighboring router must use helper mode to assist with the RSVP restart procedures.

## SEE ALSO

[Graceful Restart Concepts](#)

[Graceful Restart System Requirements](#)

[Configuring Graceful Restart for MPLS-Related Protocols](#)

[Configuring Graceful Restart](#)

## Understanding Restart Signaling-Based Helper Mode Support for OSPF Graceful Restart

Starting with Release 11.4, Junos OS supports restart signaling-based helper mode for OSPF graceful restart configurations.

**NOTE:**

- Restart signaling-based graceful restart helper mode is not supported for OSPFv3 configurations.
- Junos OS releases prior to Release 11.4 and OSPFv3 configurations support only standard helper mode as defined in RFC 3623 . For more information about the standard helper mode implementation, see RFC 3623 and the *Junos OS High Availability Configuration Guide*.

Both standard and restart signaling-based helper modes are enabled by default, irrespective of the graceful-restart configuration status on the device.

In restart signaling-based helper mode implementations, the restarting router informs the restart status to its neighbors only after the restart is complete. When the restart is complete, the restarting router sends hello messages to its helper routers with the **restart signal (RS)** bit set in the hello packet header. When a helper router receives a hello packet with the **RS** bit set in the header, the helper router returns a hello message to the restarting router. The reply hello message from the helper router contains the **ResyncState** flag and the **ResyncTimeout** timer that enable the restarting router to keep track of the helper routers that are syncing up with it. When all helpers complete the synchronization, the restarting router exits the restart mode.

For more information about restart signaling-based graceful restart helper mode implementation, see RFC 4811, *OSPF Out-of-Band Link State Database (LSDB) Resynchronization*, RFC 4812, *OSPF Restart Signaling* and RFC 4813, *OSPF Link-Local Signaling*.

**SEE ALSO**

Example: Managing Helper Modes for OSPF Graceful Restart

Tracing Restart Signaling-Based Helper Mode Events for OSPF Graceful Restart

**Graceful Restart and Layer 2 and Layer 3 VPNs**

VPN graceful restart uses three types of restart functionality:

1. BGP graceful restart functionality is used on all PE-to-PE BGP sessions. This affects sessions carrying any service signaling data for network layer reachability information (NLRI), for example, an IPv4 VPN or Layer 2 VPN NLRI.
2. OSPF, IS-IS, LDP, or RSVP graceful restart functionality is used in all core routers. Routes added by these protocols are used to resolve Layer 2 and Layer 3 VPN NLRI.

3. Protocol restart functionality is used for any Layer 3 protocol (RIP, OSPF, LDP, and so on) used between the PE and customer edge (CE) routers. This does not apply to Layer 2 VPNs because Layer 2 protocols used between the CE and PE routers do not have graceful restart capabilities.

Before VPN graceful restart can work properly, all of the components must restart gracefully. In other words, the routers must preserve their forwarding states and request neighbors to continue forwarding to the router in case of a restart. If all of the conditions are satisfied, VPN graceful restart imposes the following rules on a restarting router:

- The router must wait to receive all BGP NLRI information from other PE routers before advertising routes to the CE routers.
- The router must wait for all protocols in all routing instances to converge (or complete the restart process) before it sends CE router information to other PE routers. In other words, the router must wait for all instance information (whether derived from local configuration or advertisements received from a remote peer) to be processed before it sends this information to other PE routers.
- The router must preserve all forwarding state in the **instance.mpls.0** tables until the new labels and transit routes are allocated and announced to other PE routers (and CE routers in a carrier-of-carriers scenario).

If any condition is not met, VPN graceful restart does not succeed in providing uninterrupted forwarding between CE routers across the VPN infrastructure.

## SEE ALSO

Graceful Restart Concepts
Graceful Restart System Requirements
Configuring Logical System Graceful Restart
Verifying Graceful Restart Operation
Configuring Graceful Restart

## Graceful Restart on Logical Systems

Graceful restart for a logical system functions much as graceful restart does in the main router. The only difference is the location of the graceful-restart statement:

- For a logical system, include the graceful-restart statement at the [edit logical-systems *logical-system-name* routing-options] hierarchy level.
- For a routing instance inside a logical system, include the graceful-restart statement at both the [edit logical-systems *logical-system-name* routing-options] and [edit logical-systems *logical-system-name* routing-instances *instance-name* routing-options] hierarchy levels.

## SEE ALSO

Graceful Restart Concepts
Graceful Restart System Requirements
Configuring Logical System Graceful Restart
Verifying Graceful Restart Operation
Configuring Graceful Restart

## Graceful Restart System Requirements

Graceful restart is supported on all routing platforms. To implement graceful restart for particular features, your system must meet these minimum requirements:

- Junos OS Release 5.3 or later for aggregate route, BGP, IS-IS, OSPF, RIP, RIPng, or static route graceful restart.
- Junos OS Release 5.5 or later for RSVP on egress provider edge (PE) routers.
- Junos OS Release 5.5 or later for LDP graceful restart.
- Junos OS Release 5.6 or later for the CCC, TCC, Layer 2 VPN, or Layer 3 VPN implementations of graceful restart.
- Junos OS Release 6.1 or later for RSVP graceful restart on ingress PE routers.
- Junos OS Release 6.4 or later for PIM sparse mode graceful restart.
- Junos OS Release 7.4 or later for ES-IS graceful restart.
- Junos OS Release 8.5 or later for BFD session (helper mode only)—If a node is undergoing a graceful restart and its BFD sessions are distributed to the Packet Forwarding Engine, the peer node can help the peer with the graceful restart.
- Junos OS Release 9.2 or later for BGP to support helper mode without requiring that graceful restart be configured.

## SEE ALSO

Graceful Restart Concepts
---------------------------

# Configuring Graceful Restart

## IN THIS CHAPTER

- [Configuring Graceful Restart | 307](#)
- [Configuring Graceful Restart for Routing Protocols | 359](#)

## Configuring Graceful Restart

### SUMMARY

Follow these steps to configure graceful restart on your device.

### IN THIS SECTION

- [Enabling Graceful Restart | 307](#)
- [Configuring Graceful Restart | 308](#)
- [Configuring VPN Graceful Restart | 342](#)
- [Configuring Logical System Graceful Restart | 344](#)
- [Configuring Graceful Restart for QFabric Systems | 346](#)
- [Example: Managing Helper Modes for OSPF Graceful Restart | 351](#)
- [Tracing Restart Signaling-Based Helper Mode Events for OSPF Graceful Restart | 354](#)
- [Verifying Graceful Restart Operation | 355](#)

## Enabling Graceful Restart

Graceful restart is disabled by default. You must configure graceful restart at the [edit routing-options] or [edit routing-instances *instance-name* routing-options] hierarchy level to enable the feature globally.

For example:

```
routing-options {
    graceful-restart;
}
```

You can, optionally, modify the global settings at the individual protocol level or, as of Junos OS 15.1, at the individual routing instance level.

**NOTE:** If you configure graceful restart after a BGP or LDP session has been established, the BGP or LDP session restarts and the peers negotiate graceful restart capabilities.

To disable graceful restart, include the `disable` statement. You can do this globally for all protocols by including the `disable` statement at the `[edit routing-options]` hierarchy level, or you can disable graceful restart for a single protocol by including the `disable` statement at the `[edit protocols protocol graceful-restart]` hierarchy level. To configure a time period for complete restart, include the `restart-duration` statement. You can specify a number between 120 and 900.

For a list of hierarchy levels at which you can include this statement, see the statement summary section for this statement.

When you include the `graceful-restart` statement at the `[edit routing-options]` hierarchy level, graceful restart is also enabled for aggregate and static routes.

## SEE ALSO

[Graceful Restart Concepts](#)

[Graceful Restart System Requirements](#)

[Graceful Restart for Aggregate and Static Routes](#)

[Configuring Graceful Restart](#)

## Configuring Graceful Restart

To enable graceful restart, include the `graceful-restart` statement at the `[edit routing-instance instance-name routing-options]` or `[edit routing-options]` hierarchy level. This enables graceful restart globally for all routing protocols. You can, optionally, modify or supplement the global settings at the individual protocol level.

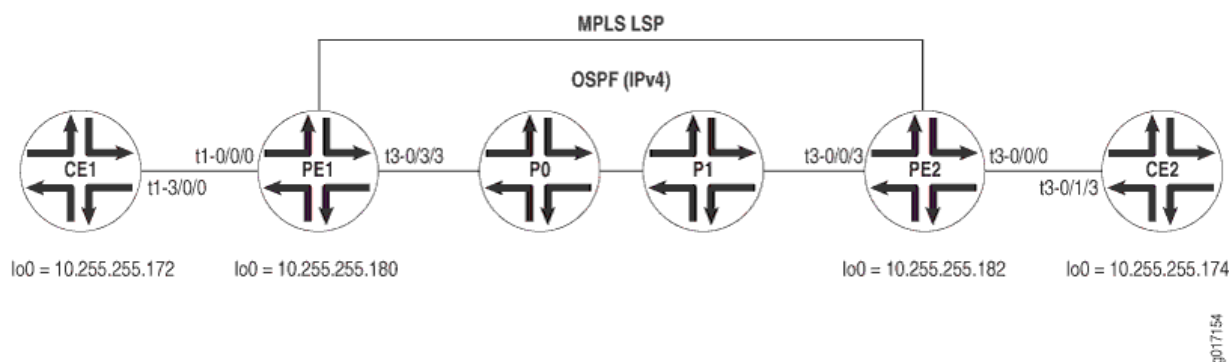
**NOTE:** When set protocols bgp group *group-name* allow network is configured to accept dynamic BGP sessions, unconfigured-peer-graceful-restart statement should be configured to avoid traffic drop during graceful restart or graceful Routing Engine switchover.

For example:

```
protocols {
  bgp {
    group ext {
      graceful-restart {
        restart-time 400;
      }
    }
  }
}
routing-options {
  graceful-restart;
}
```

Figure 22 on page 309 shows a standard MPLS VPN network. Routers CE1 and CE2 are customer edge routers, PE1 and PE2 are provider edge routers, and P0 is a provider core router. Several Layer 3 VPNs are configured across this network, as well as one Layer 2 VPN. Interfaces are shown in the diagram and are not included in the configuration example that follows.

Figure 22: Layer 3 VPN Graceful Restart Topology



Router CE1

On Router CE1, configure the following protocols on the logical interfaces of **t3-3/1/0**: OSPF on unit 101, RIP on unit 102, BGP on unit 103, and IS-IS on unit 512. Also configure graceful restart, BGP, IS-IS, OSPF, and RIP on the main instance to be able to connect to the routing instances on Router PE1.

```
[edit]
interfaces {
  t3-3/1/0 {
    encapsulation frame-relay;
    unit 100 {
      dlci 100;
      family inet {
        address 10.96.100.2/30;
      }
    }
    unit 101 {
      dlci 101;
      family inet {
        address 10.96.101.2/30;
      }
    }
    unit 102 {
      dlci 102;
      family inet {
        address 10.96.102.2/30;
      }
    }
    unit 103 {
      dlci 103;
      family inet {
        address 10.96.103.2/30;
      }
    }
    unit 512 {
      dlci 512;
      family inet {
        address 10.96.252.1/30;
      }
    }
  }
  lo0 {
    unit 0 {
      family inet {
```



```

        address 10.245.14.172/32;
        primary;
    }
    address 10.96.110.1/32;
    address 10.96.111.1/32;
    address 10.96.112.1/32;
    address 10.96.113.1/32;
    address 10.96.116.1/32;
}
family iso {
    address 47.0005.80ff.f800.0000.0108.0001.0102.4501.4172.00;
}
}
routing-options {
    graceful-restart;
    autonomous-system 65100;
}
protocols {
    bgp {
        group CE-PE-INET {
            type external;
            export BGP_INET_LB_DIRECT;
            neighbor 10.96.103.1 {
                local-address 10.96.103.2;
                family inet {
                    unicast;
                }
                peer-as 65103;
            }
        }
    }
    isis {
        export ISIS_L2VPN_LB_DIRECT;
        interface t3-3/1/0.512;
    }
    ospf {
        export OSPF_LB_DIRECT;
        area 0.0.0.0 {
            interface t3-3/1/0.101;
        }
    }
    rip {

```

```

        group RIP {
            export RIP_LB_DIRECT;
            neighbor t3-3/1/0.102;
        }
    }
}

policy-options {
    policy-statement OSPF_LB_DIRECT {
        term direct {
            from {
                protocol direct;
                route-filter 10.96.101.0/30 exact;
                route-filter 10.96.111.1/32 exact;
            }
            then accept;
        }
        term final {
            then reject;
        }
    }
    policy-statement RIP_LB_DIRECT {
        term direct {
            from {
                protocol direct;
                route-filter 10.96.102.0/30 exact;
                route-filter 10.96.112.1/32 exact;
            }
            then accept;
        }
        term final {
            then reject;
        }
    }
    policy-statement BGP_INET_LB_DIRECT {
        term direct {
            from {
                protocol direct;
                route-filter 10.96.103.0/30 exact;
                route-filter 10.96.113.1/32 exact;
            }
            then accept;
        }
        term final {

```

```

        then reject;
    }
}
policy-statement ISIS_L2VPN_LB_DIRECT {
    term direct {
        from {
            protocol direct;
            route-filter 10.96.116.1/32 exact;
        }
        then accept;
    }
    term final {
        then reject;
    }
}
}
}

```

### Router PE1

On Router PE1, configure graceful restart in the master instance, along with BGP, OSPF, MPLS, and LDP. Next, configure several protocol-specific instances of graceful restart. By including instances for BGP, OSPF, Layer 2 VPNs, RIP, and static routes, you can observe the wide range of options available when you implement graceful restart. Configure the following protocols in individual instances on the logical interfaces of **t3-0/0/0**: a static route on unit 100, OSPF on unit 101, RIP on unit 102, BGP on unit 103, and Frame Relay on unit 512 for the Layer 2 VPN instance.

```

[edit]
interfaces {
    t3-0/0/0 {
        dce;
        encapsulation frame-relay-ccc;
        unit 100 {
            dlci 100;
            family inet {
                address 10.96.100.1/30;
            }
            family mpls;
        }
        unit 101 {
            dlci 101;
            family inet {
                address 10.96.101.1/30;
            }
        }
    }
}

```

```

    }
    family mpls;
}
unit 102 {
    dlci 102;
    family inet {
        address 10.96.102.1/30;
    }
    family mpls;
}
unit 103 {
    dlci 103;
    family inet {
        address 10.96.103.1/30;
    }
    family mpls;
}
unit 512 {
    encapsulation frame-relay-ccc;
    dlci 512;
}
}
t1-0/1/0 {
    unit 0 {
        family inet {
            address 10.96.0.2/30;
        }
        family mpls;
    }
}
lo0 {
    unit 0 {
        family inet {
            address 10.245.14.176/32;
        }
        family iso {
            address 47.0005.80ff.f800.0000.0108.0001.0102.4501.4176.00;
        }
    }
}
}
routing-options {
    graceful-restart;

```

```

    router-id 10.245.14.176;
    autonomous-system 69;
}
protocols {
    mpls {
        interface all;
    }
    bgp {
        group PEPE {
            type internal;
            neighbor 10.245.14.182 {
                local-address 10.245.14.176;
                family inet-vpn {
                    unicast;
                }
                family l2vpn {
                    unicast;
                }
            }
        }
    }
    ospf {
        area 0.0.0.0 {
            interface t1-0/1/0.0;
            interface fxp0.0 {
                disable;
            }
            interface lo0.0 {
                passive;
            }
        }
    }
    ldp {
        interface all;
    }
}
policy-options {
    policy-statement STATIC-import {
        from community STATIC;
        then accept;
    }
    policy-statement STATIC-export {
        then {

```

```

        community add STATIC;
        accept;
    }
}
policy-statement OSPF-import {
    from community OSPF;
    then accept;
}
policy-statement OSPF-export {
    then {
        community add OSPF;
        accept;
    }
}
policy-statement RIP-import {
    from community RIP;
    then accept;
}
policy-statement RIP-export {
    then {
        community add RIP;
        accept;
    }
}
policy-statement BGP-INET-import {
    from community BGP-INET;
    then accept;
}
policy-statement BGP-INET-export {
    then {
        community add BGP-INET;
        accept;
    }
}
policy-statement L2VPN-import {
    from community L2VPN;
    then accept;
}
policy-statement L2VPN-export {
    then {
        community add L2VPN;
        accept;
    }
}

```

```

}
community BGP-INET members target:69:103;
community L2VPN members target:69:512;
community OSPF members target:69:101;
community RIP members target:69:102;
community STATIC members target:69:100;
}
routing-instances {
  BGP-INET {
    instance-type vrf;
    interface t3-0/0/0.103;
    route-distinguisher 10.245.14.176:103;
    vrf-import BGP-INET-import;
    vrf-export BGP-INET-export;
    routing-options {
      graceful-restart;
      autonomous-system 65103;
    }
    protocols {
      bgp {
        group BGP-INET {
          type external;
          export BGP-INET-import;
          neighbor 10.96.103.2 {
            local-address 10.96.103.1;
            family inet {
              unicast;
            }
            peer-as 65100;
          }
        }
      }
    }
  }
  L2VPN {
    instance-type l2vpn;
    interface t3-0/0/0.512;
    route-distinguisher 10.245.14.176:512;
    vrf-import L2VPN-import;
    vrf-export L2VPN-export;
    protocols {# There is no graceful-restart statement for Layer 2 VPN instances.
      l2vpn {
        encapsulation-type frame-relay;

```

```

        site CE1-ISIS {
            site-identifier 512;
            interface t3-0/0/0.512 {
                remote-site-id 612;
            }
        }
    }
}

OSPF {
    instance-type vrf;
    interface t3-0/0/0.101;
    route-distinguisher 10.245.14.176:101;
    vrf-import OSPF-import;
    vrf-export OSPF-export;
    routing-options {
        graceful-restart;
    }
    protocols {
        ospf {
            export OSPF-import;
            area 0.0.0.0 {
                interface all;
            }
        }
    }
}

RIP {
    instance-type vrf;
    interface t3-0/0/0.102;
    route-distinguisher 10.245.14.176:102;
    vrf-import RIP-import;
    vrf-export RIP-export;
    routing-options {
        graceful-restart;
    }
    protocols {
        rip {
            group RIP {
                export RIP-import;
                neighbor t3-0/0/0.102;
            }
        }
    }
}

```



```

    }
}
STATIC {
    instance-type vrf;
    interface t3-0/0/0.100;
    route-distinguisher 10.245.14.176:100;
    vrf-import STATIC-import;
    vrf-export STATIC-export;
    routing-options {
        graceful-restart;
        static {
            route 10.96.110.1/32 next-hop t3-0/0/0.100;
        }
    }
}
}
}

```

## Router P0

On Router P0, configure graceful restart in the main instance, along with OSPF, MPLS, and LDP. This allows the protocols on the PE routers to reach one another.

```

[edit]
interfaces {
    t3-0/1/3 {
        unit 0 {
            family inet {
                address 10.96.0.5/30;
            }
            family mpls;
        }
    }
    t1-0/2/0 {
        unit 0 {
            family inet {
                address 10.96.0.1/30;
            }
            family mpls;
        }
    }
}
lo0 {
    unit 0 {

```

```

        family inet {
            address 10.245.14.174/32;
        }
        family iso {
            address 47.0005.80ff.f800.0000.0108.0001.0102.4501.4174.00;
        }
    }
}
routing-options {
    graceful-restart;
    router-id 10.245.14.174;
    autonomous-system 69;
}
protocols {
    mpls {
        interface all;
    }
    ospf {
        area 0.0.0.0 {
            interface t1-0/2/0.0;
            interface t3-0/1/3.0;
            interface fxp0.0 {
                disable;
            }
            interface lo0.0 {
                passive;
            }
        }
    }
    ldp {
        interface all;
    }
}

```

## Router PE2

On Router PE2, configure BGP, OSPF, MPLS, LDP, and graceful restart in the master instance. Configure the following protocols in individual instances on the logical interfaces of **t1-0/1/3**: a static route on unit 200, OSPF on unit 201, RIP on unit 202, BGP on unit 203, and Frame Relay on unit 612 for the Layer 2

VPN instance. Also configure protocol-specific graceful restart in all routing instances, except the Layer 2 VPN instance.

```
[edit]
interfaces {
  t3-0/0/0 {
    unit 0 {
      family inet {
        address 10.96.0.6/30;
      }
      family mpls;
    }
  }
  t1-0/1/3 {
    dce;
    encapsulation frame-relay-ccc;
    unit 200 {
      dlci 200;
      family inet {
        address 10.96.200.1/30;
      }
      family mpls;
    }
    unit 201 {
      dlci 201;
      family inet {
        address 10.96.201.1/30;
      }
      family mpls;
    }
    unit 202 {
      dlci 202;
      family inet {
        address 10.96.202.1/30;
      }
      family mpls;
    }
    unit 203 {
      dlci 203;
      family inet {
        address 10.96.203.1/30;
      }
    }
  }
}
```

```

        family mpls;
    }
    unit 612 {
        encapsulation frame-relay-ccc;
        dlci 612;
    }
}
lo0 {
    unit 0 {
        family inet {
            address 10.245.14.182/32;
        }
        family iso {
            address 47.0005.80ff.f800.0000.0108.0001.0102.4501.4182.00;
        }
    }
}
}
routing-options {
    graceful-restart;
    router-id 10.245.14.182;
    autonomous-system 69;
}
protocols {
    mpls {
        interface all;
    }
    bgp {
        group PEPE {
            type internal;
            neighbor 10.245.14.176 {
                local-address 10.245.14.182;
                family inet-vpn {
                    unicast;
                }
                family l2vpn {
                    unicast;
                }
            }
        }
    }
}
}
ospf {
    area 0.0.0.0 {

```

```

        interface t3-0/0/0.0;
        interface fxp0.0 {
            disable;
        }
        interface lo0.0 {
            passive;
        }
    }
}
ldp {
    interface all;
}
policy-options {
    policy-statement STATIC-import {
        from community STATIC;
        then accept;
    }
    policy-statement STATIC-export {
        then {
            community add STATIC;
            accept;
        }
    }
    policy-statement OSPF-import {
        from community OSPF;
        then accept;
    }
    policy-statement OSPF-export {
        then {
            community add OSPF;
            accept;
        }
    }
    policy-statement RIP-import {
        from community RIP;
        then accept;
    }
    policy-statement RIP-export {
        then {
            community add RIP;
            accept;
        }
    }
}

```

```

policy-statement BGP-INET-import {
    from community BGP-INET;
    then accept;
}
policy-statement BGP-INET-export {
    then {
        community add BGP-INET;
        accept;
    }
}
policy-statement L2VPN-import {
    from community L2VPN;
    then accept;
}
policy-statement L2VPN-export {
    then {
        community add L2VPN;
        accept;
    }
}
community BGP-INET members target:69:103;
community L2VPN members target:69:512;
community OSPF members target:69:101;
community RIP members target:69:102;
community STATIC members target:69:100;
}
routing-instances {
    BGP-INET {
        instance-type vrf;
        interface t1-0/1/3.203;
        route-distinguisher 10.245.14.182:203;
        vrf-import BGP-INET-import;
        vrf-export BGP-INET-export;
        routing-options {
            graceful-restart;
            autonomous-system 65203;
        }
        protocols {
            bgp {
                group BGP-INET {
                    type external;
                    export BGP-INET-import;
                    neighbor 10.96.203.2 {

```



```

    }
  }
}
RIP {
  instance-type vrf;
  interface t1-0/1/3.202;
  route-distinguisher 10.245.14.182:202;
  vrf-import RIP-import;
  vrf-export RIP-export;
  routing-options {
    graceful-restart;
  }
  protocols {
    rip {
      group RIP {
        export RIP-import;
        neighbor t1-0/1/3.202;
      }
    }
  }
}
STATIC {
  instance-type vrf;
  interface t1-0/1/3.200;
  route-distinguisher 10.245.14.182:200;
  vrf-import STATIC-import;
  vrf-export STATIC-export;
  routing-options {
    graceful-restart;
    static {
      route 10.96.210.1/32 next-hop t1-0/1/3.200;
    }
  }
}
}
}
}

```

## Router CE2

On Router CE2, complete the Layer 2 and Layer 3 VPN configuration by mirroring the protocols already set on Routers PE2 and CE1. Specifically, configure the following on the logical interfaces of **t1-0/0/3**: OSPF on unit 201, RIP on unit 202, BGP on unit 203, and IS-IS on unit 612. Finally, configure graceful



restart, BGP, IS-IS, OSPF, and RIP on the main instance to be able to connect to the routing instances on Router PE2.

```
[edit]
interfaces {
  t1-0/0/3 {
    encapsulation frame-relay;
    unit 200 {
      dlci 200;
      family inet {
        address 10.96.200.2/30;
      }
    }
    unit 201 {
      dlci 201;
      family inet {
        address 10.96.201.2/30;
      }
    }
    unit 202 {
      dlci 202;
      family inet {
        address 10.96.202.2/30;
      }
    }
    unit 203 {
      dlci 203;
      family inet {
        address 10.96.203.2/30;
      }
    }
    unit 512 {
      dlci 512;
      family inet {
        address 10.96.252.2/30;
      }
    }
  }
  lo0 {
    unit 0 {
      family inet {
        address 10.245.14.180/32 {
```

```

        primary;
    }
    address 10.96.210.1/32;
    address 10.96.111.1/32;
    address 10.96.212.1/32;
    address 10.96.213.1/32;
    address 10.96.216.1/32;
}
family iso {
    address 47.0005.80ff.f800.0000.0108.0001.0102.4501.4180.00;
}
}
}
routing-options {
    graceful-restart;
    autonomous-system 65200;
}
protocols {
    bgp {
        group CE-PE-INET {
            type external;
            export BGP_INET_LB_DIRECT;
            neighbor 10.96.203.1 {
                local-address 10.96.203.2;
                family inet {
                    unicast;
                }
                peer-as 65203;
            }
        }
    }
    isis {
        export ISIS_L2VPN_LB_DIRECT;
        interface t1-0/0/3.612;
    }
    ospf {
        export OSPF_LB_DIRECT;
        area 0.0.0.0 {
            interface t1-0/0/3.201;
        }
    }
    rip {

```

```

        group RIP {
            export RIP_LB_DIRECT;
            neighbor t1-0/0/3.202;
        }
    }
}

policy-options {
    policy-statement OSPF_LB_DIRECT {
        term direct {
            from {
                protocol direct;
                route-filter 10.96.201.0/30 exact;
                route-filter 10.96.211.1/32 exact;
            }
            then accept;
        }
        term final {
            then reject;
        }
    }
    policy-statement RIP_LB_DIRECT {
        term direct {
            from {
                protocol direct;
                route-filter 10.96.202.0/30 exact;
                route-filter 10.96.212.1/32 exact;
            }
            then accept;
        }
        term final {
            then reject;
        }
    }
    policy-statement BGP_INET_LB_DIRECT {
        term direct {
            from {
                protocol direct;
                route-filter 10.96.203.0/30 exact;
                route-filter 10.96.213.1/32 exact;
            }
            then accept;
        }
        term final {

```

```

        then reject;
    }
}
policy-statement ISIS_L2VPN_LB_DIRECT {
    term direct {
        from {
            protocol direct;
            route-filter 10.96.216.1/32 exact;
        }
        then accept;
    }
    term final {
        then reject;
    }
}
}
}

```

### Router PE1 Status Before a Restart

The following example displays neighbor relationships on Router PE1 before a restart happens:

```

user@PE1> show bgp neighbor
Peer: 10.96.103.2+3785 AS 65100 Local: 10.96.103.1+179 AS 65103
  Type: External   State: Established   Flags: <>
  Last State: OpenConfirm   Last Event: RecvKeepAlive
  Last Error: None
  Export: [ BGP-INET-import ]
  Options: <Preference LocalAddress HoldTime GracefulRestart AddressFamily PeerAS Refresh>
  Address families configured: inet-unicast
  Local Address: 10.96.103.1 Holdtime: 90 Preference: 170
  Number of flaps: 0
  Peer ID: 10.96.110.1      Local ID: 10.96.103.1      Active Holdtime: 90
  Keepalive Interval: 30
  Local Interface: t3-0/0/0.103
  NLRI for restart configured on peer: inet-unicast
  NLRI advertised by peer: inet-unicast
  NLRI for this session: inet-unicast
  Peer supports Refresh capability (2)
  Restart time configured on the peer: 120
  Stale routes from peer are kept for: 300
  Restart time requested by this peer: 120
  NLRI that peer supports restart for: inet-unicast

```

```

NLRI peer can save forwarding state: inet-unicast
NLRI that peer saved forwarding for: inet-unicast
NLRI that restart is negotiated for: inet-unicast
NLRI of all end-of-rib markers sent: inet-unicast
Table BGP-INET.inet.0 Bit: 30001
  RIB State: BGP restart is complete
  RIB State: VPN restart is complete
  Send state: in sync
  Active prefixes:          0
  Received prefixes:        0
  Suppressed due to damping: 0
Last traffic (seconds): Received 8   Sent 3   Checked 3
Input messages:  Total 15   Updates 0   Refreshes 0   Octets 321
Output messages: Total 18   Updates 2   Refreshes 0   Octets 450
Output Queue[2]: 0

Peer: 10.245.14.182+4701 AS 69   Local: 10.245.14.176+179 AS 69
  Type: Internal   State: Established   Flags: <>
  Last State: OpenConfirm   Last Event: RecvKeepAlive
  Last Error: None
  Options: <Preference LocalAddress HoldTime GracefulRestart AddressFamily
Rib-group Refresh>
  Address families configured: inet-vpn-unicast l2vpn
  Local Address: 10.245.14.176 Holdtime: 90 Preference: 170
  Number of flaps: 1
  Peer ID: 10.245.14.182   Local ID: 10.245.14.176   Active Holdtime: 90
  Keepalive Interval: 30
  NLRI for restart configured on peer: inet-vpn-unicast l2vpn
  NLRI advertised by peer: inet-vpn-unicast l2vpn
  NLRI for this session: inet-vpn-unicast l2vpn
  Peer supports Refresh capability (2)
  Restart time configured on the peer: 120
  Stale routes from peer are kept for: 300
  Restart time requested by this peer: 120
  NLRI that peer supports restart for: inet-vpn-unicast l2vpn
  NLRI peer can save forwarding state: inet-vpn-unicast l2vpn
  NLRI that peer saved forwarding for: inet-vpn-unicast l2vpn
  NLRI that restart is negotiated for: inet-vpn-unicast l2vpn
  NLRI of all end-of-rib markers sent: inet-vpn-unicast l2vpn
Table bgp.l3vpn.0 Bit: 10000
  RIB State: BGP restart is complete
  RIB State: VPN restart is complete
  Send state: in sync

```

```

Active prefixes:          0
Received prefixes:       0
Suppressed due to damping: 0
Table bgp.l2vpn.0 Bit: 20000
RIB State: BGP restart is complete
RIB State: VPN restart is complete
Send state: in sync
Active prefixes:          1
Received prefixes:       1
Suppressed due to damping: 0
Table BGP-INET.inet.0 Bit: 30000
RIB State: BGP restart is complete
RIB State: VPN restart is complete
Send state: in sync
Active prefixes:          0
Received prefixes:       0
Suppressed due to damping: 0
Table OSPF.inet.0 Bit: 60000
RIB State: BGP restart is complete
RIB State: VPN restart is complete
Send state: in sync
Active prefixes:          0
Received prefixes:       0
Suppressed due to damping: 0
Table RIP.inet.0 Bit: 70000
RIB State: BGP restart is complete
RIB State: VPN restart is complete
Send state: in sync
Active prefixes:          0
Received prefixes:       0
Suppressed due to damping: 0
Table STATIC.inet.0 Bit: 80000
RIB State: BGP restart is complete
RIB State: VPN restart is complete
Send state: in sync
Active prefixes:          0
Received prefixes:       0
Suppressed due to damping: 0
Table L2VPN.l2vpn.0 Bit: 90000
RIB State: BGP restart is complete
RIB State: VPN restart is complete
Send state: in sync
Active prefixes:          1

```

```

Received prefixes:      1
Suppressed due to damping: 0
Last traffic (seconds): Received 28   Sent 28   Checked 28
Input messages:  Total 2       Updates 0       Refreshes 0       Octets 86
Output messages: Total 13      Updates 10      Refreshes 0       Octets 1073
Output Queue[0]: 0
Output Queue[1]: 0
Output Queue[2]: 0
Output Queue[3]: 0
Output Queue[4]: 0
Output Queue[5]: 0
Output Queue[6]: 0
Output Queue[7]: 0
Output Queue[8]: 0

```

```
user@PE1> show route instance detail
```

```
master:
```

```
Router ID: 10.245.14.176
```

```
Type: forwarding      State: Active
```

```
Restart State: Complete Path selection timeout: 300
```

```
Tables:
```

```
inet.0          : 17 routes (15 active, 0 holddown, 1 hidden)
```

```
Restart Complete
```

```
inet.3          : 2 routes (2 active, 0 holddown, 0 hidden)
```

```
Restart Complete
```

```
iso.0           : 1 routes (1 active, 0 holddown, 0 hidden)
```

```
Restart Complete
```

```
mpls.0          : 19 routes (19 active, 0 holddown, 0 hidden)
```

```
Restart Complete
```

```
bgp.l3vpn.0     : 10 routes (10 active, 0 holddown, 0 hidden)
```

```
Restart Complete
```

```
inet6.0         : 2 routes (2 active, 0 holddown, 0 hidden)
```

```
Restart Complete
```

```
bgp.l2vpn.0     : 1 routes (1 active, 0 holddown, 0 hidden)
```

```
Restart Complete
```

```
BGP-INET:
```

```
Router ID: 10.96.103.1
```

```
Type: vrf             State: Active
```

```
Restart State: Complete Path selection timeout: 300
```

```
Interfaces:
```

```
t3-0/0/0.103
```

```
Route-distinguisher: 10.245.14.176:103
```

```
Vrf-import: [ BGP-INET-import ]
```

```

Vrf-export: [ BGP-INET-export ]
Tables:
  BGP-INET.inet.0      : 4 routes (4 active, 0 holddown, 0 hidden)
  Restart Complete
L2VPN:
  Router ID: 0.0.0.0
  Type: l2vpn          State: Active
  Restart State: Complete Path selection timeout: 300
  Interfaces:
    t3-0/0/0.512
  Route-distinguisher: 10.245.14.176:512
  Vrf-import: [ L2VPN-import ]
  Vrf-export: [ L2VPN-export ]
  Tables:
    L2VPN.l2vpn.0      : 2 routes (2 active, 0 holddown, 0 hidden)
    Restart Complete
OSPF:
  Router ID: 10.96.101.1
  Type: vrf            State: Active
  Restart State: Complete Path selection timeout: 300
  Interfaces:
    t3-0/0/0.101
  Route-distinguisher: 10.245.14.176:101
  Vrf-import: [ OSPF-import ]
  Vrf-export: [ OSPF-export ]
  Tables:
    OSPF.inet.0        : 8 routes (7 active, 0 holddown, 0 hidden)
    Restart Complete
RIP:
  Router ID: 10.96.102.1
  Type: vrf            State: Active
  Restart State: Complete Path selection timeout: 300
  Interfaces:
    t3-0/0/0.102
  Route-distinguisher: 10.245.14.176:102
  Vrf-import: [ RIP-import ]
  Vrf-export: [ RIP-export ]
  Tables:
    RIP.inet.0          : 6 routes (6 active, 0 holddown, 0 hidden)
    Restart Complete
STATIC:
  Router ID: 10.96.100.1
  Type: vrf            State: Active

```



```

Restart State: Complete Path selection timeout: 300
Interfaces:
  t3-0/0/0.100
Route-distinguisher: 10.245.14.176:100
Vrf-import: [ STATIC-import ]
Vrf-export: [ STATIC-export ]
Tables:
  STATIC.inet.0      : 4 routes (4 active, 0 holddown, 0 hidden)
  Restart Complete
__juniper_private1__:
  Router ID: 0.0.0.0
  Type: forwarding   State: Active

user@PE1> show route protocol l2vpn
inet.0: 16 destinations, 17 routes (15 active, 0 holddown, 1 hidden)
Restart Complete
inet.3: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
Restart Complete
BGP-INET.inet.0: 5 destinations, 6 routes (5 active, 0 holddown, 0 hidden)
Restart Complete
OSPF.inet.0: 7 destinations, 8 routes (7 active, 0 holddown, 0 hidden)
Restart Complete
RIP.inet.0: 6 destinations, 6 routes (6 active, 0 holddown, 0 hidden)
Restart Complete
STATIC.inet.0: 4 destinations, 4 routes (4 active, 0 holddown, 0 hidden)
Restart Complete
iso.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
Restart Complete
mpls.0: 20 destinations, 20 routes (20 active, 0 holddown, 0 hidden)
Restart Complete
+ = Active Route, - = Last Active, * = Both
800003      *[L2VPN/7] 00:06:00
              > via t3-0/0/0.512, Pop      Offset: 4
t3-0/0/0.512  *[L2VPN/7] 00:06:00
              > via t1-0/1/0.0, Push 800003, Push 100004(top) Offset: -4
bgp.l3vpn.0: 10 destinations, 10 routes (10 active, 0 holddown, 0 hidden)
Restart Complete
inet6.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
Restart Complete
L2VPN.l2vpn.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
Restart Complete
+ = Active Route, - = Last Active, * = Both
10.245.14.176:512:512:611/96

```

```
*[L2VPN/7] 00:06:01
```

```
Discard
```

```
bgp.l2vpn.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
```

```
Restart Complete
```

## Router PE1 Status During a Restart

Before you can verify that graceful restart is working, you must simulate a router restart. To cause the routing process to refresh and simulate a restart, use the **restart routing** operational mode command:

```
user@PE1> restart routing
```

```
Routing protocol daemon started, pid 3558
```

The following sample output is captured during the router restart:

```
user@PE1> show bgp neighbor
```

```
Peer: 10.96.103.2 AS 65100 Local: 10.96.103.1 AS 65103
```

```
Type: External State: Active Flags: <ImportEval>
```

```
Last State: Idle Last Event: Start
```

```
Last Error: None
```

```
Export: [ BGP-INET-import ]
```

```
Options: <Preference LocalAddress HoldTime GracefulRestart AddressFamily PeerAS Refresh>
```

```
Address families configured: inet-unicast
```

```
Local Address: 10.96.103.1 Holdtime: 90 Preference: 170
```

```
Number of flaps: 0
```

```
Peer: 10.245.14.182+179 AS 69 Local: 10.245.14.176+2131 AS 69
```

```
Type: Internal State: Established Flags: <ImportEval>
```

```
Last State: OpenConfirm Last Event: RecvKeepAlive
```

```
Last Error: None
```

```
Options: <Preference LocalAddress HoldTime GracefulRestart AddressFamily Rib-group Refresh>
```

```
Address families configured: inet-vpn-unicast l2vpn
```

```
Local Address: 10.245.14.176 Holdtime: 90 Preference: 170
```

```
Number of flaps: 0
```

```
Peer ID: 10.245.14.182 Local ID: 10.245.14.176 Active Holdtime: 90
```

```
Keepalive Interval: 30
```

```
NLRI for restart configured on peer: inet-vpn-unicast l2vpn
```

```
NLRI advertised by peer: inet-vpn-unicast l2vpn
```

```
NLRI for this session: inet-vpn-unicast l2vpn
```

```
Peer supports Refresh capability (2)
```

```
Restart time configured on the peer: 120
```

```
Stale routes from peer are kept for: 300
```

Restart time requested by this peer: 120

NLRI that peer supports restart for: inet-vpn-unicast l2vpn

NLRI peer can save forwarding state: inet-vpn-unicast l2vpn

NLRI that peer saved forwarding for: inet-vpn-unicast l2vpn

NLRI that restart is negotiated for: inet-vpn-unicast l2vpn

NLRI of received end-of-rib markers: inet-vpn-unicast l2vpn

Table bgp.l3vpn.0 Bit: 10000

RIB State: BGP restart in progress

RIB State: VPN restart in progress

Send state: in sync

Active prefixes: 10

Received prefixes: 10

Suppressed due to damping: 0

Table bgp.l2vpn.0 Bit: 20000

RIB State: BGP restart in progress

RIB State: VPN restart in progress

Send state: in sync

Active prefixes: 1

Received prefixes: 1

Suppressed due to damping: 0

Table BGP-INET.inet.0 Bit: 30000

RIB State: BGP restart in progress

RIB State: VPN restart in progress

Send state: in sync

Active prefixes: 2

Received prefixes: 2

Suppressed due to damping: 0

Table OSPF.inet.0 Bit: 60000

RIB State: BGP restart is complete

RIB State: VPN restart in progress

Send state: in sync

Active prefixes: 2

Received prefixes: 2

Suppressed due to damping: 0

Table RIP.inet.0 Bit: 70000

RIB State: BGP restart is complete

RIB State: VPN restart in progress

Send state: in sync

Active prefixes: 2

Received prefixes: 2

Suppressed due to damping: 0

Table STATIC.inet.0 Bit: 80000

RIB State: BGP restart is complete

```

RIB State: VPN restart in progress
Send state: in sync
Active prefixes:          1
Received prefixes:        1
Suppressed due to damping: 0
Table L2VPN.l2vpn.0 Bit: 90000
RIB State: BGP restart is complete
RIB State: VPN restart in progress
Send state: in sync
Active prefixes:          1
Received prefixes:        1
Suppressed due to damping: 0
Last traffic (seconds): Received 0    Sent 0    Checked 0
Input messages:  Total 14    Updates 13    Refreshes 0    Octets 1053
Output messages: Total 3     Updates 0     Refreshes 0    Octets 105
Output Queue[0]: 0
Output Queue[1]: 0
Output Queue[2]: 0
Output Queue[3]: 0
Output Queue[4]: 0
Output Queue[5]: 0
Output Queue[6]: 0
Output Queue[7]: 0
Output Queue[8]: 0

```

```
user@PE1> show route instance detail
```

```
master:
```

```

Router ID: 10.245.14.176
Type: forwarding      State: Active
Restart State: Pending Path selection timeout: 300
Tables:
  inet.0                : 17 routes (15 active, 1 holddown, 1 hidden)
Restart Pending: OSPF LDP
  inet.3                : 2 routes (2 active, 0 holddown, 0 hidden)
Restart Pending: OSPF LDP
  iso.0                 : 1 routes (1 active, 0 holddown, 0 hidden)
Restart Complete
  mpls.0                : 23 routes (23 active, 0 holddown, 0 hidden)
Restart Pending: LDP VPN
  bgp.l3vpn.0           : 10 routes (10 active, 0 holddown, 0 hidden)
Restart Pending: BGP VPN
  inet6.0               : 2 routes (2 active, 0 holddown, 0 hidden)
Restart Complete

```

```

    bgp.l2vpn.0          : 1 routes (1 active, 0 holddown, 0 hidden)
    Restart Pending: BGP VPN
BGP-INET:
  Router ID: 10.96.103.1
  Type: vrf          State: Active
  Restart State: Pending Path selection timeout: 300
  Interfaces:
    t3-0/0/0.103
  Route-distinguisher: 10.245.14.176:103
  Vrf-import: [ BGP-INET-import ]
  Vrf-export: [ BGP-INET-export ]
  Tables:
    BGP-INET.inet.0      : 6 routes (5 active, 0 holddown, 0 hidden)
    Restart Pending: VPN
L2VPN:
  Router ID: 0.0.0.0
  Type: l2vpn         State: Active
  Restart State: Pending Path selection timeout: 300
  Interfaces:
    t3-0/0/0.512
  Route-distinguisher: 10.245.14.176:512
  Vrf-import: [ L2VPN-import ]
  Vrf-export: [ L2VPN-export ]
  Tables:
    L2VPN.l2vpn.0        : 2 routes (2 active, 0 holddown, 0 hidden)
    Restart Pending: VPN L2VPN
OSPF:
  Router ID: 10.96.101.1
  Type: vrf          State: Active
  Restart State: Pending Path selection timeout: 300
  Interfaces:
    t3-0/0/0.101
  Route-distinguisher: 10.245.14.176:101
  Vrf-import: [ OSPF-import ]
  Vrf-export: [ OSPF-export ]
  Tables:
    OSPF.inet.0          : 8 routes (7 active, 1 holddown, 0 hidden)
    Restart Pending: OSPF VPN
RIP:
  Router ID: 10.96.102.1
  Type: vrf          State: Active
  Restart State: Pending Path selection timeout: 300
  Interfaces:

```

```

t3-0/0/0.102
Route-distinguisher: 10.245.14.176:102
Vrf-import: [ RIP-import ]
Vrf-export: [ RIP-export ]
Tables:
  RIP.inet.0          : 8 routes (6 active, 2 holddown, 0 hidden)
  Restart Pending: RIP VPN
STATIC:
  Router ID: 10.96.100.1
  Type: vrf           State: Active
  Restart State: Pending Path selection timeout: 300
  Interfaces:
    t3-0/0/0.100
  Route-distinguisher: 10.245.14.176:100
  Vrf-import: [ STATIC-import ]
  Vrf-export: [ STATIC-export ]
  Tables:
    STATIC.inet.0      : 4 routes (4 active, 0 holddown, 0 hidden)
    Restart Pending: VPN
__juniper_private1__:
  Router ID: 0.0.0.0
  Type: forwarding     State: Active

```

```

user@PE1> show route instance summary

```

Instance	Type	Primary rib	Active/holddown/hidden
master	forwarding		
		inet.0	15/0/1
		iso.0	1/0/0
		mpls.0	35/0/0
		l3vpn.0	0/0/0
		inet6.0	2/0/0
		l2vpn.0	0/0/0
		l2circuit.0	0/0/0
BGP-INET	vrf		
		BGP-INET.inet.0	5/0/0
		BGP-INET.iso.0	0/0/0
		BGP-INET.inet6.0	0/0/0
L2VPN	l2vpn		
		L2VPN.inet.0	0/0/0
		L2VPN.iso.0	0/0/0
		L2VPN.inet6.0	0/0/0

```

OSPF          vrf          L2VPN.l2vpn.0          2/0/0
                OSPF.inet.0          7/0/0
                OSPF.iso.0           0/0/0
                OSPF.inet6.0         0/0/0
RIP            vrf          RIP.inet.0           6/0/0
                RIP.iso.0            0/0/0
                RIP.inet6.0          0/0/0
STATIC         vrf          STATIC.inet.0         4/0/0
                STATIC.iso.0         0/0/0
                STATIC.inet6.0       0/0/0
__juniper_private1__ forwarding
                __juniper_priva.inet.0 0/0/0
                __juniper_privat.iso.0 0/0/0
                __juniper_priv.inet6.0 0/0/0

```

user@PE1> **show route protocol l2vpn**

inet.0: 16 destinations, 17 routes (15 active, 1 holddown, 1 hidden)

Restart Pending: OSPF LDP

inet.3: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)

Restart Pending: OSPF LDP

BGP-INET.inet.0: 5 destinations, 6 routes (5 active, 0 holddown, 0 hidden)

Restart Pending: VPN

OSPF.inet.0: 7 destinations, 8 routes (7 active, 1 holddown, 0 hidden)

Restart Pending: OSPF VPN

RIP.inet.0: 6 destinations, 8 routes (6 active, 2 holddown, 0 hidden)

Restart Pending: RIP VPN

STATIC.inet.0: 4 destinations, 4 routes (4 active, 0 holddown, 0 hidden)

Restart Pending: VPN

iso.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)

Restart Complete

mpls.0: 24 destinations, 24 routes (24 active, 0 holddown, 0 hidden)

Restart Pending: LDP VPN

```

+ = Active Route, - = Last Active, * = Both

800001          *[L2VPN/7] 00:00:13
                 > via t3-0/0/0.512, Pop      Offset: 4
t3-0/0/0.512    *[L2VPN/7] 00:00:13
                 > via t1-0/1/0.0, Push 800003, Push 100004(top) Offset: -4

bgp.l3vpn.0: 10 destinations, 10 routes (10 active, 0 holddown, 0 hidden)
Restart Pending: BGP VPN

inet6.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
Restart Complete

L2VPN.l2vpn.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
Restart Pending: VPN L2VPN
+ = Active Route, - = Last Active, * = Both

10.245.14.176:512:512:611/96
                 *[L2VPN/7] 00:00:13
                 Discard
bgp.l2vpn.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
Restart Pending: BGP VPN

```

## SEE ALSO

Enabling Graceful Restart

[Configuring Graceful Restart for Routing Protocols | 359](#)

Configuring Graceful Restart for MPLS-Related Protocols

Configuring VPN Graceful Restart

Configuring Logical System Graceful Restart

Verifying Graceful Restart Operation

## Configuring VPN Graceful Restart

### IN THIS SECTION

 [Configuring Graceful Restart Globally | 343](#)



## ● Configuring Graceful Restart for the Routing Instance | 343

Graceful restart allows a router whose VPN control plane is undergoing a restart to continue to forward traffic while recovering its state from neighboring routers. Without graceful restart, a control plane restart disrupts any VPN services provided by the router. Graceful restart is supported on Layer 2 VPNs, Layer 3 VPNs, virtual-router routing instances, and VPLS.

To implement graceful restart for a Layer 2 VPN or Layer 3 VPN, perform the configuration tasks described in the following sections:

### Configuring Graceful Restart Globally

To enable graceful restart, include the `graceful-restart` statement at the `[edit routing-options]` hierarchy level. To configure a global duration for the graceful restart period, include the `restart-duration` statement at the `[edit routing-options graceful-restart]` hierarchy level.

```
[edit]
routing-options {
  graceful-restart {
    disable;
    restart-duration seconds;
  }
}
```

To disable graceful restart globally, include the `disable` statement at the `[edit routing-options graceful-restart]` hierarchy level.

### Configuring Graceful Restart for the Routing Instance

For Layer 3 VPNs only, you must also configure graceful restart for all routing and MPLS-related protocols within a routing instance by including the `graceful-restart` statement at the `[edit routing-instances instance-name routing-options]` hierarchy level. Because you can configure multi-instance BGP and multi-instance LDP, graceful restart for a carrier-of-carriers scenario is supported. To configure the duration of the graceful restart period for the routing instance, include the `restart-duration` statement at the `[edit routing-instances instance-name routing-options]`.

```
[edit]
routing-instances {
```

```

instance-name {
  routing-options {
    graceful-restart {
      disable;
      restart-duration seconds;
    }
  }
}

```

You can disable graceful restart for individual protocols with the `disable` statement at the [edit routing-instances *instance-name* protocols *protocol-name* graceful-restart] hierarchy level.

## RELATED DOCUMENTATION

Graceful Restart Concepts

Graceful Restart System Requirements

Graceful Restart and Layer 2 and Layer 3 VPNs

Verifying Graceful Restart Operation

Configuring Graceful Restart

## Configuring Logical System Graceful Restart

### IN THIS SECTION

- [Enabling Graceful Restart Globally | 344](#)
- [Configuring Graceful Restart for a Routing Instance | 345](#)

Graceful restart for a logical system functions much as graceful restart does in the main router. The only difference is the location of the `graceful-restart` statement.

The following topics describe what to configure to implement graceful restart in a logical system:

### Enabling Graceful Restart Globally

To enable graceful restart in a logical system, include the `graceful-restart` statement at the [edit logical-systems *logical-system-name* routing-options] hierarchy level. To configure a global duration of the graceful

restart period, include the restart-duration statement at the [edit logical-systems *logical-system-name* routing-options graceful-restart] hierarchy level.

```
[edit]
logical-systems {
  logical-system-name {
    routing-options {
      graceful-restart {
        disable;
        restart-duration seconds;
      }
    }
  }
}
```

To disable graceful restart globally, include the disable statement at the [edit logical-systems *logical-system-name* routing-options graceful-restart] hierarchy level.

### Configuring Graceful Restart for a Routing Instance

For Layer 3 VPNs only, you must also configure graceful restart globally for a routing instance inside a logical system. To configure, include the graceful-restart statement at the [edit logical-systems *logical-system-name* routing-instances *instance-name* routing-options] hierarchy level. Because you can configure multi-instance BGP and multi-instance LDP, graceful restart for a carrier-of-carriers scenario is supported. To configure the duration of the graceful restart period for the routing instance, include the restart-duration statement at the [edit logical-systems *logical-system-name* routing-instances *instance-name* routing-options].

```
[edit]
logical-systems {
  logical-system-name {
    routing-instances {
      instance-name {
        routing-options {
          graceful-restart {
            disable;
            restart-duration seconds;
          }
        }
      }
    }
  }
}
```

```
}
}
```

To disable graceful restart for individual protocols with the `disable` statement at the `[edit logical-systems logical-system-name routing-instances instance-name protocols protocol-name graceful-restart]` hierarchy level.

## RELATED DOCUMENTATION

[Graceful Restart Concepts](#)

[Graceful Restart System Requirements](#)

[Graceful Restart on Logical Systems](#)

[Verifying Graceful Restart Operation](#)

[Configuring Graceful Restart](#)

## Configuring Graceful Restart for QFabric Systems

### IN THIS SECTION

- [Enabling Graceful Restart | 347](#)
- [Configuring Graceful Restart Options for BGP | 348](#)
- [Configuring Graceful Restart Options for OSPF and OSPFv3 | 348](#)
- [Tracking Graceful Restart Events | 350](#)

When you configure graceful restart in the QFabric CLI, the QFabric system applies the configuration to the network Node group to participate in graceful restart operations with devices external to the QFabric system. Such configuration preserves routing table state and helps neighboring routing devices to resume routing operations more quickly after a system restart. This also enables the network Node group to resume routing operations rapidly if there is a restart in the QFabric system (such as a software upgrade). As a result, we recommend enabling graceful restart for routing protocols in the QFabric CLI.

**NOTE:** The QFabric system also uses graceful restart internally within the fabric to facilitate interfabric resiliency and recovery. This internal feature is enabled by default with no configuration required.

## Enabling Graceful Restart

By default, graceful restart is disabled. To enable graceful restart, include the **graceful-restart** statement at the **[edit routing-instance *instance-name* routing-options]** or **[edit routing-options]** hierarchy level.

For example:

```
routing-options {
  graceful-restart;
}
```

To configure the duration of the graceful restart period, include the **restart-duration** at the **[edit routing-options graceful-restart]** hierarchy level.

**NOTE:** Helper mode (the ability to assist a neighboring router attempting a graceful restart) is enabled by default when you start the routing platform, even if graceful restart is not enabled. You can disable helper mode on a per-protocol basis.

```
[edit]
routing-options {
  graceful-restart {
    disable;
    restart-duration seconds;
  }
}
```

To disable graceful restart globally, include the **disable** statement at the **[edit routing-options graceful-restart]** hierarchy level.

When graceful restart is enabled for all routing protocols at the **[edit routing-options graceful-restart]** hierarchy level, you can disable graceful restart on a per-protocol basis.

**NOTE:** If you configure graceful restart after a BGP or LDP session has been established, the BGP or LDP session restarts and the peers negotiate graceful restart capabilities. Also, the BGP peer routing statistics are reset to zero.

## Configuring Graceful Restart Options for BGP

To configure the duration of the BGP graceful restart period, include the **restart-time** statement at the **[edit protocols bgp graceful-restart]** hierarchy level. To set the length of time the router waits to receive messages from restarting neighbors before declaring them down, include the **stale-routes-time** statement at the **[edit protocols bgp graceful-restart]** hierarchy level.

```
[edit]
protocols {
  bgp {
    graceful-restart {
      disable;
      restart-time seconds;
      stale-routes-time seconds;
    }
  }
}
routing-options {
  graceful-restart;
}
```

To disable BGP graceful restart capability for all BGP sessions, include the **disable** statement at the **[edit protocols bgp graceful-restart]** hierarchy level.

**NOTE:** To set BGP graceful restart properties or disable them for a group, include the desired statements at the **[edit protocols bgp group *group-name* graceful-restart]** hierarchy level.

To set BGP graceful restart properties or disable them for a specific neighbor in a group, include the desired statements at the **[edit protocols bgp group *group-name* neighbor *ip-address* graceful-restart]** hierarchy level.

**NOTE:** Configuring graceful restart for BGP resets the BGP peer routing statistics to zero. Also, existing BGP sessions restart, and the peers negotiate graceful restart capabilities.

## Configuring Graceful Restart Options for OSPF and OSPFv3

To configure the duration of the OSPF/OSPFv3 graceful restart period, include the **restart-duration** statement at the **[edit protocols (ospf | ospf3) graceful-restart]** hierarchy level. To specify the length of time for which the router notifies helper routers that it has completed graceful restart, include the

**notify-duration** at the **[edit protocols (ospf | ospfv3) graceful-restart]** hierarchy level. Strict OSPF link-state advertisement (LSA) checking results in the termination of graceful restart by a helping router. To disable strict LSA checking, include the **no-strict-lsa-checking** statement at the **[edit protocols (ospf | ospfv3) graceful-restart]** hierarchy level.

```
[edit]
protocols {
  ospf | ospfv3{
    graceful-restart {
      disable;
      helper-disable
      no-strict-lsa-checking;
      notify-duration seconds;
      restart-duration seconds;
    }
  }
}
routing-options {
  graceful-restart;
}
```

To disable OSPF/OSPFv3 graceful restart, include the **disable** statement at the **[edit protocols (ospf | ospfv3) graceful-restart]** hierarchy level.

Starting with Release 11.3, the Junos OS supports both the standard (based on RFC 3623, *Graceful OSPF Restart*) and the restart signaling-based (as specified in RFC 4811, RFC 4812, and RFC 4813) helper modes for OSPF version 2 graceful restart configurations. Both the standard and restart signaling-based helper modes are enabled by default. To disable the helper mode for OSPF version 2 graceful restart configurations, include the **helper-disable <both | restart-signaling | standard>** statement at the **[edit protocols ospf graceful-restart]** hierarchy level. Note that the last committed statement always takes precedence over the previous one.

```
[edit protocols ospf]
  graceful-restart {
    helper-disable <both | restart-signaling | standard>
  }
```

To reenabling the helper mode, delete the **helper-disable** statement from the configuration by using the **delete protocols ospf graceful-restart helper-disable <restart-signaling | standard | both>** command. In this case also, the last executed command takes precedence over the previous ones.

**NOTE:**

Restart signaling-based helper mode is not supported for OSPFv3 configurations. To disable helper mode for OSPFv3 configurations, include the **helper-disable** statement at the **[edit protocols ospfv3 graceful-restart]** hierarchy level.

**TIP:** You can also track graceful restart events with the **traceoptions** statement at the **[edit protocols (ospf | ospf3)]** hierarchy level. For more information, see "[Tracking Graceful Restart Events](#)" on page 350.

**NOTE:** If you configure BFD and graceful restart for OSPF, graceful restart might not work as expected.

## Tracking Graceful Restart Events

To track the progress of a graceful restart event, you can configure graceful restart trace options flags for IS-IS and OSPF/OSPFv3. To configure graceful restart trace options, include the **graceful-restart** statement at the **[edit protocols *protocol*/traceoptions flag]** hierarchy level:

```
[edit protocols]
isis {
  traceoptions {
    flag graceful-restart;
  }
}
(ospf | ospf3) {
  traceoptions {
    flag graceful-restart;
  }
}
```

## RELATED DOCUMENTATION

[Graceful Restart Concepts](#)

[Verifying Graceful Restart Operation](#)



## Example: Managing Helper Modes for OSPF Graceful Restart

### IN THIS SECTION

- [Requirements | 353](#)
- [Overview | 353](#)
- [Verification | 353](#)

### Configuration

#### Step-by-Step Procedure

Both standard and restart signaling-based helper modes are enabled by default, irrespective of the graceful-restart configuration status on the routing device. Junos OS allows you to disable or enable the helper modes based on your requirements.

To configure the helper mode options for graceful restart:

1. To enable graceful restart, add the graceful-restart statement at the [edit routing-options] hierarchy level.

```
[edit routing-options]  
user@host# set graceful-restart
```

The helper modes, both standard and restart signaling-based, are enabled by default.

2. To disable one or both of the helper modes, add the helper-disable <both | restart-signaling | standard> statement at the [edit protocols ospf graceful-restart] hierarchy level.
  - To disable both standard and restart signaling-based helper modes:

```
[edit protocols ospf graceful-restart]  
user@host# set helper-disable both
```

- To disable only the restart signaling-based helper mode:

```
[edit protocols ospf graceful-restart]
user@host# set helper-disable restart-signaling
```

- To disable only the standard helper mode:

```
[edit protocols ospf graceful-restart]
user@host# set helper-disable standard
```

**NOTE:** You must commit the configuration before the change takes effect.  
The last committed statement always takes precedence over the previous one.

3. To enable one or both of the helper modes when the helper modes are disabled, delete the helper-disable <both | restart-signaling | standard> statement from the [edit protocols ospf graceful-restart] hierarchy level.

- To enable both standard and restart signaling-based helper modes:

```
[edit protocols ospf graceful-restart]
user@host# delete helper-disable
```

- To enable the restart signaling-based helper mode:

```
[edit protocols ospf graceful-restart]
user@host# delete helper-disable restart-signaling
```

- To enable the standard helper mode:

```
[edit protocols ospf graceful-restart]
user@host# delete helper-disable standard
```

**NOTE:** You must commit the configuration before the change takes effect.  
The last committed statement always takes precedence over the previous one.

## Requirements

M Series or T Series routers running Junos OS Release 11.4 or later and EX Series switches.

## Overview

Junos OS Release 11.4 extends OSPF graceful restart support to include restart signaling-based helper mode. Both standard (RFC 3623-based) and restart signaling-based helper modes are enabled by default, irrespective of the graceful-restart configuration status on the routing device.

Junos OS, however, enables you to choose between the helper modes with the `helper-disable <standard | restart-signaling | both>` statement.

## Verification

### IN THIS SECTION

- [Verifying OSPF Graceful Restart and Helper Mode Configuration | 353](#)

Confirm that the configuration is working properly.

### *Verifying OSPF Graceful Restart and Helper Mode Configuration*

## Purpose

Verify the OSPF graceful restart and helper mode configuration on a router.

## Action

- Enter the `run show ospf overview` command from configuration mode.

```
user@host# run show ospf overview
```

```
~
```

```
~
```

```
~
```

```
Restart: Enabled
```

```
Restart duration: 180 sec
```

```
Restart grace period: 210 sec
Graceful restart helper mode: Enabled
Restart-signaling helper mode: Enabled
~
~
~
```

## Meaning

The output shows that graceful restart and both of the helper modes are enabled.

## SEE ALSO

Understanding Restart Signaling-Based Helper Mode Support for OSPF Graceful Restart

Tracing Restart Signaling-Based Helper Mode Events for OSPF Graceful Restart

## Tracing Restart Signaling-Based Helper Mode Events for OSPF Graceful Restart

Junos OS provides a tracing option to log restart signaling-based helper mode events for OSPF graceful restart. To enable tracing for restart signaling-based helper mode events, include the `traceoptions flag restart-signaling` statement at the `[edit protocols ospf]` hierarchy level.

To enable tracing for restart signaling-based events:

1. Create a log file for saving the log.

```
[edit protocols ospf]
user@host# set traceoptions file ospf-log
```

where *ospf-log* is the name of the log file.

2. Enable tracing for restart signaling-based helper mode events.

```
[edit protocols ospf]
user@host# set traceoptions flag restart-signaling
```

### 3. Commit the configuration.

```
[edit protocols ospf]
user@host# commit
```

The logs are saved to the *ospf-log* file in the */var/log* folder.

### Viewing the Log File

To view the restart signaling-based events from the log file, type:

```
user@host> file show /var/log/ospf-log | match "restart signaling"
Jun 25 14:44:08.890216 OSPF Restart Signaling: Start helper mode for nbr ip 14.19.3.2 id
10.10.10.1
Jun 25 14:44:11.358636 OSPF restart signaling: Received DBD with R bit set from nbr ip=14.19.3.2
id=10.10.10.1. Start oob-resync.
Jun 25 14:44:11.380198 OSPF restart signaling: Received DBD with LR bit on from nbr ip=14.19.3.2
id=10.10.10.1. Save its oob-resync capability 1
Jun 25 14:44:11.467200 OSPF restart signaling: nbr fsm for nbr ip=14.19.3.2 id=10.10.10.1 moving
to state Full. Reset oob-resync parameters.
```

### SEE ALSO

Understanding Restart Signaling-Based Helper Mode Support for OSPF Graceful Restart

Example: Managing Helper Modes for OSPF Graceful Restart

### Verifying Graceful Restart Operation

#### IN THIS SECTION

- [Graceful Restart Operational Mode Commands | 356](#)
- [Verifying BGP Graceful Restart | 356](#)
- [Verifying IS-IS and OSPF Graceful Restart | 357](#)
- [Verifying CCC and TCC Graceful Restart | 358](#)

This topic contains the following sections:

## Graceful Restart Operational Mode Commands

To verify proper operation of graceful restart, use the following commands:

- `show bgp neighbor` (for BGP graceful restart)
- `show log` (for IS-IS and OSPF/OSPFv3 graceful restart)
- `show (ospf | ospfv3) overview` (for OSPF/OSPFv3 graceful restart)
- `show rsvp neighbor detail` (for RSVP graceful restart—helper router)
- `show rsvp version` (for RSVP graceful restart—restarting router)
- `show ldp session detail` (for LDP graceful restart)
- `show connections` (for CCC and TCC graceful restart)
- `show route instance detail` (for Layer 3 VPN graceful restart and for any protocols using graceful restart in a routing instance)
- `show route protocol l2vpn` (for Layer 2 VPN graceful restart)

For more information about these commands and a description of their output fields, see the [CLI Explorer](#).

## Verifying BGP Graceful Restart

To view graceful restart information for BGP sessions, use the `show bgp neighbor` command:

```
user@PE1> show bgp neighbor 192.0.2.10
Peer: 192.0.2.10+179 AS 64496 Local: 192.0.2.5+1106 AS 64496
  Type: Internal    State: Established    Flags: <>
  Last State: OpenConfirm    Last Event: RecvKeepAlive
  Last Error: None
  Export: [ static ]
Options:<Preference LocalAddress HoldTime GracefulRestart Damping PeerAS Refresh>
  Local Address: 192.0.2.5 Holdtime: 90 Preference: 170
  IPsec SA Name: hope
  Number of flaps: 0
  Peer ID: 192.0.2.10    Local ID: 192.0.2.5    Active Holdtime: 90
  Keepalive Interval: 30
  NLRI for restart configured on peer: inet-unicast
  NLRI advertised by peer: inet-unicast
  NLRI for this session: inet-unicast
```

```

Peer supports Refresh capability (2)
Restart time configured on the peer: 180
Stale routes from peer are kept for: 180
Restart time requested by this peer: 300
NLRI that peer supports restart for: inet-unicast
NLRI that peer saved forwarding for: inet-unicast
NLRI that restart is negotiated for: inet-unicast
NLRI of received end-of-rib markers: inet-unicast
NLRI of all end-of-rib markers sent: inet-unicast
Table inet.0 Bit: 10000
RIB State: restart is complete
Send state: in sync
Active prefixes: 0
Received prefixes: 0
Suppressed due to damping: 0
Last traffic (seconds): Received 19   Sent 19   Checked 19
Input messages:  Total 2       Updates 1       Refreshes 0       Octets 42
Output messages: Total 3       Updates 0       Refreshes 0       Octets 116
Output Queue[0]: 0

```

## Verifying IS-IS and OSPF Graceful Restart

To view graceful restart information for IS-IS and OSPF, configure traceoptions (see ["Tracking Graceful Restart Events" on page 367](#)).

Here is the output of a traceoptions log from an OSPF restarting router:

```

Oct  8 05:20:12 Restart mode - sending grace lsas
Oct  8 05:20:12 Restart mode - estimated restart duration timer triggered
Oct  8 05:20:13 Restart mode - Sending more grace lsas

```

Here is the output of a traceoptions log from an OSPF helper router:

```

Oct  8 05:20:14 Helper mode for neighbor 192.0.2.5
Oct  8 05:20:14 Received multiple grace lsa from 192.0.2.5

```

## Verifying CCC and TCC Graceful Restart

To view graceful restart information for CCC and TCC connections, use the `show connections` command. The following example assumes four remote interface CCC connections between CE1 and CE2:

```
user@PE1> show connections
```

```
CCC and TCC connections [Link Monitoring On]
```

Legend for status (St)	Legend for connection types
UN -- uninitialized	if-sw: interface switching
NP -- not present	rmt-if: remote interface switching
WE -- wrong encapsulation	lsp-sw: LSP switching
DS -- disabled	
Dn -- down	Legend for circuit types
-> -- only outbound conn is up	intf -- interface
<- -- only inbound conn is up	tlsp -- transmit LSP
Up -- operational	rlsp -- receive LSP
RmtDn -- remote CCC down	
Restart -- restarting	

### CCC Graceful restart : Restarting

Connection/Circuit	Type	St	Time last up	# Up trans
CE1-CE2-0	rmt-if	Restart	-----	0
fe-1/1/0.0	intf	Up		
PE1-PE2-0	tlsp	Up		
PE2-PE1-0	rlsp	Up		
CE1-CE2-1	rmt-if	Restart	-----	0
fe-1/1/0.1	intf	Up		
PE1-PE2-1	tlsp	Up		
PE2-PE1-1	rlsp	Up		
CE1-CE2-2	rmt-if	Restart	-----	0
fe-1/1/0.2	intf	Up		
PE1-PE2-2	tlsp	Up		
PE2-PE1-2	rlsp	Up		
CE1-CE2-3	rmt-if	Restart	-----	0
fe-1/1/0.3	intf	Up		
PE1-PE2-3	tlsp	Up		
PE2-PE1-3	rlsp	Up		



RELATED DOCUMENTATION

Graceful Restart Concepts
Configuring Graceful Restart for QFabric Systems

Release History Table

Release	Description
15.1	You can, optionally, modify the global settings at the individual protocol level or, as of Junos OS 15.1, at the individual routing instance level.

Configuring Graceful Restart for Routing Protocols

SUMMARY

You can configure graceful restart for routing protocols with the steps below.

IN THIS SECTION

- [Enabling Graceful Restart | 360](#)
- [Configuring Graceful Restart Options for BGP | 361](#)
- [Using Control Plane Dependent BFD along with Graceful Restart Helper Mode | 362](#)
- [Configuring Graceful Restart Options for ES-IS | 363](#)
- [Configuring Graceful Restart Options for IS-IS | 363](#)
- [Configuring Graceful Restart Options for OSPF and OSPFv3 | 364](#)
- [Configuring Graceful Restart Options for RIP and RIPng | 366](#)
- [Configuring Graceful Restart Options for PIM Sparse Mode | 366](#)
- [Tracking Graceful Restart Events | 367](#)
- [Configuring Graceful Restart for MPLS-Related Protocols | 368](#)

## Enabling Graceful Restart

By default, graceful restart is disabled. To enable graceful restart, include the **graceful-restart** statement at the **[edit routing-instance *instance-name* routing-options]** or **[edit routing-options]** hierarchy level.

For example:

```
routing-options {
  graceful-restart;
}
```

To configure the duration of the graceful restart period, include the **restart-duration** at the **[edit routing-options graceful-restart]** hierarchy level.

**NOTE:** Helper mode (the ability to assist a neighboring router attempting a graceful restart) is enabled by default when you start the routing platform, even if graceful restart is not enabled. You can disable helper mode on a per-protocol basis.

```
[edit]
routing-options {
  graceful-restart {
    disable;
    restart-duration seconds;
  }
}
```

To disable graceful restart globally, include the **disable** statement at the **[edit routing-options graceful-restart]** hierarchy level.

When graceful restart is enabled for all routing protocols at the **[edit routing-options graceful-restart]** hierarchy level, you can disable graceful restart on a per-protocol basis.

**NOTE:** If you configure graceful restart after a BGP or LDP session has been established, the BGP or LDP session restarts and the peers negotiate graceful restart capabilities. Also, the BGP peer routing statistics are reset to zero.

## Configuring Graceful Restart Options for BGP

To configure the duration of the BGP graceful restart period, include the **restart-time** statement at the **[edit protocols bgp graceful-restart]** hierarchy level. To set the length of time the router waits to receive messages from restarting neighbors before declaring them down, include the **stale-routes-time** statement at the **[edit protocols bgp graceful-restart]** hierarchy level.

```
[edit]
protocols {
  bgp {
    graceful-restart {
      disable;
      restart-time seconds;
      stale-routes-time seconds;
    }
  }
}
routing-options {
  graceful-restart;
}
```

To disable BGP graceful restart capability for all BGP sessions, include the **disable** statement at the **[edit protocols bgp graceful-restart]** hierarchy level.

**NOTE:** To set BGP graceful restart properties or disable them for a group, include the desired statements at the **[edit protocols bgp group *group-name* graceful-restart]** hierarchy level.

To set BGP graceful restart properties or disable them for a specific neighbor in a group, include the desired statements at the **[edit protocols bgp group *group-name* neighbor *ip-address* graceful-restart]** hierarchy level.

**NOTE:** Configuring graceful restart for BGP resets the BGP peer routing statistics to zero. Also, existing BGP sessions restart, and the peers negotiate graceful restart capabilities.

**NOTE:** Do not configure both Bidirectional Forwarding Detection (BFD) for BGP and graceful restart for BGP. Routing performance may be sub-optimal if you do this.

## Using Control Plane Dependent BFD along with Graceful Restart Helper Mode

When BFD is control plane dependent and the device detects a BFD down event and is not already entering the graceful restart helper mode, this is treated as a regular BFD down event and the device enters the graceful restart helper mode. This behavior makes the control plane dependent BFD unusable in conjunction with graceful restart.

Include the `dont-help-shared-fate-bfd-down` statement at the `[edit protocols bgp graceful-restart]` hierarchy to ensure that the device does not enter the graceful restart helper mode and data traffic continues to be forwarded to an alternate path even if there is an interface failure (without a control plane restart on the BGP neighbor).

```
[edit]
protocols {
  bgp {
    graceful-restart {
      disable;
      dont-help-shared-fate-bfd-down;
      restart-time seconds;
      stale-routes-time seconds;
    }
  }
}
routing-options {
  graceful-restart;
}
```

Starting in Junos OS Release 18.3R1, you can prevent SRX Series devices from entering the graceful restart helper mode when the device is configured with BFD with a single-hop external BGP (EBGP), by including the `dont-help-shared-fate-bfd-down` statement at the `[edit protocols bgp graceful-restart]` hierarchy.

### SEE ALSO

| [dont-help-shared-fate-bfd-down](#) | 1002

## Configuring Graceful Restart Options for ES-IS

On J Series Services Routers, to configure the duration of the ES-IS graceful restart period, include the `restart-duration` statement at the `[edit protocols esis graceful-restart]` hierarchy level.

```
[edit]
protocols {
  esis {
    graceful-restart {
      disable;
      restart-duration seconds;
    }
  }
}
routing-options {
  graceful-restart;
}
```

To disable ES-IS graceful restart capability, include the `disable` statement at the `[edit protocols esis graceful-restart]` hierarchy level.

## Configuring Graceful Restart Options for IS-IS

To configure the duration of the IS-IS graceful restart period, include the `restart-duration` statement at the `[edit protocols isis graceful-restart]` hierarchy level.

```
[edit]
protocols {
  isis {
    graceful-restart {
      disable;
      helper-disable;
      restart-duration seconds;
    }
  }
}
routing-options {
  graceful-restart;
}
```

To disable IS-IS graceful restart helper capability, include the `helper-disable` statement at the `[edit protocols isis graceful-restart]` hierarchy level. To disable IS-IS graceful restart capability, include the `disable` statement at the `[edit protocols isis graceful-restart]` hierarchy level.

**NOTE:** Starting with Junos OS Release 12.3, if adjacencies between the Routing Engine and the neighboring peer 'helper' routers time out, graceful restart protocol extensions are unable to notify the peer 'helper' routers about the impending restart. Graceful restart can then stop and cause interruptions in traffic.

To ensure that these adjacencies are kept, change the hold-time for IS-IS protocols from the default of 27 seconds to a value higher than 40 seconds.

**NOTE:** You can also track graceful restart events with the `traceoptions` statement at the `[edit protocols isis]` hierarchy level. For more information, see ["Tracking Graceful Restart Events" on page 367](#).

## Configuring Graceful Restart Options for OSPF and OSPFv3

To configure the duration of the OSPF/OSPFv3 graceful restart period, include the **restart-duration** statement at the `[edit protocols (ospf | ospf3) graceful-restart]` hierarchy level. To specify the length of time for which the router notifies helper routers that it has completed graceful restart, include the **notify-duration** at the `[edit protocols (ospf | ospf3) graceful-restart]` hierarchy level. Strict OSPF link-state advertisement (LSA) checking results in the termination of graceful restart by a helping router. To disable strict LSA checking, include the **no-strict-lsa-checking** statement at the `[edit protocols (ospf | ospf3) graceful-restart]` hierarchy level.

```
[edit]
protocols {
  ospf | ospfv3{
    graceful-restart {
      disable;
      helper-disable
      no-strict-lsa-checking;
      notify-duration seconds;
      restart-duration seconds;
    }
  }
}
routing-options {
```

```
    graceful-restart;
}
```

To disable OSPF/OSPFv3 graceful restart, include the **disable** statement at the **[edit protocols (ospf | ospfv3) graceful-restart]** hierarchy level.

Starting with Release 11.3, the Junos OS supports both the standard (based on RFC 3623, *Graceful OSPF Restart*) and the restart signaling-based (as specified in RFC 4811, RFC 4812, and RFC 4813) helper modes for OSPF version 2 graceful restart configurations. Both the standard and restart signaling-based helper modes are enabled by default. To disable the helper mode for OSPF version 2 graceful restart configurations, include the **helper-disable <both | restart-signaling | standard>** statement at the **[edit protocols ospf graceful-restart]** hierarchy level. Note that the last committed statement always takes precedence over the previous one.

```
[edit protocols ospf]
  graceful-restart {
    helper-disable <both | restart-signaling | standard>
  }
```

To reenable the helper mode, delete the **helper-disable** statement from the configuration by using the **delete protocols ospf graceful-restart helper-disable <restart-signaling | standard | both>** command. In this case also, the last executed command takes precedence over the previous ones.

#### NOTE:

Restart signaling-based helper mode is not supported for OSPFv3 configurations. To disable helper mode for OSPFv3 configurations, include the **helper-disable** statement at the **[edit protocols ospfv3 graceful-restart]** hierarchy level.

**TIP:** You can also track graceful restart events with the **traceoptions** statement at the **[edit protocols (ospf | ospfv3)]** hierarchy level. For more information, see ["Tracking Graceful Restart Events" on page 367](#).

**NOTE:** You cannot enable OSPFv3 graceful restart between a routing platform running Junos OS Release 7.5 and earlier and a routing platform running Junos OS Release 7.6 or later. As a workaround, make sure both routing platforms use the same Junos OS version.

## Configuring Graceful Restart Options for RIP and RIPng

To configure the duration of the RIP or RIPng graceful restart period, include the `restart-time` statement at the `[edit protocols (rip | ripng) graceful-restart]` hierarchy level.

```
[edit]
protocols {
  (rip | ripng) {
    graceful-restart {
      disable;
      restart-time seconds;
    }
  }
}
routing-options {
  graceful-restart;
}
```

To disable RIP or RIPng graceful restart capability, include the `disable` statement at the `[edit protocols (rip | ripng) graceful-restart]` hierarchy level.

## Configuring Graceful Restart Options for PIM Sparse Mode

PIM sparse mode continues to forward existing multicast packet streams during a graceful restart, but does not forward new streams until after the restart is complete. After a restart, the routing platform updates the forwarding state with any updates that were received from neighbors and occurred during the restart period. For example, the routing platform relearns the join and prune states of neighbors during the restart, but does not apply the changes to the forwarding table until after the restart.

PIM sparse mode-enabled routing platforms generate a unique 32-bit random number called a generation identifier. Generation identifiers are included by default in PIM hello messages, as specified in the IETF Internet draft *Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)*. When a routing platform receives PIM hellos containing generation identifiers on a point-to-point interface, Junos OS activates an algorithm that optimizes graceful restart.

Before PIM sparse mode graceful restart occurs, each routing platform creates a generation identifier and sends it to its multicast neighbors. If a PIM sparse mode-enabled routing platform restarts, it creates a new generation identifier and sends it to its neighbors. When a neighbor receives the new identifier, it resends multicast updates to the restarting router to allow it to exit graceful restart efficiently. The restart phase completes when either the PIM state becomes stable or when the restart interval timer expires.



If a routing platform does not support generation identifiers or if PIM is enabled on multipoint interfaces, the PIM sparse mode graceful restart algorithm does not activate, and a default restart timer is used as the restart mechanism.

To configure the duration of the PIM graceful restart period, include the `restart-duration` statement at the `[edit protocols pim graceful-restart]` hierarchy level:

```
[edit]
protocols {
  pim {
    graceful-restart {
      disable;
      restart-duration seconds;
    }
  }
}
routing-options {
  graceful-restart;
}
```

To disable PIM sparse mode graceful restart capability, include the `disable` statement at the `[edit protocols pim graceful-restart]` hierarchy level.

**NOTE:** Multicast forwarding can be interrupted in two ways. First, if the underlying routing protocol is unstable, multicast reverse-path-forwarding (RPF) checks can fail and cause an interruption. Second, because the forwarding table is not updated during the graceful restart period, new multicast streams are not forwarded until graceful restart is complete.

## Tracking Graceful Restart Events

To track the progress of a graceful restart event, you can configure graceful restart trace options flags for IS-IS and OSPF/OSPFv3. To configure graceful restart trace options, include the **`graceful-restart`** statement at the `[edit protocols protocol traceoptions flag]` hierarchy level:

```
[edit protocols]
isis {
  traceoptions {
    flag graceful-restart;
  }
}
```

```
(ospf | ospf3) {
    traceoptions {
        flag graceful-restart;
    }
}
```

## Configuring Graceful Restart for MPLS-Related Protocols

### IN THIS SECTION

- [Configuring Graceful Restart Globally | 368](#)
- [Configuring Graceful Restart Options for RSVP, CCC, and TCC | 368](#)
- [Configuring Graceful Restart Options for LDP | 369](#)

This section contains the following topics:

### Configuring Graceful Restart Globally

To configure graceful restart globally for all MPLS-related protocols, include the `graceful-restart` statement at the `[edit routing-options]` hierarchy level. To configure the duration of the graceful restart period, include the **restart-duration** at the `[edit routing-options graceful-restart]` hierarchy level:

```
[edit]
routing-options {
    graceful-restart {
        disable;
        restart-duration seconds;
    }
}
```

To disable graceful restart globally, include the `disable` statement at the `[edit routing-options graceful-restart]` hierarchy level.

### Configuring Graceful Restart Options for RSVP, CCC, and TCC

Because CCC and TCC rely on RSVP, you must modify these three protocols as a single group.

To configure how long the router retains the state of its RSVP neighbors while they undergo a graceful restart, include the `maximum-helper-recovery-time` statement at the `[edit protocols rsvp graceful-restart]` hierarchy level. This value is applied to all neighboring routers, so it should be based on the time required by the slowest RSVP neighbor to recover.

To configure the delay between when the router discovers that a neighboring router has gone down and when it declares the neighbor down, include the `maximum-helper-restart-time` statement at the `[edit protocols rsvp graceful-restart]` hierarchy level. This value is applied to all neighboring routers, so it should be based on the time required by the slowest RSVP neighbor to restart.

```
[edit]
protocols {
  rsvp {
    graceful-restart {
      disable;
      helper-disable;
      maximum-helper-recovery-time;
      maximum-helper-restart-time;
    }
  }
}
routing-options {
  graceful-restart;
}
```

To disable RSVP, CCC, and TCC graceful restart, include the `disable` statement at the `[edit protocols rsvp graceful-restart]` hierarchy level. To disable RSVP, CCC, and TCC helper capability, include the `helper-disable` statement at the `[edit protocols rsvp graceful-restart]` hierarchy level.

### Configuring Graceful Restart Options for LDP

When configuring graceful restart for LDP, you can include the following optional statements at the `[edit protocols ldp graceful-restart]` hierarchy level:

```
[edit protocols ldp graceful-restart]
disable;
helper-disable;
maximum-neighbor-reconnect-time seconds;
maximum-neighbor-recovery-time seconds;
reconnect-time seconds;
recovery-time seconds;
```

```
[edit routing-options]
graceful-restart;
```

The statements have the following effects on the graceful restart process:

- To configure the length of time required to reestablish a session after a graceful restart, include the `reconnect-time` statement; the range is 30 through 300 seconds. To limit the maximum reconnect time allowed from a restarting neighbor router, include the `maximum-neighbor-reconnect-time` statement; the range is 30 through 300 seconds.
- To configure the length of time that helper routers are required to maintain the old forwarding state during a graceful restart, include the `recovery-time` statement; the range is 120 through 1800 seconds. On the helper router, you can configure a statement that overrides the request from the restarting router and sets the maximum length of time the helper router will maintain the old forwarding state. To configure this feature, include the `maximum-neighbor-recovery-time` statement; the range is 140 through 1900 seconds.

**NOTE:** The value for the **recovery-time** and `maximum-neighbor-recovery-time` statements at the `[edit protocols ldp graceful-restart]` hierarchy level should be approximately 80 seconds longer than the value for the `restart-duration` statement at the `[edit routing-options graceful-restart]` hierarchy level. Otherwise, a warning message appears when you try to commit the configuration.

- To disable LDP graceful restart capability, include the `disable` statement. To disable LDP graceful restart helper capability, include the `helper-disable` statement.

## SEE ALSO

Graceful Restart Concepts
Graceful Restart System Requirements
Graceful Restart and MPLS-Related Protocols
Verifying Graceful Restart Operation
Configuring Graceful Restart

Release History Table

Release	Description
12.3	Starting with Junos OS Release 12.3, if adjacencies between the Routing Engine and the neighboring peer 'helper' routers time out, graceful restart protocol extensions are unable to notify the peer 'helper' routers about the impending restart.

RELATED DOCUMENTATION

Graceful Restart Concepts
Graceful Restart System Requirements
Graceful Restart and Routing Protocols
Verifying Graceful Restart Operation
Configuring Graceful Restart

# 11

PART

## Power Management Overview

---

[Understanding Power Management | 373](#)

[Configuring Power Management | 380](#)

[Redundant Power System Overview | 383](#)

---

# Understanding Power Management

## IN THIS CHAPTER

- [Understanding Power Management on EX Series Switches | 373](#)

## Understanding Power Management on EX Series Switches

### SUMMARY

Power management on EX series switches helps prevent your switch from being disrupted if there's not enough power for all the switch components.

### IN THIS SECTION

- [Power Priority of Line Cards | 374](#)
- [Power Supply Redundancy | 378](#)

The power management feature for Juniper Networks Ethernet Switches helps ensure that normal operation of the system is not disrupted because of insufficient power to the switch. For example:

- Power management ensures that operating line cards continue to receive power if a user installs a new line card in an operating switch when power is insufficient for both the new and existing line cards.
- Power management reserves a certain amount of power to power supply redundancy, so that if a power supply fails, the switch can continue to operate normally. If power management must use some of this reserved power to provide power to switch components, it raises an alarm to indicate that power supply redundancy no longer exists and that normal operations might be disrupted if a power supply fails.
- If power supply failure requires power management to power down some components, it does so gracefully by powering down line cards and PoE ports in the order specified by the user.

Power management manages power to switch components by employing a power budget policy. In its power budget policy, power management:

- Budgets power for each installed switch component that requires power. With the exception of *PoE* power for line cards that support PoE, the amount that power management budgets for each component is the maximum power that component might consume under worst case operating conditions. For example, for the fan tray, power management budgets the amount of power required to run the fans at their maximum speed setting, even if the current fan speed is much lower.
- Reserves a set amount of power for power supply redundancy. In its default configuration, power management manages the switch for  $N+1$  power redundancy, which ensures uninterrupted system operation if one power supply fails. For example, if a switch has four online 3000 W power supplies, power management reserves 3000 W in its power budget policy for redundancy. It allocates the remaining 9000 W to normal operating power.
- Specifies the rules under which components receive power. These rules are designed to ensure the least disruption to switch operation under conditions of insufficient power. For example, power management provides power to core system components, such as the Routing Engines, before it provides power to line cards.

You can configure certain aspects of power management's budget policy, specifically:

- The power priority of individual line cards. By assigning different power priorities to the line cards, you can determine which line cards are more likely to receive power in the event of insufficient power.
- The power redundancy configuration. The default power redundancy configuration is  $N+1$ ; you can optionally configure  $N+N$ . For example, if you have deployed two independent AC power feeds to the switch, configure  $N+N$  redundancy. When you configure power management for  $N+N$  redundancy, it reserves the appropriate amount of power in its power budget and reports insufficient power conditions accordingly.

These configurable items are discussed further in:

## Power Priority of Line Cards

The power priority of line cards determines:

- The order in which line cards are allocated power
- The order in which line cards that support PoE are allocated power for PoE
- How power is reallocated in cases of changes in power availability or demand in an operating switch

**NOTE:** On EX6200 switches, the four 10-Gigabit Ethernet *SFP+* uplink ports on a Switch Fabric and Routing Engine (SRE) module are treated like a line card in the power budget.



This section covers:

## How a Line Card's Power Priority Is Determined

Using the CLI, you can assign an explicit power priority to a line-card slot. If more than one slot has the same assigned priority, the power priority is determined by slot number, with the lowest-numbered slots receiving power first.

By default, all slots in an EX8200 switch are assigned the lowest priority. Thus if you do not explicitly assign priorities to slots, power priority is determined by slot number, with slot 0 having the highest priority.

In an EX6200 switch, all slots are assigned the lowest priority, except for the slots containing an SRE module. Slots containing an SRE module are automatically assigned the highest priority. This means that the line cards that represent the 10-Gigabit Ethernet SFP+ ports on SRE modules have the highest priority among the line cards.

## Line Card Priority and Line Card Power

When an EX6200 or EX8200 switch is powered on, power management allocates power to components according to its power budget policy. After power management has allocated power to the base chassis components, it allocates the remaining available power to the line cards. It powers on the line cards in priority order until all line cards are powered on or the available power (including reserved power, if necessary) is exhausted. Thus if available power is exhausted before all line cards receive power, higher-priority cards are powered on while lower-priority cards remain powered off.

A lower-priority card might receive power while a higher-priority card does not if the remaining available power is sufficient to power on the lower-priority card but not the higher-priority card. For example, if a line card requiring 450 W is in a higher-priority slot than line card requiring 330 W, the line card requiring 330 W receives the power if there is less than 450 W but more than 330 W remaining in the power budget.

Line cards that have been administratively taken offline are not allocated power.

**NOTE:** Because power management does not allocate power to a line card that has been administratively taken offline, a line card that has been taken offline in an EX6200 or EX8200 switch is not automatically brought online when you commit a configuration. You must explicitly use the `request chassis fpc slot slot-number online` command to bring a line card online that was taken offline previously. This behavior differs from other platforms running Juniper Networks Junos operating system (Junos OS), which automatically bring an offline FPC online when you commit a configuration.

If power management cannot power on a line card because of insufficient power, it raises a major (red) alarm.

## Line Card Priority and PoE Power

After all line cards have been powered on, power management allocates any remaining available power, including reserved power, to the PoE power budgets of line cards that have PoE ports. Power management allocates PoE power to line cards in the order of power priority. If enough power is available, a line card receives its full PoE power budget before power management allocates PoE power to the next highest-priority line card. If not enough power is available, a line card receives partial PoE power and lower-priority line cards receive no PoE power.

If power management is unable to allocate enough power to meet the PoE power budget for a line card, it logs a message to the system log.

The default PoE power budget for a line card is the amount of power needed to supply the maximum supported power to all PoE ports. In cases where powered devices do not require the maximum power or in which some PoE ports are not used for powered devices, you can configure a smaller PoE power budget for a line card. By configuring a smaller PoE power budget, you make more power available for the PoE power budgets of lower-priority line cards.

You can also configure the power priority of the PoE ports on a line card. If power management is unable to allocate enough power to a line card to meet its PoE power budget, the line card PoE controller will turn off power to PoE ports in reverse priority order as required to meet the reduced power allocation.

See [Configuring PoE Interfaces on EX Series Switches](#) for more information on how to configure the PoE power budget for a line card and how to configure PoE port priorities.

## Line Card Priority and Changes in the Power Budget

In an operating switch, power management dynamically reallocates power in response to changes in power availability or demand or changes in line card priority. Power management uses line card priority to determine how to reallocate power in response to the following events:

- A power supply fails, is removed, or is taken offline:
  - If power is insufficient to meet the PoE power allocations of all PoE line cards, power management deallocates PoE power from the line cards in reverse priority order until power is sufficient to meet the remaining PoE power allocations.
  - If power is insufficient to meet the base (non-PoE) power requirements of all the line cards, all PoE power is deallocated. If, after the deallocation of PoE power, power is still not sufficient, power management turns off line cards in reverse priority order until power is sufficient for the remaining line cards.

- A new line card is inserted or a line card is brought online:
  - If the line card supports PoE and there is insufficient power to meet its PoE power budget, PoE power is reallocated from lower-priority line cards. If not enough PoE power can be reallocated from lower-priority line cards, the new line card receives a partial PoE power allocation.
  - If there is insufficient power to power on the new line card, PoE power is removed from PoE line cards in reverse priority order until the new line card can be powered on.
  - If the removal of all PoE power is insufficient to free up enough power to power on the line card, the line card remains powered off and the PoE line cards continue to receive their PoE power allocations. To minimize disruption on an operating switch, lower-priority line cards are not turned off to provide power to the new line card. However, if you restart the switch, power management reruns the current power budget policy and powers line cards on or off based on their priority. As a result, line cards receive power strictly by priority order and previously operating line cards might no longer receive power.
- A new power supply is brought online:
  - Any line cards that were powered off because of insufficient power are powered on in priority order.
  - After all line cards are powered on, remaining power is allocated to the PoE power budgets of line cards in priority order.
- A line card is removed or taken offline, freeing up power:
  - Any line cards that were powered down because of insufficient power are powered on in priority order.
  - After all line cards are powered on, any remaining power is allocated to the PoE power budgets of line cards in priority order.
- A user changes the assigned power priority of one or more line cards when power is insufficient to meet the power budget:
  - PoE power to the line cards is reallocated based on the new power priorities.
  - Base power allocation to the line cards is not changed—in other words, power management does not power down line cards that had been receiving power because they are now a lower priority. However, if you restart the switch, power management reruns the current power budget policy and powers line cards on or off based on their priority. As a result, line cards receive power strictly by priority order and previously operating line cards might no longer receive power.

If, because of insufficient power, power management reduces or eliminates the PoE power budget for a line card, it logs a message to the system log. If power management must power down a line card because of insufficient power, it raises a major (red) alarm.

# Power Supply Redundancy

By default, power management in EX Series switches is configured to manage the power supplies for  $N+1$  redundancy, in which one power supply is held in reserve for backup if one of the other power supplies is removed or fails.

You can configure power management to manage the power supplies for  $N+N$  redundancy. In  $N+N$  redundancy, power management holds  $N$  power supplies in reserve for backup. For example, if your switch has six power supplies and you configure  $N+N$  redundancy, power management makes three power supplies available for normal operating power and reserves three power supplies for redundancy (3+3). If you have an odd number of power supplies, power management allocates one more power supply to normal operating power than to redundant power. For example, if you have five power supplies, the  $N+N$  configuration is 3+2.

Given the same number of power supplies, an  $N+N$  configuration usually provides less normal operating power than an  $N+1$  configuration because the  $N+N$  configuration holds more power in reserve for backup. [Table 8 on page 378](#) shows the effect on normal operating power in  $N+1$  and  $N+N$  configurations.

**Table 8: Available Operating Power in  $N+1$  and  $N+N$  Redundancy Configurations**

Number of Power Supplies at $n$ W Each	Normal Operating Power in $N+1$ Configuration	Normal Operating Power in $N+N$ Configuration
2	1 x ( $n$ W)	1 x ( $n$ W)
3	2 x ( $n$ W)	2 x ( $n$ W)
4	3 x ( $n$ W)	2 x ( $n$ W)
5 (EX8200 switches only)	4 x ( $n$ W)	3 x ( $n$ W)
6 (EX8200 switches only)	5 x ( $n$ W)	3 x ( $n$ W)

To compensate for the reduced normal operating power, power management on EX8200 switches allocates less power to the chassis in an  $N+N$  configuration than in an  $N+1$  configuration. This reduction in allocated chassis power allows a switch in an  $N+N$  configuration to power more line cards than it could without the reduction. For the EX8208 switch, the power allocated for the chassis is reduced to 1200 W from 1600 W; for the EX8216 switch, it is reduced to 1800 W from 2400 W.

**NOTE:** To achieve the reduction in allocated chassis power in an EX8200 switch, power management reduces the maximum fan speed to 60 percent in an  $N+N$  configuration from 80 percent in an  $N+1$  configuration. Because the maximum fan speed is reduced, it is possible that a line card that overheats would be shut down sooner in an  $N+N$  configuration than in an  $N+1$  configuration.

On EX6200 switches, the same amount of power is allocated for the chassis in  $N+N$  configurations as in  $N+1$  configurations.

Power management automatically recalculates the reserved power and normal operating power as power supplies go online or offline. For example, if you have an  $N+N$  configuration with three online 2000 W power supplies, power management allocates 2000 W to reserved power. If you bring a fourth 2000 W power supply online, power management then allocates 4000 W to reserved power. If a power supply goes offline again, power management once again allocates 2000 W to reserved power.

When power is insufficient to meet the budgeted power requirements, power management raises alarms as follows:

- A minor (yellow) alarm is raised when insufficient power exists to maintain the configured  $N+1$  or  $N+N$  power reserves, but all line cards are still receiving their base and PoE power allocations. If this condition persists for 5 minutes, the alarm becomes a major (red) alarm. Even though operation of the switch is unaffected in this condition, you should remedy it as quickly as possible because a power supply failure might cause a disruption in switch operation.
- A major (red) alarm is raised when insufficient power exists to provide all the line cards with their base and PoE power allocations. One or more PoE ports might be down or one or more line cards might be down.

Power management clears all alarms when sufficient power is available to meet normal operating and reserved power requirements.

## RELATED DOCUMENTATION

*Understand Alarm Types and Severity Levels on EX Series Switches*

Configuring the Power Priority of Line Cards (CLI Procedure)

Configuring Power Supply Redundancy (CLI Procedure)

[Understanding Power Management on EX Series Switches | 373](#)

# Configuring Power Management

## IN THIS CHAPTER

- [Configuring Power Management | 380](#)

## Configuring Power Management

### SUMMARY

Follow the steps below to configure power management on your switch.

### IN THIS SECTION

- [Configuring the Power Priority of Line Cards \(CLI Procedure\) | 380](#)
- [Configuring Power Supply Redundancy \(CLI Procedure\) | 381](#)

## Configuring the Power Priority of Line Cards (CLI Procedure)

The power management facility on EX6200 and EX8200 switches allows you to assign power priorities to the slots occupied by line cards. Power management provides power to the slots in priority order, which means that line cards in higher priority slots are more likely to receive power than line cards in lower priority slots if power to the switch is insufficient to power all the line cards.

The power priority you assign to a PoE line card affects both the order in which it receives base power and the order in which it receives PoE power. Base power is allocated first to all line cards in priority order. PoE power is then allocated to the PoE line cards in priority order.

When assigning power priority to slots, keep these points in mind:

- 0 is the highest priority. The number of priority levels depends on the number of slots in a switch—for example, for an EX8208 switch, which has eight slots, you can assign a priority of 0 through 7 to a slot.
- All slots are assigned the lowest priority by default.

- If a group of slots shares the same assigned priority, each slot's power priority within the group is based on its slot number, with the lowest-numbered slots receiving power first. For example, if slot 3 and slot 7 each have an assigned power priority of 2, slot 3 has the higher power priority.
- On EX6200 switches, slots containing a Switch Fabric and Routing Engine (SRE) module are automatically assigned the highest priority. If you assign a priority of 0 to a slot that has a lower number than a slot an SRE module is in, the slot with an SRE module still receives power first. You cannot change the power priority of slot containing an SRE module.

To assign or change the power priority for a slot:

```
[edit chassis]
user@switch# set fpc slot power-budget-priority priority
```

For example, to set slot 6 to priority 0, enter:

```
[edit chassis]
user@switch# set fpc 6 power-budget-priority 0
```

## SEE ALSO

Configuring Power Supply Redundancy (CLI Procedure)

[Understanding Power Management on EX Series Switches | 373](#)

[Understanding Power Management on EX Series Switches | 373](#)

## Configuring Power Supply Redundancy (CLI Procedure)

By default, the power management feature in EX Series switches is configured to manage the power supplies for  $N+1$  redundancy, in which one power supply is held in reserve for backup if any one of the other power supplies is removed or fails.

You can configure power management to manage the power supplies for  $N+N$  redundancy. For example, to set up your AC power supplies for dual power feed,  $N+N$  redundancy is required. In  $N+N$  redundancy, power management allocates half of the online power supplies to normal operating power and half to redundant power. If you have an odd number of online power supplies, power management allocates one more power supply to normal operating power than to redundant power.

This topic describes how to configure power management for  $N+N$  redundancy and how to revert back to  $N+1$  redundancy if your deployment needs change.

Before you configure power management for  $N+N$  redundancy, ensure that you have sufficient power supplies to meet the power requirements of an  $N+N$  configuration. Use the `show chassis power-budget-statistics` command to display your current power budget.

**NOTE:** To allow more power to be available to line cards in an EX8200 switch, power management compensates for the reduced normal operating power in an  $N+N$  configuration by allocating less power to the chassis than it does in an  $N+1$  configuration. For the EX8208 switch, the power allocated to the chassis is reduced to 1200 W from 1600 W. For the EX8216 switch, it is reduced to 1800 W from 2400 W. In determining whether you have enough power for an  $N+N$  configuration, take this reduction of allocated chassis power into account.

The reduction in allocated chassis power is achieved by reducing the maximum fan speed to 60 percent in an  $N+N$  configuration from 80 percent in an  $N+1$  configuration. Because the maximum fan speed is reduced, it is possible that a line card that overheats would be shut down sooner in an  $N+N$  configuration than in an  $N+1$  configuration.

On EX6200 switches, the same amount of power is allocated for the chassis in  $N+N$  configurations as in  $N+1$  configurations.

To configure  $N+N$  redundancy:

```
[edit chassis]user@switch# set psu redundancy n-plus-n
```

To revert back to  $N+1$  redundancy:

```
[edit chassis]user@switch# delete chassis psu redundancy n-plus-n
```

## SEE ALSO

[Understanding Power Management on EX Series Switches | 373](#)

[Understanding Power Management on EX Series Switches | 373](#)



# Redundant Power System Overview

## IN THIS CHAPTER

- [Understanding the EX Series Redundant Power System | 383](#)

## Understanding the EX Series Redundant Power System

### SUMMARY

The Redundant Power System (RPS) provides backup power to a switch if the primary power source fails.

### IN THIS SECTION

- [EX Series Redundant Power System Hardware Overview | 383](#)
- [Understanding How Power Priority Is Determined and Set for Switches Connected to the EX Series Redundant Power System | 387](#)
- [Determining and Setting Priority for Switches Connected to an EX Series RPS | 389](#)

## EX Series Redundant Power System Hardware Overview

### IN THIS SECTION

- [Benefits of the EX Series Redundant Power System | 384](#)
- [Switch Models and Configurations Supported by the RPS | 384](#)
- [When a Switch's Power Supply Fails | 386](#)
- [Components of the RPS | 386](#)

You can use the EX Series Redundant Power System (RPS) to provide backup power for Juniper Networks EX2200 Ethernet Switches, (except Juniper Networks EX2200-C Ethernet Switches) and Juniper Networks EX3300 Ethernet Switches that are standalone switches or are members of a *Virtual Chassis*.

Most EX Series switches have a built-in capability for redundant power supplies—therefore, if one power supply fails on those switches, the other power supply takes over. However, EX2200 switches and EX3300 switches have only one internal fixed power supply. If an EX2200 switch or EX3300 switch is deployed in a critical situation, we recommend that you connect a an RPS to that switch to supply backup power during a loss of power.

RPS is not a primary power supply—it only provides backup power to switches when the single dedicated power supply fails. An RPS operates in parallel with the single dedicated power supplies of the switches connected to it and provides all connected switches enough power to support either Power over Ethernet (PoE) or non-PoE devices when the power supplies on the switches fail.

An RPS can hold up to three power supplies connected to as many as six switches—how that power is allocated is up to you. You determine whether or not to connect switches that provide PoE and you determine which switches have priority. Priority becomes an issue when you connect more than three switches that provide PoE to a fully loaded RPS because a switch providing PoE requires more power than a switch that does not provide PoE. Because a power supply can support only one switch providing PoE, the RPS can become oversubscribed when too many switches that must have enough power for PoE have a power failure.

### **Benefits of the EX Series Redundant Power System**

Provides power backup—You connect up to six EX2200, EX3300, or a combination of these switches and supply power to any three of them.

Protection from high-voltage input and short circuits—RPS provides protection from high-voltage input and short circuits.

### **Switch Models and Configurations Supported by the RPS**

The RPS supports all EX3300 switches and EX2200 switches except EX2200-C switches. You can simultaneously connect any supported switches to the same RPS, whether the switches are standalone switches or are configured in a Virtual Chassis.

All power provided by RPS is either PoE or non-PoE. By default, RPS supports switches that provide PoE. If even one switch provides PoE, then the RPS must be configured to provide enough power for PoE. When enough power for PoE is supplied, one switch can be powered by each power supply. If the switches are not providing PoE power, two switches can be powered by one RPS power supply—you can reconfigure an RPS to provide non-PoE power using a feature called multi-backup.

Table 9 on page 385 lists some possible scenarios and RPS solutions. These examples assume that each RPS is fully loaded with three power supplies.

**Table 9: Sample Requirements and RPS Solutions**

Switches Requiring Backup	You need this RPS configuration:
Six switches that do not provide PoE to attached devices	One RPS can simultaneously provide power to all six switches if you change the power default to multi-backup—this indicates that no attached switch provides PoE to any devices.
One switch that provides PoE to other devices or two switches that do not provide PoE to any devices	One RPS will always back up all three switches, whether or not they provide PoE to connected devices. Leave the power at the default setting (no multi-backup) and let RPS determine that two switches need only minimum power and one switch provides PoE and therefore needs extra power. RPS automatically supplies the correct level of power.
One EX Series Virtual Chassis member that supplies PoE, one switch that supplies PoE, and one switch that does not supply PoE to any connected devices	One RPS will always back up all three switches. Leave the power default setting (no multi-backup) and let RPS determine that one switch needs only minimum power, one switch needs extra power because it supplies PoE, and the Virtual Chassis member also provides PoE to connected devices.
One switch that supplies PoE and five switches that do not supply PoE	<p>You have two options.</p> <p>Option 1—Use one RPS: Up to three switches that do or do not supply PoE can be backed up simultaneously. You can prioritize the six switches to determine which three are most important if all six fail at once. You must leave the power default setting (no multi-backup) because you have one switch that supplies PoE to attached devices and therefore requires more power.</p> <p>Option 2—Use Two RPSs: In this case, you can connect three switches to each RPS and all switches will be backed up if they all fail at once. Alternatively, you can change the power default to multi-backup on one RPS and connect all five switches that do not supply PoE to that RPS, leaving the other RPS to back up the switch that supplies PoE.</p>
EX Series Virtual Chassis	Use as many RPSs as needed to back up all members of the Virtual Chassis.

### When a Switch's Power Supply Fails

Because the power supplies for both EX3300 switches and EX2200 switches are internal, if the switch's power supply fails, you must replace the switch. You should remove or replace a switch with a failed power supply as soon as possible.

Do not try to use an RPS as a primary power supply because an RPS cannot boot or reboot a switch. Each switch connected to the RPS must have its own dedicated power supply and must have booted up using the internal power supply.

If a switch is deployed in a large network center where RPS has a separate source of electricity than the switches it supports, the RPS supplies power when only the switch's electricity fails. In this case, you would not have to replace the switch because the power supply is still functional. The switch will resume using its own internal power supply when electricity to the switch is restored.

### Components of the RPS

[Table 10 on page 386](#) lists and describes the components of an RPS:

**Table 10: Redundant Power System Components**

Component	Value
Power supplies that can be installed	Up to three EX-PWR3-930-AC power supplies. One is included and additional power supplies must be ordered separately.
Switch connector ports on RPS	6 (2 per power supply)
Power cords (for connecting power supplies to the AC power source outlet)	Up to three power cords, one per power supply.
RPS cables (for connecting a switch to a power supply installed in the RPS)	6 (1 for each RPS-to-switch connection). One cable is supplied with the RPS. Additional cables must be ordered separately.

## Understanding How Power Priority Is Determined and Set for Switches Connected to the EX Series Redundant Power System

### IN THIS SECTION

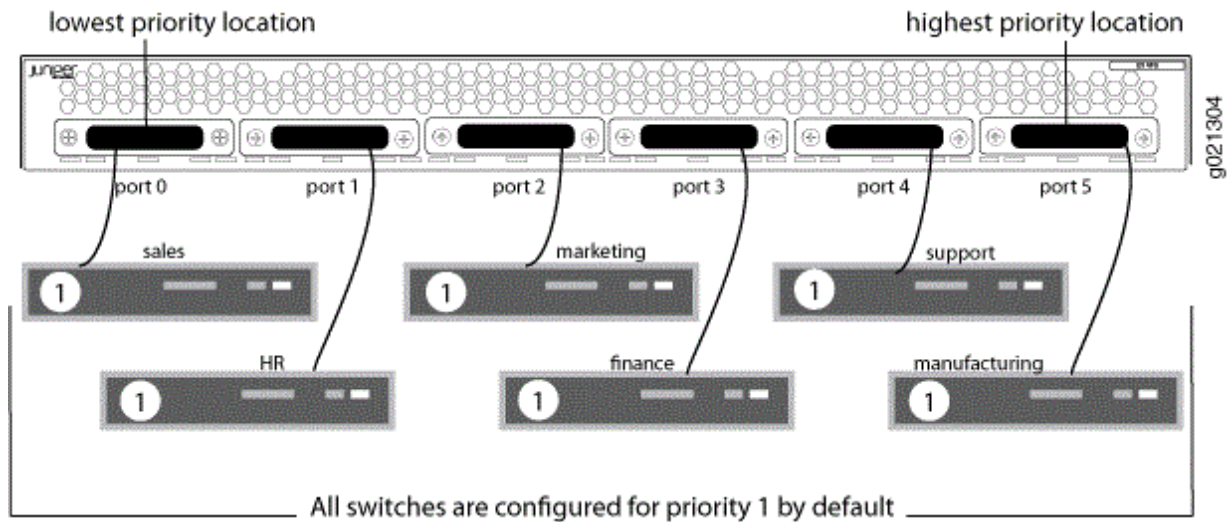
- [Default RPS Priority | 387](#)
- [Changing the Priority of Switches on an EX Series RPS | 388](#)

The Redundant Power System (RPS) is designed to provide backup power to switches that lack built-in redundant power supplies. The RPS provides backup power to switches that either supply power over Ethernet (PoE), which require more power, or switches that do not supply PoE, which require less power. A power supply can either power one PoE device or two non-PoE devices. That means if an RPS is fully loaded with three power supplies, supports PoE switches, and more than three PoE switches have a power failure, some switches will not be powered. You can, however, determine which switches will be powered when an RPS is oversubscribed. When too many connected switches fail, the switches are given power based on their priority. Priority is also reconfigured when any power change takes place. For example, if three switches are already being backed up and another switch has a power failure, the RPS detects this, reconfigures the current top priorities, and allots power accordingly.

### Default RPS Priority

While six non-PoE switches can all simultaneously be backed up with three power supplies, only three PoE switches can be backed up (because PoE uses more power). This means that an RPS with four or more PoE switches connected will have to select three of them for backup. You can determine priority by the connector positions you use to connect the switches. By default, an RPS assigns priority to switches based on their switch connector port location, with the leftmost port having the lowest priority and the rightmost port having the highest priority. If the PoE switches shown in [Figure 23 on page 388](#) all fail, the manufacturing, support, and finance switches will be backed up because they are connected to the rightmost connectors.

**Figure 23: Default PoE Switch Priority Is Determined by Connector Port Location**

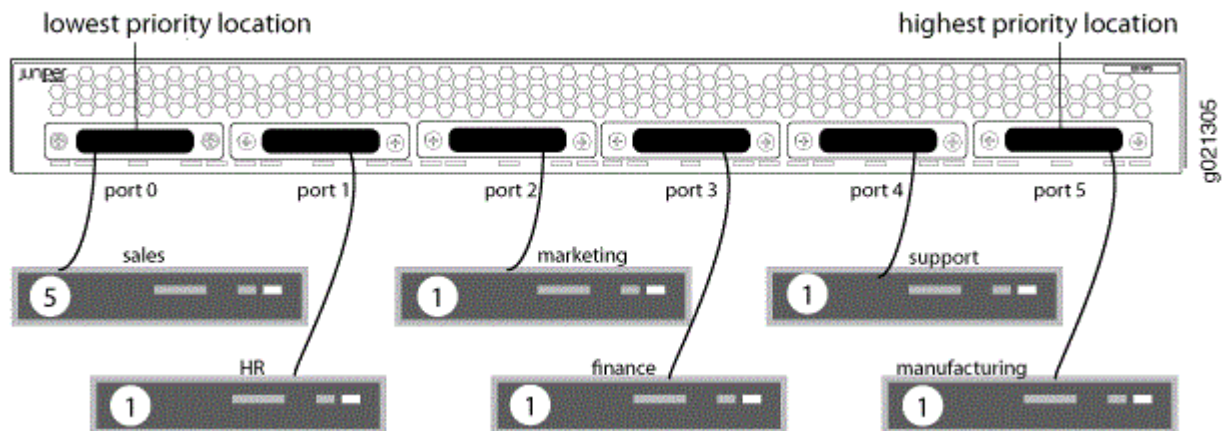


### Changing the Priority of Switches on an EX Series RPS

There is a way to alter the priority of PoE switches on an RPS without disconnecting the cables. You can optionally reconfigure any of the attached switches from their CLIs to establish a switch's RPS priority—this CLI configuration overcomes the priority determined by the switch connector port location. Priority ranges from zero (off) to 1 (lowest) through 6 (highest). By default, all switches are configured to 1, the lowest priority. Let's say that the sales switch is reconfigured from the switch's CLI for priority 5 (second highest).

Now in [Figure 24 on page 388](#), with the sales switch configured for RPS 5 from the CLI, the highest priority changes to sales (because 5 is higher than 1), then manufacturing, and then support.

**Figure 24: Switch Priority After CLI Configuration**



When assigning power priority to switches by using the CLI on the switch, keep these points in mind:

- By default, all switches are assigned priority 1 (lowest) and derive precedence from the location of their connector port on the RPS, with the rightmost port having highest priority.
- Priority 0 assigned from a switch CLI means that the RPS does not provide any backup power to the switch. Essentially, this turns off RPS support.
- Priority 6 assigned from a switch CLI is the highest priority and priority 1 is the lowest priority.
- The CLI command that assigns priority to EX2200 switches is slightly different from the CLI command that assigns priority to EX3300 switches because EX3300 switches can be configured as a *Virtual Chassis*.
- If two or more switches are assigned the same priority value from the switches' CLIs, then the power priority for those switches is determined by the RPS switch connector port location, with the ports to the right receiving priority.
- If a single power supply is installed, the RPS can provide backup power to one switch out of all the switches connected to the RPS. If you do not need any PoE power backup on any switch, you can increase the number of supported switches to two per power supply. Switches connected to an RPS must be either all PoE or all non-PoE.
- The RPS discontinues supplying backup power to a lower-priority switch if it detects a backup power need for a higher-priority switch at the same time.

## SEE ALSO

Determining and Setting Priority for Switches Connected to an EX Series RPS

## Determining and Setting Priority for Switches Connected to an EX Series RPS

### IN THIS SECTION

- [Using RPS Default Configuration | 390](#)
- [Setting the EX Series RPS Priority for a Switch \(CLI\) | 390](#)

A Redundant Power System (RPS) provides backup power according to the RPS priority configured on the standalone EX Series switches or Virtual Chassis member switches connected to it. If all switches connected to the RPS are set to the default priority of 1, the priority is determined on the basis of the RPS port to which they are connected, with higher port numbers having the higher priorities.

The number of switches for which an RPS can provide backup power depends on whether the switches provide power over Ethernet (PoE).

- **PoE:** A fully loaded RPS provides backup power to a maximum of three switches that are enabled for PoE—the result in this case is one switch powered per power supply. If more than three PoE-enabled switches are connected to the RPS and the RPS is already providing backup power to three switches when another switch's power supply fails, the RPS detects this and re-allots backup power as required. It would then stop providing backup power to a low-priority switch to provide backup power to a higher-priority switch.
- **Non-PoE:** If you changed the RPS power setting to non-PoE with the command `request redundant-power-system multi-backup`, your RPS is configured to provide back up power to as many as six non-PoE switches on a fully loaded RPS. Each power supply can support two switches when the switches do not need enough power for PoE.

**NOTE:** Before an RPS can back up a switch connected to it, the switch's RPS status must be ARMED. There are two ways to determine whether a switch's RPS status is ARMED—either check that the corresponding port LED on the RPS is lit and on steady or issue this command from the switch's CLI: `show chassis redundant-power-system`.

This topic describes how to determine and set the power priority for a switch connected to an RPS.

### Using RPS Default Configuration

No configuration is required on an RPS if you:

- Plan to back up as many as six non-PoE switches
- Back up three PoE switches with three RPS power supplies
- Back up four or more PoE switches with RPS three power supplies and let the RPS port to which the switch is connected determine the priority

By default, an RPS assigns priority to switches on the basis of their switch connector port location, with the with higher port numbers having the higher priorities. By default, all switches are themselves configured with the same RPS priority (priority 1, the lowest), which is why priority is derived from the RPS connector port numbers.

### Setting the EX Series RPS Priority for a Switch (CLI)

Each switch connected to RPS has an RPS priority value—that priority value determines which PoE switches receive power first from the RPS. By default, all switches are configured for priority 1 so priority is then determined by switch connector port location, left (lowest) to right (highest).



You can change the priority of a switch to 0 (off), or 1 (lowest) through 6 (highest) from the switch itself —this configuration takes precedence over switch connector port location.

To set or change the priority for a switch that does not support Virtual Chassis:

```
[edit]
user@switch# set redundant-power-system priority
```

To set or change the priority for a switch that supports Virtual Chassis:

```
[edit]
user@switch# set redundant-power-system member vc-member-id priority priority-number
```

Where member is 0 for a switch that has never been configured in a Virtual Chassis.

## RELATED DOCUMENTATION

Understanding How Power Priority Is Determined and Set for Switches Connected to the EX Series Redundant Power System

# 12

PART

## Configuring Virtual Router Redundancy Protocol (VRRP)

---

Understanding How the VRRP Router Failover Mechanism Prevents Network  
Failures | 393

Configuring VRRP | 412

---

# Understanding How the VRRP Router Failover Mechanism Prevents Network Failures

## IN THIS CHAPTER

- [Understanding VRRP | 393](#)

## Understanding VRRP

### SUMMARY

Virtual Router Redundancy Protocol (VRRP) can be used to create virtual redundant routing platforms on a LAN, enabling traffic on the LAN to be routed without relying on a single routing platform.

### IN THIS SECTION

- [Understanding VRRP | 393](#)
- [VRRP and VRRP for IPv6 Overview | 398](#)
- [Understanding VRRP Between QFabric Systems | 398](#)
- [Junos OS Support for VRRPv3 | 403](#)
- [VRRP failover-delay Overview | 409](#)

## Understanding VRRP

For Ethernet, Fast Ethernet, Gigabit Ethernet, 10-Gigabit Ethernet, and logical interfaces, you can configure the Virtual Router Redundancy Protocol (VRRP) or VRRP for IPv6. VRRP enables hosts on a LAN to make use of redundant routing platforms on that LAN without requiring more than the static configuration of a single default route on the hosts. The VRRP routing platforms share the IP address corresponding to the default route configured on the hosts. At any time, one of the VRRP routing platforms is the primary (active) and the others are backups. If the primary routing platform fails, one of the backup routing platforms becomes the new primary routing platform, providing a virtual default routing platform and enabling traffic on the LAN to be routed without relying on a single routing platform. Using VRRP, a backup device can take over a failed default device within a few seconds. This is

done with minimum VRRP traffic and without any interaction with the hosts. Virtual Router Redundancy Protocol is not supported on management interfaces.

Devices running VRRP dynamically elect primary and backup devices. You can also force assignment of primary and backup devices using priorities from 1 through 255, with 255 being the highest priority. In VRRP operation, the default primary device sends advertisements to backup devices at regular intervals. The default interval is 1 second. If a backup device does not receive an advertisement for a set period, the backup device with the next highest priority takes over as primary and begins forwarding packets.

**NOTE:** Priority 255 cannot be set for routed VLAN interfaces (RVIs).

**NOTE:** To minimize network traffic, VRRP is designed in such a way that only the device that is acting as the primary sends out VRRP advertisements at any given point in time. The backup devices do not send any advertisement until and unless they take over primary role.

VRRP for IPv6 provides a much faster switchover to an alternate default router than IPv6 neighbor discovery procedures. Typical deployments use only one backup router.

**NOTE:** Do not confuse the VRRP primary and backup routing platforms with the primary and backup member switches of a *Virtual Chassis* configuration. The primary and backup members of a Virtual Chassis configuration compose a single host. In a VRRP topology, one host operates as the primary routing platform and another operates as the backup routing platform, as shown in [Figure 27 on page 397](#).

VRRP is defined in RFC 3768, *Virtual Router Redundancy Protocol*. VRRP for IPv6 is defined in draft-ietf-vrrp-ipv6-spec-08.txt, *Virtual Router Redundancy Protocol for IPv6*. See also draft-ietf-vrrp-unified-mib-06.txt, *Definitions of Managed Objects for the VRRP over IPv4 and IPv6*.

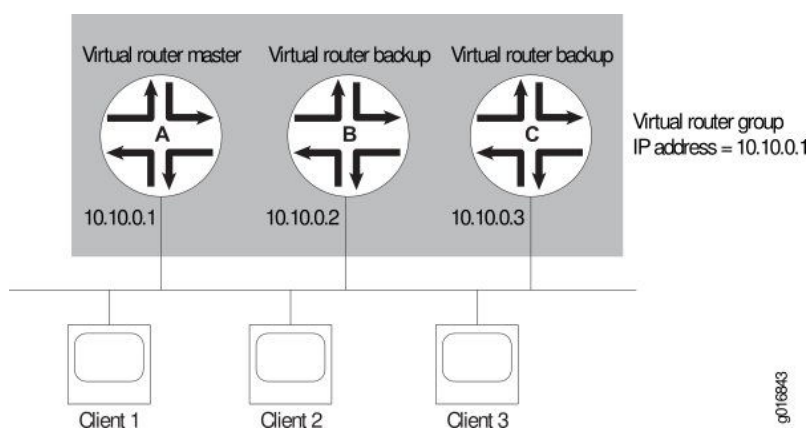
**NOTE:** Even though VRRP, as defined in RFC 3768, does not support authentication, the Junos OS implementation of VRRP supports authentication as defined in RFC 2338. This support is achieved through the backward compatibility options in RFC 3768.

**NOTE:** On EX2300 and EX3400 switches, the VRRP protocol must be configured with a Hello interval of 2 seconds or more with dead interval not less than 6 seconds to prevent flaps during

CPU intensive operations events such as routing engine switchover, interface flaps, and exhaustive data collection from the packet forwarding engine.

Figure 25 on page 395 illustrates a basic VRRP topology. In this example, Routers A, B, and C are running VRRP and together make up a virtual router. The IP address of this virtual router is 10.10.0.1 (the same address as the physical interface of Router A).

Figure 25: Basic VRRP



Because the virtual router uses the IP address of the physical interface of Router A, Router A is the primary VRRP router, while routers B and C function as backup VRRP routers. Clients 1 through 3 are configured with the default gateway IP address of 10.10.0.1. As the primary router, Router A forwards packets sent to its IP address. If the primary virtual router fails, the router configured with the higher priority becomes the primary virtual router and provides uninterrupted service for the LAN hosts. When Router A recovers, it becomes the primary virtual router again.

**NOTE:** In some cases, during an inherit session, there is a small time frame during which two routers are in Primary-Primary state. In such cases, the VRRP groups that inherit the state do send out VRRP advertisements every 120 seconds. So, it takes the routers up to 120 seconds to recover after moving to Primary-Backup state from Primary-Primary state.

ACX series routers can support up to 64 VRRP group entries. These can be a combination of IPv4 or IPv6 families. If either of the family (IPv4 or IPv6) is solely configured for VRRP, then 64 unique VRRP group identifiers are supported. If both IPv4 and IPv6 families share the same VRRP group, then only 32 unique VRRP identifiers are supported.

**NOTE:** ACX Series routers support VRRP version 3 for IPv6 addresses.

ACX5448 router supports RFC 3768 VRRP version 2 and RFC 5798 VRRP version 3. ACX5448 router also supports configuring VRRP over aggregated Ethernet and integrated routing and bridging (IRB) interfaces.

The following limitations apply while configuring VRRP on ACX5448 router:

- Configure a maximum of 16 VRRP groups.
- Interworking of VRRP version 2 and VRRP version 3 is not supported.
- VRRP delegate processing is not supported.
- VRRP version 2 authentication is not supported.

Figure 25 on page 395 illustrates a basic VRRP topology with EX Series switches. In this example, Switches A, B, and C are running VRRP and together they make up a virtual routing platform. The IP address of this virtual routing platform is 10.10.0.1 (the same address as the physical interface of Switch A).

**Figure 26: Basic VRRP on EX Series Switches**

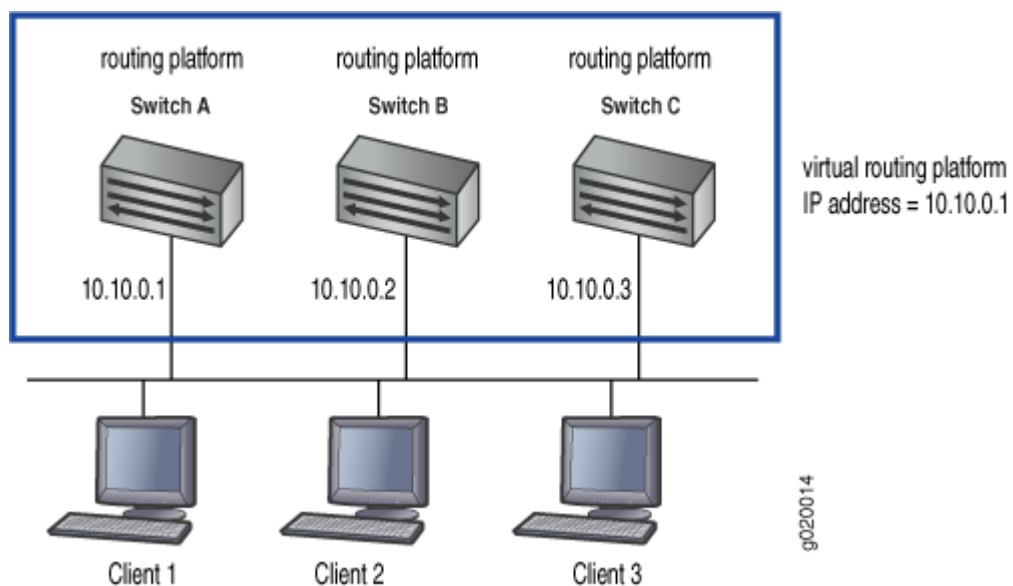
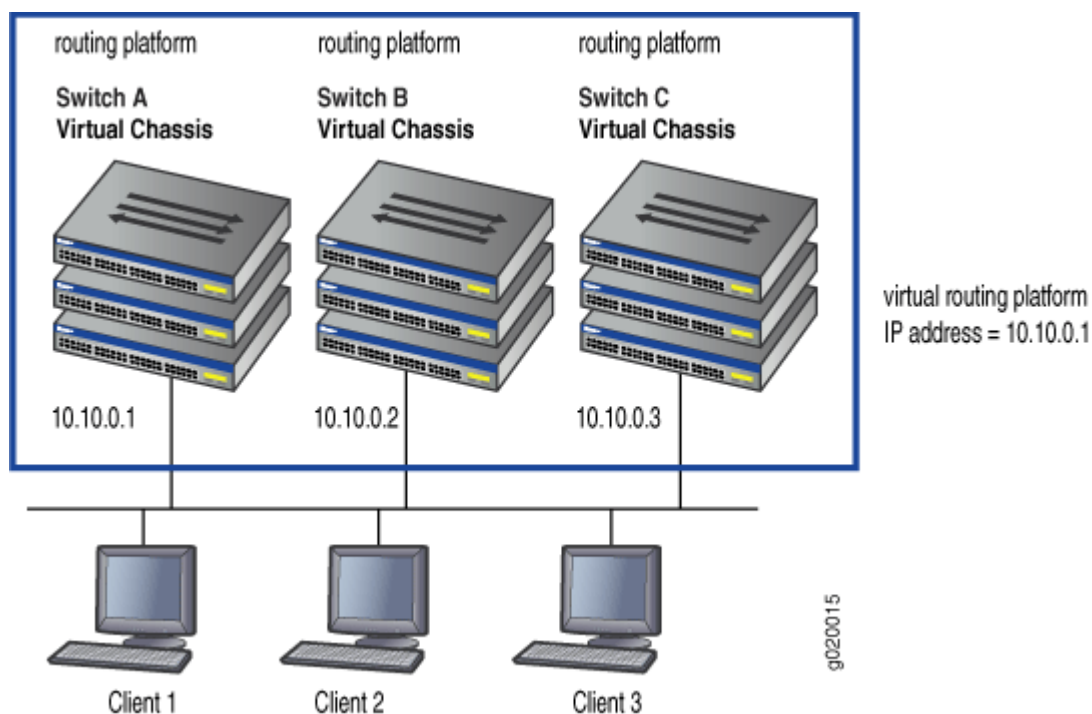


Figure 27 on page 397 illustrates a basic VRRP topology using Virtual Chassis configurations. Switch A, Switch B, and Switch C are each composed of multiple interconnected Juniper Networks EX4200 Ethernet Switches. Each Virtual Chassis configuration operates as a single switch, which is running

VRRP, and together they make up a virtual routing platform. The IP address of this virtual routing platform is 10.10.0.1 (the same address as the physical interface of Switch A).

**Figure 27: VRRP on Virtual Chassis Switches**



Because the virtual routing platform uses the IP address of the physical interface of Switch A, Switch A is the primary VRRP routing platform, while Switch B and Switch C function as backup VRRP routing platforms. Clients 1 through 3 are configured with the default gateway IP address of 10.10.0.1 as the primary router. Switch A, forwards packets sent to its IP address. If the primary routing platform fails, the switch configured with the higher priority becomes the primary virtual routing platform and provides uninterrupted service for the LAN hosts. When Switch A recovers, it becomes the primary virtual routing platform again.

## SEE ALSO

[Understanding High Availability Features on Juniper Networks Routers | 2](#)

[High Availability Features for EX Series Switches Overview | 9](#)

Junos OS Support for VRRPv3

Configuring Basic VRRP Support

Configuring VRRP

Configuring VRRP for IPv6 (CLI Procedure)

## VRRP and VRRP for IPv6 Overview

You can configure the Virtual Router Redundancy Protocol (VRRP) and VRRP for IPv6 for the following interfaces:

- Ethernet
- Fast Ethernet
- Tri-Rate Ethernet copper
- Gigabit Ethernet
- 10-Gigabit Ethernet LAN/WAN PIC
- Ethernet logical interfaces

VRRP and VRRP for IPv6 allow hosts on a LAN to make use of redundant routers on that LAN without requiring more than the static configuration of a single default route on the hosts. The VRRP routers share the IP address corresponding to the default route configured on the hosts. At any time, one of the VRRP routers is the primary (active) and the others are backups. If the primary fails, one of the backup routers becomes the new primary router, thus always providing a virtual default router and allowing traffic on the LAN to be routed without relying on a single router.

VRRP is defined in RFC 3768, *Virtual Router Redundancy Protocol*.

For VRRP and VRRP for IPv6 overview information, configuration guidelines, and statement summaries, see the [Junos OS High Availability User Guide](#).

### SEE ALSO

Configuring VRRP and VRRP for IPv6

[Ethernet Interfaces User Guide for Routing Devices](#)

## Understanding VRRP Between QFabric Systems

### IN THIS SECTION

- [VRRP Differences on QFabric Systems | 399](#)
- [Configuration Details | 399](#)



Juniper Networks QFabric systems support the Virtual Router Redundancy Protocol (VRRP). This topic covers:

### VRRP Differences on QFabric Systems

Configuring servers on your network with static routes to a default gateway minimizes configuration effort and complexity and reduces processing overhead. However, a failure of the default gateway normally results in a catastrophic event, isolating the servers. Using Virtual Router Redundancy Protocol (VRRP) enables you to dynamically provide alternative gateways for servers if the primary gateway fails.

Switches configured with VRRP share a virtual IP (VIP) address, which is the address you configure as the default route on the servers. In normal VRRP operation, one of the switches is the VRRP primary, meaning that it owns the VIP and is the active default gateway. The other devices are backups. The switches dynamically assign primary and backup roles based on priorities that you configure. If the primary fails, the backup switch with the highest priority becomes the primary and takes ownership of the VIP within a few seconds. This is done without any interaction with the servers.

You can configure two QFabric systems to participate in a VRRP configuration as if they were two standalone switches. However, in normal VRRP operation, only one system can be the primary for a given VRRP group at any one time, which means that only one system can act as a default gateway using the VIP configured for the group. When running VRRP over two QFabric systems, you might want both systems to simultaneously use the VIP to act as a gateway and forward traffic. To achieve this, you can configure a firewall filter to block the VRRP advertisement packets between the QFabric systems on the link between the two network Node groups. When you do this, both QFabric systems act as primary and forward traffic received by the VIP (which is the default gateway address that you configure on servers connected to both QFabric systems). If you use VMware's vMotion, this configuration allows virtual machines to transition between servers connected to the QFabric systems without updating their default gateway information. For example, a virtual machine running on a server connected to a QFabric system in data center A can transition to a server connected to a QFabric system in data center B without needing to resolve a new gateway IP address and MAC address because both QFabric systems use the same VIP.

**NOTE:** To use a firewall filter to block VRRP traffic, create a firewall term that matches traffic for protocol vrrp and discards that traffic.

### Configuration Details

Configuring a VRRP group across two QFabric systems is similar to configuring VRRP on two switches. The main differences are listed here:

- All the interfaces in both QFabric systems that participate in VRRP must be members of the same VLAN.

- You must create routed VLAN interfaces (RVIs) in that VLAN on both QFabric systems.
- The IP addresses that you assign to both RVIs must be in the same subnet.
- You must configure VRRP on the RVIs.
- Both RVIs must be members of the same VRRP group. This is what allows the two QFabric systems to share a virtual IP address.

The following tables list the elements of an example VRRP configuration running on two QFabric systems—QFabric system A and QFabric system B. This example is configured so that both QFabric systems act as the VRRP primary for VIP 10.1.1.50/24 and assumes that a firewall filter blocks the VRRP advertisements between the systems. [Table 11 on page 400](#) lists the required characteristics of the RVIs in the example configuration.

**NOTE:** Most of the configuration settings in the following tables would also apply in a traditional VRRP configuration. However, the advertisement interval and priority settings would need to be different (as noted).

**Table 11: RVIs on QFabric systems in example VRRP configuration**

RVI on QFabric System A	RVI on QFabric System B
vlan.100	vlan.200
Member of VLAN 100. (Note that the VLAN is the same on both QFabric systems.)	Member of VLAN 100
IP address 10.1.1.100/24	IP address 10.1.1.200/24
Member of VRRP group 500	Member of VRRP group 500
Virtual IP address 10.1.1.50/24	Virtual IP address 10.1.1.50/24

You must configure VRRP on the RVIs on both QFabric systems. [Table 12 on page 401](#) lists the elements of a sample VRRP configuration on each RVI. Note that with the exception of the priority, the parameters *must* be the same on both systems.

**Table 12: Sample VRRP configuration each RVI**

VRRP on RVI on QFabric System A	VRRP on RVI on QFabric System B
VRRP group 500	VRRP group 500
Virtual IP address 10.1.1.50/24	Virtual IP address 10.1.1.50/24
Advertisement interval 60 seconds. (In a normal VRRP configuration, you would set this interval to be much smaller, such as 1 second. However, in this configuration these packets are blocked by the firewall filter on the interface that connects to QFabric system B, so there is no need to send them frequently.)	Advertisement interval 60 seconds
Authentication type md5	Authentication type md5
Authentication key \$9\$1.4EIMVb2aGi4aZjkqzFRhSeWx7-wY2aM8	Authentication key \$9\$1.4EIMVb2aGi4aZjkqzFRhSeWx7-wY2aM8
Priority 254. (In a normal VRRP configuration, this value would be different on the two systems and the system with the higher value would be the primary. However, in this configuration both systems are acting as primary, so you do not have to configure different values.)	Priority 254

**NOTE:** Priority 255 is not supported for RVIs.

Table 13 on page 401 lists the all the interfaces on QFabric system A in the example configuration and identifies what they connect to.

**Table 13: Interfaces on QFabric system A. All interfaces are members of VLAN 100.**

VLAN 100 Interfaces on QFabric System A	Connects To
vlan.100	vlan.200

Network Node group interface QFA-NNG:xe-0/0/0	QFB-NNG:xe-0/0/0 on QFabric system B
Network Node group interface QFA-NNG:xe-0/0/1	Redundant server Node group interface QFA-RSNG:xe-0/0/0
Redundant server Node group interface QFA-RSNG:xe-0/0/0	Connects to a network Node group interface QFA-NNG:xe-0/0/1
Redundant server Node group interface QFA-RSNG:xe-0/0/1	LAN with servers running virtual machines

[Table 14 on page 402](#) lists all the interfaces on QFabric system B in the example configuration and identifies what they connect to.

**Table 14: Interfaces on QFabric system B. All interfaces are members of VLAN 100 (same as on QFabric system A).**

VLAN 100 Interfaces on QFabric System B	Connects To
vlan.200	vlan.100
Network Node group interface QFB-NNG:xe-0/0/0	QFA-NNG:xe-0/0/0 on QFabric system A
Network Node group interface QFB-NNG:xe-0/0/1	Redundant server Node group interface QFB-RSNG:xe-0/0/0
Redundant server Node group interface QFB-RSNG:xe-0/0/0	Connects to a network Node group interface QFB-NNG:xe-0/0/1
Redundant server Node group interface QFB-RSNG:xe-0/0/1	LAN with servers running virtual machines

## SEE ALSO

Understanding VRRP

[Configuring Basic VRRP Support for QFX](#)

Example: Configuring VRRP for Load Sharing

## Junos OS Support for VRRPv3

### IN THIS SECTION

- [Junos OS VRRP Support | 403](#)
- [IPv6 VRRP Checksum Behavioral Differences | 404](#)
- [VRRP Interoperability | 405](#)
- [Upgrading from VRRPv2 to VRRPv3 | 405](#)
- [Functionality of VRRPv3 Features | 408](#)

The advantage of using VRRPv3 is that VRRPv3 supports both IPv4 and IPv6 address families, whereas VRRPv2 supports only IPv4 addresses.

The following topics describe the Junos OS support for and interoperability of VRRPv3, as well as some differences between VRRPv3 and its precursors:

### Junos OS VRRP Support

In releases earlier than Release 12.2, Junos OS supported RFC 3768, *Virtual Router Redundancy Protocol (VRRP)* (for IPv4) and Internet draft draft-ietf-vrrp-ipv6-spec-08, *Virtual Router Redundancy Protocol for IPv6*.

VRRPv3 is not supported on routers that use releases earlier than Junos OS Release 12.2 and is also not supported for IPv6 on QFX10000 switches.

**NOTE:** VRRPv3 for IPv6 is supported on QFX10002-60C.

Starting with Release 12.2, Junos OS supports:

- RFC 3768, *Virtual Router Redundancy Protocol (VRRP)*
- RFC 5798, *Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6*
- RFC 6527, *Definitions of Managed Objects for Virtual Router Redundancy Protocol Version 3 (VRRPv3)*

**NOTE:** VRRP (for IPv6) on routers that use Junos OS Release 12.2 and later releases does not interoperate with VRRP (for IPv6) on routers with earlier Junos OS releases because of the differences in VRRP checksum calculations. See ["IPv6 VRRP Checksum Behavioral Differences" on page 404](#).

## IPv6 VRRP Checksum Behavioral Differences

You must consider the following checksum differences when enabling IPv6 VRRP networks:

- In releases earlier than Junos OS Release 12.2, when VRRP for IPv6 is configured, the VRRP checksum is calculated according to section 5.3.8 of RFC 3768, *Virtual Router Redundancy Protocol (VRRP)*.
- Starting with Junos OS Release 12.2, when VRRP for IPv6 is configured, irrespective of VRRPv3 being enabled or not, the VRRP checksum is calculated according to section 5.2.8 of RFC 5798, *Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6*.

Moreover, the pseudoheader is included only when calculating the IPv6 VRRP checksum. The pseudoheader is not included when calculating the IPv4 VRRP checksum.

To make the router with Junos OS Release 12.2 (or later Junos OS releases) IPv6 VRRP interoperate with the router running a Junos OS release earlier than Release 12.2, include the `checksum-without-pseudoheader` configuration statement at the `[edit protocols vrrp]` hierarchy level in the router running Junos OS Release 12.2 or later.

- The `tcpdump` utility in Junos OS Release 12.2 and later calculates the VRRP checksum according to RFC 5798, *Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6*. Therefore, when `tcpdump` parses IPv6 VRRP packets that are received from older Junos OS releases (earlier than Junos OS Release 12.2), the `bad vrrp cksum` message is displayed:

```
23:20:32.657328 Out
...
-----original packet-----
00:00:5e:00:02:03 > 33:33:00:00:00:12, ethertype IPv6 (0x86dd), length 94: (class
0xc0, hlim 255, next-header: VRRP (112), length: 40) fe80::224:dcff:fe47:57f > ff02::12:
VRRPv3-advertisement 40: vrid=3 prio=100 intvl=100(centisec) (bad vrrp cksum b4e2!)
addrs(2): fe80::200:5eff:fe00:3,2001:4818:f000:14::1
          3333 0000 0012 0000 5e00 0203 86dd 6c00
          0000 0028 70ff fe80 0000 0000 0000 0224
          dcff fe47 057f ff02 0000 0000 0000 0000
          0000 0000 0012 3103 6402 0064 b4e2 fe80
```

```
0000 0000 0000 0200 5eff fe00 0003 2001
4818 f000 0014 0000 0000 0000 0001
```

You can ignore this message because it does not indicate VRRP failure.

## VRRP Interoperability

In releases earlier than Junos OS Release 12.2, VRRP (IPv6) followed Internet draft draft-ietf-vrrp-ipv6-spec-08, but checksum was calculated based on RFC 3768 section 5.3.8. Starting with Release 12.2, VRRP (IPv6) follows RFC 5798 and checksum is calculated based on RFC 5798 section 5.2.8. Because of the differences in VRRP checksum calculations, IPv6 VRRP configured on routers that use Junos OS Release 12.2 and later releases does not interoperate with IPv6 VRRP configured in releases before Junos OS Release 12.2.

To make the router with Junos OS Release 12.2 (or later Junos OS releases) IPv6 VRRP interoperate with the router running Junos OS releases earlier than Release 12.2, include the `checksum-without-pseudoheader` configuration statement at the `[edit protocols vrrp]` hierarchy level in the router with Junos OS Release 12.2 or later.

Here are some general points to know about VRRP interoperability:

- If you have configured VRRPv3 (IPv4 or IPv6) on routers that use Junos OS Release 12.2 or later releases, it will not operate with routers that use Junos OS Release 12.1 or earlier releases. This is because only Junos OS Release 12.2 and later releases support VRRPv3.
- VRRP (IPv4 or IPv6) configured on routers that use Junos OS Release 12.2 and later releases interoperate with VRRP (IPv4 or IPv6) configured on routers that use releases earlier than Junos OS Release 12.2.
- VRRPv3 for IPv4 does not interoperate with the previous versions of VRRP. If VRRPv2 IPv4 advertisement packets are received by a router on which VRRPv3 is enabled, the router transitions itself to the backup state to avoid creating multiple primaries in the network. Due to this behavior, you must be cautious when enabling VRRPv3 on your existing VRRPv2 networks. See ["Upgrading from VRRPv2 to VRRPv3" on page 405](#) for more information.

**NOTE:** VRRPv3 advertisement packets are ignored by the routers on which previous versions of VRRP are configured.

## Upgrading from VRRPv2 to VRRPv3

Enable VRRPv3 in your network only if VRRPv3 can be enabled on all the VRRP routers in your network.

Enable VRRPv3 on your VRRPv2 network only when upgrading from VRRPv2 to VRRPv3. Mixing the two versions of VRRP is not a permanent solution.



**CAUTION:** VRRP version change is considered catastrophic and disruptive and may not be hitless. The packet loss duration depends on many factors, such as number of VRRP groups, the interfaces and FPCs involved, and the load of other services and protocols running on the router.

Upgrading from VRRPv2 to VRRPv3 must be done very carefully to avoid traffic loss, due to these considerations:

- It is not possible to configure VRRPv3 on all routers simultaneously.
- During the transition period, both VRRPv2 and VRRPv3 operate in the network.
- Changing VRRP versions restarts the state machine for all VRRP groups.
- VRRPv3 (for IPv4) routers default to the backup state when they get VRRPv2 (for IPv4) advertisement packets.
- VRRPv2 (for IPv4) packets are always given the highest priority.
- Checksum differences between VRRPv2 and VRRPv3 (for IPv6) can create multiple primary routers.

Disable VRRPv3 (for IPv6) on the backup routers while upgrading to avoid creating multiple primary routers.

[Table 15 on page 407](#) illustrates the steps and events that take place during a VRRPv2 to VRRPv3 transition. In [Table 15 on page 407](#), two VRRPv2 routers, R1 and R2, are configured in two groups, G1 and G2. Router R1 acts as the primary for G1, and Router R2 acts as the primary for G2.



**Table 15: VRRPv2 to VRRPv3 Transition Steps and Events**

1. Upgrade Router R1 with Junos OS Release 12.2 or later.
  - Router R2 becomes the primary for both G1 and G2.
  - After the upgrade of Router R1 is completed, Router R1 becomes the primary for G1.
  - Router R2 remains the primary for G2.
2. Upgrade Router R2 with Junos OS Release 12.2 or later.
  - Router R1 becomes the primary for both G1 and G2.
  - After the upgrade of Router R2 is completed, Router R2 becomes the primary for G2.
  - Router R1 remains the primary for G1.

For IPv4	For IPv6
<ol style="list-style-type: none"> <li>1. Enable VRRPv3 on Router R1.               <ul style="list-style-type: none"> <li>• Router R1 becomes the backup for both G1 and G2 because VRRPv2 IPv4 advertisement packets are given higher priority.</li> </ul> </li> <li>2. Enable VRRPv3 on Router R2.               <ul style="list-style-type: none"> <li>• Router R1 becomes the primary for G1.</li> <li>• Router R2 becomes the primary for G2.</li> </ul> </li> </ol>	<ol style="list-style-type: none"> <li>1. Deactivate G1 and G2 on Router R2.               <ul style="list-style-type: none"> <li>• G1 and G2 on Router R1 become primary.</li> </ul> </li> <li>2. Enable VRRPv3 on Router R1.               <ul style="list-style-type: none"> <li>• Router R1 becomes the primary for both G1 and G2.</li> </ul> </li> <li>3. Enable VRRPv3 on Router R2.</li> <li>4. Activate G1 and G2 on Router R2.               <ul style="list-style-type: none"> <li>• Router R2 becomes the primary for G2.</li> <li>• Router R1 remains the primary for G1.</li> </ul> </li> </ol>

When enabling VRRPv3, make sure that VRRPv3 is enabled on all the VRRP routers in the network because VRRPv3 (IPv4) does not interoperate with the previous versions of VRRP. For example, if VRRPv2 IPv4 advertisement packets are received by a router on which VRRPv3 is enabled, the router transitions itself to the backup state to avoid creating multiple primaries in the network.

You can enable VRRPv3 by configuring the **version-3** statement at the [edit protocols vrrp] hierarchy level (for IPv4 or IPv6 networks). Configure the same protocol version on all VRRP routers on the LAN.

## Functionality of VRRPv3 Features

Some Junos OS features differ in VRRPv3 from previous VRRP versions.

### VRRPv3 Authentication

When VRRPv3 (for IPv4) is enabled, it does not allow authentication.

- The `authentication-type` and `authentication-key` statements cannot be configured for any VRRP groups.
- You must use non-VRRP authentication.

### VRRPv3 Advertisement Intervals

VRRPv3 (for IPv4 and IPv6) advertisement intervals must be set with the `fast-interval` statement at the [edit interfaces *interface-name* unit 0 family inet address *ip-address* vrrp-group *group-name*] hierarchy level.

- Do not use the `advertise-interval` statement (for IPv4).
- Do not use the `inet6-advertise-interval` statement (for IPv6).

### Unified ISSU for VRRPv3

Design changes for VRRP unified in-service software upgrade (ISSU) are made in Junos OS Release 15.1 to achieve the following functionality:

- Maintain protocol adjacency with peer routers during unified ISSU. Protocol adjacency created on peer routers for the router undergoing unified ISSU should not flap, which means that VRRP on the remote peer router should not flap.
- Maintain interoperability with competitive or complementary equipment.
- Maintain interoperability with other Junos OS releases and other Juniper Network products.

The values of the following configurations (found at the [edit interfaces *interface-name* unit 0 family inet address *ip-address* vrrp-group *group-name*] hierarchy level) need to be kept at maximum values to support unified ISSU:

- On the primary router, the advertisement interval (the `fast-interval` statement) needs to be kept at 40950 milliseconds.
- On the backup router, the primary-down interval (the `advertisements-threshold` statement) needs to be kept at the largest threshold value.

This VRRP unified ISSU design only works for VRRPv3. It is not supported on VRRPv1 or VRRPv2. Other limitations include the following:

- The VRRP unified ISSU takes care of VRRP only. Packet forwarding is the responsibility of the Packet Forwarding Engine. The Packet Forwarding Engine unified ISSU should ensure uninterrupted traffic flow.
- VRRP is not affected by any change event during unified ISSU, for example, the switchover of the primary Routing Engine to backup or the backup Routing Engine to primary.
- VRRP might stop and discard any running timer before entering into unified ISSU. This means the expected action upon the expiry of the timer never takes place. However, you can defer unified ISSU until the expiration of all running timers.
- Unified ISSU at both local and remote routers cannot be done simultaneously.

## SEE ALSO

Understanding VRRP  
Configuring Basic VRRP Support

## VRRP failover-delay Overview

### IN THIS SECTION

- [When failover-delay Is Not Configured | 410](#)
- [When failover-delay Is Configured | 411](#)

Failover is a backup operational mode in which the functions of a network device are assumed by a secondary device when the primary device becomes unavailable because of a failure or a scheduled down time. Failover is typically an integral part of mission-critical systems that must be constantly available on the network.

VRRP does not support session synchronization between members. If the primary device fails, the backup device with the highest priority takes over as primary and will begin forwarding packets. Any existing sessions will be dropped on the backup device as out-of-state.

A fast failover requires a short delay. Thus, failover-delay configures the failover delay time, in milliseconds, for VRRP and VRRP for IPv6 operations. Junos OS supports a range of 50 through 100000 milliseconds for delay in failover time.

The VRRP process (vrrpd) running on the Routing Engine communicates a VRRP primary role change to the Packet Forwarding Engine for every VRRP session. Each VRRP group can trigger such

communication to update the Packet Forwarding Engine with its own state or the state inherited from an active VRRP group. To avoid overloading the Packet Forwarding Engine with such messages, you can configure a failover-delay to specify the delay between subsequent Routing Engine to Packet Forwarding Engine communications.

The Routing Engine communicates a VRRP primary role change to the Packet Forwarding Engine to facilitate necessary state change on the Packet Forwarding Engine, such as reprogramming of Packet Forwarding Engine hardware filters, VRRP sessions and so on. The following sections elaborate the Routing Engine to Packet Forwarding Engine communication in two scenarios:

### **When failover-delay Is Not Configured**

Without failover-delay configured, the sequence of events for VRRP sessions operated from the Routing Engine is as follows:

1. When the first VRRP group detected by the Routing Engine changes state, and the new state is primary, the Routing Engine generates appropriate VRRP announcement messages. The Packet Forwarding Engine is informed about the state change, so that hardware filters for that group are reprogrammed without delay. The new primary then sends gratuitous ARP message to the VRRP groups.
2. The delay in failover timer starts. By default, failover-delay timer is:
  - 500 milliseconds—when the configured VRRP announcement interval is less than 1 second.
  - 2 seconds—when the configured VRRP announcement interval is 1 second or more, and the total number of VRRP groups on the router is 255.
  - 10 seconds—when the configured VRRP announcement interval is 1 second or more, and the number of VRRP groups on the router is more than 255.
3. The Routing Engine performs one-by-one state change for subsequent VRRP groups. Every time there is a state change, and the new state for a particular VRRP group is primary, the Routing Engine generates appropriate VRRP announcement messages. However, communication toward the Packet Forwarding Engine is suppressed until the failover-delay timer expires.
4. After failover-delay timer expires, the Routing Engine sends message to the Packet Forwarding Engine about all VRRP groups that managed to change the state. As a consequence, hardware filters for those groups are reprogrammed, and for those groups whose new state is primary, gratuitous ARP messages are sent.

This process repeats until state transition for all VRRP groups is complete.

Thus, without configuring failover-delay, the full state transition (including states on the Routing Engine and the Packet Forwarding Engine) for the first VRRP group is performed immediately, while state transition on the Packet Forwarding Engine for remaining VRRP groups is delayed by at least 0.5-10

seconds, depending on the configured VRRP announcement timers and the number of VRRP groups. During this intermediate state, receiving traffic for VRRP groups for state changes that were not yet completed on the Packet Forwarding Engine might be dropped at the Packet Forwarding Engine level due to deferred reconfiguration of hardware filters.

**When failover-delay Is Configured**

When failover-delay is configured, the sequence of events for VRRP sessions operated from the Routing Engine is modified as follows:

1. The Routing Engine detects that some VRRP groups require a state change.
2. The failover-delay starts for the period configured. The allowed failover-delay timer range is 50 through 100000 milliseconds.
3. The Routing Engine performs one-by-one state change for the VRRP groups. Every time there is a state change, and the new state for a particular VRRP group is primary, the Routing Engine generates appropriate VRRP announcement messages. However, communication toward the Packet Forwarding Engine is suppressed until the failover-delay timer expires.
4. After failover-delay timer expires, the Routing Engine sends message to the Packet Forwarding Engine about all VRRP groups that managed to change the state. As a consequence, hardware filters for those groups are reprogrammed, and for those groups whose new state is primary, gratuitous ARP messages are sent.

This process repeats until state transition for all VRRP groups is complete.

Thus, when failover-delay is configured even the Packet Forwarding Engine state for the first VRRP group is deferred. However, the network operator has the advantage of configuring a failover-delay value that best suits the need of the network deployment to ensure minimal outage during VRRP state change.

failover-delay influences only VRRP sessions operated by the VRRP process (vrrpd) running on the Routing Engine. For VRRP sessions distributed to the Packet Forwarding Engine, failover-delay configuration has no effect.

**SEE ALSO**

| [failover-delay](#)

**Release History Table**

Release	Description
12.2	Junos OS Release 12.2 and later releases support VRRPv3.

# Configuring VRRP

## IN THIS CHAPTER

- [Configuring VRRP | 412](#)

## Configuring VRRP

### SUMMARY

Configure virtual router redundancy protocol (VRRP) on your device with the steps and examples below.

### IN THIS SECTION

- [Configuring Basic VRRP Support | 414](#)
- [Example: Configuring VRRP for IPv4 | 419](#)
- [Configuring VRRP and VRRP for IPv6 | 429](#)
- [Configuring VRRP for IPv6 \(CLI Procedure\) | 431](#)
- [Example: Configuring VRRP for IPv6 | 433](#)
- [Configuring VRRP Authentication \(IPv4 Only\) | 445](#)
- [Configuring VRRP Preemption and Hold Time | 446](#)
- [Configuring the Advertisement Interval for the VRRP Primary Router | 448](#)
- [Configuring the Startup Period for VRRP Operations | 451](#)
- [Configuring a Backup Router to Preempt the VRRP Primary Router | 451](#)
- [Configuring a Backup to Accept Packets Destined for the Virtual IP Address | 452](#)

- [Modifying the Preemption Hold-Time Value for the VRRP Primary Router | 453](#)
- [Configuring the Asymmetric Hold Time for VRRP Routers | 454](#)
- [Configuring Passive ARP Learning for Backup VRRP Routers | 454](#)
- [Configuring VRRP Route Tracking | 455](#)
- [Configuring a Logical Interface to Be Tracked for a VRRP Group | 457](#)
- [Configuring a Route to Be Tracked for a VRRP Group | 460](#)
- [Example: Configuring Multiple VRRP Owner Groups | 462](#)
- [Configuring Inheritance for a VRRP Group | 471](#)
- [Configuring an Interface to Accept All Packets Destined for the Virtual IP Address of a VRRP Group | 472](#)
- [Configuring the Silent Period to Avoid Alarms Due to Delay in Receiving VRRP Advertisement Packets | 473](#)
- [Enabling the Distributed Periodic Packet Management Process for VRRP | 474](#)
- [Improving the Convergence Time for VRRP | 476](#)
- [Configuring VRRP to Improve Convergence Time | 477](#)
- [Tracing VRRP Operations | 479](#)
- [Example: Configuring VRRP for Load Sharing | 480](#)
- [Troubleshooting VRRP | 489](#)

## Configuring Basic VRRP Support

**NOTE:** Starting in Junos OS Release 13.2, VRRP nonstop active routing (NSR) is enabled only when you configure the nonstop-routing statement at the [edit routing-options] or [edit logical system *logical-system-name* routing-options] hierarchy level.

The Virtual Router Redundancy Protocol (VRRP) groups multiple routing devices into a virtual router. At any time, one of the VRRP routing platforms is the primary (active) and the others are backups. If the primary fails, one of the backup routing platforms becomes the new primary router.

To configure basic VRRP support, configure VRRP groups on interfaces by including the `vrrp-group` statement:

```
vrrp-group group-id {
    priority number;
    virtual-address [ addresses ];
}
```

An interface can be a member of multiple VRRP groups. Within a VRRP group, the primary virtual router and the backup virtual router must be configured on different routing platforms.

You can include this statement at the following hierarchy level:

- [edit interfaces *interface-name* unit *logical-unit-number* family inet address *address*]

Mandatory parameters to configure a VRRP group are as follows (examples will follow):

1. Configure the group identifier (mandatory).
2. Configure the group:
  - Configure the virtual IP address of one or more virtual routers that are members of the VRRP group (mandatory).
  - Configure the virtual link-local address (VRRP for IPv6 only). The virtual link-local address is autogenerated when you enable VRRPv3 on the interface. You may explicitly define a virtual link-local address for each VRRP for the IPv6 group. The virtual link-local address must be on the same subnet as the physical interface address.
  - Configure the priority for the routing platform to become the primary virtual router (mandatory).

When choosing a VRRP group identifier, consider the following:



- In Junos OS releases prior to 17.3R1, you should not use the same VRRP group identifier on more than one subinterface on a given physical interface. This causes the VRRP virtual MAC address to be deleted from the packet forwarding engine, resulting in packet drops due to unknown MAC address. If your VRRP configuration needs to scale beyond 255 groups, consider configuring VRRP over an integrated routing and bridging (IRB) interface, since this restriction does not apply to IRB interfaces.
- Starting in Junos OS release 17.3R1, if network-services is configured in IP mode, don't configure the same VRRP group ID for multiple VRRP sessions on the same physical interface unless VRRP delegation is disabled. If multiple VRRP sessions are configured on the same physical interface with the same VRRP group ID while VRRP delegation is enabled, the other VRRP virtual IP addresses become unreachable when one of the logical interfaces is deleted.
- Starting in Junos OS release 17.3R1, if network-services is configured in enhanced-ip mode, you can use the same VRRP group ID for multiple VRRP sessions.

When configuring a virtual IP address, consider the following:

- The virtual IP address must be the same for all routing platforms in the VRRP group.
- If you configure a virtual IP address to be the same as the physical interface's address, the interface becomes the primary virtual router for the group. In this case, you must configure the priority to be 255, and you must configure preemption by including the `preempt` statement.
- If the virtual IP address you choose is not the same as the physical interface's address, you must ensure that the virtual IP address does not appear anywhere else in the routing platform's configuration. Verify that you do not use this address for other interfaces, for the IP address of a tunnel, or for the IP address of static ARP entries.
- You cannot configure a virtual IP address to be the same as the interface's address for an aggregated Ethernet interface. This configuration is not supported.
- For VRRP for IPv6, the `EUI-64` option cannot be used. In addition, the Duplicate Address Detection (DAD) process will not run for virtual IPv6 addresses.
- You cannot configure the same virtual IP address on interfaces that belong to the same logical system and routing instance combination. However, you can configure the same virtual IP address on interfaces that belong to different logical systems and routing instance combinations.

In determining what priority will make a given routing platform in a VRRP group a primary or backup, consider the following:

- You can force assignment of primary and backup routers using priorities from 1 through 255, where 255 is the highest priority.
- The priority value for the VRRP router that owns the IP address(es) associated with the virtual router must be 255.

- VRRP routers backing up a virtual router must use priority values from 1 through 254.
- The default priority value for VRRP routers backing up a virtual router is 100.
- Are there tracked interfaces or routes with priority costs?

The priority cost is the value associated with a tracked logical interface or route that is to be subtracted from the configured VRRP priority when the tracked logical interface or route goes down, forcing a new primary router election. The value of a priority cost can be from 1 through 254. The sum of the priority costs for all tracked logical interfaces or routes must be less than or equal to the configured priority of the VRRP group.

**NOTE:** Mixed tagging (configuring two logical interfaces on the same Ethernet port, one with single-tag framing and one with dual-tag framing) is supported only for interfaces on Gigabit Ethernet IQ2 and IQ PICs. If you include the `flexible-vlan-tagging` statement at the `[edit interfaces interface-name]` hierarchy level for a VRRP-enabled interface on a PIC that does not support mixed tagging, VRRP on that interface is disabled. In the output of the `show vrrp summary operational` command, the interface status is listed as Down.

**NOTE:** If you enable MAC source address filtering on an interface, you must include the virtual MAC address in the list of source MAC addresses that you specify in the `source-address-filter` statement at the `[edit interfaces interface-name]` hierarchy level. (For more information, see the [Junos OS Network Interfaces Library for Routing Devices](#).) MAC addresses ranging from 00:00:5e:00:01:00 through 00:00:5e:00:01:ff are reserved for VRRP, as defined in RFC 2378. The VRRP group number must be the decimal equivalent of the last hexadecimal byte of the virtual MAC address.

Here are specific examples of configuring a VRRP group.

### Configuring for VRRP IPv4 Groups

To configure basic VRRP (IPv4) groups on interfaces:

**NOTE:** You can also configure a VRRP IPv4 group at the `[edit logical-systems logical-system-name]` hierarchy level.

## 1. Configure the group identifier.

```
[edit interfaces interface-name unit logical-unit-number family inet address address]
user@device# set vrrp-group group-id
```

Assign a value from 0 through 255.

## 2. Configure the VRRP for IPv4 group:

- Configure the virtual IP address of one or more virtual routers that are members of the VRRP group.

```
[edit interfaces interface-name unit logical-unit-number family inet address address]
user@device# set vrrp-group group-id virtual-address [ addresses ]
```

Normally, you configure only one virtual IP address per group. However, you can configure up to eight addresses. Do not include a prefix length in a virtual IP address.

- Configure the priority for this routing platform to become the primary virtual router.

```
[edit interfaces interface-name unit logical-unit-number family inet address address]
user@device# set vrrp-group group-id priority number
```

Configure the value used to elect the primary virtual router in the VRRP group. It can be a number from 1 through 255. The default value for backup routers is 100. A larger value indicates a higher priority. The routing platform with the highest priority within the group becomes the primary router. Primary router sends periodic VRRP advertisement messages to each virtual routers. The backup routers do not attempt to preempt the primary router unless it has higher priority. This eliminates service disruption unless a more preferred path becomes available. It is possible to administratively prohibit all preemption attempts, with the exception of a VRRP router becoming primary router of any virtual router associated with addresses it owns.

## Configuring VRRP for IPv6 Groups

To configure basic VRRP for IPv6 groups on interfaces:

**NOTE:** You can also configure a VRRP IPv6 group at the [edit logical-systems *logical-system-name*] hierarchy level.

## 1. Configure the group identifier.

```
[edit interfaces interface-name unit logical-unit-number family inet6 address ipv6-address]
user@device# set vrrp-inet6-group group-id
```

Assign a value from 0 through 255.

## 2. Configure the VRRP for IPv6 group:

- Configure the virtual IP address of one or more virtual routers that are members of the VRRP group.

```
[edit interfaces interface-name unit logical-unit-number family inet6 address ipv6-address]
user@device# set vrrp-inet6-group group-id virtual-inet6-address [ ipv6-addresses ]
```

Normally, you configure only one virtual IP address per group. However, you can configure up to eight addresses. Do not include a prefix length in a virtual IP address.

- Configure the virtual link-local address.

```
[edit interfaces interface-name unit logical-unit-number family inet6 address ipv6-address]
user@device# set vrrp-inet6-group group-id virtual-link-local-address ipv6-address
```

You must explicitly define a virtual link-local address for each VRRP for IPv6 group. Otherwise, when you attempt to commit the configuration, the commit request fails. The virtual link-local address must be on the same subnet as the physical interface address.

- Configure the priority for this routing platform to become the primary virtual router.

```
[edit interfaces interface-name unit logical-unit-number family inet6 address ipv6-address]
user@device# set vrrp-inet6-group group-id priority number
```

Configure the value used to elect the primary virtual router in the VRRP group. It can be a number from 1 through 255. The default value for backup routers is 100. A larger value indicates a higher priority. The routing platform with the highest priority within the group becomes the primary router. If there are two or more backup routers with the same priority, the router that has the highest primary address becomes the primary.

## SEE ALSO

Configuring a Logical Interface to Be Tracked for a VRRP Group
Configuring a Route to Be Tracked for a VRRP Group
Junos OS Support for VRRPv3
Understanding VRRP
Configuring the Startup Period for VRRP Operations
Configuring VRRP Authentication (IPv4 Only)
Configuring the Advertisement Interval for the VRRP Primary Router
Configuring VRRP

## Example: Configuring VRRP for IPv4

### IN THIS SECTION

- [Requirements | 419](#)
- [Overview | 419](#)
- [Configuring VRRP | 420](#)
- [Verification | 426](#)

This example shows how to configure VRRP properties for IPv4.

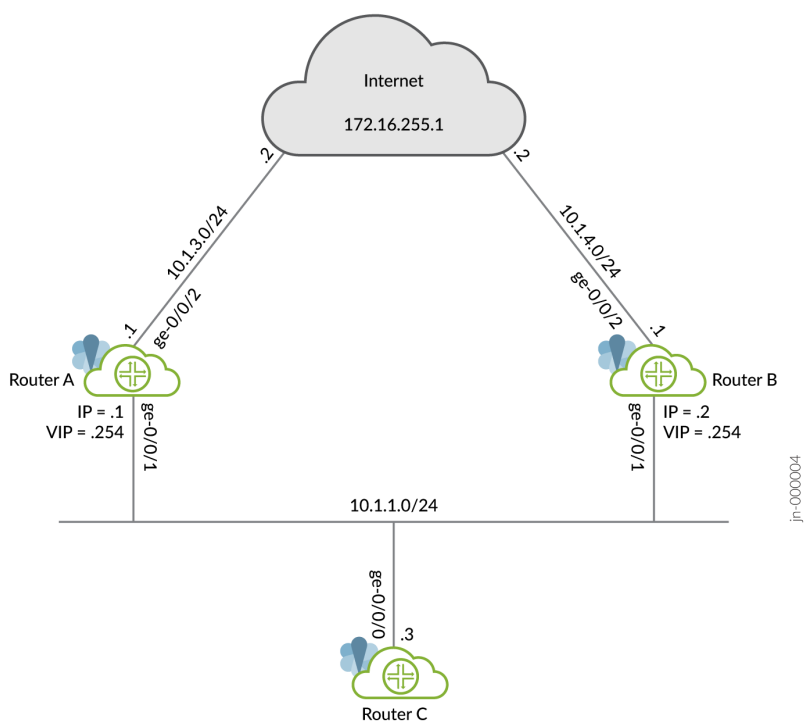
### Requirements

This example uses the following hardware and software components:

- Three routers
- Junos OS Release 11.3 or later
  - This example has been recently updated and revalidated on Junos OS Release 21.1R1.
  - For details on VRRP support for specific platform and Junos OS release combinations, see [Feature Explorer](#).

### Overview

This example uses a VRRP group, which has a virtual address for IPv4. Devices on the LAN use this virtual address as their default gateway. If the primary router fails, the backup router takes over for it.



## Configuring VRRP

### IN THIS SECTION

- [Configuring Router A | 421](#)
- [Configuring Router B | 423](#)
- [Configuring Router C | 425](#)

## Configuring Router A

### CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the [edit] hierarchy level.

```
set interfaces ge-0/0/1 unit 0 family inet address 10.1.1.1/24 vrrp-group 1 virtual-address 10.1.1.254
set interfaces ge-0/0/1 unit 0 family inet address 10.1.1.1/24 vrrp-group 1 priority 110
set interfaces ge-0/0/1 unit 0 family inet address 10.1.1.1/24 vrrp-group 1 accept-data
set interfaces ge-0/0/1 unit 0 family inet address 10.1.1.1/24 vrrp-group 1 track interface ge-0/0/2 priority-cost 20
set interfaces ge-0/0/2 unit 0 family inet address 10.1.3.1/24
set routing-options static route 0.0.0.0/0 next-hop 10.1.3.2
```

### Step-by-Step Procedure

To configure this example:

1. Configure the interfaces.

```
[edit]
user@routerA# set interfaces ge-0/0/1 unit 0 family inet address 10.1.1.1/24
user@routerA# set interfaces ge-0/0/2 unit 0 family inet address 10.1.3.1/24
```

2. Configure the IPv4 VRRP group identifier and the virtual IP address.

```
[edit interfaces ge-0/0/1 unit 0 family inet address 10.1.1.1/24]
user@routerA# set vrrp-group 1 virtual-address 10.1.1.254
```

3. Configure the priority for RouterA higher than RouterB to become the primary virtual router. RouterB is using the default priority of 100.

```
[edit interfaces ge-0/0/1 unit 0 family inet address 10.1.1.1/24]
user@routerA# set vrrp-group 1 priority 110
```

4. Configure track interface to track whether the interface connected to the Internet is up, down, or not present to change the priority of the VRRP group.

```
[edit interfaces ge-0/0/1 unit 0 family inet address 10.1.1.1/24]
user@routerA# set vrrp-group 1 track interface ge-0/0/2 priority-cost 20
```

5. Configure accept-data to enable the primary router to accept all packets destined for the virtual IP address.

```
[edit interfaces ge-0/0/1 unit 0 family inet address 10.1.1.1/24]
user@routerA# set vrrp-group 1 accept-data
```

6. Configure a static route for traffic to the Internet.

```
[edit]
user@routerA# set routing-options static route 0.0.0.0/0 next-hop 10.1.3.2
```

## Results

From configuration mode, confirm your configuration by entering the `show interfaces` and `show routing-options` commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
[edit]
user@routerA# show interfaces
ge-0/0/1 {
  unit 0 {
    family inet {
      address 10.1.1.1/24 {
        vrrp-group 1 {
          virtual-address 10.1.1.254;
          priority 110;
          accept-data;
          track {
            interface ge-0/0/2 {
              priority-cost 20;
            }
          }
        }
      }
    }
  }
}
```



```

    }
  }
}
}
}
ge-0/0/2 {
  unit 0 {
    family inet {
      address 10.1.3.1/24;
    }
  }
}
}

```

```

[edit]
user@routerA# show routing-options
static {
  route 0.0.0.0/0 next-hop 10.1.3.2;
}

```

If you are done configuring the device, enter `commit` from configuration mode.

### ***Configuring Router B***

#### **CLI Quick Configuration**

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the `[edit]` hierarchy level.

```

set interfaces ge-0/0/1 unit 0 family inet address 10.1.1.2/24 vrrp-group 1 virtual-address 10.1.1.254
set interfaces ge-0/0/1 unit 0 family inet address 10.1.1.2/24 vrrp-group 1 accept-data
set interfaces ge-0/0/2 unit 0 family inet address 10.1.4.1/24
set routing-options static route 0.0.0.0/0 next-hop 10.1.4.2

```

#### **Step-by-Step Procedure**

To configure this example:

## 1. Configure the interfaces.

```
[edit]
user@routerB# set interfaces ge-0/0/1 unit 0 family inet address 10.1.1.2/24
user@routerB# set interfaces ge-0/0/2 unit 0 family inet address 10.1.4.1/24
```

## 2. Configure the IPv4 VRRP group identifier and the virtual IP address.

```
[edit interfaces ge-0/0/1 unit 0 family inet address 10.1.1.2/24]
user@routerB# set vrrp-group 1 virtual-address 10.1.1.254
```

## 3. Configure accept-data to enable the backup router to accept all packets destined for the virtual IP address in the event the backup router becomes primary.

```
[edit interfaces ge-0/0/1 unit 0 family inet address 10.1.1.2/24]
user@routerB# set vrrp-group 1 accept-data
```

## 4. Configure a static route for traffic to the Internet.

```
[edit]
user@routerB# set routing-options static route 0.0.0.0/0 next-hop 10.1.4.2
```

## Results

From configuration mode, confirm your configuration by entering the `show interfaces` and `show routing-options` commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
[edit]
user@routerB# show interfaces
ge-0/0/1 {
  unit 0 {
    family inet {
      address 10.1.1.2/24 {
        vrrp-group 1 {
          virtual-address 10.1.1.254;
          accept-data;
```

```

    }
  }
}
}
}
ge-0/0/2 {
  unit 0 {
    family inet {
      address 10.1.4.1/24;
    }
  }
}
}

```

```

[edit]
user@routerB# show routing-options
static {
  route 0.0.0.0/0 next-hop 10.1.4.2;
}

```

If you are done configuring the device, enter `commit` from configuration mode.

### *Configuring Router C*

#### CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the `[edit]` hierarchy level.

```

set interfaces ge-0/0/0 unit 0 family inet address 10.1.1.3/24
set routing-options static route 0.0.0.0/0 next-hop 10.1.1.254

```

## Verification

### IN THIS SECTION

- [Verifying That VRRP Is Working on Router A | 426](#)
- [Verifying That VRRP Is Working on Router B | 427](#)
- [Verifying Router C Reaches the Internet Transiting Router A | 427](#)
- [Verifying Router B Becomes Primary for VRRP | 428](#)

### *Verifying That VRRP Is Working on Router A*

#### Purpose

Verify that VRRP is active on Router A and that its role in the VRRP group is correct.

#### Action

Use the following commands to verify that VRRP is active on Router A, that the router is primary for group 1 and the interface connected to the Internet is being tracked.

```
user@routerA> show vrrp
```

Interface	State	Group	VR state	VR Mode	Timer	Type	Address
ge-0/0/1.0	up	1	master	Active	A 0.779	lcl	10.1.1.1
						vip	10.1.1.254

```
user@routerA> show vrrp track
```

Track Int	State	Speed	VRRP Int	Group	VR State	Current prio
ge-0/0/2.0	up	1g	ge-0/0/1.0	1	master	110

#### Meaning

The `show vrrp` command displays fundamental information about the VRRP configuration. This output shows that the VRRP group is active and that this router has assumed the primary role. The `lcl` address is the physical address of the interface and the `vip` address is the virtual address shared by both routers.

The `Timer` value (A 0.779) indicates the remaining time (in seconds) in which this router expects to receive a VRRP advertisement from the other router.

### *Verifying That VRRP Is Working on Router B*

#### **Purpose**

Verify that VRRP is active on Router B and that its role in the VRRP group is correct.

#### **Action**

Use the following command to verify that VRRP is active on Router B and that the router is backup for group 1.

```
user@routerB> show vrrp
```

Interface	State	Group	VR state	VR Mode	Timer	Type	Address
ge-0/0/1.0	up	1	backup	Active	D 2.854	lcl	10.1.1.2
						vip	10.1.1.254
						mas	10.1.1.1

#### **Meaning**

The `show vrrp` command displays fundamental information about the VRRP configuration. This output shows that the VRRP group is active and that this router has assumed the backup role. The `lcl` address is the physical address of the interface and the `vip` address is the virtual address shared by both routers. The `Timer` value (D 2.854) indicates the remaining time (in seconds) in which this router expects to receive a VRRP advertisement from the other router.

### *Verifying Router C Reaches the Internet Transiting Router A*

#### **Purpose**

Verify connectivity to the Internet from Router C.

#### **Action**

Use the following commands to verify that Router C can reach the Internet.

```
user@routerC> ping 172.16.255.1 count 2
PING 172.16.255.1 (172.16.255.1): 56 data bytes
```

```
64 bytes from 172.16.255.1: icmp_seq=0 ttl=63 time=9.394 ms
64 bytes from 172.16.255.1: icmp_seq=1 ttl=63 time=30.536 ms

--- 172.16.255.1 ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max/stddev = 9.394/19.965/30.536/10.571 ms
```

```
user@routerC> traceroute 172.16.255.1
traceroute to 172.16.255.1 (172.16.255.1), 30 hops max, 52 byte packets
 1  10.1.1.1  3.781 ms  37.650 ms  3.877 ms
 2  172.16.255.1  31.581 ms  31.337 ms  27.170 ms
```

## Meaning

The ping command shows reachability to the Internet and the traceroute command shows that Router A is being transited.

### *Verifying Router B Becomes Primary for VRRP*

## Purpose

Verify that Router B becomes primary for VRRP when the interface between Router A and the Internet goes down.

## Action

Use the following commands to verify that Router B is primary and that Router C can reach the Internet transiting Router B.

```
user@routerA> show vrrp track detail
Tracked interface: ge-0/0/2.0
  State: down, Speed: 1g
  Incurred priority cost: 20
Tracking VRRP interface: ge-0/0/1.0, Group: 1
  VR State: backup
```

```
Current priority: 90, Configured priority: 110
Priority hold-time: disabled
```

```
user@routerB> show vrrp
```

Interface	State	Group	VR state	VR Mode	Timer	Type	Address
ge-0/0/1.0	up	1	master	Active	A 0.079	lcl	10.1.1.2
						vip	10.1.1.254

```
user@routerC> traceroute 172.16.255.1
```

```
traceroute to 172.16.255.1 (172.16.255.1), 30 hops max, 52 byte packets
```

```
1  10.1.1.2  6.532 ms  3.800 ms  2.958 ms
2  172.16.255.1  44.359 ms  16.268 ms  22.823 ms
```

## Meaning

The `show vrrp track detail` command shows the tracked interface is down on Router A, that the priority has dropped to 90, and that Router A is now the backup. The `show vrrp` command shows that Router B is now the primary for VRRP and the `traceroute` command shows that Router B is now being transited.

## SEE ALSO

[Understanding VRRP](#)

[Configuring VRRP](#)

[Configuring VRRP Route Tracking](#)

## Configuring VRRP and VRRP for IPv6

To configure VRRP or VRRP for IPv6, include the `vrrp-group` or `vrrp-inet6-group` statement, respectively. These statements are available at the following hierarchy levels:

- [edit interfaces *interface-name* unit *logical-unit-number* family inet address *address*]
- [edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number* family inet address *address*]

The VRRP and VRRP IPv6 configuration statements are as follows:

```
(vrrp-group | vrrp-inet-group) group-number {
    (accept-data | no-accept-data);
    advertise-interval seconds;
    authentication-key key;
    authentication-type authentication;
    fast-interval milliseconds;
    (preempt | no-preempt) {
        hold-time seconds;
    }
    priority-number number;
    track {
        priority-hold-time;
        interface interface-name {
            priority-cost priority;
            bandwidth-threshold bits-per-second {
                priority-cost;
            }
        }
    }
    virtual-address [ addresses ];
}
```

You can configure VRRP IPv6 with a global unicast address.

To trace VRRP and VRRP for IPv6 operations, include the `traceoptions` statement at the `[edit protocols vrrp]` hierarchy level:

```
[edit protocols vrrp]
traceoptions {
    file <filename> <files number <match regular-expression <microsecond-stamp> <size size>
    <world-readable | no-world-readable>;
    flag flag;
    no-remote-trace;
}
```

When there are multiple VRRP groups, there is a few seconds delay between the time the first gratuitous ARP is sent out and the rest of the gratuitous ARP are sent. Configuring `failover-delay` compensates for this delay. To configure the failover delay from 500 to 2000 milliseconds for VRRP and



VRRP for IPv6 operations, include the `failover-delay milliseconds` statement at the `[edit protocols vrrp]` hierarchy level:

```
[edit protocols vrrp]
failover-delay milliseconds;
```

To configure the startup period for VRRP and VRRP for IPv6 operations, include the `startup-silent-period` statement at the `[edit protocols vrrp]` hierarchy level:

```
[edit protocols vrrp]
startup-silent-period seconds;
```

To enable VRRPv3, set the `version-3` statement at the `[edit protocols vrrp]` hierarchy level:

```
[edit protocols vrrp]
version-3;
```

## SEE ALSO

[failover-delay | 1150](#)

[traceoptions](#)

[failover-delay | 1150](#)

[vrrp-group | 1192](#)

[VRRP and VRRP for IPv6 Overview](#)

[Ethernet Interfaces User Guide for Routing Devices](#)

## Configuring VRRP for IPv6 (CLI Procedure)

By configuring the Virtual Router Redundancy Protocol (VRRP) on EX Series switches, you can enable hosts on a LAN to make use of redundant routing platforms on that LAN without requiring more than the static configuration of a single default route on the hosts. You can configure VRRP for IPv6 on Gigabit Ethernet, 10-Gigabit Ethernet, and logical interfaces.

To configure VRRP for IPv6:

1. Configure VRRP group support on interfaces:

```
[edit interfaces interface-name unit logical-unit-number family inet6 address address]

user@switch# set vrrp-inet6-group group-id priority number virtual-inet6-address address
virtual-link-local-address ipv6-address
```

You must explicitly define a virtual link local address for each VRRP for IPv6 group. Otherwise, when you attempt to commit the configuration, the commit request fails. The virtual link local address must be on the same subnet as the physical interface address.

2. If you want to configure the priority order in which this switch functioning as a backup router becomes the primary router if the primary router becomes nonoperational, configure a priority for this switch:

```
[edit interfaces interface-name unit logical-unit-number family inet6 address address vrrp-
inet6-group group-id]

user@switch# set priority number
```

3. Specify the interval in milliseconds in which the primary router sends advertisement packets to the members of the VRRP group:

```
[edit interfaces interface-name unit logical-unit-number family inet6 address address vrrp-
inet6-group group-id]

user@switch# set inet6-advertise-interval milliseconds
```

4. By default, a higher-priority backup router preempts a lower-priority primary router.

- To explicitly enable the primary router to be preempted:

```
[edit interfaces interface-name unit logical-unit-number family inet6 address address vrrp-
inet6-group group-id]

user@switch# set preempt
```

- To prohibit a higher-priority backup router from preempting a lower priority primary router:

```
[edit interfaces interface-name unit logical-unit-number family inet6 address address vrrp-
inet6-group group-id]

user@switch# set no-preempt
```

## SEE ALSO

[show vrrp](#)

Understanding VRRP

## Example: Configuring VRRP for IPv6

### IN THIS SECTION

- [Requirements | 433](#)
- [Overview | 433](#)
- [Configuring VRRP | 434](#)
- [Verification | 441](#)

This example shows how to configure VRRP properties for IPv6.

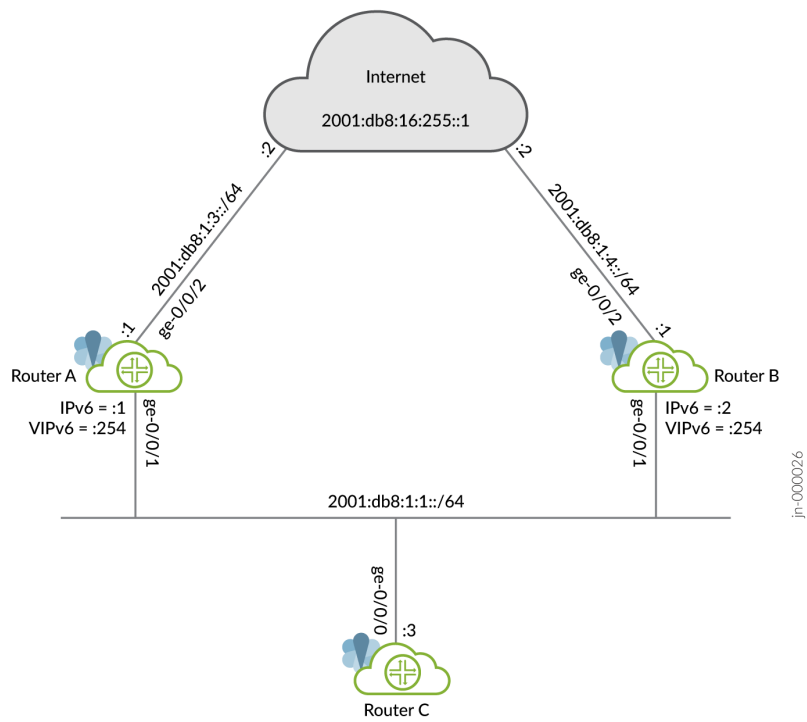
### Requirements

This example uses the following hardware and software components:

- Three routers
- Junos OS Release 11.3 or later
  - This example has been recently updated and revalidated on Junos OS Release 21.1R1.
  - For details on VRRP support for specific platform and Junos OS release combinations, see [Feature Explorer](#).

### Overview

This example uses a VRRP group, which has a virtual address for IPv6. Devices on the LAN use this virtual address as their default gateway. If the primary router fails, the backup router takes over for it.



## Configuring VRRP

### IN THIS SECTION

- [Configuring Router A | 435](#)
- [Configuring Router B | 438](#)
- [Configuring Router C | 441](#)

## Configuring Router A

### CLI Quick Configuration

To quickly configure this example, copy the following commands, paste into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the [edit] hierarchy level.

```
set interfaces ge-0/0/1 unit 0 family inet6 address 2001:db8:1:1::1/64 vrrp-inet6-group 1
virtual-inet6-address 2001:db8:1:1::254
set interfaces ge-0/0/1 unit 0 family inet6 address 2001:db8:1:1::1/64 vrrp-inet6-group 1
priority 110
set interfaces ge-0/0/1 unit 0 family inet6 address 2001:db8:1:1::1/64 vrrp-inet6-group 1 accept-
data
set interfaces ge-0/0/1 unit 0 family inet6 address 2001:db8:1:1::1/64 vrrp-inet6-group 1 track
interface ge-0/0/2 priority-cost 20
set interfaces ge-0/0/2 unit 0 family inet6 address 2001:db8:1:3::1/64
set protocols router-advertisement interface ge-0/0/1.0 virtual-router-only
set protocols router-advertisement interface ge-0/0/1.0 prefix 2001:db8:1:1::/64
set routing-options rib inet6.0 static route 0::0/0 next-hop 2001:db8:1:3::2
```

### Step-by-Step Procedure

To configure this example:

1. Configure the interfaces.

```
[edit]
user@routerA# set interfaces ge-0/0/1 unit 0 family inet6 address 2001:db8:1:1::1/64
user@routerA# set interfaces ge-0/0/2 unit 0 family inet6 address 2001:db8:1:3::1/64
```

2. Configure the IPv6 VRRP group identifier and the virtual IP address.

```
[edit interfaces ge-0/0/1 unit 0 family inet6 address 2001:db8:1:1::1/64]
user@routerA# set vrrp-inet6-group 1 virtual-inet6-address 2001:db8:1:1::254
```

3. Configure the priority for RouterA higher than RouterB to become the primary virtual router. RouterB is using the default priority of 100.

```
[edit interfaces ge-0/0/1 unit 0 family inet6 address 2001:db8:1:1::1/64]
user@routerA# set vrrp-inet6-group 1 priority 110
```

4. Configure track interface to track whether the interface connected to the Internet is up, down, or not present to change the priority of the VRRP group.

```
[edit interfaces ge-0/0/1 unit 0 family inet6 address 2001:db8:1:1::1/64]
user@routerA# set vrrp-inet6-group 1 track interface ge-0/0/2 priority-cost 20
```

5. Configure accept-data to enable the primary router to accept all packets destined for the virtual IP address.

```
[edit interfaces ge-0/0/1 unit 0 family inet6 address 2001:db8:1:1::1/64]
user@routerA# set vrrp-inet6-group 1 accept-data
```

6. Configure a static route for traffic to the Internet.

```
[edit]
user@routerA# set routing-options rib inet6.0 static route 0::0/0 next-hop 2001:db8:1:3::2
```

7. For VRRP for IPv6, you must configure the interface on which VRRP is configured to send IPv6 router advertisements for the VRRP group. When an interface receives an IPv6 router solicitation message, it sends an IPv6 router advertisement to all VRRP groups configured on it.

```
[edit protocols router-advertisement interface ge-0/0/1.0]
user@routerA# set prefix 2001:db8:1:1::/64
```

8. Configure router advertisements to be sent only for VRRP IPv6 groups configured on the interface if the groups are in the primary state.

```
[edit protocols router-advertisement interface ge-0/0/1.0]
user@routerA# set virtual-router-only
```

## Results

From configuration mode, confirm your configuration by entering the `show interfaces`, `show protocols router-advertisement` and `show routing-options` commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
[edit]
user@routerA# show interfaces
ge-0/0/1 {
  unit 0 {
    family inet6 {
      address 2001:db8:1:1::1/64 {
        vrrp-inet6-group 1 {
          virtual-inet6-address 2001:db8:1:1::254;
          priority 110;
          accept-data;
          track {
            interface ge-0/0/2 {
              priority-cost 20;
            }
          }
        }
      }
    }
  }
}
ge-0/0/2 {
  unit 0 {
    family inet6 {
      address 2001:db8:1:3::1/64;
    }
  }
}
```

```
[edit]
user@routerA# show protocols router-advertisement
interface ge-0/0/1.0 {
  virtual-router-only;
```

```
prefix 2001:db8:1:1::/64;
}
```

```
[edit]
user@routerA# show routing-options
rib inet6.0 {
    static {
        route 0::0/0 next-hop 2001:db8:1:3::2;
    }
}
```

If you are done configuring the device, enter `commit` from configuration mode.

### *Configuring Router B*

#### CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the `[edit]` hierarchy level.

```
set interfaces ge-0/0/1 unit 0 family inet6 address 2001:db8:1:1::2/64 vrrp-inet6-group 1
virtual-inet6-address 2001:db8:1:1::254
set interfaces ge-0/0/1 unit 0 family inet6 address 2001:db8:1:1::2/64 vrrp-inet6-group 1
priority 110
set interfaces ge-0/0/1 unit 0 family inet6 address 2001:db8:1:1::2/64 vrrp-inet6-group 1 accept-
data
set protocols router-advertisement interface ge-0/0/1.0 virtual-router-only
set protocols router-advertisement interface ge-0/0/1.0 prefix 2001:db8:1:1::/64
```

#### Step-by-Step Procedure

To configure this example:



1. Configure the interfaces.

```
[edit]
user@routerB# set interfaces ge-0/0/1 unit 0 family inet6 address 2001:db8:1:1::2/64
user@routerB# set interfaces ge-0/0/2 unit 0 family inet6 address 2001:db8:1:4::1/64
```

2. Configure the IPv6 VRRP group identifier and the virtual IP address.

```
[edit interfaces ge-0/0/1 unit 0 family inet6 address 2001:db8:1:1::2/64]
user@routerB# set vrrp-inet6-group 1 virtual-inet6-address 2001:db8:1:1::254
```

3. Configure accept-data to enable the backup router to accept all packets destined for the virtual IP address in the event the backup router becomes primary.

```
[edit interfaces ge-0/0/1 unit 0 family inet6 address 2001:db8:1:1::2/64]
user@routerB# set vrrp-inet6-group 1 accept-data
```

4. Configure a static route for traffic to the Internet.

```
[edit]
user@routerB# set routing-options rib inet6.0 static route 0::0/0 next-hop 2001:db8:1:4::2
```

5. Configure the interface on which VRRP is configured to send IPv6 router advertisements for the VRRP group. When an interface receives an IPv6 router solicitation message, it sends an IPv6 router advertisement to all VRRP groups configured on it.

```
[edit protocols router-advertisement interface ge-0/0/1.0]
user@routerB# set prefix 2001:db8:1:1::/64
```

6. Configure router advertisements to be sent only for VRRP IPv6 groups configured on the interface if the groups are in the primary state.

```
[edit protocols router-advertisement interface ge-0/0/1.0]
user@routerB# set virtual-router-only
```

## Results

From configuration mode, confirm your configuration by entering the `show interfaces`, `show protocols router-advertisement` and `show routing-options` commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
[edit]
user@routerB# show interfaces
ge-0/0/1 {
  unit 0 {
    family inet6 {
      address 2001:db8:1:1::2/64 {
        vrrp-inet6-group 1 {
          virtual-inet6-address 2001:db8:1:1::254;
          accept-data;
        }
      }
    }
  }
}
ge-0/0/2 {
  unit 0 {
    family inet6 {
      address 2001:db8:1:4::1/64;
    }
  }
}
```

```
[edit]
user@routerB# show protocols router-advertisement
interface ge-0/0/1.0 {
  virtual-router-only;
  prefix 2001:db8:1:1::/64;
}
```

```
[edit]
user@routerB# show routing-options
rib inet6.0 {
  static {
```

```

        route 0::0/0 next-hop 2001:db8:1:4::2;
    }
}

```

If you are done configuring the device, enter `commit` from configuration mode.

### *Configuring Router C*

## CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the [edit] hierarchy level.

```

set interfaces ge-0/0/0 unit 0 family inet6 address 2001:db8:1:1::3/64
set routing-options rib inet6.0 static route 0::0/0 next-hop 2001:db8:1:1::254

```

## Verification

### IN THIS SECTION

- [Verifying That VRRP Is Working on Router A | 441](#)
- [Verifying That VRRP Is Working on Router B | 442](#)
- [Verifying Router C Reaches the Internet Transiting Router A | 443](#)
- [Verifying Router B Becomes Primary for VRRP | 444](#)

### *Verifying That VRRP Is Working on Router A*

## Purpose

Verify that VRRP is active on Router A and that its role in the VRRP group is correct.

## Action

Use the following commands to verify that VRRP is active on Router A, that the router is primary for group 1 and the interface connected to the Internet is being tracked.

```
user@routerA> show vrrp
```

Interface	State	Group	VR state	VR Mode	Timer	Type	Address
ge-0/0/1.0	up	1	master	Active	A 0.690	lcl	2001:db8:1:1::1
						vip	fe80::200:5eff:fe00:201
						vip	2001:db8:1:1::254

```
user@routerA> show vrrp track
```

Track Int	State	Speed	VRRP Int	Group	VR State	Current prio
ge-0/0/2.0	up	1g	ge-0/0/1.0	1	master	110

## Meaning

The `show vrrp` command displays fundamental information about the VRRP configuration. This output shows that the VRRP group is active and that this router has assumed the primary role. The `lcl` address is the physical address of the interface and the `vip` address is the virtual address shared by both routers. The `Timer` value (A 0.690) indicates the remaining time (in seconds) in which this router expects to receive a VRRP advertisement from the other router.

### *Verifying That VRRP Is Working on Router B*

## Purpose

Verify that VRRP is active on Router B and that its role in the VRRP group is correct.

## Action

Use the following command to verify that VRRP is active on Router B and that the router is backup for group 1.

```
user@routerB> show vrrp
```

Interface	State	Group	VR state	VR Mode	Timer	Type	Address
ge-0/0/1.0	up	1	backup	Active	D 2.947	lcl	2001:db8:1:1::2
						vip	fe80::200:5eff:fe00:201

vip	2001:db8:1:1::254
mas	fe80::5668:a0ff:fe99:2d7d

## Meaning

The `show vrrp` command displays fundamental information about the VRRP configuration. This output shows that the VRRP group is active and that this router has assumed the backup role. The `lcl` address is the physical address of the interface and the `vip` address is the virtual address shared by both routers. The `Timer` value (0 2.947) indicates the remaining time (in seconds) in which this router expects to receive a VRRP advertisement from the other router.

## *Verifying Router C Reaches the Internet Transiting Router A*

### Purpose

Verify connectivity to the Internet from Router C.

### Action

Use the following commands to verify that Router C can reach the Internet.

```
user@routerC> ping 2001:db8:16:255::1 count 2
PING6(56=40+8+8 bytes) 2001:db8:1:1::3 --> 2001:db8:16:255::1
16 bytes from 2001:db8:16:255::1, icmp_seq=0 hlim=63 time=12.810 ms
16 bytes from 2001:db8:16:255::1, icmp_seq=1 hlim=63 time=30.139 ms

--- 2001:db8:16:255::1 ping6 statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max/std-dev = 12.810/21.474/30.139/8.664 ms
```

```
user@routerC> traceroute 2001:db8:16:255::1
traceroute6 to 2001:db8:16:255::1 (2001:db8:16:255::1) from 2001:db8:1:1::3, 64 hops max, 12
byte packets
 1  2001:db8:1:1::1 (2001:db8:1:1::1) 9.891 ms 32.353 ms 7.859 ms
 2  2001:db8:16:255::1 (2001:db8:16:255::1) 257.483 ms 19.877 ms 7.451 ms
```

## Meaning

The ping command shows reachability to the Internet and the traceroute command shows that Router A is being transited.

### *Verifying Router B Becomes Primary for VRRP*

## Purpose

Verify that Router B becomes primary for VRRP when the interface between Router A and the Internet goes down.

## Action

Use the following commands to verify that Router B is primary and that Router C can reach the Internet transiting Router B.

```
user@routerA> show vrrp track detail
Tracked interface: ge-0/0/2.0
State: down, Speed: 1g
Incurred priority cost: 20
Tracking VRRP interface: ge-0/0/1.0, Group: 1
VR State: backup
Current priority: 90, Configured priority: 110
Priority hold-time: disabled
```

```
user@routerB> show vrrp
```

Interface	State	Group	VR state	VR Mode	Timer	Type	Address
ge-0/0/1.0	up	1	master	Active	A 0.119	lcl	2001:db8:1:1::2
						vip	fe80::200:5eff:fe00:201
						vip	2001:db8:1:1::254

```
user@routerC> traceroute 2001:db8:16:255::1
traceroute6 to 2001:db8:16:255::1 (2001:db8:16:255::1) from 2001:db8:1:1::3, 64 hops max, 12
byte packets
 1 2001:db8:1:1::2 (2001:db8:1:1::2) 52.945 ms 344.383 ms 29.540 ms
 2 2001:db8:16:255::1 (2001:db8:16:255::1) 46.168 ms 24.744 ms 23.867 ms
```

## Meaning

The `show vrrp track detail` command shows the tracked interface is down on Router A, that the priority has dropped to 90, and that Router A is now the backup. The `show vrrp` command shows that Router B is now the primary for VRRP and the `traceroute` command shows that Router B is now being transited.

## SEE ALSO

[Understanding VRRP](#)

[Configuring VRRP](#)

[Configuring VRRP Route Tracking](#)

## Configuring VRRP Authentication (IPv4 Only)

VRRP (IPv4 only) protocol exchanges can be authenticated to guarantee that only trusted routing platforms participate in routing in an autonomous system (AS). By default, VRRP authentication is disabled. You can configure one of the following authentication methods. Each VRRP group must use the same method.

- Simple authentication—Uses a text password included in the transmitted packet. The receiving routing platform uses an authentication key (password) to verify the packet.
- Message Digest 5 (MD5) algorithm—Creates the authentication data field in the IP authentication header. This header is used to encapsulate the VRRP PDU. The receiving routing platform uses an authentication key (password) to verify the authenticity of the IP authentication header and VRRP PDU.

To enable authentication and specify an authentication method, include the `authentication-type` statement:

```
authentication-type authentication;
```

***authentication*** can be **simple** or **md5**. The authentication type must be the same for all routing platforms in the VRRP group.

You can include this statement at the following hierarchy levels:

- [edit interfaces *interface-name* unit *logical-unit-number* family inet address *address* vrrp-group *group-id*]
- [edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number* family inet address *address* vrrp-group *group-id*]

If you include the authentication-type statement, you can configure a key (password) on each interface by including the authentication-key statement:

```
authentication-key key;
```

**key** (the password) is an ASCII string. For simple authentication, it can be from 1 through 8 characters long. For MD5 authentication, it can be from 1 through 16 characters long. If you include spaces, enclose all characters in quotation marks (" "). The key must be the same for all routing platforms in the VRRP group.

You can include this statement at the following hierarchy levels:

- [edit interfaces *interface-name* unit *logical-unit-number* family inet address *address* vrrp-group *group-id*]
- [edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number* family inet address *address* vrrp-group *group-id*]

**NOTE:** When VRRPv3 is enabled, the authentication-type and authentication-key statements cannot be configured for any VRRP groups. Therefore, if authentication is required, you need to configure alternative non-VRRP authentication mechanisms.

## SEE ALSO

Understanding VRRP
Junos OS Support for VRRPv3
Configuring Basic VRRP Support
Configuring VRRP

## Configuring VRRP Preemption and Hold Time

### IN THIS SECTION

- [Configuring VRRP Preemption | 447](#)
- [Configuring the Preemption Hold Time | 447](#)



## Configuring VRRP Preemption

By default, a higher-priority VRRP backup switch preempts a lower-priority primary switch. To explicitly enable this behavior, include the following statement:

```
preempt;
```

To prohibit a higher-priority VRRP backup switch from preempting a lower-priority primary switch, include the following statement on the lower-priority switch:

```
no-preempt;
```

You can include these statements at the following hierarchy level:

- [edit interfaces *interface-name* unit *logical-unit-number* family inet address *address* vrrp-group *group-id*]

## Configuring the Preemption Hold Time

You can also configure a preemption hold time, which is the number of seconds a higher-priority backup router that has just started up waits before preempting the primary router. You might want to configure a hold time so that routing protocols or other Junos OS components converge before preemption occurs.

The hold time is applied only on startup. By default, the hold-time value is 0 seconds, meaning that preemption can occur immediately after the backup router starts up.

To modify the preemption hold-time value, configure the following statement:

```
hold-time seconds;
```

The hold time can be from 0 through 3600 seconds.

You can include this statement at the following hierarchy level:

- [edit interfaces *interface-name* unit *logical-unit-number* family inet address vrrp-group *group-id*] preempt

## RELATED DOCUMENTATION

---

Understanding VRRP

---

Configuring Basic VRRP Support

---

Example: Configuring VRRP for Load Sharing

---

## Configuring the Advertisement Interval for the VRRP Primary Router

### IN THIS SECTION

- [Modifying the Advertisement Interval in Seconds | 449](#)
- [Modifying the Advertisement Interval in Milliseconds | 449](#)

By default, the primary router sends VRRP advertisement packets every second to all members of the VRRP group. These packets indicate that the primary router is still operational. If the primary router fails or becomes unreachable, the backup router with the highest priority value becomes the new primary router.

You can modify the advertisement interval in seconds or in milliseconds. The interval must be the same for all routing platforms in the VRRP group.

For VRRP for IPv6, you must configure IPv6 router advertisements for the interface on which VRRP is configured to send IPv6 router advertisements for the VRRP group. To do so, include the `interface interface-name` statement at the `[edit protocols router-advertisement]` hierarchy level. (For information about this statement and guidelines, see the [Junos OS Routing Protocols Library for Routing Devices](#).) When an interface receives an IPv6 router solicitation message, it sends an IPv6 router advertisement to all VRRP groups configured on it. In the case of logical systems, IPv6 router advertisements are not sent to VRRP groups.

**NOTE:** The primary VRRP for an IPv6 router must respond to a router solicitation message with the virtual IP address of the router. However, when the `interface interface-name` statement is included at the `[edit protocols router-advertisement]` hierarchy level, the backup VRRP for an IPv6 router might send a response before the VRRP primary responds, so that the default route of the client is not set to the primary VRRP router's virtual IP address. To avoid this situation, include the `virtual-router-only` statement at the `[edit protocols router-advertisement interface interface-name]` hierarchy level. When this statement is included, router advertisements are sent only for VRRP IPv6 groups configured on the interface (if the groups are in the primary state). You must include this statement on both the primary and backup VRRP for IPv6 routers.

**NOTE:** In an EVPN network, including the `virtual-router-only` statement at the `[edit protocols router-advertisement interface interface-name]` hierarchy level restricts the router advertisements to be sent only for the link local virtual-gateway-address.

This topic contains the following sections:

### Modifying the Advertisement Interval in Seconds

To modify the time, in seconds, between the sending of VRRP advertisement packets, include the `advertise-interval` statement:

```
advertise-interval seconds;
```

The interval can be from 1 through 255 seconds.

You can include this statement at the following hierarchy levels:

- `[edit interfaces interface-name unit logical-unit-number family inet address address vrrp-group group-id]`
- `[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family inet address address vrrp-group group-id]`

**NOTE:** When VRRPv3 is enabled, the `advertise-interval` statement cannot be used to configure advertisement intervals. Instead, use the `fast-interval` statement to configure advertisement intervals.

### Modifying the Advertisement Interval in Milliseconds

To modify the time, in milliseconds, between the sending of VRRP advertisement packets, include the `fast-interval` statement:

```
fast-interval milliseconds;
```

The interval can be from 10 through 40,950 milliseconds.

You can include this statement at the following hierarchy levels:

- `[edit interfaces interface-name unit logical-unit-number family (inet | inet6) address address (vrrp-group | vrrp-inet6-group) group-id]`

- [edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number* family (inet | inet6) address *address* (vrrp-group | vrrp-inet6-group) *group-id*]

**NOTE:** In the VRRP PDU, Junos OS sets the advertisement interval to 0. When you configure VRRP with other vendors' routers, the fast-interval statement works correctly only when the other routers also have an advertisement interval set to 0 in the VRRP PDUs. Otherwise, Junos OS interprets other routers' settings as advertisement timer errors.

To modify the time, in milliseconds, between the sending of VRRP for IPv6 advertisement packets, include the inet6-advertise-interval statement:

```
inet6-advertise-interval ms;
```

The range of values is from 100 through 40,950 milliseconds (ms).

You can include this statement at the following hierarchy levels:

- [edit interfaces *interface-name* unit *logical-unit-number* family inet6 address *address* vrrp-inet6-group *group-id*]
- [edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number* family inet6 address *address* vrrp-inet6-group *group-id*]

**NOTE:** When VRRPv3 is enabled, the inet6-advertise-interval statement cannot be used to configure advertisement intervals. Instead, use the fast-interval statement to configure advertisement intervals.

## RELATED DOCUMENTATION

[Understanding VRRP](#)

[Junos OS Support for VRRPv3](#)

[Configuring Basic VRRP Support](#)

[Configuring a Backup Router to Preempt the VRRP Primary Router](#)

[Modifying the Preemption Hold-Time Value for the VRRP Primary Router](#)

[Configuring the Asymmetric Hold Time for VRRP Routers](#)

[Configuring the Silent Period to Avoid Alarms Due to Delay in Receiving VRRP Advertisement Packets](#)

## Configuring the Startup Period for VRRP Operations

To configure the startup period for VRRP operations, include the `startup-silent-period` statement at the `[edit protocols vrrp]` hierarchy level:

```
[edit protocols vrrp]
startup-silent-period seconds;
```

**NOTE:** During the silent startup period, the `show vrrp detail` command output shows a value of 0 for Master priority, and your own IP address for Master router. These values indicate that the Primary selection is not completed yet, and these values can be ignored.

### SEE ALSO

Understanding VRRP
Configuring Basic VRRP Support
Configuring VRRP Authentication (IPv4 Only)
Configuring VRRP

## Configuring a Backup Router to Preempt the VRRP Primary Router

By default, a higher-priority backup router preempts a lower-priority primary router. To explicitly enable the primary router to be preempted, include the `preempt` statement:

```
preempt;
```

You can include this statement at the following hierarchy levels:

- `[edit interfaces interface-name unit logical-unit-number family (inet | inet6) address address (vrrp-group | vrrp-inet6-group) group-id]`
- `[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family (Inet | inet6) address address (vrrp-group | vrrp-inet6-group) group-id]`

To prohibit a higher-priority backup router from preempting a lower-priority primary router, include the `no-preempt` statement:

```
no-preempt;
```

## SEE ALSO

Understanding VRRP

Configuring the Advertisement Interval for the VRRP Primary Router

Modifying the Preemption Hold-Time Value for the VRRP Primary Router

Configuring the Asymmetric Hold Time for VRRP Routers

Configuring VRRP

## Configuring a Backup to Accept Packets Destined for the Virtual IP Address

By default, a switch configured to be a VRRP backup but acting as the primary does not process packets sent to the virtual IP address—that is, packets in which the destination address is the virtual IP address. To configure a backup switch to process packets sent to the virtual IP address while it is acting as the primary, include the `accept-data` statement on the backup:

```
accept-data;
```

You can include this statement at the following hierarchy level:

- [edit interfaces *interface-name* unit *logical-unit-number* family inet address *address* vrrp-group] *group-id*

To explicitly prohibit the backup from accepting packets destined for the virtual IP address while acting as primary, include the `no-accept-data` statement:

```
no-accept-data;
```

If you include the `accept-data` statement, configure the connected hosts so that they:

- Process gratuitous ARP requests.
- Do not use packets other than ARP replies to update their ARP cache.

This statement is disabled by default. If you enable it, your configuration does not comply with RFC 3768.

To restrict incoming IP packets to ICMP only, you must configure firewall filters to accept only ICMP packets.

## SEE ALSO

Understanding VRRP

Configuring Basic VRRP Support

Example: Configuring VRRP for Load Sharing

## Modifying the Preemption Hold-Time Value for the VRRP Primary Router

The hold time is the maximum number of seconds that can elapse before a higher-priority backup router preempts the primary router. You might want to configure a hold time so that all Junos OS components converge before preemption.

By default, the hold-time value is 0 seconds. A value of 0 means that preemption can occur immediately after the backup router comes online. Note that the hold time is counted from the time the backup router comes online. The hold time is only valid when the VRRP router is just coming online.

To modify the preemption hold-time value, include the `hold-time` statement:

```
hold-time seconds;
```

The hold time can be from 0 through 3600 seconds.

You can include this statement at the following hierarchy levels:

- [edit interfaces *interface-name* unit *logical-unit-number* family (inet | inet6) address *address* (vrrp-group | vrrp-inet6-group) *group-id* preempt]
- [edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number* family (inet | inet6) address *address* (vrrp-group | vrrp-inet6-group) *group-id* preempt]

## SEE ALSO

Configuring the Advertisement Interval for the VRRP Primary Router

Configuring a Backup Router to Preempt the VRRP Primary Router

Configuring the Asymmetric Hold Time for VRRP Routers

Configuring VRRP

## Configuring the Asymmetric Hold Time for VRRP Routers

In Junos OS Release 9.5 and later, the `asymmetric-hold-time` statement at the `[edit protocols vrrp]` hierarchy level enables you to configure a VRRP primary router to switch over to the backup router immediately—that is, without waiting for the priority hold time to expire—when a tracked interface or route goes down or when the bandwidth of a tracked interface decreases. Such events can cause an immediate reduction in the priority based on the configured priority cost for the event, and trigger a primary-role election.

However, when the tracked route or interface comes up again, or when the bandwidth for a tracked interface increases, the backup (original primary) router waits for the hold time to expire before it updates the priority and initiates the switchover if the priority is higher than the priority for the VRRP primary (original backup) router.

If the `asymmetric-hold-time` statement is not configured, the VRRP primary waits for the hold time to expire before it initiates a switchover when a tracked route goes down or when the bandwidth of a tracked interface decreases.

### Example: Configuring Asymmetric Hold Time

```
[edit]
user@host# set protocols vrrp asymmetric-hold-time
[edit]
user@host# show protocols vrrp
asymmetric-hold-time;
```

### SEE ALSO

- Configuring the Advertisement Interval for the VRRP Primary Router
- Configuring a Backup Router to Preempt the VRRP Primary Router
- Modifying the Preemption Hold-Time Value for the VRRP Primary Router
- Configuring VRRP

## Configuring Passive ARP Learning for Backup VRRP Routers

By default, the backup VRRP router drops ARP requests for the VRRP-IP to VRRP-MAC address translation. This means that the backup router does not learn the ARP (IP-to-MAC address) mappings for the hosts sending the requests. When it detects a failure of the primary router and transitions to become the new primary router, the backup router must re-learn all the entries that were present in the ARP cache of the primary router. In environments with many directly attached hosts, such as metro



Ethernet environments, the number of ARP entries to learn can be high. This can cause a significant transition delay, during which the traffic transmitted to some of the hosts might be dropped.

Passive ARP learning enables the ARP cache in the backup router to hold approximately the same contents as the ARP cache in the primary router, thus preventing the problem of learning ARP entries in a burst. To enable passive ARP learning, include the `passive-learning` statement at the `[edit system arp]` hierarchy level:

```
[edit system arp]
passive-learning;
```

We recommend setting passive learning on both the backup and primary VRRP routers. Doing so prevents the need to manually intervene when the primary router becomes the backup router. While a router is operating as the primary router, the passive learning configuration has no operational impact. The configuration takes effect only when the router is operating as a backup router.

For information about configuring gratuitous ARP and the ARP aging timer, see the [Junos OS Administration Library for Routing Devices](#).

## SEE ALSO

| Understanding VRRP

## Configuring VRRP Route Tracking

Configure Routers R1 and R2 to run VRRP. Configure static routes and a policy for exporting the static routes on Router R3. The VRRP routing instances on R2 track the routes that are advertised by R3.

### On Router R1

```
[edit interfaces]
ge-1/0/3 {
  unit 0 {
    vlan-id 1;
    family inet {
      address 200.100.50.2/24 {
        vrrp-group 0 {
          virtual-address 200.100.50.101;
          priority 195;
        }
      }
    }
  }
}
```

```

    }
}

```

## On Router R2

```

[edit interfaces]
ge-1/0/1 {
    unit 0 {
        vlan-id 1;
        family inet {
            address 200.100.50.1/24 {
                vrrp-group 0 {
                    virtual-address 200.100.50.101;
                    priority 200;
                    track {
                        route 59.0.58.153/32 routing-instance default priority-cost 5;
                        route 59.0.58.154/32 routing-instance default priority-cost 5;
                        route 59.0.58.155/32 routing-instance default priority-cost 5;
                    }
                }
            }
        }
    }
}

```

## On Router R3

```

[edit]
policy-options {
    policy-statement static-policy {
        term term1 {
            then accept;
        }
    }
}
protocols {
    ospf {
        export static-policy;
        reference-bandwidth 4g;
        area 0.0.0.0 {
            interface all;

```

```

        interface fxp0.0 {
            disable;
        }
    }
}
routing-options {
    static {
        route 59.0.0.153/32 next-hop 45.45.45.46;
        route 59.0.0.154/32 next-hop 45.45.45.46;
        route 59.0.0.155/32 next-hop 45.45.45.46;
    }
}

```

## SEE ALSO

Understanding VRRP

Configuring a Route to Be Tracked for a VRRP Group

Configuring VRRP

*Example: Configuring VRRP for IPv6*

## Configuring a Logical Interface to Be Tracked for a VRRP Group

VRRP can track whether a logical interface is up, down, or not present, and can also dynamically change the priority of the VRRP group based on the state of the tracked logical interface, triggering a new primary router election. VRRP can also track the operational speed of a logical interface and dynamically update the priority of the VRRP group when the speed crosses a configured threshold.

When interface tracking is enabled, you cannot configure a priority of 255 (a priority of 255 designates the primary router). For each VRRP group, you can track up to 10 logical interfaces.

To configure a logical interface to be tracked, include the following statements:

```

track {
    interface interface-name {
        bandwidth-threshold bits-per-second priority-cost priority;
        priority-cost priority;
    }
}

```

```
priority-hold-time seconds;
}
```

```
interface et-0/0/0 {
    priority-cost 30;
}
```

You can include these statements at the following hierarchy levels:

- [edit interfaces *interface-name* unit *logical-unit-number* family inet address *address* *vrrp-group* *group-id*]
- [edit interfaces *interface-name* unit *logical-unit-number* family inet6 address *address* *vrrp-inet6-group* *group-id*]
- [edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number* family inet address *address* *vrrp-group* *group-id*]
- [edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number* family inet6 address *address* *vrrp-inet6-group* *group-id*]

The interface specified is the interface to be tracked for the VRRP group. The priority hold time is the minimum length of time that must elapse between dynamic priority changes. A tracking event, such as an interface state change (up or down) or a change in bandwidth, triggers one of the following responses:

- The first tracking event initiates the priority hold timer, and also initializes the pending priority based on the current priority and the priority cost. However, the current priority remains unchanged.
- A tracking event or a manual configuration change that occurs while the priority hold timer is on triggers a pending priority update. However, the current priority remains unchanged.

This ensures that Junos OS does not initiate primary role elections every time a tracked interface flaps.

When the priority hold time expires, the current priority inherits the value from the pending priority, and the pending priority ceases.

**NOTE:** If you have configured *asymmetric-hold-time*, VRRP does not wait for the priority hold time to expire before initiating primary role elections if a tracked interface fails (state changes from up to down), or if the available bandwidth for a tracked interface decreases. For more information about *asymmetric-hold-time*, see *Configuring the Asymmetric Hold Time for VRRP Routers*.

There are two *priority-cost* statements that show at this hierarchy level. The *bandwidth-threshold* statement specifies a threshold for the tracked interface. When the bandwidth of the tracked interface drops

below the configured bandwidth threshold value, the VRRP group uses the bandwidth threshold priority cost. You can track up to five bandwidth threshold statements for each tracked interface. Just under the interface statement there is a priority-cost statement that gives the value to subtract from priority when the interface is down.

The sum of the priority costs for all tracked logical interfaces must be less than or equal to the configured priority of the VRRP group. If you are tracking more than one interface, the router applies the sum of the priority costs for the tracked interfaces (at most, only one priority cost for each tracked interface) to the VRRP group priority.

Prior to Junos OS Release 15.1, an adjusted priority could not be zero. If the difference between the priority costs and the configured priority of the VRRP group was zero, the adjusted priority would become 1.

**NOTE:** In Junos OS Release 15.1 and later, an adjusted priority can be zero.

The priority value zero (0) indicates that the current primary router has stopped participating in VRRP. Such a priority value is used to trigger one of the backup routers to quickly transition to the primary router without having to wait for the current primary to time out.

If you are tracking more than one interface, the router applies the sum of the priority costs for the tracked interfaces (at most, only one priority cost for each tracked interface) to the VRRP group priority. However, the interface priority cost and bandwidth threshold priority cost values for each VRRP group are not cumulative. The router uses only one priority cost to a tracked interface as indicated in [Table 16 on page 459](#).

**Table 16: Interface State and Priority Cost Usage**

Tracked Interface State	Priority Cost Usage
Down	$\text{priority-cost } \textit{priority}$
Not down; media speed below one or more bandwidth thresholds	Priority cost of the lowest applicable bandwidth threshold

You must configure an interface priority cost only if you have configured no bandwidth thresholds. If you have not configured an interface priority cost value, and the interface is down, the interface uses the bandwidth threshold priority cost value of the lowest bandwidth threshold.

## SEE ALSO

Understanding VRRP

Configuring a Route to Be Tracked for a VRRP Group

Configuring VRRP

## Configuring a Route to Be Tracked for a VRRP Group

VRRP can track whether a route is reachable (that is, the route exists in the routing table of the routing instance included in the configuration) and dynamically change the priority of the VRRP group based on the reachability of the tracked route, triggering a new primary router election.

To configure a route to be tracked, include the following statements:

```
track {
    priority-hold-time seconds;
    route prefix/prefix-length routing-instance instance-name priority-cost priority;
}
```

You can include these statements at the following hierarchy levels:

- [edit interfaces *interface-name* unit *logical-unit-number* family inet address *address* *vrrp-group* *group-id*]
- [edit interfaces *interface-name* unit *logical-unit-number* family inet6 address *address* *vrrp-inet6-group* *group-id*]
- [edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number* family inet address *address* *vrrp-group* *group-id*]
- [edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number* family inet6 address *address* *vrrp-inet6-group* *group-id*]

The route prefix specified is the route to be tracked for the VRRP group. The priority hold time is the minimum length of time that must elapse between dynamic priority changes. A route tracking event, such as adding a route to or removing a route from the routing table, might trigger one or more of the following:

- The first tracking event initiates the priority hold timer, and also initializes the pending priority based on the current priority and the priority cost. However, the current priority remains unchanged.
- A tracking event or a manual configuration change that occurs while the priority hold timer is on triggers a pending priority update. However, the current priority remains unchanged.

When the priority hold time expires, the current priority inherits the value from the pending priority, and the pending priority ceases.

This ensures that Junos OS does not initiate primary role elections every time a tracked route flaps.

**NOTE:** If you have configured `asymmetric-hold-time`, VRRP does not wait for the priority hold time to expire before initiating primary role elections if a tracked route is removed from the routing table. For more information about `asymmetric-hold-time`, see [Configuring the Asymmetric Hold Time for VRRP Routers](#).

The routing instance is the routing instance in which the route is to be tracked. If the route is in the default, or global, routing instance, specify the instance name as `default`.

**NOTE:** Tracking a route that belongs to a routing instance from a different logical system is not supported.

The priority cost is the value to be subtracted from the configured VRRP priority when the tracked route goes down, forcing a new primary router election. The value can be from 1 through 254.

The sum of the priority costs for all tracked routes must be less than or equal to the configured priority of the VRRP group. If you are tracking more than one route, the router applies the sum of the priority costs for the tracked routes (at most, only one priority cost for each tracked route) to the VRRP group priority.

Prior to Junos OS Release 15.1, an adjusted priority could not be zero. If the difference between the priority costs and the configured priority of the VRRP group was zero, the adjusted priority would become 1.

**NOTE:** In Junos OS Release 15.1 and later, an adjusted priority can be zero.

The priority value zero (0) indicates that the current primary router has stopped participating in VRRP. Such a priority value is used to trigger one of the backup routers to quickly transition to the primary router without having to wait for the current primary to time out.

## SEE ALSO

---

[Understanding VRRP](#)

---

[Configuring a Logical Interface to Be Tracked for a VRRP Group](#)

---

[Configuring VRRP Route Tracking](#)

## Example: Configuring Multiple VRRP Owner Groups

### IN THIS SECTION

- [Requirements | 462](#)
- [Overview | 462](#)
- [Configuration | 462](#)
- [Verification | 471](#)

These examples show how to configure multiple virtual router redundancy protocol (VRRP) IPv4 and IPv6 owner groups.

### Requirements

This example uses the following hardware and software components:

- A EX-Series, M-Series, MX-Series, or T-Series router.
- Junos OS release 12.3 or later

### Overview

Multiple VRRP owner groups allows users to reuse interface address identifiers (IFAs) as virtual IP addresses (VIPs). You can configure multiple IPv4 owner groups, multiple IPv6 owner groups, or a mix of IPv4 and IPv6 owner groups.

### Configuration

### IN THIS SECTION

- [CLI Quick Configuration | 463](#)
- [Configuring multiple IPv4 owner groups | 464](#)
- [Configuring multiple IPv6 owner groups | 465](#)
- [Configuring multiple IPv4 and IPv6 owner groups | 466](#)
- [Results | 468](#)



### *CLI Quick Configuration*

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the [edit] hierarchy level.

#### Multiple IPv4 owner groups

```
edit interfaces ge-1/0/0 unit 0 family inet
set address 10.0.0.2/24 vrrp-group 2 virtual-address 10.0.0.4 accept-data
set address 20.0.0.2/24 vrrp-group 3 virtual-address 20.0.0.2 priority 255
set address 30.0.0.2/24 vrrp-group 4 virtual-address 30.0.0.2 priority 255
```

#### Multiple IPv6 owner groups

```
edit interfaces ge-1/0/0 unit 0 family inet6
set address 2001:4818:f000:20::1/64 vrrp-inet6-group 1 virtual-inet6-address 2001:4818:f000:20::1
set address 2001:4818:f000:20::1/64 vrrp-inet6-group 1 virtual-link-local-address
fe80:4818:f000:20::1
set address 2001:4818:f000:20::1/64 vrrp-inet6-group 1 priority 255
set address fe80:4818:f000:13::2/64
set address 2001:1000:f000:20::1/64 vrrp-inet6-group 2 virtual-inet6-address
2001:1000:f000:20::1
set address 2001:1000:f000:20::1/64 vrrp-inet6-group 2 virtual-link-local-address
fe80:1000:f000:20::1
set address 2001:1000:f000:20::1/64 vrrp-inet6-group 2 priority 255
set address 2001:2000:f000:20::1/64 vrrp-inet6-group 3 virtual-inet6-address 2001:2000:f000:20::2
set address 2001:2000:f000:20::1/64 vrrp-inet6-group 3 virtual-link-local-address
fe80:2000:f000:20::2
set address 2001:2000:f000:20::1/64 vrrp-inet6-group 3 priority 250
```

#### Multiple IPv4 and IPv6 owner groups

```
edit interfaces ge-1/0/0 unit 0
set family inet address 10.0.0.1/24 vrrp-group 5 virtual-address 10.0.0.1
set family inet address 10.0.0.1/24 vrrp-group 5 priority 255
set family inet6 address 2001:4818:f000:20::1/64 vrrp-inet6-group 1 virtual-inet6-address
2001:4818:f000:20::1
set family inet6 address 2001:4818:f000:20::1/64 vrrp-inet6-group 1 virtual-link-local-address
fe80:4818:f000:20::1
set family inet6 address 2001:4818:f000:20::1/64 vrrp-inet6-group 1 priority 255
```

```

set family inet6 address 2001:1000:f000:20::1/64 vrrp-inet6-group 2 virtual-inet6-address
2001:1000:f000:20::1
set family inet6 address 2001:1000:f000:20::1/64 vrrp-inet6-group 2 virtual-link-local-address
fe80:1000:f000:20::1
set family inet6 address 2001:1000:f000:20::1/64 vrrp-inet6-group 2 priority 255
set family inet6 address 2001:2000:f000:20::1/64 vrrp-inet6-group 3 virtual-inet6-address
2001:2000:f000:20::2
set family inet6 address 2001:2000:f000:20::1/64 vrrp-inet6-group 3 virtual-link-local-address
fe80:2000:f000:20::2
set family inet6 address 2001:2000:f000:20::1/64 vrrp-inet6-group 3 priority 250

```

### *Configuring multiple IPv4 owner groups*

#### **Step-by-Step Procedure**

To configure multiple IPv4 owner groups:

1. Create an IPv4 interface on the device

```

[edit]
user@host# edit interfaces ge-1/0/0 unit 0 family inet

```

2. Configure the first IPv4 owner group

```

[edit interfaces ge-1/0/0 unit 0 family inet]
user@host# set address 10.0.0.2/24 vrrp-group 2 virtual-address 10.0.0.4 accept-data

```

3. Configure the second IPv4 owner group

```

[edit interfaces ge-1/0/0 unit 0 family inet]
user@host# set address 20.0.0.2/24 vrrp-group 3 virtual-address 20.0.0.2 priority 255

```

4. Configure the third IPv4 owner group

```

[edit interfaces ge-1/0/0 unit 0 family inet]
user@host# set address 30.0.0.2/24 vrrp-group 4 virtual-address 30.0.0.2 priority 255

```

## *Configuring multiple IPv6 owner groups*

### Step-by-Step Procedure

To configure multiple IPv6 owner groups:

1. Create an IPv6 interface on the device

```
[edit]
user@host# edit interfaces ge-1/0/0 unit 0 family inet6
```

2. Configure the inet6 address for the first IPv6 owner group

```
[edit interfaces ge-1/0/0 unit 0 family inet6]
user@host# set address 2001:4818:f000:20::1/64 vrrp-inet6-group 1 virtual-inet6-address
2001:4818:f000:20::1
```

- 3.

```
[edit interfaces ge-1/0/0 unit 0 family inet6]
user@host# set address 2001:4818:f000:20::1/64 vrrp-inet6-group 1 virtual-link-local-
address fe80:4818:f000:20::1
```

- 4.

```
[edit interfaces ge-1/0/0 unit 0 family inet6]
user@host# set address 2001:4818:f000:20::1/64 vrrp-inet6-group 1 priority 255
```

- 5.

```
[edit interfaces ge-1/0/0 unit 0 family inet6]
user@host# set family inet6 address 2001:1000:f000:20::1/64 vrrp-inet6-group 2 virtual-
inet6-address 2001:1000:f000:20::1
```

- 6.

```
[edit interfaces ge-1/0/0 unit 0 family inet6]
user@host# set family inet6 address 2001:1000:f000:20::1/64 vrrp-inet6-group 2 virtual-link-
local-address fe80:1000:f000:20::1
```

7.

```
[edit interfaces ge-1/0/0 unit 0 family inet6]
user@host# set family inet6 address 2001:1000:f000:20::1/64 vrrp-inet6-group 2 priority 255
```

8.

```
[edit interfaces ge-1/0/0 unit 0 family inet6]
user@host# set family inet6 address 2001:2000:f000:20::1/64 vrrp-inet6-group 3 virtual-
inet6-address 2001:2000:f000:20::2
```

9.

```
[edit interfaces ge-1/0/0 unit 0 family inet6]
user@host# set family inet6 address 2001:2000:f000:20::1/64 vrrp-inet6-group 3 virtual-link-
local-address fe80:2000:f000:20::2
```

10.

```
[edit interfaces ge-1/0/0 unit 0 family inet6]
user@host# set address 2001:2000:f000:20::1/64 vrrp-inet6-group 3 priority 250
```

### *Configuring multiple IPv4 and IPv6 owner groups*

#### **Step-by-Step Procedure**

To configure multiple IPv4 and IPv6 owner groups:

1. Create an interface on the device

```
[edit]
user@host# edit interfaces ge-1/0/0 unit 0
```

2. Configure the family inet address and virtual address for the IPv4 owner group

```
[edit interfaces ge-1/0/0 unit 0]
user@host# set family inet address 10.0.0.1/24 vrrp-group 5 virtual-address 10.0.0.1
```

3. Set the priority of the IPv4 owner group to 255

```
[edit interfaces ge-1/0/0 unit 0]  
set family inet address 10.0.0.1/24 vrrp-group 5 priority 255
```

4. Configure the inet6 address for the first IPv6 owner group

```
[edit interfaces ge-1/0/0 unit 0]  
set family inet6 address 2001:4818:f000:20::1/64 vrrp-inet6-group 1 virtual-inet6-address  
2001:4818:f000:20::1
```

5. Set the virtual link local address for the first IPv6 owner group

```
[edit interfaces ge-1/0/0 unit 0]  
set family inet6 address 2001:4818:f000:20::1/64 vrrp-inet6-group 1 virtual-link-local-  
address fe80:4818:f000:20::1
```

6. Set the first IPv6 owner group's priority to 255

```
[edit interfaces ge-1/0/0 unit 0]  
set family inet6 address 2001:4818:f000:20::1/64 vrrp-inet6-group 1 priority 255
```

7. Configure the inet6 address for the second IPv6 owner group

```
[edit interfaces ge-1/0/0 unit 0]  
set family inet6 address 2001:1000:f000:20::1/64 vrrp-inet6-group 2 virtual-inet6-address  
2001:1000:f000:20::1
```

8. Set the virtual link local address for the second IPv6 owner group

```
[edit interfaces ge-1/0/0 unit 0]  
set family inet6 address 2001:1000:f000:20::1/64 vrrp-inet6-group 2 virtual-link-local-  
address fe80:1000:f000:20::1
```

9. Set the second IPv6 owner group's priority to 255

```
[edit interfaces ge-1/0/0 unit 0]
set family inet6 address 2001:1000:f000:20::1/64 vrrp-inet6-group 2 priority 255
```

10. Configure the inet6 address for the third IPv6 owner group

```
[edit interfaces ge-1/0/0 unit 0]
set family inet6 address 2001:2000:f000:20::1/64 vrrp-inet6-group 3 virtual-inet6-address
2001:2000:f000:20::2
```

11. Set the virtual link local address for the third IPv6 owner group

```
[edit interfaces ge-1/0/0 unit 0]
set family inet6 address 2001:2000:f000:20::1/64 vrrp-inet6-group 3 virtual-link-local-
address fe80:2000:f000:20::2
```

12. Set the third IPv6 owner group's priority to 250

```
[edit interfaces ge-1/0/0 unit 0]
set family inet6 address 2001:2000:f000:20::1/64 vrrp-inet6-group 3 priority 250
```

## Results

### Multiple IPv4 owner groups

```
[edit interfaces]
ge-1/0/0
  unit 0 {
    family inet {
      address 10.0.0.2/24 {
        vrrp-group 2 {
          virtual-address 10.0.0.4;
          accept-data;
        }
      }
      address 20.0.0.2/24 {
```

```

        vrrp-group 3 {
            virtual-address 20.0.0.2;
            priority 255;
        }
    }
    address 30.0.0.2/24 {
        vrrp-group 4 {
            virtual-address 30.0.0.2;
            priority 255;
        }
    }
}

```

### Multiple IPv6 owner groups

```

[edit interfaces]
ge-1/0/0
  unit 0 {
    family inet6 {
      address 2001:4818:f000:20::1/64 {
        vrrp-inet6-group 1 {
          virtual-inet6-address 2001:4818:f000:20::1;
          virtual-link-local-address fe80:4818:f000:20::1;
          priority 255;
        }
      }
      address fe80:4818:f000:13::2/64;
      address 2001:1000:f000:20::1/64 {
        vrrp-inet6-group 2 {
          virtual-inet6-address 2001:1000:f000:20::1;
          virtual-link-local-address fe80:1000:f000:20::1;
          priority 255;
        }
      }
      address 2001:2000:f000:20::1/64 {
        vrrp-inet6-group 3 {
          virtual-inet6-address 2001:2000:f000:20::2;
          virtual-link-local-address fe80:2000:f000:20::2;
          priority 250;
        }
      }
    }
  }
}

```

```

    }
}

```

### Multiple IPv4 and IPv6 owner groups

```

[edit interfaces]
ge-1/0/0
  unit 0 {
    family inet {
      address 10.0.0.1/24 {
        vrrp-group 5 {
          virtual-address 10.0.0.1;
          priority 255;
        }
      }
    }
    family inet6 {
      address 2001:4818:f000:20::1/64 {
        vrrp-inet6-group 1 {
          virtual-inet6-address 2001:4818:f000:20::1;
          virtual-link-local-address fe80:4818:f000:20::1;
          priority 255;
        }
      }
      address 2001:1000:f000:20::1/64 {
        vrrp-inet6-group 2 {
          virtual-inet6-address 2001:1000:f000:20::1;
          virtual-link-local-address fe80:1000:f000:20::1;
          priority 255;
        }
      }
      address 2001:2000:f000:20::1/64 {
        vrrp-inet6-group 3 {
          virtual-inet6-address 2001:2000:f000:20::2;
          virtual-link-local-address fe80:2000:f000:20::2;
          priority 250;
        }
      }
    }
  }
}

```



## Verification

To verify the configuration, run the `show interfaces ge-1/0/0` command, or use whichever name you assigned to the interface.

## SEE ALSO

Tracing VRRP Operations

Configuring Inheritance for a VRRP Group

## Configuring Inheritance for a VRRP Group

Junos OS enables you to configure VRRP groups on the various subnets of a VLAN to inherit the state and configuration of one of the groups, which is known as the *active VRRP group*. When the **vrrp-inherit-from** configuration statement is included in the configuration, only the active VRRP group, from which the other VRRP groups are inheriting the state, sends out frequent VRRP advertisements, and processes incoming VRRP advertisements. The groups that are inheriting the state do not process any incoming VRRP advertisement because the state is always inherited from the active VRRP group. However, the groups that are inheriting the state do send out VRRP advertisements once every 2 to 3 minutes to facilitate MAC address learning on the switches placed between the VRRP routers.

If the `vrrp-inherit-from` statement is not configured, each of the VRRP primary groups in the various subnets on the VLAN sends out separate VRRP advertisements and adds to the traffic on the VLAN.

To configure inheritance for a VRRP group, include the `vrrp-inherit-from` statement at the `[edit interfaces interface-name unit logical-unit-number family inet address address vrrp-group group-id]` hierarchy level.

```
[edit interfaces interface-name unit logical-unit-number family inet address address vrrp-group
group-id]
vrrp-inherit-from vrrp-group;
```

When you configure a group to inherit a state from another group, the inheriting groups and the active group must be on the same physical interface and logical system. However, the groups do not need to necessarily be on the same routing instance (as was in Junos OS releases earlier than 9.6), VLAN, or logical interface.

When you include the `vrrp-inherit-from` statement for a VRRP group, the VRRP group inherits the following parameters from the active group:

- **advertise-interval**
- **authentication-key**

- **authentication-type**
- **fast-interval**
- **preempt | no-preempt**
- **priority**
- **track interfaces**
- **track route**

However, you can configure the `accept-data | no-accept-data` statement for the group to specify whether the interface should accept packets destined for the virtual IP address.

## SEE ALSO

| Understanding VRRP

## Configuring an Interface to Accept All Packets Destined for the Virtual IP Address of a VRRP Group

In VRRP implementations where the router acting as the primary router is not the IP address owner—the IP address owner is the router that has the interface whose actual IP address is used as the virtual router's IP address (virtual IP address)—the primary router accepts only the ARP packets from the packets that are sent to the virtual IP address. Junos OS enables you to override this limitation with the help of the **accept-data** configuration. When the `accept-data` statement is included in the configuration, the primary router accepts all packets sent to the virtual IP address even when the primary router is not the IP address owner.

**NOTE:** If the primary router is the IP address owner or has its priority set to 255, the primary router, by default, accepts all packets addressed to the virtual IP address. In such cases, the **accept-data** configuration is not required.

To configure an interface to accept all packets sent to the virtual IP address, include the `accept-data` statement:

```
accept-data;
```

You can include this statement at the following hierarchy levels:

- [edit interfaces *interface-name* unit *logical-unit-number* family (inet | inet6) address *address* (vrrp-group | vrrp-inet6-group) *group-id*]
- [edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number* family (Inet | inet6) address *address* (vrrp-group | vrrp-inet6-group) *group-id*]

To prevent a primary router that is the IP address owner or has its priority set to 255 from accepting packets other than the ARP packets addressed to the virtual IP address, include the `no-accept-data` statement:

```
no-accept-data;
```

#### NOTE:

- If you want to restrict the incoming IP packets to ICMP packets only, you must configure firewall filters to accept only ICMP packets.
- If you include the `accept-data` statement, your routing platform configuration does not comply with RFC 3768 (see section 6.4.3 of RFC 3768, *Virtual Router Redundancy Protocol (VRRP)*).

## SEE ALSO

Understanding VRRP

Configuring VRRP

## Configuring the Silent Period to Avoid Alarms Due to Delay in Receiving VRRP Advertisement Packets

The silent period starts when the interface state is changed from down to up. During this period, the Primary Down Event is ignored. Configure the silent period interval to avoid alarms caused by the delay or interruption of the incoming VRRP advertisement packets during the interface startup phase.

To configure the silent period interval that the Primary Down Event timer ignores, include the `startup-silent-period` statement at the [edit protocols vrrp] hierarchy level:

```
[edit protocols vrrp]
startup-silent-period seconds;
```

**NOTE:** During the silent startup period, the `show vrrp detail` command output shows a value of 0 for Master priority and your IP address for Master router. These values indicate that the Primary selection is not completed yet, and these values can be ignored.

When you have configured **startup-silent-period**, the Primary Down Event is ignored until the **startup-silent-period** expires.

For example, configure a VRRP group, *vrrp-group1*, with an advertise interval of 1 second, startup silent period of 10 seconds, and an interface *interface1* with a priority less than 255.

When *interface1* transitions from down to up:

- The *vrrp-group1* group moves to the backup state, and starts the Primary Down Event timer (3 seconds; three times the value of the advertise interval, which is 1 second in this case).
- If no VRRP PDU is received during the 3-second period, the **startup-silent-period** (10 seconds in this case) is checked, and if the startup silent period has not expired, the Primary Down Event timer is restarted. This is repeated until the **startup-silent-period** expires. In this example, the Primary Down Event timer runs four times (12 seconds) by the time the 10-second startup silent period expires.
- If no VRRP PDU is received by the end of the fourth 3-second cycle, *vrrp-group1* takes over the primary role.

## SEE ALSO

Understanding VRRP

[startup-silent-period](#) | 1177

## Enabling the Distributed Periodic Packet Management Process for VRRP

Typically, VRRP advertisements are sent by the VRRP process (*vrrpd*) on the primary VRRP router at regular intervals to let other members of the group know that the VRRP primary router is operational.

When the *vrrpd* process is busy and does not send VRRP advertisements, the backup VRRP routers might assume that the primary router is down and take over as the primary router, causing unnecessary flaps. This takeover might occur even though the original primary router is still active and available and might resume sending advertisements after the traffic has decreased. To address this problem and to reduce the load on the *vrrpd* process, Junos OS uses the periodic packet management process (*ppmd*) to send VRRP advertisements on behalf of the *vrrpd* process. However, you can further delegate the job of sending VRRP advertisements to the distributed *ppmd* process that resides on the Packet Forwarding Engine.

The ability to delegate the sending of VRRP advertisements to the distributed ppm process ensures that the VRRP advertisements are sent even when the ppm process—which is now responsible for sending VRRP advertisements—is busy. Such delegation prevents the possibility of false alarms when the ppm process is busy. The ability to delegate the sending of VRRP advertisements to distributed ppm also adds to scalability because the load is shared across multiple ppm instances and is not concentrated on any single unit.

**NOTE:** CPU-intensive VRRP advertisements, such as advertisements with MD5 authentication, continue to be processed by the VRRP process on the Routing Engine even when distributed ppm is enabled.

**NOTE:** VRRP is supported by graceful Routing Engine switchover only in the case that PPM delegation is enabled (the default).

**NOTE:** Aggregated Ethernet and integrated routing and bridging (IRB) delegation is supported only for MPC line cards. Routing devices with inbuilt MPCs such as the MX104 and below do not support this feature.

To configure the distributed ppm process to send VRRP advertisements, include the `delegate-processing` statement at the `[edit protocols vrrp]` hierarchy level:

```
[edit protocols vrrp]
  delegate-processing;
```

To configure the distributed ppm process to send VRRP advertisements over aggregated Ethernet and IRB interfaces, include the `delegate-processing ae-irb` statement at the `[edit protocols vrrp]` hierarchy level:

```
[edit protocols vrrp]
  delegate-processing ae-irb;
```

## SEE ALSO

Understanding VRRP

[delegate-processing \(VRRP\) | 1147](#)

## Improving the Convergence Time for VRRP

You can enable faster convergence time for the configured Virtual Router Redundancy Protocol (VRRP), thereby reducing the traffic restoration time to less than 1 second. To improve the convergence time for the VRRP, perform the following tasks:

- **Configure the distributed periodic packet management process**—When the VRRP process is busy and does not send VRRP advertisements, the backup VRRP routers might assume that the primary router is down and take over as the primary router, causing unnecessary flaps. To address this problem and to reduce the load on the VRRP process, Junos OS uses the distributed periodic packet management (PPM) process to send VRRP advertisements on behalf of the VRRP process.

To configure the distributed PPM process, include the `delegate-processing` statement at the `[edit protocols vrrp]` hierarchy level.

- **Disable the skew timer**—The skew timer in VRRP is used to ensure that two backup routers do not switch to the primary state at the same time in case of a failover situation. When there is only one primary router and one backup router in the network deployment, you can disable the skew timer, thereby reducing the time required to transition to the primary state.

To disable the skew timer, include the `skew-timer-disable` statement at the `[edit protocols vrrp]` hierarchy level.

- **Configure the number of fast advertisements that can be missed by a backup router before it starts transitioning to the master state**—The backup router waits until a certain number of advertisement packets are lost after which it transitions to the primary state. This waiting time can be fatal in scenarios such as router failure or link failure. To avoid such a situation and to enable faster convergence time, in Junos OS Release 12.2 and later, you can configure a fast advertisement interval value that specifies the number of fast advertisements that can be missed by a backup router before it starts transitioning to the primary state.

To configure the fast advertisement interval, include the `global-advertisements-threshold` statement at the `[edit protocols vrrp]` hierarchy level.

- **Configure inheritance of VRRP groups**—Junos OS enables you to configure VRRP groups on the various subnets of a virtual LAN (VLAN) to inherit the state and configuration of one of the groups, which is known as the active VRRP group. When the `vrrp-inherit-from` statement is included in the configuration, only the active VRRP group, from which the other VRRP groups inherit the state, sends out frequent VRRP advertisements and processes incoming VRRP advertisements. Use `inherit groups` for scaled configurations. For example, if you have 1000 VRRP groups with an advertisement interval of 100 ms, then use `inherit groups`.

To configure inheritance for a VRRP group, include the `vrrp-inherit-from` statement at the `[edit interfaces interface-name unit logical-unit-number family inet address address vrrp-group group-id]` hierarchy level.

- **Disable duplicate address detection for IPv6 interfaces**—Starting with Junos OS Release 15.1, duplicate address detection is a feature of the Neighbor Discovery Protocol for IPv6. Duplicate address detection is enabled by default and determines whether an address is already in use by another node. When detection address detection is enabled, convergence time is high after an IPv6 interface that has been configured for VRRP tracking comes up. To disable duplicate address detection, include the `ipv6-duplicate-addr-detection transmits 0` statement at the `[edit system internet-options]` hierarchy level. To disable duplicate address detection only for a specific interface, include the `dad-disable` statement at the `[edit interfaces interface-name unit logical-unit-number family inet6]` hierarchy level.

#### NOTE:

- Inheritance of VRRP groups is supported with all types of interfaces. Other measures to reduce convergence time, such as VRRP distribution, disabling skew timer, and reducing advertisement threshold.
- Compared to other routers, the convergence time and the traffic restoration time are less for MX Series routers with MPCs.
- Reduction in convergence time is applicable for all types of configurations at the physical interface but the convergence time might not be less than 1 second for all the configurations. The convergence time depends on the number of groups that are transitioning from the backup to the primary state and the interval at which these groups are transitioning.

## SEE ALSO

Configuring Inheritance for a VRRP Group

Configuring VRRP to Improve Convergence Time

[delegate-processing \(VRRP\) | 1147](#)

[global-advertisements-threshold | 1153](#)

[skew-timer-disable | 1175](#)

## Configuring VRRP to Improve Convergence Time

You can enable faster convergence time for the configured Virtual Router Redundancy Protocol (VRRP), thereby reducing the traffic restoration time to less than 1 second. To improve the convergence time for VRRP, perform the following tasks.

Before you begin, configure VRRP. See [Configuring VRRP](#).

1. Configure the distributed periodic packet management (PPM) process to send VRRP advertisements when the VRRP process is busy.

```
[edit]
user@host# set protocols vrrp delegate-processing
```

2. Disable the skew timer to reduce the time required to transition to the primary state.

```
[edit]
user@host# set protocols vrrp skew-timer-disable
```

**NOTE:** When there is only one primary router and one backup router in the network deployment, you can disable the skew timer, thereby reducing the time required to transition to the primary state.

3. Configure the number of fast advertisements that can be missed by a backup router before it starts transitioning to the primary state.

```
[edit]
user@host# set protocols vrrp global-advertisement-threshold advertisement-value
```

4. Configure VRRP groups on the various subnets of a VLAN to inherit the state and to configure one of the groups.

```
[edit]
user@host# set interfaces interface-name unit logical-unit-number family inet address address
vrrp-group group-id
```

5. Verify the configuration.

```
[edit]
user@host# show protocols vrrp
```

**NOTE:**



- Inheritance of VRRP groups is supported with all types of interfaces. Other measures to reduce convergence time, such as VRRP distribution, disabling skew timer, and reducing advertisement threshold, are not applicable when VRRP is configured over integrated routing and bridging (IRB) interfaces, aggregated Ethernet interfaces, and multichassis link aggregation group (MC-LAG) interfaces.
- Compared to other routers, the convergence time and the traffic restoration time are less for MX Series routers with MPCs.
- Reduction in convergence time is applicable for all types of configurations at the physical interface, but the convergence time might not be less than 1 second for all the configurations. The convergence time depends on the number of groups that are transitioning from the backup to the primary state and the interval at which these groups are transitioning.

## SEE ALSO

Improving the Convergence Time for VRRP

Configuring Inheritance for a VRRP Group

[delegate-processing \(VRRP\) | 1147](#)

[global-advertisements-threshold | 1153](#)

[skew-timer-disable | 1175](#)

## Tracing VRRP Operations

To trace VRRP operations, include the `traceoptions` statement at the `[edit protocols vrrp]` hierarchy level.

By default, VRRP logs the error, data carrier detect (DCD) configuration, and routing socket events in a file in the `/var/log` directory. By default, this file is named `/var/log/vrrpd`. The default file size is 1 megabyte (MB), and three files are created before the first one gets overwritten.

To change the configuration of the logging file, include the `traceoptions` statement at the `[edit protocols vrrp]` hierarchy level:

```
[edit protocols vrrp]
traceoptions {
    file filename <files number> <match regular-expression> <microsecond-stamp> <size size>
    <world-readable | no-world-readable>;
    flag flag;
    no-remote-trace;
```

```
}
flag flag;
```

You can specify the following VRRP tracing flags:

- **all**—Trace all VRRP operations.
- **database**—Trace all database changes.
- **general**—Trace all general events.
- **interfaces**—Trace all interface changes.
- **normal**—Trace all normal events.
- **packets**—Trace all packets sent and received.
- **state**—Trace all state transitions.
- **timer**—Trace all timer events.

## SEE ALSO

Understanding VRRP

## Example: Configuring VRRP for Load Sharing

### IN THIS SECTION

- [Requirements | 481](#)
- [Overview and Topology | 481](#)
- [Configuring VRRP on Both Switches | 483](#)
- [Verification | 487](#)

If you do not want to dedicate a switch to be a VRRP backup (and therefore leave it idle unless the primary fails), you can create a load-sharing configuration in which each participating switch simultaneously acts as a primary and a backup.

One reason to use a load-sharing (active-active) configuration is that you are more likely to actively monitor and maintain both switches and notice if a problem occurs on either of them. If you use a

configuration in which one switch is only a backup (an active-backup configuration), you might be less likely to pay attention to the backup switch while it is idle. In the worst case, this could lead to the backup switch developing an undetected problem and not being able to perform adequately when a failover occurs.

## Requirements

This example uses the following hardware and software components:

- Two switches
- Junos OS Release 11.3 or later
- Static routing or a dynamic routing protocol enabled on both switches.

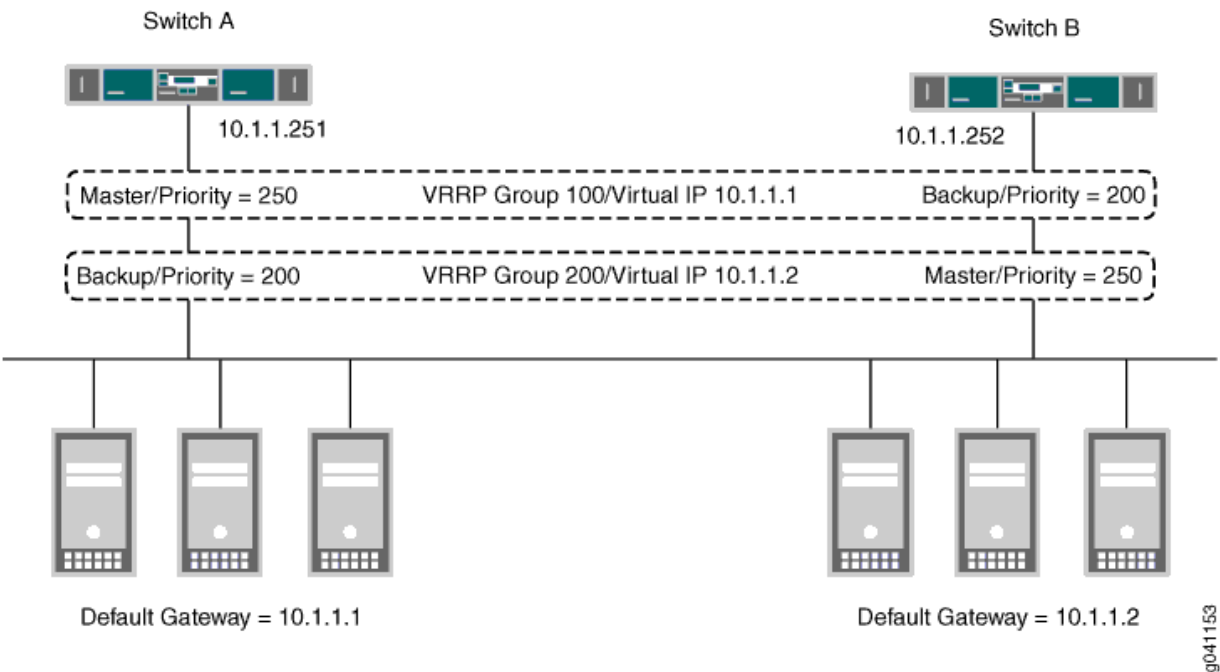
## Overview and Topology

### IN THIS SECTION

- [Topology | 482](#)

This example uses two VRRP groups, each of which has its own virtual IP address. Devices on the LAN use one of these virtual IP addresses as their default gateway. If one of the switches fails, the other switch takes over for it. In the topology shown in [Figure 28 on page 482](#), for example, Switch A is the primary for VRRP group 100. If Switch A fails, Switch B takes over and forwards traffic that the end devices send to the default gateway address 10.1.1.1.

Figure 28: VRRP Load-Sharing Configuration



This example shows a simple configuration to illustrate the basic steps for configuring two switches running VRRP to back each other up. [Table 17 on page 482](#) lists VRRP settings for each switch.

**Topology**

Table 17: Settings for VRRP Load-Sharing Example

Switch A	Switch B
VRRP Group 100: <ul style="list-style-type: none"><li>Interface address: 10.1.1.251</li><li>VIP: 10.1.1.1</li><li>Priority: 250</li></ul>	VRRP Group 100: <ul style="list-style-type: none"><li>Interface address: 10.1.1.252</li><li>VIP: 10.1.1.1</li><li>Priority: 200</li></ul>

Table 17: Settings for VRRP Load-Sharing Example *(Continued)*

Switch A	Switch B
VRRP Group 200: <ul style="list-style-type: none"><li>• Interface address: 10.1.1.251</li><li>• VIP: 10.1.1.2</li><li>• Priority: 200</li></ul>	VRRP Group 200: <ul style="list-style-type: none"><li>• Interface address: 10.1.1.252</li><li>• VIP: 10.1.1.2</li><li>• Priority: 250</li></ul>

In addition to configuring the two switches as shown, you must configure your end devices so that some of them use one of the virtual IP addresses as their default gateway and the remaining end devices use the other virtual IP address as their default gateway.

Note that if a failover occurs, the remaining switch might be unable to handle all of the traffic, depending on the demand.

Configuring VRRP on Both Switches

IN THIS SECTION

Procedure | 483

Procedure

CLI Quick Configuration

Enter the following on Switch A:

```
[edit]
set interfaces xe-0/0/0 unit 0 family inet address 10.1.1.251/24 vrrp-group 100 virtual-address 10.1.1.1
set interfaces xe-0/0/0 unit 0 family inet address 10.1.1.251/24 vrrp-group 100 priority 250
set interfaces xe-0/0/0 unit 0 family inet address 10.1.1.251/24 vrrp-group 200 virtual-address 10.1.1.2
set interfaces xe-0/0/0 unit 0 family inet address 10.1.1.251/24 vrrp-group 200 priority 200
```

Enter the following on Switch B:

```
[edit]
set interfaces xe-0/0/0 unit 0 family inet address 10.1.1.252/24 vrrp-group 100 virtual-address 10.1.1.1
set interfaces xe-0/0/0 unit 0 family inet address 10.1.1.252/24 vrrp-group 100 priority 200
set interfaces xe-0/0/0 unit 0 family inet address 10.1.1.252/24 vrrp-group 200 virtual-address 10.1.1.2
set interfaces xe-0/0/0 unit 0 family inet address 10.1.1.252/24 vrrp-group 200 priority 250
```

## Step-by-Step Procedure

Configure the VRRP groups and priorities on Switch A:

1. Create VRRP group 100 on Switch A and configure the virtual IP address for the group:

```
[edit]
user@switch# set interfaces xe-0/0/0 unit 0 family inet address 10.1.1.252/24 vrrp-group 100
virtual-address 10.1.1.1
```

2. Assign the VRRP priority for this interface in this group:

```
[edit]
user@switch# set interfaces xe-0/0/0 unit 0 family inet address 10.1.1.251/24 vrrp-group 100
priority 250
```

3. Create VRRP group 200 on Switch A and configure the virtual IP address for the group:

```
[edit]
user@switch# set interfaces xe-0/0/0 unit 0 family inet address 10.1.1.251/24 vrrp-group 200
virtual-address 10.1.1.2
```

4. Assign the VRRP priority for this interface in this group:

```
[edit]
user@switch# set interfaces xe-0/0/0 unit 0 family inet address 10.1.1.251/24 vrrp-group 200
priority 200
```

## Step-by-Step Procedure

Configure the VRRP groups and priorities on Switch B:

1. Create VRRP group 100 on Switch B and configure the virtual IP address for the group:

```
[edit]
user@switch# set interfaces xe-0/0/0 unit 0 family inet address 10.1.1.252/24 vrrp-group 100
virtual-address 10.1.1.1
```

2. Assign the VRRP priority for this interface in this group:

```
[edit]
user@switch# set interfaces xe-0/0/0 unit 0 family inet address 10.1.1.252/24 vrrp-group 100
priority 200
```

Switch A remains the primary for group 100 because it has the highest priority for this group.

3. Create VRRP group 200 on Switch A and configure the virtual IP address for the group:

```
[edit]
user@switch# set interfaces xe-0/0/0 unit 0 family inet address 10.1.1.252/24 vrrp-group 200
virtual-address 10.1.1.2
```

4. Assign the VRRP priority for this interface in this group:

```
[edit]
user@switch# set interfaces xe-0/0/0 unit 0 family inet address 10.1.1.251/24 vrrp-group 200
priority 250
```

Switch B becomes the primary for group 200 because it has the highest priority for this group.

## Results

Display the results of the configuration on Switch A:

```
user@switch> show configuration
interfaces {
  xe-0/0/0 {
```

```

    unit 0 {
        family inet {
            address 10.1.1.251 {
                vrrp-group 100 {
                    virtual address 10.1.1.1
                    priority 250
                }
                vrrp-group 200 {
                    virtual address 10.1.1.2
                    priority 200
                }
            }
        }
    }
}

```

Display the results of the configuration on Switch B:

```

user@switch> show configuration
interfaces {
    xe-0/0/0 {
        unit 0 {
            family inet {
                address 10.1.1.252 {
                    vrrp-group 100 {
                        virtual address 10.1.1.1
                        priority 200
                    }
                    vrrp-group 200 {
                        virtual address 10.1.1.2
                        priority 250
                    }
                }
            }
        }
    }
}

```



Verification

IN THIS SECTION

- [Verifying that VRRP Is Working on Switch A | 487](#)
- [Verifying that VRRP Is Working on Switch B | 488](#)

*Verifying that VRRP Is Working on Switch A*

Purpose

Verify that VRRP is active on Switch A and that the primary and backup roles are correct.

Action

Use the following command to verify that VRRP is active on Switch A and that the switch is primary for group 100 and backup for group 200.

```
user@switch> show vrrp
```

Interface	State	Group	VR state	Timer		Type
Address						
xe-0/0/0.0	up	100	master	A .0327	lcl	10.1.1.251
					vip	10.1.1.1
xe-0/0/0.0	up	200	backup	A .0327	lcl	10.1.1.251
					vip	10.1.1.2

Meaning

The `show vrrp` command displays fundamental information about the VRRP configuration. This output shows that both VRRP groups are active and that this switch has assumed the correct primary and backup roles. The **lcl** address is the physical address of the interface and the **vip** address is the virtual address shared by both switches. The **Timer** value (**A .0327**) indicates the remaining time (in seconds) in which this switch expects to receive a VRRP advertisement from the other switch. If an advertisement for group 200 does not arrive before the timer expires, Switch A asserts itself as the primary for this group.

### Verifying that VRRP Is Working on Switch B

#### Purpose

Verify that VRRP is active on Switch B and that the primary and backup roles are correct.

#### Action

Use the following command to verify that VRRP is active on Switch B and that the switch is backup for group 100 and primary for group 200.

```
user@switch> show vrrp
```

Interface	State	Group	VR state	Timer	Type	
Address						
xe-0/0/0.0	up	100	backup	A .0327	lcl	10.1.1.252
					vip	10.1.1.1
xe-0/0/0.0	up	200	master	A .0327	lcl	10.1.1.252
					vip	10.1.1.2

#### Meaning

The `show vrrp` command displays fundamental information about the VRRP configuration. This output shows that both VRRP groups are active and that this switch has assumed the correct primary and backup roles. The **lcl** address is the physical address of the interface and the **vip** address is the virtual address shared by both switches. The **Timer** value (**A .0327**) indicates the remaining time (in seconds) in which this switch expects to receive a VRRP advertisement from the other switch. If an advertisement for group 100 does not arrive before the timer expires, Switch B asserts itself as the primary for this group.

#### SEE ALSO

Understanding VRRP
<a href="#">Configuring Basic VRRP Support for QFX</a>

# Troubleshooting VRRP

IN THIS SECTION

- Problem | 489
- Solution | 489

Problem

Description

If you configure multiple VRRP groups on an interface (using multiple VLANs), traffic for some of the groups might be briefly dropped if a failover occurs. This can happen because the new primary must send gratuitous ARP replies for each VRRP group to update the ARP tables in the connected devices, and there is a short delay between each gratuitous ARP reply. Traffic sent by devices that have not yet received the gratuitous ARP reply is dropped (until the device receives the reply and learns the MAC address of the new primary).

Solution

Configure a failover delay so that the new primary delays sending gratuitous ARP replies for the period that you set. This allows the new primary to send the ARP replies for all of the VRRP groups simultaneously.

SEE ALSO

| [failover-delay](#)

Release History Table

Release	Description
18.1R1	Primary router sends periodic VRRP advertisement messages to each virtual routers. The backup routers do not attempt to preempt the primary router unless it has higher priority. This eliminates service disruption unless a more preferred path becomes available. It is possible to administratively prohibit all preemption attempts, with the exception of a VRRP router becoming primary router of any virtual router associated with addresses it owns.

17.3R1	Starting in Junos OS release 17.3R1, if network-services is configured in IP mode, don't configure the same VRRP group ID for multiple VRRP sessions on the same physical interface unless VRRP delegation is disabled.
17.3R1	Starting in Junos OS release 17.3R1, if network-services is configured in enhanced-ip mode, you can use the same VRRP group ID for multiple VRRP sessions.
15.1	In Junos OS Release 15.1 and later, an adjusted priority can be zero.
15.1	Prior to Junos OS Release 15.1, an adjusted priority could not be zero.
13.2	Starting in Junos OS Release 13.2, VRRP nonstop active routing (NSR) is enabled only when you configure the nonstop-routing statement at the [edit routing-options] or [edit logical system <i>logical-system-name</i> routing-options] hierarchy level.

# 13

PART

## Performing Unified In-Service Software Upgrade (ISSU)

---

Getting Started with Unified ISSU and Understanding How Unified ISSU Works |  
492

Unified ISSU System Requirements | 504

Performing a Unified ISSU | 532

Performing an ISSR | 589

---

# Getting Started with Unified ISSU and Understanding How Unified ISSU Works

## IN THIS CHAPTER

- [Understanding Unified ISSU | 492](#)

## Understanding Unified ISSU

### SUMMARY

Unified in-service software upgrade (ISSU) is a feature that minimizes traffic loss during the software upgrade process.

### IN THIS SECTION

- [Getting Started with Unified In-Service Software Upgrade | 492](#)
- [Understanding the Unified ISSU Process | 493](#)
- [Understanding In-Service Software Upgrade \(ISSU\) | 501](#)
- [Understanding In-Service Software Upgrade \(ISSU\) in ACX5000 Series Routers | 502](#)

## Getting Started with Unified In-Service Software Upgrade

The unified in-service software upgrade (ISSU) feature enables you to upgrade between two different Junos OS releases with no disruption on the control plane and with minimal disruption of traffic.

To quickly access the information you need, click on the link in [Table 18 on page 493](#).

**Table 18: Locating the Information You Need to Work With ISSU**

Task You Need to Perform	Where The Information Is Located
Verify unified ISSU support for your device	<a href="#">"Unified ISSU System Requirements" on page 504</a>
Perform a unified ISSU	Example: Performing a Unified ISSU
Verify that the unified ISSU is successful	Verifying a Unified ISSU
Understand how the unified ISSU process works	Understanding the Unified ISSU Process

Unified ISSU takes advantage of the redundancy provided by dual Routing Engines and works in conjunction with the graceful Routing Engine switchover feature and the nonstop active routing feature.

Unified ISSU provides the following benefits:

- Eliminates network downtime during software image upgrades
- Reduces operating costs, while delivering higher service levels
- Allows fast implementation of new features

## SEE ALSO

[Understanding High Availability Features on Juniper Networks Routers | 2](#)

## Understanding the Unified ISSU Process

### IN THIS SECTION

- [Understanding the Unified ISSU Process on a Router | 494](#)
- [Understanding the Unified ISSU Process on the TX Matrix Router | 498](#)

This topic explains the unified ISSU processes that take place on a router, on a TX Matrix router, on a TX Matrix Plus router and its connected line-card chassis (LCCs), as well as on a TX Matrix Plus router with 3D SIBs and its connected LCCs.

## Understanding the Unified ISSU Process on a Router

### IN THIS SECTION

- [Unified ISSU Process on a Router | 494](#)

This topic describes the processes that take place on a router with dual Routing Engines when you initiate a unified in-service software upgrade (ISSU).

### *Unified ISSU Process on a Router*

After you use the `request system software in-service-upgrade` command, the following process occurs.

In *Figure 1* through *Figure 6* below:

- A solid line indicates the high-speed internal link between a Routing Engine and a Packet Forwarding Engine.
- A dotted line indicates the messages exchanged between the Packet Forwarding Engine and the chassis process (chassisd) on the Routing Engine.
- RE0m and RE1b indicate primary and backup Routing Engines, respectively.
- The check mark indicates that the device is running the new version of software.

**NOTE:** Unified ISSU can only upgrade up to three major releases ahead of the current release on a device. To upgrade to a release more than three releases ahead of the current release on a device, use the unified ISSU process to upgrade the device to one or more intermediate releases until the device is within three major releases of the target release.

**NOTE:** The following process pertains to all supported routing platforms except the TX Matrix router and TX Matrix Plus router. On most routers, the Packet Forwarding Engine resides on a Flexible PIC Concentrator (FPC). However, on an M120 router, the Forwarding Engine Board (FEB) replaces the functions of a Packet Forwarding Engine. In the illustrations and steps, when considering an M120 router, you can regard the Packet Forwarding Engine as an FPC. As an additional step on an M120 router, after the FPCs and PICs have been upgraded, the FEBs are upgraded.



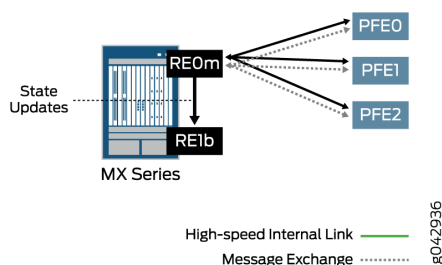
1. The primary Routing Engine validates the router configuration to ensure that it can be committed when you use the new software version.

Checks are made for the following:

- Disk space is available for the `/var` file system on both Routing Engines.
- The configuration is supported by a unified ISSU.
- The PICs are supported by a unified ISSU.
- Graceful Routing Engine switchover is enabled.
- Nonstop active routing is enabled.

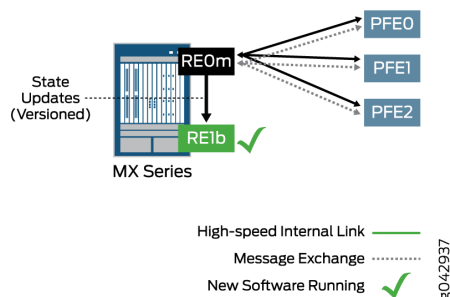
These checks are the same as the checks made when you enter the `request system software validate in-service-upgrade` command. If there is insufficient disk space available on either of the Routing Engines, the unified ISSU process fails and returns an error message. However, unsupported PICs do not prevent a unified ISSU. If there are unsupported PICs, the system issues a warning to indicate that these PICs will restart during the upgrade. Similarly, if there is an unsupported protocol configured, the system issues a warning that packet loss might occur for the unsupported protocol during the upgrade.

**Figure 29: Device Status Before Starting a Unified ISSU**



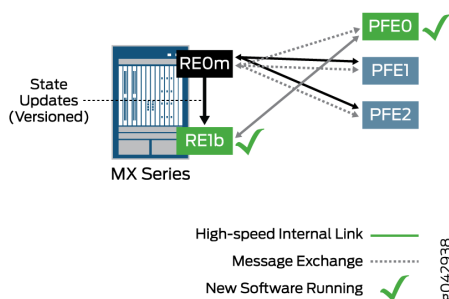
2. After the validation succeeds, the management process installs (copies) the new software image to the backup Routing Engine.
3. The backup Routing Engine is rebooted.
4. After the backup Routing Engine is rebooted and is running the new software, the kernel state synchronization process (`ksyncd`) synchronizes (copies) the configuration file and the kernel state from the primary Routing Engine.

Figure 30: Device Status After the Backup Routing Engine Is Upgraded



5. After the configuration file and the kernel state are synchronized to the backup Routing Engine, the chassis process (chassisd) on the primary Routing Engine prepares other software processes for the unified ISSU. The chassis process informs the various software processes (such as rpd, apsd, bfdd, and so on) about the unified ISSU and waits for responses from them. When all the processes are ready, the chassis process sends an ISSU\_PREPARE message to the FPCs installed in the router. You can display the unified ISSU process messages by using the `show log messages` command.
6. The Packet Forwarding Engine on each FPC saves its state and downloads the new software image from the backup Routing Engine. Next, each Packet Forwarding Engine sends an ISSU\_READY message to the chassis process.

Figure 31: Device Status After One Packet Forwarding Engine Downloads the New Software

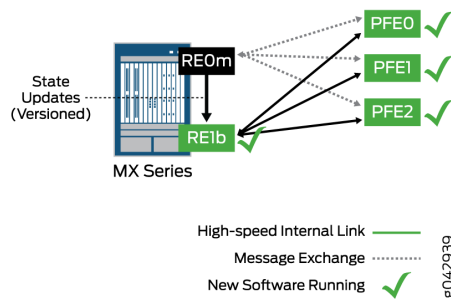


7. After receiving an ISSU\_READY message from a Packet Forwarding Engine, the chassis process sends an ISSU\_REBOOT message to the FPC on which the Packet Forwarding Engine resides. The FPC reboots with the new software image. After the FPC is rebooted, the Packet Forwarding Engine restores the FPC state, and a high-speed internal link is established with the backup Routing Engine running the new software. The chassis process link is also reestablished with the primary Routing Engine.

**NOTE:** The Packet Forwarding Engine reboots that occur during an unified ISSU are designed to have a very short window of down time.

8. After all Packet Forwarding Engines have sent a READY message using the chassis process on the primary Routing Engine, other software processes are prepared for a Routing Engine switchover. The system is ready for a switchover at this point.

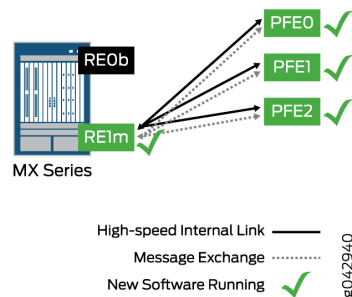
**Figure 32: Device Status Before the Routing Engine Switchover**



**NOTE:** For M120 routers, the FEBs are upgraded at this point. When all FEBs have been upgraded, the system is ready for a switchover.

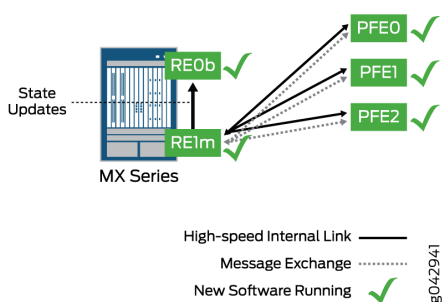
9. The Routing Engine switchover occurs, and the Routing Engine (re1) that was the backup now becomes the primary Routing Engine.

**Figure 33: Device Status After the Routing Engine Switchover**



10. The new backup Routing Engine is now upgraded to the new software image. (This step is skipped if you have specified the `no-old-master-upgrade` option in the `request system software in-service-upgrade` command.)

**Figure 34: Device Status After the Unified ISSU Is Complete**



11. When the backup Routing Engine has been successfully upgraded, the unified ISSU is complete.

## Understanding the Unified ISSU Process on the TX Matrix Router

### IN THIS SECTION

- [Unified ISSU Process on the TX Matrix Router | 498](#)

This topic describes the processes that take place on a TX Matrix router when you initiate a unified in-service software upgrade (ISSU).

### *Unified ISSU Process on the TX Matrix Router*

This section describes the processes that take place on a TX Matrix router and the routers acting as connected line-card chassis (LCCs).

**NOTE:** A routing matrix is a multichassis architecture that consists of a TX Matrix router and from one to four T640 routers. From the perspective of the user interface, the routing matrix appears as a single router. The TX Matrix router controls all the T640 routers in the routing matrix.

Each router has dual Routing Engines.

After you use the "[request system software in-service-upgrade](#)" on page 1270 command on a TX Matrix router, the following process occurs:

1. The management process (mgd) on the primary Routing Engine of the TX Matrix router (global primary) checks the current configuration.  
  
Checks are made for the following:
  - Disk space is available for the `/var` file system on all Routing Engines.
  - The configuration is supported by a unified ISSU.
  - The PICs are supported by a unified ISSU.
  - Graceful Routing Engine switchover is enabled.
  - Nonstop active routing is enabled.
2. After successful validation of the configuration, the management process copies the new image to the backup Routing Engines on the TX Matrix router and the T640 routers.
3. The kernel synchronization process (ksyncd) on the backup Routing Engines synchronizes the kernels on the backup Routing Engines with the kernels on the primary Routing Engines.
4. The global backup Routing Engine is upgraded with the new software. Next the global backup Routing Engine is rebooted. Then the global backup Routing Engine synchronizes the configuration and kernel state from the global primary Routing Engine.
5. The LCC backup Routing Engines are upgraded and rebooted. Then the LCC backup Routing Engines connect with the upgraded global backup Routing Engine and synchronize the configuration and kernel state.
6. The unified ISSU control moves from the management process to the chassis process (chassisd). The chassis process informs the various software processes (such as rpd, apsd, bfdd, and so on) about the unified ISSU and waits for responses from them.
7. After receiving messages from the software processes indicating that the processes are ready for unified ISSU, the chassis process on the global primary Routing Engine sends messages to the chassis process on the routing nodes to start the unified ISSU.
8. The chassis process on the routing nodes sends ISSU\_PREPARE messages to the field-replaceable units (FRUs), such as FPCs and intelligent PICs.
9. After receiving an ISSU\_PREPARE message, the Packet Forwarding Engines save the current state information and download the new software image from the backup Routing Engines. Next, each

Packet Forwarding Engine sends ISSU\_READY messages to the chassis process. You can display the unified ISSU process messages by using the `show log messages` command.

10. After receiving an ISSU\_READY message from the Packet Forwarding Engines, the chassis process sends an ISSU\_REBOOT message to the FRUs. While the upgrade is in progress, the FRUs keep sending ISSU\_IN\_PROGRESS messages to the chassis process on the routing nodes. The chassis process on each routing node, in turn, sends an ISSU\_IN\_PROGRESS message to the chassis process on the global primary Routing Engine.

**NOTE:** The Packet Forwarding Engine reboots that occur during a unified ISSU are designed to have a very short window of down time.

11. After the unified ISSU reboot, the Packet Forwarding Engines restore the saved state information and connect back to the routing nodes. The chassis process on each routing node sends an ISSU\_READY message to the chassis process on the global primary Routing Engine. The CM\_MSG\_READY message from the chassis process on the routing nodes indicate that the unified ISSU is complete on the FRUs.
12. The unified ISSU control moves back to the management process on the global primary Routing Engine.
13. The management process initiates Routing Engine switchover on the primary Routing Engines.
14. Routing Engine switchover occurs on the TX Matrix router and the T640 routers.
15. After the switchover, the FRUs connect to the new primary Routing Engines. Then the chassis manager and Packet Forwarding Engine manager on the T640 router FRUs connect to the new primary Routing Engines on the T640 routers.
16. The management process on the global primary Routing Engine initiates the upgrade process on the old primary Routing Engines on the T640 routers. (This step is skipped if you have specified the `no-old-master-upgrade` option in the `request system software in-service-upgrade` command.)
17. After the Routing Engines that were previously the primaries on the T640 routers are upgraded, the management process initiates the upgrade of the Routing Engine that was previously the global primary on the TX Matrix router.
18. After a successful unified ISSU, the TX Matrix router and the T640 routers are rebooted if you specified the `reboot` option in the `request system software in-service-upgrade` command.

## RELATED DOCUMENTATION

Getting Started with Unified In-Service Software Upgrade

Best Practices for Performing a Unified ISSU

[Unified ISSU System Requirements | 504](#)

Example: Performing a Unified ISSU

[request system software validate in-service-upgrade | 1327](#)

## Understanding In-Service Software Upgrade (ISSU)

### IN THIS SECTION

- [In-Service Software Upgrade Process | 501](#)

An in-service software upgrade (ISSU) enables you to upgrade between two different Junos OS releases with minimal disruption on the control plane and with minimal disruption of traffic. During an ISSU, the Junos OS runs in two separate virtual machines (VMs)—one VM is in the primary role acting as the primary Routing Engine, and the other VM is in the backup role acting as the backup Routing Engine. The Junos OS is upgraded on the backup VM. After a successful software upgrade, the backup VM then becomes the primary VM, and the original primary VM is no longer needed and is shut down.



**Video:** [How Does ISSU Work on the QFX5100?](#)

ISSU provides the following benefits:

- Eliminates network downtime during software image upgrades
- Reduces operating costs, while delivering higher service levels
- Allows fast implementation of new features

### In-Service Software Upgrade Process

When you request an ISSU on a standalone device:

1. The management process (mgd) verifies that non-stop routing (NSR), graceful Routing Engine switchover (GRES), and non-stop bridging (NSB) are enabled.
2. The switch downloads and validates the software package.
3. The ISSU state machine spawns the backup Routing Engine (RE) with the newer software.
4. The ISSU state machine checks to see if the backup RE has synchronized all of the data with the primary RE.

5. The ISSU state machine moves the devices (for example, forwarding ASIC, FPGA, management port and serial console) from the primary RE to the backup RE.
6. The primary role is switched between the REs, so the backup RE becomes the primary RE.
7. The old primary RE is shut down.

## SEE ALSO

[In-Service Software Upgrade \(ISSU\) System Requirements](#)

Performing an In-Service Software Upgrade (ISSU) with Non-Stop Routing

## Understanding In-Service Software Upgrade (ISSU) in ACX5000 Series Routers

### IN THIS SECTION

- [In-Service Software Upgrade Process | 502](#)

An in-service software upgrade (ISSU) enables you to upgrade between two different Junos OS releases with minimal disruption on the control plane and with minimal disruption of traffic. During an ISSU, the Junos OS runs in two separate virtual machines (VMs)—one VM is in the primary role acting as the primary Routing Engine, and the other VM is in the backup role acting as the backup Routing Engine. The Junos OS is upgraded on the backup VM. After a successful software upgrade, the backup VM then becomes the primary VM, and the original primary VM is no longer needed and is shut down.

**NOTE:** ISSU is supported in Junos OS Release 15.1X54-D60 or later for ACX5000 Series routers.

ISSU provides the following benefits:

- Eliminates network downtime during software image upgrades
- Reduces operating costs, while delivering higher service levels
- Allows fast implementation of new features

### In-Service Software Upgrade Process

When you request an ISSU on a standalone device:



1. The management process (mgd) verifies that non-stop routing (NSR), graceful Routing Engine switchover (GRES), and non-stop bridging (NSB) are enabled.
2. The router downloads and validates the software package.
3. The ISSU state machine spawns the backup Routing Engine (RE) with the newer software.
4. The ISSU state machine checks to see if the backup RE has synchronized all of the data with the primary RE.
5. The ISSU state machine moves the devices (for example, forwarding ASIC, FPGA, management port and serial console) from the primary RE to the backup RE.
6. The primary role is switched between the REs, so the backup RE becomes the primary RE.
7. The old primary RE is shut down.

# Unified ISSU System Requirements

## IN THIS CHAPTER

- [Unified ISSU System Requirements | 504](#)

## Unified ISSU System Requirements

### SUMMARY

Unified in-service software upgrade (ISSU) requires you to meet the device and configuration requirements listed below.

### IN THIS SECTION

- [General Unified ISSU Considerations for All Platforms | 505](#)
- [Unified ISSU Considerations for MX Series Routers | 506](#)
- [Unified ISSU Considerations for PTX Series Routers | 508](#)
- [Unified ISSU Considerations for T Series Routers | 508](#)
- [Unified ISSU Considerations for EX Series Switches | 509](#)
- [Unified ISSU Platform Support | 509](#)
- [Unified ISSU Protocol Support for M Series, MX Series, and T Series Routers and EX9200 Switches | 511](#)
- [Unified ISSU Feature Support | 511](#)
- [Unified ISSU PIC Support Considerations | 512](#)

The unified in-service software upgrade (ISSU) feature enables you to upgrade your device between two different Junos OS releases with no disruption on the control plane and with minimal disruption of

traffic. Unified ISSU is supported only on dual Routing Engine platforms. In addition, the graceful Routing Engine switchover (GRES) and nonstop active routing (NSR) features must be enabled.

To access an interactive tool for verifying hardware support for unified ISSU, see the [Juniper Networks Feature Explorer](#).

This section contains the following topics:

## General Unified ISSU Considerations for All Platforms

Unified ISSU has the following caveats:

- To upgrade to Junos OS Releases 21.2R1 or 22.1R1, you need to include the `no-validate` option when issuing the `in-service-upgrade` command. The syntax for this command is `request system software in-service-upgrade /var/tmp/package-name.tgz no-validate`

Junos OS releases prior to 20.4R2 do not support the `no-validate` option with unified ISSU. In order to upgrade from an older release to Junos OS Releases 21.2R1 or 22.1R1 with unified ISSU, you must first upgrade to a release that supports the `no-validate` option for unified ISSU, such as 20.4R2.

- We recommend that you not use unified ISSU to upgrade from an earlier Junos OS release to Junos OS Release 14.2.R1 or 15.1.R1. ISSU is not supported in Junos OS Release 14.2. For more information about Junos OS Release 14.2, see the [Release Notes for Junos OS Release 14.2](#). For more information about Junos OS Release 15.1, see the [Release Notes for Junos OS Release 15.1](#).
- Using unified ISSU to upgrade from an earlier Junos OS release to Junos OS Release 17.1R1 or later does not work if VPLS dynamic profiles are configured and enhanced subscriber management is not configured.
- The primary Routing Engine and backup Routing Engine must be running the same software version before you can perform a unified ISSU.
- The unified ISSU process is terminated and a message is displayed if the Junos OS version specified for installation is a version earlier than the one currently running on the device.
- The unified ISSU process is terminated if the specified upgrade has conflicts with the current configuration, components supported, and so forth.
- You cannot take PICs offline or bring them online during a unified ISSU.
- User-initiated GRES is blocked when the device is undergoing a unified ISSU.
- Unified ISSU does not support extension application packages developed with the Junos SDK.
- To downgrade from a unified ISSU-capable release to a previous software release (unified ISSU-capable or not), use the `request system software add package-name` command. Unlike an upgrade using the unified ISSU process, a downgrade using the `request system software add package-name` command can

cause network disruptions and loss of data. For more information about the use of the `request system software add package-name` command, see the [Junos OS Software Installation and Upgrade Guide](#).

- Unicast reverse-path-forwarding (RPF)-related statistics are not saved across a unified ISSU, and the unicast RPF counters are reset to zero during a unified ISSU.
- BGP session uptime and downtime statistics are not synchronized between the primary and backup Routing Engines during a unified ISSU. The backup Routing Engine maintains its own session uptime based on the time when the backup first becomes aware of the established sessions. For example, if the backup Routing Engine is rebooted (or if you run `restart routing` on the backup Routing Engine), the backup Routing Engine uptime is a short duration, because the backup has just learned about the established sessions. If the backup is operating when the BGP sessions first come up on the primary, the uptime on the primary and the uptime on the backup are almost the same duration. After a Routing Engine switchover, the new primary continues from the time left on the backup Routing Engine.
- If proxy ARP is enabled on your device, you must delete the `unconditional-src-learn` statement from the `[edit interfaces interface-name unit 0 family inet]` hierarchy level before the unified ISSU process begins and include it after the unified ISSU process is complete. Note that the `unconditional-src-learn` statement is not included by default.

## Unified ISSU Considerations for MX Series Routers

Unified ISSU has the following caveats for MX Series routers:

- On MX Series 3D Universal Edge Routers (with Modular Port Concentrator/Modular Interface Card (MPC/MIC) interfaces), unified ISSU is supported starting with Junos OS Release 11.2.
- On MX Series 3D Universal Edge Routers with MPC3E and MPC4E interfaces, unified ISSU is supported starting with Junos OS Release 13.3.
- Unified ISSU is supported with Junos OS Release 17.4R1 for MX Series routers with MPC-3D-16XGE-SFPP, MPC-3D-NG, MPC-3D-16XGE-SFPP-R-B, MPC-SEPTUM-S, MPC2E-3D-NG, MPC2E-3D-NG-IR-B, MPC2E-3D-NG-Q, MPC2E-3D-NG-Q-IR-B, MPC2E-3D-NG-Q-R-B, MPC2E-3D-NG-R-B, MPC3E-3D-NG, MPC3E-3D-NG-IR-B, MPC3E-3D-NG-Q, MPC3E-3D-NG-Q-IR-B, MPC3E-3D-NG-Q-R-B, MPC3E-3D-NG-R-B, MPC4E-3D-2CGE-8XGE, MPC4E-3D-2CGE8XGE-IR-B, MPC4E-3D-2CGE8XGE-R-B, MPC4E-3D-32XGE-IR-B, MPC4E-3D-32XGE-R-B, MPC4E-3D-32XGE-SFPP, MPC5E-100G10G, MPC5E-100G10G-IRB, MPC5E-100G10G-RB, MPC5E-40G10G, MPC5E-40G10G-IRB, MPC5E-40G10G-RB, MPC5EQ-100G10G, MPC5EQ-100G10G-IRB, MPC5EQ-100G10G-RB, MPC5EQ-40G10G, MPC5EQ-40G10G-IRB, MPC5EQ-40G10G-RB, MPC7E-10G, MPC7E-10G-IRB, MPC7E-10G-RB, MPC7E-MRATE, MPC7E-MRATE-IRB, MPC7E-MRATE-RB, MPC7EQ-10G-B, MPC7EQ-10G-IRB, MPC7EQ-10G-RB, MPC7EQ-MRATE-B, MPC7EQ-MRATE-IRB, MPC7EQ-MRATE-RB Flexible Port

Concentrators (FPCs). If you perform a unified ISSU on a MX Series router with these FPCs installed, the FPCs need to be rebooted in order to complete the unified ISSU process.

- Unified ISSU for MX Series routers does not support the IEEE 802.1ag OAM and IEEE 802.3ah protocols.
- Unified ISSU is not supported when clock synchronization is configured for Synchronous Ethernet, Precision Time Protocol (PTP), and hybrid mode on the MICs and MPCEs on MX240, MX480, and MX960 routers. If clock synchronization is configured, the unified ISSU process terminates.

**NOTE:** For Junos OS Releases 22.1R1 and above, you can use the `request system software in-service-upgrade` command with the `handle-incompatible-config` option to automatically deactivate/activate clock synchronization for PTP and Synchronous Ethernet on the MX960, MX10003, MX10008, MX10016, MX2010, and MX2020 routers.

- On MX Series routers with MPC/MIC interfaces, the policers for transit traffic and statistics are disabled temporarily during the unified ISSU process.
- On MX Series MPCs, interface-specific and firewall filter statistics are preserved across a unified ISSU. During the unified ISSU, counter and policer operations are disabled.
- To preserve statistics across a unified ISSU on MX Series routers with MPC/MIC interfaces, the router stores the statistics data as binary large objects. The router collects the statistics before the unified ISSU is initialized, and restores the statistics after the unified ISSU completes. No statistics are collected during the unified ISSU process.
- After a unified ISSU operation is completed, an MPC reboot is required for MACsec to work. If you upgrade a router from an earlier Junos OS release to Release 14.2R2 or Release 15.1R1 using unified ISSU and MACsec is configured on that router, you must reboot the MPC for MACsec to function properly.
- When there is a large number of subscribers configured, the Layer 2 scheduler can become oversubscribed. The unified ISSU process might terminate when the system runs out of schedulers. The system generates log messages with ISSU failures and CRC errors on the control plane. If you encounter this issue, please contact JTAC for assistance in eliminating the Layer 2 scheduler oversubscription in your configuration.
- MX Series routers support Link Aggregation Control Protocol (LACP) with fast hellos during unified ISSU. This support is disabled by default. You must enable the `fast-hello-issu` option on the main router and on the peer routers before starting unified ISSU. Note that the peer router must also be an MX Series router for this functionality to work.

## Unified ISSU Considerations for PTX Series Routers

Unified ISSU has the following caveats for PTX Series routers:

- Starting with Junos OS Release 13.2, unified ISSU is supported on the PTX5000 and PTX3000 with the FPC-PTX-P1-A FPC. However, you can perform unified ISSU only from Junos OS Release 13.2 to 13.3 and from Junos OS Release 14.1 to a later release. You must *not* perform unified ISSU from Junos OS Release 13.2 or 13.3 to 14.1 and later releases.
- Link Aggregation Control Protocol (LACP) is not supported during unified ISSU on PTX Series routers. You must disable the `lacp` statement at the `[edit interfaces interface-name aggregated-ether-options]` hierarchy level before the unified ISSU process begins and enable it after the unified ISSU process is complete.

## Unified ISSU Considerations for T Series Routers

Unified ISSU has the following caveats for T Series devices:

- During the unified ISSU process on a routing matrix with TX Matrix Plus routers with 3D SIBs, only 75 percent of the traffic remains uninterrupted.
- The scale supported on T640-FPC2-E, T640-FPC2-E2, T640-FPC3-E, and T640-FPC3-E2 Flexible Port Concentrators (FPCs) is less than that supported on T640-FPC1-ES, T640-FPC2-ES, T640-FPC3-ES, T1600-FPC4-ES, and T640-FPC4-1P-ES FPCs because of differences in hardware configuration. Therefore, when a unified ISSU is performed, if the configured scale on any of the FPCs is more than what is supported on that FPC, field-replaceable unit (FRU) upgrade of that FPC fails. To check the current hardware configuration of an FPC, use the `show chassis fpc operational` command.
- The PD-4XGE-XFP PIC goes offline during a unified ISSU if the PIC is installed in a T-1600-FPC4-ES with part number 710-013037 revision 12 or earlier.
- In the FPCs on T4000 routers, interface-specific and firewall filter statistics are preserved across a unified ISSU. During the unified ISSU, counter and policer operations are disabled.
- To preserve statistics across a unified ISSU on T4000 routers with FPC/PIC interfaces, the router stores the statistics data as binary large objects. The router collects the statistics before the unified ISSU is initialized, and restores the statistics after the unified ISSU completes. No statistics are collected during the unified ISSU process.
- To verify that statistics are preserved across the unified ISSU, you can issue CLI operational commands such as `show interfaces statistics` after the unified ISSU completes.
- When you configure the unified ISSU feature on the T4000 Core Router, you can also configure LACP. However, LACP periodic fast mode is not supported. If you configure LACP periodic

transmission, set it to slow mode at both sides before initiating a unified ISSU. If fast mode is configured, the configuration can be committed without any commit or system log error messages, but you might notice that a larger than expected amount of traffic drops because of the LACP links going down during a unified ISSU.

### Unified ISSU Considerations for EX Series Switches

Unified ISSU has the following caveats for EX Series devices:

- EX9204, EX9208, EX9214, and EX9251, and EX9253 switches do not support LACP fast timer configuration starting with Junos OS Release 17.4. If the LACP fast timer is configured, there will be LAG interface flaps traffic loss during ISSU. We recommend moving to LACP slow before beginning ISSU on these devices.

### Unified ISSU Platform Support

Table 19 on page 509 lists the platforms that support unified ISSU when dual Routing Engines are installed and the first Junos OS release that supports unified ISSU on those platforms. In addition to verifying that your platform supports unified ISSU, you need to verify that the field-replaceable unit, such as PICs, that are installed also support unified ISSU.

To access an interactive tool for verifying hardware support for unified ISSU, see the Juniper Networks Feature Explorer (<https://pathfinder.juniper.net/feature-explorer/>).

**Table 19: Unified ISSU Support for Dual Routing Engine Platforms**

Platform	Junos OS Release
EX9200 switch	<ul style="list-style-type: none"> <li>• 12.3R3 or later</li> <li>• 14.2R1 or later on EX9200-32XS, EX9200-4QS, and EX9200-2C-8XS</li> <li>• 17.1R1 or later on EX9200-6QS</li> </ul>
M10i router	9.5R1
M120 router	9.2R1
M320 router	9.0R1

**Table 19: Unified ISSU Support for Dual Routing Engine Platforms *(Continued)***

Platform	Junos OS Release
MX240 router	9.3R1
MX480 router	9.3R1
MX960 router	9.3R1
MX2010 router	13.2R1
MX2020 router	13.2R1
MX104 router	14.1R1
MX Series Virtual Chassis	14.1R1
MX10003 router	18.2R1
PTX5000 router	13.2R1
PTX3000 router	13.2R1
T320 router	9.0R1
T640 router	9.0R1
T1600 router	9.1R1
T4000 router	12.3R1
TX Matrix router	9.3R1



**Table 19: Unified ISSU Support for Dual Routing Engine Platforms (*Continued*)**

Platform	Junos OS Release
TX Matrix Plus router	12.3R2
TX Matrix Plus routers with 3D SIBs	14.1R1

## Unified ISSU Protocol Support for M Series, MX Series, and T Series Routers and EX9200 Switches

To find out which releases support ISSU, please use the [ISSU Feature Explorer](#) tool on the Juniper Networks website. The ISSU Feature Explorer tool contains information about the Juniper Networks devices that support ISSU, the releases that support ISSU for each device, and the SKUs that support ISSU for each release.

**NOTE:** To gain access to the ISSU Feature Explorer tool, you need to log in with a customer or partner account on the Juniper Networks website. For more information on setting up a Juniper Networks account, please see the [Juniper Networks Guide to Creating a User Account](#).

## Unified ISSU Feature Support

Unified ISSU supports most Junos OS features starting in Junos OS Release 9.0. However, the following constraints apply:

- Link Aggregation Control Protocol (LACP)—Link changes are not processed until after the unified ISSU is complete.
- Automatic Protection Switching (APS)—Network changes are not processed until after the unified ISSU is complete.
- Ethernet Operation, Administration, and Management (OAM) as defined by IEEE 802.3ah and by IEEE 802.1ag—When a Routing Engine switchover occurs, the OAM hello message times out, triggering protocol convergence.
- Ethernet circuit cross-connect (CCC) encapsulation—Circuit changes are not processed until after the unified ISSU is complete.
- Logical systems—On devices that have logical systems configured on them, only the primary logical system supports unified ISSU.

**NOTE:** Starting with Junos OS Release 16.1R1, while performing a unified ISSU from a FreeBSD 6.1-based Junos OS to an upgraded FreeBSD 10.x-based Junos OS, the configuration must be validated on a remote host or on a Routing Engine. The remote host or the Routing Engine must be running a Junos OS with an upgraded FreeBSD. In addition, only a few selected directories and files are preserved while upgrading from FreeBSD 6.1-based Junos OS to FreeBSD 10.x-based Junos OS. See [Upgrading Junos OS with Upgraded FreeBSD](#).

## Unified ISSU PIC Support Considerations

The following sections list the PICs that are supported by unified ISSU.

**NOTE:** For information about ISSU support on individual PICs based on device and release, use the [ISSU Feature Explorer](#) tool.

**NOTE:** For information about Flexible PIC Concentrator (FPC) types, FPC/PIC compatibility, and the initial Junos OS release in which a particular PIC is supported on an FPC, see the PIC guide for your platform.

## PIC Considerations

Take the following PIC restrictions into consideration before performing a unified ISSU:

- **Unsupported PICs**—If a PIC is not supported by unified ISSU, at the beginning of the upgrade, the software issues a warning that the PIC will be taken offline. After the PIC is brought offline and the unified ISSU is complete, the PIC is brought back online with the new firmware.
- **PIC combinations**—For some PICs, newer Junos OS services can require significant Internet Processor ASIC memory, and some configuration rules might limit certain combinations of PICs on particular platforms. With a unified ISSU:
  - If a PIC combination is not supported by the software version that the device is being upgraded from, the validation check displays a message and terminates the upgrade.
  - If a PIC combination is not supported by the software version to which the device is being upgraded, the validation check displays a message and terminates the upgrade, even if the PIC combination is supported by the software version from which the device is being upgraded.
- **Interface statistics**—Interface statistics might be incorrect because:

- During bootup of the new microkernel on the Packet Forwarding Engine, host-bound traffic is not handled and might be dropped, causing packet loss.
- During the hardware update of the Packet Forwarding Engine and its interfaces, traffic is halted and discarded. (The duration of the hardware update depends on the number and type of interfaces and on the device configuration.)
- During a unified ISSU, periodic statistics collection is halted. If hardware counters saturate or wrap around, the software does not display accurate interface statistics.
- CIR oversubscription—If oversubscription of the committed information rate (CIR) is configured on logical interfaces:
  - And the sum of the CIR exceeds the physical interface's bandwidth, after a unified ISSU is performed, each logical interface might not be given its original CIR.
  - And the sum of the delay buffer rate configured on logical interfaces exceeds the physical interface's bandwidth, after a unified ISSU is performed, each logical interface might not receive its original delay-buffer-rate calculation.

## SONET/SDH PICs

Table 20 on page 513 lists the SONET/SDH PICs that are supported during a unified ISSU.

**Table 20: Unified ISSU PIC Support: SONET/SDH**

PIC Type	Number of Ports	Model Number	Device
OC3c/STM1	4	PB-4OC3-SON-MM—(EOL) PB-4OC3-SON-SMIR—(EOL)	M120 M320, T320, T640, T1600
		PE-4OC3-SON-MM—(EOL) PE-4OC3-SON-SMIR—(EOL)	M10i
	2	PE-2OC3-SON-MM—(EOL) PE-2OC3-SON-SMIR—(EOL)	
OC3c/STM1 with SFP	2	PE-2OC3-SON-SFP	M10i

Table 20: Unified ISSU PIC Support: SONET/SDH (Continued)

PIC Type	Number of Ports	Model Number	Device
OC3c/STM1, SFP (Multi-Rate)	4 OC3 ports, 4 OC12 ports	PB-4OC3-4OC12-SON-SFP	M120 M320, MX Series, T320, T640, T1600, T4000, TX Matrix Plus, TX Matrix Plus with 3D SIBs
	4 OC3 ports, 1 OC12 port	PB-4OC3-1OC12-SON-SFP PB-4OC3-1OC12-SON2-SFP	
		PE-4OC3-1OC12-SON-SFP	M10i
OC12c/STM4	1	PE-1OC12-SON-SFP PE-1OC12-SON-MM—(EOL) PE-1OC12-SON-SMIR—(EOL)	M10i
		PB-1OC12-SON-MM—(EOL) PB-1OC12-SON-SMIR—(EOL)	M120, M320, T320, T640, T1600, T4000, TX Matrix, TX Matrix Plus with 3D SIBs
	4	PB-4OC12-SON-MM PB-4OC12-SON-SMIR	
OC12c/STM4, SFP	1	PB-1OC12-SON-SFP	M120, M320, T320, T640, T1600, TX Matrix, TX Matrix Plus
OC48c/STM16, SFP	1	PB-1OC48-SON-SFP PB-1OC48-SON-B-SFP	M120, M320, MX Series, T320, T640, T1600, TX Matrix, T4000, TX Matrix Plus, TX Matrix Plus with 3D SIBs
	4	PC-4OC48-SON-SFP	
OC192/STM64	1	PC-1OC192-SON-VSR	MX Series routers

**Table 20: Unified ISSU PIC Support: SONET/SDH (Continued)**

PIC Type	Number of Ports	Model Number	Device
OC192/STM64, XFP	1	PC-1OC192-SON-LR PC-1OC192-SON-SR2 PC-1OC192-VSR	M320, T320, T640, T1600, T4000, TX Matrix Plus with 3D SIBs
OC192/STM64, XFP	4	PD-4OC192-SON-XFP	M120, T640, T1600, T4000, TX Matrix Plus with 3D SIBs
	1	PC-1OC192-SON-XFP	T4000, MX Series routers, TX Matrix Plus with 3D SIBs
OC768/STM256	1	PD-1OC768-SON-SR	T640, T1600, T4000, TX Matrix Plus, TX Matrix Plus with 3D SIBs

### Fast Ethernet and Gigabit Ethernet PICs

Table 21 on page 516 lists the Fast Ethernet and Gigabit Ethernet PICs that are supported during a unified ISSU.

**NOTE:** Starting with Junos OS Release 9.2, new Ethernet IQ2 PIC features might cause the software to reboot the PIC when a unified ISSU is performed. For information about applicable new Ethernet IQ2 PIC features, refer to the release notes for the specific Junos OS release.

**Table 21: Unified ISSU PIC Support: Fast Ethernet and Gigabit Ethernet**

PIC Type	Number of Ports	Model Number	Device
Fast Ethernet	4	PB-4FE-TX	M120, M320, T320, T640, T1600, TX Matrix
		PE-4FE-TX	M10i
	8	PB-8FE-FX	M120, M320
		PE-8FE-FX	M10i
	12	PB-12FE-TX-MDI PB-12FE-TX-MDIX	M120, M320, T320
		PE-12FE-TX-MDI PE-12FE-TX-MDIX	M10i
	48	PB-48FE-TX-MDI PB-48FE-TX-MDIX	M120, M320, T320
Gigabit Ethernet, RJ-45	40	EX9200-40T	EX9200
Gigabit Ethernet, SFP	1	PE-1GE-SFP	M10i
		PB-1GE-SFP	M120, M320, T320, T640, T1600, T4000, TX Matrix, TX Matrix Plus, TX Matrix Plus with 3D SIBs
	2	PB-2GE-SFP	
	4	PB-4GE-SFP	
	10	PC-10GE-SFP	

Table 21: Unified ISSU PIC Support: Fast Ethernet and Gigabit Ethernet *(Continued)*

PIC Type	Number of Ports	Model Number	Device
	40	EX9200-40F	EX9200
Gigabit Ethernet IQ, SFP	1	PE-1GE-SFP-QPP	M10i
		PB-1GE-SFP-QPP	M120, M320, T320, T640, T1600, T4000, TX Matrix, TX Matrix Plus, TX Matrix Plus with 3D SIBs
	2	PB-2GE-SFP-QPP	
Gigabit Ethernet IQ2, SFP	4	PB-4GE-TYPE1-SFP-IQ2	M120, M320, T320, T640, T1600, T4000, TX Matrix, TX Matrix Plus, TX Matrix Plus with 3D SIBs
	8	PB-8GE-TYPE2-SFP-IQ2 PC-8GE-TYPE3-SFP-IQ2	
Gigabit Ethernet IQ2, XFP	1	PC-1XGE-TYPE3-XFP-IQ2	M120, M320, T320, T640, T1600, TX Matrix, TX Matrix Plus, TX Matrix Plus with 3D SIBs
10-Gigabit Ethernet XFP	4	PD-4XGE-XFP  <b>NOTE:</b> This PIC goes offline during a unified ISSU if the PIC is inserted on T-1600-FPC4-ES with part number 710-013037 revision 12 or below.	T640, T1600, T4000, TX Matrix, TX Matrix Plus, TX Matrix Plus with 3D SIBs
10-Gigabit Ethernet SFP +	10	PD-5-10XGE-SFPP	T640, T1600, T4000, TX Matrix Plus, TX Matrix Plus with 3D SIBs
	24	P1-PTX-24-10GE-SFPP EX9200-6QS	PTX5000 EX9200

**Table 21: Unified ISSU PIC Support: Fast Ethernet and Gigabit Ethernet (Continued)**

PIC Type	Number of Ports	Model Number	Device
	32	EX9200-32XS	EX9200
10-Gigabit Ethernet, DWDM	1	PC-1XGE-DWDM-CBAND	M120, M320, T320, T640, T1600, TX Matrix, TX Matrix Plus, TX Matrix Plus with 3D SIBs
10-Gigabit Ethernet, DWDM OTN	1	PC-1XGE-DWDM-OTN	T4000, TX Matrix Plus with 3D SIBs
10-Gigabit Ethernet LAN/WAN PIC with SFP +	12	PF-12XGE-SFPP	T4000, TX Matrix Plus with 3D SIBs
	24	PF-24XGE-SFPP	T4000, TX Matrix Plus with 3D SIBs
10-Gigabit Ethernet, SFP +	32	14.2R1 or later EX9200-32XS	EX9200
10-Gigabit Ethernet, XENPAK	1	PC-1XGE-XENPAK	M120, M320, T320, T640, T1600, T4000, TX Matrix, TX Matrix Plus, TX Matrix Plus with 3D SIBs
40-Gigabit Ethernet, CFP	2	P1-PTX-2-40GE-CFP	PTX5000
10-Gigabit Ethernet, 40-Gigabit Ethernet, QFSP+	16/4	14.2R1 or later EX9200-4QS	EX9200
	24/6	17.1R1 or later EX9200-6QS	
	48/12	P2-10G-40G-QSFPP	PTX5000



**Table 21: Unified ISSU PIC Support: Fast Ethernet and Gigabit Ethernet (Continued)**

PIC Type	Number of Ports	Model Number	Device
100-Gigabit Ethernet, CFP	1	PF-1CGE-CFP	T4000, TX Matrix Plus with 3D SIBs
	2	P1-PTX-2-100GE-CFP	PTX5000
	4	P2-100GE-CFP2	PTX5000
100-Gigabit Ethernet CFP/10-Gigabit Ethernet SFP+	2/8	EX9200-2C-8XS	EX9200
100-Gbps DWDM OTN	2	P1-PTX-2-100G-WDM	PTX5000
100-Gbps OTN, CFP2	4	P2-100GE-OTN	PTX5000

## Channelized PICs

[Table 22 on page 519](#) lists the channelized PICs that are supported during a unified ISSU.

**Table 22: Unified ISSU PIC Support: Channelized**

PIC Type	Number of Ports	Model Number	Platform
Channelized E1 IQ	10	PB-10CHE1-RJ48-QPP	M120, M320, T320, T640, T1600, TX Matrix
		PB-10CHE1-RJ48-QPP-N	M120
		PE-10CHE1-RJ48-QPP	M10i
		PE-10CHE1-RJ48-QPP-N	

**Table 22: Unified ISSU PIC Support: Channelized (Continued)**

PIC Type	Number of Ports	Model Number	Platform
Channelized T1 IQ	10	PB-10CHT1-RJ48-QPP	M320, T320, T640, T1600
		PE-10CHT1-RJ48-QPP	M10i
Channelized OC IQ	1	PB-1CHOC12SMIR-QPP PB-1CHSTM1-SMIR-QPP PB-1CHOC3-SMIR-QPP	M120, M320, T320, T640, T1600, TX Matrix, TX Matrix Plus
		PE-1CHOC12SMIR-QPP PE-1CHOC3-SMIR-QPP	M10i
Channelized DS3 to DS0 IQ	4	PB-4CHDS3-QPP	M120, M320, T320, T640, T1600, TX Matrix, TX Matrix Plus
		PE-4CHDS3-QPP	M10i
Channelized STM 1	1	PE-1CHSTM1-SMIR-QPP	M10i

## Tunnel Services PICs

[Table 23 on page 520](#) lists the Tunnel Services PICs that are supported during a unified ISSU.

**Table 23: Unified ISSU PIC Support: Tunnel Services**

PIC Type	Model Number	Platform
1-Gbps Tunnel	PE-TUNNEL	M10i

**Table 23: Unified ISSU PIC Support: Tunnel Services (Continued)**

PIC Type	Model Number	Platform
	PB-TUNNEL-1	M120, M320, T320, T640, T1600, TX Matrix, TX Matrix Plus
4-Gbps Tunnel	PB-TUNNEL	
10-Gbps Tunnel	PC-TUNNEL	

## ATM PICs

Table 24 on page 521 lists the ATM PICs that are supported during a unified ISSU. The table includes support on Enhanced III FPCs.

**Table 24: Unified ISSU PIC Support: ATM**

PIC Type	Number of Ports	Model Number	Platform
DS3	4	PB-4DS3-ATM2	M120, M320, T320, T640, T1600, TX Matrix
		PE-4DS3-ATM2	M10i
E3	4	PB-4E3-ATM2	M120, M320, T320, T640, T1600, TX Matrix, TX Matrix Plus
	2	PE-2E3-ATM2	M10i
OC3/STM1	2	PB-2OC3-ATM2-MM PB-2OC3-ATM2-SMIR	M120, M320, T320, T640, T1600, TX Matrix, TX Matrix Plus
		PE-2OC3-ATM2-MM PE-2OC3-ATM2-SMIR	M10i

**Table 24: Unified ISSU PIC Support: ATM (Continued)**

PIC Type	Number of Ports	Model Number	Platform
OC12/STM4	1	PB-1OC12-ATM2-MM PB-1OC12-ATM2-SMIR	M120, M320, T320, T640, T1600, TX Matrix, TX Matrix Plus
	2	PB-2OC12-ATM2-MM PB-2OC12-ATM2-SMIR	M120, M320, T320, T640, T1600, T4000, TX Matrix, TX Matrix Plus, TX Matrix Plus with 3D SIBs
	1	PE-1OC12-ATM2-MM PE-1OC12-ATM2-SMIR	M10i
OC48/STM16	1	PB-1OC48-ATM2-SFP	M120, M320, T320, T640, T1600, TX Matrix, TX Matrix Plus

## Serial PICs

Unified ISSU supports the following 2-port EIA-530 serial PICs:

- PB-2EIA530 on M320 routers with Enhanced III FPCs, and on M120 routers
- PE-2EIA530 on M10i routers

## DS3, E1, E3, and T1 PICs

Unified ISSU supports the following PICs on M120, M320, and T320 routers; T640 and T1600 routers; and the TX Matrix router:

- 4-Port DS3 PIC (PB-4DS3)
- 4-Port E1 Coaxial PIC (PB-4E1-COAX)
- 4-Port E1 RJ48 PIC (PB-4E1-RJ48)
- 4-Port E3 IQ PIC (PB-4E3-QPP)
- 4-Port T1 PIC (PB-4T1-RJ48)

**NOTE:** Unified ISSU is also supported on the 4-Port DS3 PIC (PB-4DS3) and the 4-Port E3 IQ PIC (PB-4E3-QPP) on the TX Matrix Plus router.

Unified ISSU supports the following PICs on M10i routers:

- 2-Port DS3 PIC (PE-2DS3)
- 4-Port DS3 PIC (PE-4DS3)
- 4-Port E1 PICs (PE-4E1-COAX and PE-4E1-RJ48)
- 2-Port E3 PIC (PE-2E3)
- 4-Port T1 PIC (PE-4T1-RJ48)
- 4-Port E3 IQ PIC (PE-4E3-QPP)

### Enhanced IQ PICs

Unified ISSU supports the following PICs on M120 router, M320 router, and on T320 routers; T640 routers, T1600 routers, TX Matrix router, and the TX Matrix Plus router:

- 1-Port Channelized OC12/STM4 Enhanced IQ PIC (PB-1CHOC12-STM4-IQE-SFP)
- 1-Port nonchannelized OC12/STM4 Enhanced IQ PIC (PB-1OC12-STM4-IQE-SFP)
- 4-Port Channelized DS3/E3 Enhanced IQ PIC (PB-4CHDS3-E3-IQE-BNC)
- 4-Port nonchannelized DS3/E3 Enhanced IQ PIC (PB-4DS3-E3-IQE-BNC)
- 4-Port nonchannelized SONET/SDH OC48/STM16 Enhanced IQ (IQE) PIC with SFP (PC-4OC48-STM16-IQE-SFP)

Unified ISSU supports 1-port Channelized OC48/STM16 Enhanced IQ (IQE) PIC with SFP (PB-1CHOC48-STM16-IQE-SFP) on MX Series routers.

### Enhanced IQ2 Ethernet Services Engine (ESE) PIC

Unified ISSU supports the enhanced IQ2 ESE PICs listed in [Table 25 on page 524](#).

**Table 25: Unified ISSU Support: Enhanced IQ2 Ethernet Services Engine (ESE) PIC**

Model Number	Number of Ports	Platform
PC-8GE-TYPE3-SFP-IQ2E	8	M120, M320, T320, T640, T4000 TX Matrix, TX Matrix Plus, TX Matrix Plus with 3D SIBs
PB-8GE-TYPE2-SFP-IQ2E	8	M120, M320, T320, T640, TX Matrix, TX Matrix Plus, TX Matrix Plus with 3D SIBs
PB-4GE-TYPE1-SFP-IQ2E	4	M120, M320, T320, T640
PC-1XGE-TYPE3-XFP-IQ2E	1	M120, M320, T320, T640, T4000, TX Matrix, TX Matrix Plus, TX Matrix Plus with 3D SIBs
PB-1CHOC48-STM16-IQE	1	M120, M320, T320, T640, T4000, TX Matrix, TX Matrix Plus, TX Matrix Plus with 3D SIBs
PE-4GE-TYPE1-SFP-IQ2E	4	M10i
PE-4GE-TYPE1-SFP-IQ2	4	M10i

### Unified ISSU FPC Support on T4000 Routers

In the FPCs on T4000 routers, interface-specific and firewall filter statistics are preserved across a unified ISSU. During the unified ISSU, counter and policer operations are disabled.

To preserve statistics across a unified ISSU on T4000 routers with FPC/PIC interfaces, the router stores the statistics data as binary large objects. The router collects the statistics before the unified ISSU is initialized, and restores the statistics after the unified ISSU completes. No statistics are collected during the unified ISSU process.

To verify that statistics are preserved across the unified ISSU, you can issue CLI operational commands such as `show interfaces statistics` after the unified ISSU completes.

Unified ISSU is supported on the following FPCs:

- T4000 FPC5 (model numbers—T4000-FPC5-3D and T4000-FPC5-LSR)
- Enhanced Scaling FPC4-1P (model number—T640-FPC4-1P-ES)
- Enhanced Scaling FPC4 (T1600-FPC4-ES)
- Enhanced Scaling FPC3 (T640-FPC3-ES)
- Enhanced Scaling FPC2 (T640-FPC2-ES)

**NOTE:** The aforementioned FPCs are also supported on TX Matrix Plus routers with 3D SIBs.

## Unified ISSU Support on MX Series 3D Universal Edge Routers

The following sections list the Dense Port Concentrators (DPCs), Flexible PIC Concentrators (FPCs), Modular Port Concentrators (MPCs), and Modular Interface Cards (MICs) that are supported during a unified ISSU on MX Series routers.

### Unified ISSU DPC and FPC Support on MX Series Routers

Unified ISSU supports all DPCs except the Multiservices DPC on MX Series routers. Unified ISSU also supports Type 2 FPC (MX-FPC2) and Type 3 FPC (MX-FPC3) on MX Series routers. For more information about DPCs and FPCs on MX Series routers, go to [https://www.juniper.net/documentation/en\\_US/release-independent/junos/information-products/pathway-pages/mx-series/](https://www.juniper.net/documentation/en_US/release-independent/junos/information-products/pathway-pages/mx-series/).

### Unified ISSU MIC and MPC Support on MX Series Routers

Unified ISSU supports all the Modular Port Concentrators (MPCs) and Modular Interface Cards (MICs) listed in [Table 26 on page 526](#) and [Table 27 on page 527](#). Unified ISSU is not supported on MX80 routers.

In the MPCs on MX Series routers, interface-specific and firewall filter statistics are preserved across a unified ISSU. During the unified ISSU, counter and policer operations are disabled.

To preserve statistics across a unified ISSU on MX Series routers with MPC/MIC interfaces, the router stores the statistics data as binary large objects. The router collects the statistics before the unified ISSU is initialized, and restores the statistics after the unified ISSU completes. No statistics are collected during the unified ISSU process.

To verify that statistics are preserved across the unified ISSU, you can issue CLI operational commands such as `show interfaces statistics` after the unified ISSU completes.

**Table 26: Unified ISSU Support: MX Series Router MPCs**

MPC Type	Number of Ports	Model Number	Platform
MPC1	—	MX-MPC1-3D	MX Series routers
MPC1E	—	MX-MPC1E-3D	MX Series routers
MPC1 Q	—	MX-MPC1-3D-Q	MX Series routers
MPC1E Q	—	MX-MPC1E-3D-Q	MX Series routers
MPC2	—	MX-MPC2-3D	MX Series routers
MPC2E	—	MX-MPC2E-3D	MX Series routers
MPC2 Q	—	MX-MPC2-3D-Q	MX Series routers
MPC2E Q	—	MX-MPC2E-3D-Q	MX Series routers
MPC2 EQ	—	MX-MPC2-3D-EQ	MX Series routers
MPC2E EQ	—	MX-MPC2E-3D-EQ	MX Series routers
16x10GE MPC	16	MPC-3D-16XGE-SFPP	MX Series routers
MPC3E	—	MX-MPC3E-3D	MX Series routers
32x10GE MPC4E	32	MPC4E-3D-32XGE-SFPP	MX Series routers
2x100GE + 8x10GE MPC4E	10	MPC4E-3D-2CGE-8XGE	MX Series routers
6x40GE + 24x10GE MPC5E	30	MPC5E-40G10G	MX Series routers



**Table 26: Unified ISSU Support: MX Series Router MPCs (Continued)**

MPC Type	Number of Ports	Model Number	Platform
6x40GE + 24x10GE MPC5EQ	30	MPC5EQ-40G10G	MX Series routers
2x100GE + 4x10GE MPC5E	6	MPC5E-100G10G	MX Series routers
2x100GE + 4x10GE MPC5EQ	6	MPC5EQ-100G10G	MX Series routers
MPC6E	2	MX2K-MPC6E	MX Series routers
MPC7E (multi-rate)	12	MPC7E-MRATE	MX Series routers
MPC7E 10G	40	MPC7E-10G	MX Series routers
MPC8E	—	MX2K-MPC8E	MX Series routers
MPC9E	—	MX2K-MPC9E	MX Series routers

**Table 27: Unified ISSU Support: MX Series Router MICs**

MIC Type	Number of Ports	Model Number	Platform
ATM MIC with SFP	8	MIC-3D-8OC3-2OC12-ATM	MX Series routers
Channelized SONET/SDH OC192/STM64 MIC with XFP	4	MIC-3D-1OC192-XFP	MX Series routers
Channelized OC3/STM1 (Multi-Rate) Circuit Emulation MIC with SFP	4	MIC-3D-4COC3-1COC12-CE	MX Series routers
Channelized E1/T1 Circuit Emulation MIC	16	MIC-3D-16CHE1-T1-CE	MX Series routers

**Table 27: Unified ISSU Support: MX Series Router MICs (Continued)**

MIC Type	Number of Ports	Model Number	Platform
Channelized SONET/SDH OC3/STM1 (Multi-Rate) MICs with SFP	4	MIC-3D-4CHOC3-2CHOC12	MX Series routers
Channelized SONET/SDH OC3/STM1 (Multi-Rate) MICs with SFP	8	MIC-3D-4CHOC3-2CHOC12	MX Series routers
Channelized DS3/E3 MIC	8	MIC-3D-8CHDS3-E3-B	MX Series routers
DS3/E3	8	MIC-3D-8DS3-E3	MX Series routers
See <a href="#">MIC MRATE</a> for MIC Type	12	MIC MRATE	MX Series routers
40-Gigabit Ethernet MIC with QSFP	2	MIC3-3D-2X40GE-QSFP	MX Series routers
10-Gigabit Ethernet MIC with SFPP	10	MIC3-3D-10XGE-SFPP	MX Series routers
100-Gigabit Ethernet MIC with CXP	1	MIC3-3D-1X100GE-CXP	MX Series routers
100-Gigabit Ethernet MIC with CFP	1	MIC3-3D-1X100GE-CFP	MX Series routers
Gigabit Ethernet MIC with SFP	20	MIC-3D-20GE-SFP	MX Series routers
10-Gigabit Ethernet MIC with SFP+ (24 Ports)	24	MIC6-10G	MX Series routers
10-Gigabit Ethernet DWDM OTN MIC (non-OTN mode only)	24	MIC6-10G-OTN	MX Series routers
100-Gigabit Ethernet MIC with CFP2 (non-OTN mode only)	2	MIC6-100G-CFP2	MX Series routers

**Table 27: Unified ISSU Support: MX Series Router MICs (Continued)**

MIC Type	Number of Ports	Model Number	Platform
100-Gigabit Ethernet MIC with CXP (4 Ports)	4	MIC6-100G-CXP	MX Series routers
10-Gigabit Ethernet MICs with XFP	2	MIC-3D-2XGE-XFP	MX Series routers
10-Gigabit Ethernet MICs with XFP	4	MIC-3D-4XGE-XFP	MX Series routers
SONET/SDH OC3/STM1 (Multi-Rate) MICs with SFP	4	MIC-3D-4OC3OC12-1OC48	MX Series routers
SONET/SDH OC3/STM1 (Multi-Rate) MICs with SFP	8	MIC-3D-8OC3OC12-4OC48	MX Series routers
Tri-Rate Copper Ethernet MIC	40	MIC-3D-40GE-TX	MX Series routers
100-Gigabit DWDM OTn MIC with CFP2-ACO	1	MIC3-100G-DWDM	MX960 routers

**NOTE:** Note that unified ISSU is supported only by the MICs listed in [Table 27 on page 527](#).

**NOTE:** Consider the following guidelines before performing a unified ISSU on an MX Series router with ATM interfaces at scale:

- The PPP keepalive interval must be 10 seconds or greater. PPP requires three keepalives to fail before it brings down the session. Thirty seconds (ten seconds multiplied by three) provides a safe margin to maintain PPP sessions across the unified ISSU in case of any traffic loss during the operation. Configure the interval with the keepalives statement at the [edit interfaces at-*interface-name*] or [edit interfaces at-*interface-name* unit *logical-unit-number*] hierarchy level.

- The OAM F5 loopback cell period must be 20 seconds or greater to maintain ATM connectivity across the unified ISSU. Configure the interval with the `oam-period` statement at the `[edit interfaces at-interface-name unit logical-unit-number]` hierarchy level.

## Unified ISSU Limitations on MX Series Routers

Unified ISSU is currently not supported when clock synchronization is configured for Synchronous Ethernet, Precision Time Protocol (PTP), and hybrid mode on MX80 routers and on the MICs and MPCEs on MX240, MX480, and MX960 routers.

**NOTE:** For Junos OS Releases 22.1R1 and above, you can use the `request system software in-service-upgrade` command with the `handle-incompatible-config` option to automatically deactivate/activate clock synchronization for PTP and Synchronous Ethernet on the MX960, MX10003, MX10008, MX10016, MX2010, and MX2020 routers.

**NOTE:** Before enabling ISSU on MX routers, when upgrading from a Junos OS Release 14.1 or earlier to Junos OS Release 14.2 or later, you must disable IGMP snooping, and PIM snooping, in all protocol hierarchies. This includes the bridge-domain and routing-instances hierarchies.

**NOTE:** On MX Series routers with MPC/MIC interfaces, the policers for transit traffic and statistics are disabled temporarily during the unified ISSU process.

## Release History Table

Release	Description
17.4	Unified ISSU is supported with Junos OS Release 17.4R1 for MX Series routers
17.4	EX9204, EX9208, EX9214, and EX9251, and EX9253 switches do not support LACP fast timer configuration starting with Junos OS Release 17.4.
16.1R1	Starting with Junos OS Release 16.1R1, while performing a unified ISSU from a FreeBSD 6.1-based Junos OS to an upgraded FreeBSD 10.x-based Junos OS, the configuration must be validated on a remote host or on a Routing Engine.

13.3	On MX Series 3D Universal Edge Routers with MPC3E and MPC4E interfaces, unified ISSU is supported starting with Junos OS Release 13.3.
13.2	Starting with Junos OS Release 13.2, unified ISSU is supported on the PTX5000 and PTX3000 with the FPC-PTX-P1-A FPC.
11.2	On MX Series 3D Universal Edge Routers (with Modular Port Concentrator/Modular Interface Card (MPC/MIC) interfaces), unified ISSU is supported starting with Junos OS Release 11.2.

RELATED DOCUMENTATION

Getting Started with Unified In-Service Software Upgrade
Best Practices for Performing a Unified ISSU
Understanding the Unified ISSU Process
Example: Performing a Unified ISSU
<a href="#">Configuring LACP for Aggregated Ethernet Interfaces</a>
<i>request system software validate on (Junos OS with Upgraded FreeBSD)</i>

# Performing a Unified ISSU

## IN THIS CHAPTER

- [Performing a Unified ISSU | 532](#)

## Performing a Unified ISSU

### SUMMARY

Follow the steps below to perform a unified ISSU.

### IN THIS SECTION

- [Best Practices for Performing a Unified ISSU | 532](#)
- [Example: Performing a Unified ISSU | 533](#)
- [Performing an In-Service Software Upgrade \(ISSU\) with Non-Stop Routing | 572](#)
- [Performing an In-Service Software Upgrade \(ISSU\) in ACX5000 Series Routers | 576](#)
- [How to Use Unified ISSU with Enhanced Mode | 581](#)
- [Verifying a Unified ISSU | 585](#)
- [Troubleshooting Unified ISSU Problems | 587](#)
- [Managing and Tracing BFD Sessions During Unified ISSU Procedures | 587](#)

### Best Practices for Performing a Unified ISSU

When you are planning to perform a unified in-service software upgrade (ISSU), choose a time when your network is as stable as possible. As with a normal upgrade, Telnet sessions, SNMP, and CLI access are briefly interrupted. In addition, the following restrictions apply:

- The primary Routing Engine and backup Routing Engine must be running the same software version before you can perform a unified ISSU.
- Verify that your platform supports the unified ISSU feature.
- Read the “Unified ISSU Considerations” topic in the chapter ["Unified ISSU System Requirements"](#) on [page 504](#) to anticipate any special circumstances that might affect your upgrade.

## SEE ALSO

Example: Performing a Unified ISSU

Verifying a Unified ISSU

Troubleshooting Unified ISSU Problems

## Example: Performing a Unified ISSU

### IN THIS SECTION

- [Requirements | 533](#)
- [Overview | 535](#)
- [Configuration | 535](#)
- [Verifying Dual Routing Engines and Enabling GRES and NSR | 536](#)
- [Verifying the Software Versions and Backing Up the Device Software | 539](#)
- [Adjusting Timers and Changing Feature-Specific Configuration | 540](#)
- [Upgrading and Rebooting Both Routing Engines Automatically | 542](#)
- [Restoring Feature-Specific Configuration | 550](#)
- [Upgrading Both Routing Engines and Rebooting the New Backup Routing Engine Manually | 552](#)
- [Upgrading and Rebooting Only One Routing Engine | 561](#)

This example shows how to perform a unified in-service software upgrade (ISSU).

### Requirements

This example uses the following hardware and software components:

- MX480 router with dual Routing Engines

- Junos OS Release 13.3R6 as the starting release
- Junos OS Release 14.1R4 as the ending release

### Before You Begin

Before you perform a unified ISSU, be sure you:

- Perform a compatibility check to ensure that the software and hardware components and the configuration on the device support unified ISSU by using the `"request system software validate in-service-upgrade"` on page 1327 command
- Read the chapter ["Unified ISSU System Requirements" on page 504](#) to anticipate any special circumstances that might affect your upgrade.
  - Verify that your platform supports the unified ISSU feature.
  - Verify that the field-replaceable units (FRUs) installed in your platform support the unified ISSU feature or that you can accept the results of performing the upgrade with some FRUs that do not support unified ISSU.
  - Verify that the protocols and features configured on your platform support the unified ISSU feature or that you can accept the results of performing the upgrade with some protocols and features that do not support unified ISSU.
- Download the software package from the Juniper Networks Support website at <https://www.juniper.net/support/> and place the package on your local server.

**BEST PRACTICE:** When you access the Download Software web page for your device, record the md5 checksum. After downloading the software package to your device, confirm that it is not modified in any way by using the `file checksum md5` command. For more information about verifying the md5 checksum, see <https://kb.juniper.net/InfoCenter/index?page=content&id=KB17665>.

**NOTE:** Starting with Junos OS Release 16.1R1, while performing a unified ISSU from a FreeBSD 6.1 based Junos OS to an upgraded FreeBSD 10.x based Junos OS, the configuration must be validated on a remote host or on a routing engine. The remote host or the routing engine must be running a Junos OS with an upgraded FreeBSD. In addition, only a few selected directories and files will be preserved while upgrading from FreeBSD 6.1 based Junos OS to FreeBSD 10.x based Junos OS. See [Upgrading Junos OS with Upgraded FreeBSD](#) and `request system software validate on (Junos OS with Upgraded FreeBSD)`



## Overview

### IN THIS SECTION

- [Topology | 535](#)

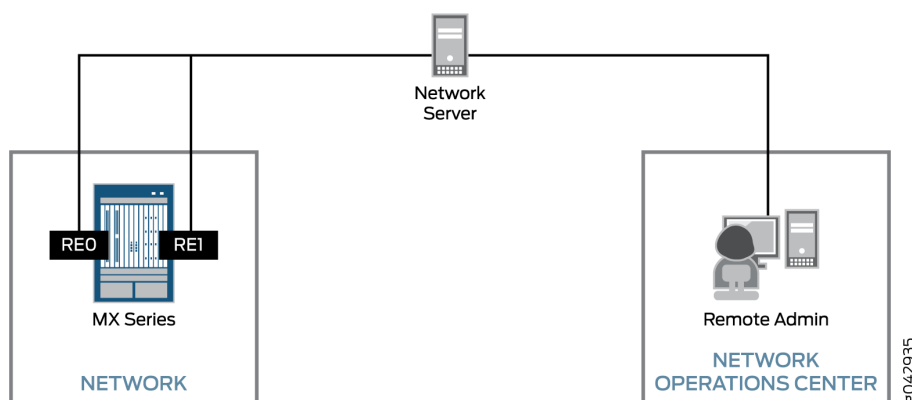
This procedure can be used to upgrade M Series, T Series, MX Series, EX Series, and PTX Series devices that have dual Routing Engines installed and support unified ISSU.

In the example, the hostnames, filenames, and FRUs are representational. When you perform the procedure on your device, the hostnames, filenames, and FRUs are different. The command output is truncated to only show the text of interest in this procedure.

### *Topology*

[Figure 35 on page 535](#) shows the topology used in this example.

**Figure 35: Unified ISSU Example Topology**



### Configuration

There are variations of the procedure depending on if you want to install the new software on one or both Routing Engines and if you want to automatically reboot both Routing Engines or manually reboot one of the Routing Engines.

In all cases, you must verify that dual Routing Engines are installed and that graceful Routing Engine switchover (GRES) and nonstop active routing (NSR) are enabled. We recommend that you back up the device software before the upgrade.

To perform a unified ISSU, select the appropriate tasks from the following list:

- ["Verifying Dual Routing Engines and Enabling GRES and NSR" on page 536](#)
- ["Verifying the Software Versions and Backing Up the Device Software" on page 539](#)
- ["Adjusting Timers and Changing Feature-Specific Configuration" on page 540](#)
- ["Upgrading and Rebooting Both Routing Engines Automatically" on page 542](#)
- ["Restoring Feature-Specific Configuration" on page 550](#)
- ["Upgrading Both Routing Engines and Rebooting the New Backup Routing Engine Manually" on page 552](#)
- ["Upgrading and Rebooting Only One Routing Engine" on page 561](#)

## Verifying Dual Routing Engines and Enabling GRES and NSR

### IN THIS SECTION

- [Procedure | 536](#)

### *Procedure*

#### Step-by-Step Procedure

Enabling GRES and NSR is required regardless of which variation of the unified ISSU procedure you use.

To verify that your device has dual Routing Engines and to enable GRES and NSR:

1. Log in to your device.

2. Verify that dual Routing Engines are installed in your device by using the `show chassis hardware` command.

```
user@host> show chassis hardware
Routing Engine 0 REV 01   740-051822   9013086837   RE-S-1800x4
Routing Engine 1 REV 01   740-051822   9013086740   RE-S-1800x4
```

The command output contains lines listing Routing Engine 0 and Routing Engine 1.

3. By default, GRES is disabled; if you have not already done so, enable GRES by including the `graceful-switchover` statement at the `[edit chassis redundancy]` hierarchy level on the primary Routing Engine.

```
[edit ]
user@host# set chassis redundancy graceful-switchover
```

4. By default, NSR is disabled; if you have not already done so, enable NSR by including the `nonstop-routing` statement at the `[edit routing-options]` hierarchy level.

```
[edit]
user@host# set routing-options nonstop-routing
```

5. When you configure NSR, you must also include the `commit synchronize` statement at the `[edit system]` hierarchy level so that configuration changes are synchronized on both Routing Engines.

```
[edit]
user@host# set system commit synchronize
```

6. After you have verified your configuration and are satisfied with it, commit the changes by using the `commit` command.

```
[edit]
user@host# commit
commit complete
```

When you enable GRES and commit the configuration, the CLI prompt changes to indicate which Routing Engine you are using. For example:

```
{master} [edit]
user@host#
```

7. Exit configuration mode by using the `exit` command.

```
{master} [edit]
user@host# exit
Exiting configuration mode
```

8. Verify that NSR is configured on the primary Routing Engine (re0) by using the `show task replication` command.

```
{master}
user@host> show task replication
    Stateful Replication: Enabled
    RE mode: Master

    Protocol           Synchronization Status
    -----
    OSPF                Complete
    IS-IS               Complete
```

In the output, verify that the Synchronization Status field displays Complete.

9. Verify that GRES is enabled on the backup Routing Engine (re1) by using the `show system switchover` command.

```
user@host> request routing-engine login re1
{backup}
user@host> show system switchover
Graceful switchover: On
Configuration database: Ready
Kernel database: Ready
Peer state: Steady State
```

In the output, verify that the Graceful switchover field state displays On. For more information about the `show system switchover` command, see ["show system switchover" on page 1526](#).

## Verifying the Software Versions and Backing Up the Device Software

### IN THIS SECTION

- [Procedure | 539](#)

### *Procedure*

#### Step-by-Step Procedure

Unified ISSU requires that both Routing Engines are running the same version of Junos OS before the upgrade. As a preventive measure in case any problems occur during an upgrade, it is a best practice to back up the system software to the device hard disk.

To verify the software versions and back up the device software:

1. Verify that the same version of Junos OS is installed and running on both Routing Engines by using the `show version` command.

```
{backup}
user@host> show version invoke-on all-routing-engines
re0:
-----
Hostname: host
Model: mx480
Junos: 13.3R6.5
JUNOS Base OS boot [13.3R6.5]
JUNOS Base OS Software Suite [13.3R6.5]
JUNOS 64-bit Kernel Software Suite [13.3R6.5]
JUNOS Crypto Software Suite [13.3R6.5]
JUNOS Packet Forwarding Engine Support (M/T/EX Common) [13.3R6.5]
JUNOS Packet Forwarding Engine Support (MX Common) [13.3R6.5]
JUNOS Online Documentation [13.3R6.5]

re1:
-----
Hostname: host
Model: mx480
Junos: 13.3R6.5
```

```

JUNOS Base OS boot [13.3R6.5]
JUNOS Base OS Software Suite [13.3R6.5]
JUNOS 64-bit Kernel Software Suite [13.3R6.5]
JUNOS Crypto Software Suite [13.3R6.5]
JUNOS Packet Forwarding Engine Support (M/T/EX Common) [13.3R6.5]
JUNOS Packet Forwarding Engine Support (MX Common) [13.3R6.5]
JUNOS Online Documentation [13.3R6.5]

```

2. Back up the system software to the device hard disk by using the `request system snapshot` command on *each* Routing Engine.

**NOTE:** The root file system is backed up to `/altroot`, and `/config` is backed up to `/altconfig`. After you issue the `request system snapshot` command, the device flash and hard disks are identical. You can return to the previous version of the software only by booting the device from removable media.

```

{backup}
user@host> request system snapshot
user@host> request routing-engine login re0
{master}
user@host> request system snapshot

```

## Adjusting Timers and Changing Feature-Specific Configuration

### IN THIS SECTION

- [Procedure | 540](#)

### *Procedure*

#### Step-by-Step Procedure

If you have any of the following feature-specific configuration on your device, perform the appropriate steps.

To adjust timers and change feature-specific configuration:

1. Bidirectional Forwarding Detection (BFD) sessions temporarily increase their detection and transmission timers during unified ISSU procedures. After the upgrade, these timers revert to the values in use before the unified ISSU started.

If BFD is enabled on your device and you want to disable the BFD timer negotiation during the unified ISSU, include the `no-issu-timer-negotiation` statement at the `[edit protocols bfd]` hierarchy level.

```
{master} [edit]
user@host# set protocols bfd no-issu-timer-negotiation
```

**NOTE:** If you include this statement, the BFD timers maintain their original values during the unified ISSU, and the BFD sessions might flap during the unified ISSU or Routing Engine switchover, depending on the detection intervals.

2. If proxy ARP is enabled on your M Series, MX Series, or EX 9200 Series device, remove the `unconditional-src-learn` statement from the `[edit interfaces interface-name unit 0 family inet]` hierarchy level.

By default the statement is not included. This example shows the `ge-0/0/1` interface only.

```
{master} [edit]
user@host# delete interfaces ge-0/0/1 unit 0 family inet unconditional-src-learn
```

3. If LACP is enabled on your PTX Series device, remove the `lacp` statement from the `[edit interfaces interface-name aggregated-ether-options]` hierarchy level.

```
{master} [edit]
user@host# delete interfaces aex aggregated-ether-options lacp
```

4. If ATM Point-to-Point Protocol (PPP) is enabled on your M Series or T Series device, set the keepalive interval to 10 seconds or greater.

PPP requires three keepalives to fail before it brings down the session. Thirty seconds (10 seconds x three) provides a safe margin to maintain PPP sessions in case of any traffic loss during the unified ISSU operation.

This example shows the at-0/0/1 interface only.

```
{master} [edit]
user@host# set interfaces at-0/0/1 unit 0 keepalives interval 10
```

5. If ATM OAM is enabled on your M Series or T Series device, set the OAM F5 loopback cell period to 20 seconds or greater to maintain ATM connectivity across the unified ISSU.

Include the oam-period statement at the [edit interfaces *interface-name* unit *logical-unit-number*] hierarchy level and specify 20 seconds. This example shows the at-0/0/1 interface only.

```
{master} [edit]
user@host# set interfaces at-0/0/1 unit 0 oam-period 20
```

6. After you have verified your configuration and are satisfied with it, commit the changes by using the `commit` command.

```
{master} [edit]
user@host# commit
commit complete
```

7. Exit configuration mode by using the `exit` command.

```
{master} [edit]
user@host# exit
{master}
user@host>
```

## Upgrading and Rebooting Both Routing Engines Automatically

### IN THIS SECTION

- [Procedure | 543](#)



*Procedure*

**Step-by-Step Procedure**

In this procedure, both Routing Engines automatically reboot. Rebooting both Routing Engines automatically is the most common scenario. Variations to this procedure are described in other sections.

Table 28 on page 543 shows the Routing Engine status prior to starting the unified ISSU.

**Table 28: Routing Engine Status Before Upgrading**


RE0	RE1
Primary	Backup
Old software version installed	Old software version installed
Old software version running	Old software version running

To upgrade and reboot both Routing Engines automatically:

1. Copy the Junos OS software package to the device by using the `file copy ftp://username@hostname.net/ filename /var/tmp/ filename` command.

We recommend that you copy the package to the `/var/tmp` directory, which is a large file system on the hard disk.

```
{master}
user@host> file copy ftp://myid@myhost.mydomain.net/jinstall64-14.1R4.10-domestic-signed.tgz
/var/tmp/jinstall64-14.1R4.10-domestic-signed.tgz
```



**BEST PRACTICE:** When you access the Download Software web page for your device, record the md5 checksum. After downloading the software package to your device, confirm that it is not modified in any way by using the `file checksum md5` command. For more information about verifying the md5 checksum, see <https://kb.juniper.net/InfoCenter/index?page=content&id=KB17665> .

2. On the primary Routing Engine, start the upgrade by using the request `system software in-service-upgrade package-name` reboot command.

**NOTE:** Do not try running any additional commands until after the Connection closed message is displayed and your session is disconnected.

```
{master}
user@host> request system software in-service-upgrade
/var/tmp/jinstall64-14.1R4.10-domestic-signed.tgz reboot
Chassis ISSU Check Done
ISSU: Validating Image
FPC 0 will be offlined (In-Service-Upgrade not supported)
PIC 0/0 will be offlined (In-Service-Upgrade not supported)
PIC 0/1 will be offlined (In-Service-Upgrade not supported)
Do you want to continue with these actions being taken ? [yes,no] (no) yes

Checking compatibility with configuration
Initializing...
Using jbase-13.3R6.5
Verified manifest signed by PackageProductionEc_2015
Using /var/tmp/jinstall64-14.1R4.10-domestic-signed.tgz
Verified jinstall64-14.1R4.10-domestic.tgz signed by PackageProductionEc_2015
Using jinstall64-14.1R4.10-domestic.tgz
Using jbundle64-14.1R4.10-domestic.tgz
Checking jbundle requirements on /
Using jbase-14.1R4.10.tgz
Verified manifest signed by PackageProductionEc_2015
Verified jbase-14.1R4.10 signed by PackageProductionEc_2015
Using /var/v/c/tmp/jbundle/jboot-14.1R4.10.tgz
Using jcrypto64-14.1R4.10.tgz
Verified manifest signed by PackageProductionEc_2015
Verified jcrypto64-14.1R4.10 signed by PackageProductionEc_2015
Using jdocs-14.1R4.10.tgz
Verified manifest signed by PackageProductionEc_2015
Verified jdocs-14.1R4.10 signed by PackageProductionEc_2015
Using jkernel64-14.1R4.10.tgz
Using jpfe-14.1R4.10.tgz
Verified SHA1 checksum of jpfe-M10-14.1R4.10.tgz
Verified SHA1 checksum of jpfe-M120-14.1R4.10.tgz
Verified SHA1 checksum of jpfe-M160-14.1R4.10.tgz
Verified SHA1 checksum of jpfe-M320-14.1R4.10.tgz
Verified SHA1 checksum of jpfe-M40-14.1R4.10.tgz
Verified SHA1 checksum of jpfe-M7i-14.1R4.10.tgz
```

```

Verified SHA1 checksum of jpfe-T-14.1R4.10.tgz
Verified SHA1 checksum of jpfe-X2000-14.1R4.10.tgz
Verified SHA1 checksum of jpfe-X960-14.1R4.10.tgz
Verified SHA1 checksum of jpfe-common-14.1R4.10.tgz
Using jplatform-14.1R4.10.tgz
Verified manifest signed by PackageProductionEc_2015
Verified jplatform-14.1R4.10 signed by PackageProductionEc_2015
Using jroute-14.1R4.10.tgz
Verified manifest signed by PackageProductionEc_2015
Verified jroute-14.1R4.10 signed by PackageProductionEc_2015
Using jruntime-14.1R4.10.tgz
Verified manifest signed by PackageProductionEc_2015
Verified jruntime-14.1R4.10 signed by PackageProductionEc_2015
Using jruntime64-14.1R4.10.tgz
Verified manifest signed by PackageProductionEc_2015
Verified jruntime64-14.1R4.10 signed by PackageProductionEc_2015
Using jservices-14.1R4.10.tgz
Using jservices-crypto-14.1R4.10.tgz
Hardware Database regeneration succeeded
Validating against /config/juniper.conf.gz
mgd: commit complete
Validation succeeded
ISSU: Preparing Backup RE
Pushing /var/tmp/jinstall64-14.1R4.10-domestic-signed.tgz to re1:/var/tmp/
jinstall64-14.1R4.10-domestic-signed.tgz
Installing package '/var/tmp/jinstall64-14.1R4.10-domestic-signed.tgz' ...
Verified jinstall64-14.1R4.10-domestic.tgz signed by PackageProductionEc_2015
Verified jinstall64-14.1R4.10-domestic.tgz signed by PackageProductionRSA_2015
Adding jinstall64...
Verified manifest signed by PackageProductionEc_2015

```

```

WARNING:   This package will load JUNOS 14.1R4.10 software.
WARNING:   It will save JUNOS configuration files, and SSH keys
WARNING:   (if configured), but erase all other files and information
WARNING:   stored on this machine. It will attempt to preserve dumps
WARNING:   and log files, but this can not be guaranteed. This is the
WARNING:   pre-installation stage and all the software is loaded when
WARNING:   you reboot the system.

```

```
Saving the config files ...
```

```
NOTICE: uncommitted changes have been saved in /var/db/config/juniper.conf.pre-install
```

```
Installing the bootstrap installer ...
```

```

WARNING:      A REBOOT IS REQUIRED TO LOAD THIS SOFTWARE CORRECTLY. Use the
WARNING:      'request system reboot' command when software installation is
WARNING:      complete. To abort the installation, do not reboot your system,
WARNING:      instead use the 'request system software delete jinstall'
WARNING:      command as soon as this operation completes.

```

Saving state for rollback ...

Backup upgrade done

Rebooting Backup RE

Rebooting re1

ISSU: Backup RE Prepare Done

Waiting for Backup RE reboot

GRES operational

Initiating Chassis In-Service-Upgrade

Chassis ISSU Started

ISSU: Preparing Daemons

ISSU: Daemons Ready for ISSU

ISSU: Starting Upgrade for FRUs

ISSU: Preparing for Switchover

ISSU: Ready for Switchover

Checking In-Service-Upgrade status

Item	Status	Reason
FPC 0	Offline	Offlined by cli command

Resolving mastership...

Complete. The other routing engine becomes the master.

ISSU: RE switchover Done

ISSU: Upgrading Old Master RE

Installing package '/var/tmp/jinstall64-14.1R4.10-domestic-signed.tgz' ...

Verified jinstall64-14.1R4.10-domestic.tgz signed by PackageProductionEc\_2015

Verified jinstall64-14.1R4.10-domestic.tgz signed by PackageProductionRSA\_2015

Adding jinstall64...

Verified manifest signed by PackageProductionEc\_2015

```

WARNING:      This package will load JUNOS 14.1R4.10 software.

```

```

WARNING:      It will save JUNOS configuration files, and SSH keys

```

```

WARNING:      (if configured), but erase all other files and information

```

```

WARNING:      stored on this machine. It will attempt to preserve dumps

```

```

WARNING:      and log files, but this can not be guaranteed. This is the

```

```

WARNING:      pre-installation stage and all the software is loaded when

```

```

WARNING:      you reboot the system.

```

Saving the config files ...

```

NOTICE: uncommitted changes have been saved in /var/db/config/juniper.conf.pre-install
Installing the bootstrap installer ...

WARNING:      A REBOOT IS REQUIRED TO LOAD THIS SOFTWARE CORRECTLY. Use the
WARNING:      'request system reboot' command when software installation is
WARNING:      complete. To abort the installation, do not reboot your system,
WARNING:      instead use the 'request system software delete jinstall'
WARNING:      command as soon as this operation completes.

Saving package file in /var/sw/pkg/jinstall64-14.1R4.10-domestic-signed.tgz ...
Saving state for rollback ...
ISSU: Old Master Upgrade Done
ISSU: IDLE
Shutdown NOW!
[pid 10149]

{backup}
user@host>

{backup}
user@host>
*** FINAL System shutdown message from user@host ***

System going down IMMEDIATELY

Connection closed by foreign host.

```

When the Routing Engine that was previously the primary is rebooted, you are logged out of the device.

3. Wait a few minutes and then log in to the device again.

[Table 29 on page 547](#) shows the Routing Engine status after the unified ISSU.

**Table 29: Routing Engine Status After Upgrading and Rebooting Both Routing Engines**

RE0	RE1
Backup	Primary

**Table 29: Routing Engine Status After Upgrading and Rebooting Both Routing Engines *(Continued)***

RE0	RE1
New software version installed	New software version installed
New software version running	New software version running

You are logged in to the new backup Routing Engine (re0).

4. Verify that both Routing Engines have been upgraded by using the `show version` command.

```
{backup}
user@host> show version invoke-on all-routing-engines
re0:
-----
Hostname: host
Model: mx480
Junos: 14.1R4.10
JUNOS Base OS boot [14.1R4.10]
JUNOS Base OS Software Suite [14.1R4.10]
JUNOS Packet Forwarding Engine Support (M/T/EX Common) [14.1R4.10]
JUNOS Packet Forwarding Engine Support (MX Common) [14.1R4.10]
JUNOS platform Software Suite [14.1R4.10]
JUNOS Runtime Software Suite [14.1R4.10]
JUNOS Online Documentation [14.1R4.10]

re1:
-----
Hostname: host
Model: mx480
Junos: 14.1R4.10
JUNOS Base OS boot [14.1R4.10]
JUNOS Base OS Software Suite [14.1R4.10]
JUNOS Packet Forwarding Engine Support (M/T/EX Common) [14.1R4.10]
JUNOS Packet Forwarding Engine Support (MX Common) [14.1R4.10]
JUNOS platform Software Suite [14.1R4.10]
JUNOS Runtime Software Suite [14.1R4.10]
JUNOS Online Documentation [14.1R4.10]
```

5. If you want to, you can optionally display the unified ISSU log messages by using the `show log messages` command.
6. If you want to, you can optionally make `re0` the primary Routing Engine by using the `request chassis routing-engine master acquire` command.

```
{backup}
user@host> request chassis routing-engine master
acquire
Attempt to become the master routing engine ? [yes,no] (no) yes

Resolving mastership...
Complete. The local routing engine becomes the master.

{master}
user@host>
```

Table 30 on page 549 shows the Routing Engine status after Step 5 is completed.

**Table 30: Routing Engine Status After Upgrading, Rebooting, and Switching Primary Role**

RE0	RE1
Primary	Backup
New software version installed	New software version installed
New software version running	New software version running

7. Perform the applicable steps in ["Restoring Feature-Specific Configuration" on page 550](#).
8. If you are satisfied with the results of your testing, you can optionally back up the system software to the device's hard disk by using the `request system snapshot` command on *each* Routing Engine.

**NOTE:** The root file system is backed up to `/altroot`, and `/config` is backed up to `/altconfig`. After you issue the `request system snapshot` command, you cannot easily return to the previous

version of the software, because the device flash and hard disks are identical. To return to the previous version of the software, you must boot the device from removable media.

```
{master}
user@host> request system snapshot
user@host> request routing-engine login re1
{backup}
user@host> request system snapshot
```

## Restoring Feature-Specific Configuration

### IN THIS SECTION

- [Procedure | 550](#)

### *Procedure*

#### Step-by-Step Procedure

If you have any of the following feature-specific configuration on your device, perform the appropriate steps.

To restore feature-specific configuration:

1. If BFD is enabled on your device and you previously disabled the BFD timer negotiation, delete the `no-issu-timer-negotiation` statement at the `[edit protocols bfd]` hierarchy level.

```
{master} [edit]
user@host# delete protocols bfd no-issu-timer-negotiation
```

2. If proxy ARP is enabled on your M Series, MX Series, or EX9200 device and you previously removed the `unconditional-src-learn` statement, include the statement again.



This example shows the ge-0/0/1 interface only.

```
{master} [edit]
user@host# set interfaces ge-0/0/1 unit 0 family inet unconditional-src-learn
```

3. If LACP is enabled on your PTX Series device and you previously removed the `lacp` statement, include the statement again.

```
{master} [edit]
user@host# set interfaces aex aggregated-ether-options lacp
```

4. If ATM PPP is enabled on your M Series or T Series device and you previously set the `keepalive` interval to 10 seconds or greater, restore the original value.

This example shows the at-0/0/1 interface only and shows the interval being set to the default 3 seconds.

```
{master} [edit]
user@host# set interfaces at-0/0/1 unit 0 keepalives interval 3
```

5. If ATM OAM is enabled on your M Series or T Series device and you previously set the OAM F5 loopback cell period to 20 seconds or greater, change the configuration back to the original value.

This example shows the at-0/0/1 interface only and shows the period being set to 10 seconds.

```
{master} [edit]
user@host# set interfaces at-0/0/1 unit 0 oam-period 10
```

6. After you have verified your configuration and are satisfied with it, commit the changes by using the `commit` command.

```
{master} [edit]
user@host# commit
commit complete
```

7. Exit configuration mode by using the **exit** command.

```
{master} [edit]
user@host# exit
{master}
user@host>
```

## Upgrading Both Routing Engines and Rebooting the New Backup Routing Engine Manually

### IN THIS SECTION

- [Procedure | 552](#)

### *Procedure*

#### Step-by-Step Procedure

In certain circumstances, you might want to install the new software on only one Routing Engine and reboot only the primary until after you can test the new software. A Routing Engine does not start running the new software until after it is rebooted.


The advantage is if the results of your testing requires you to downgrade the software, you can switch Routing Engines to run the old software on one Routing Engine and then install the old software on the other Routing Engine. This is not the typical scenario.

To upgrade both Routing Engines and to reboot the new backup Routing Engine manually:

1. Perform the steps in ["Verifying Dual Routing Engines and Enabling GRES and NSR" on page 536](#).
2. Perform the steps in ["Verifying the Software Versions and Backing Up the Device Software" on page 539](#).
3. Perform the steps in ["Adjusting Timers and Changing Feature-Specific Configuration" on page 540](#).
4. Copy the Junos OS software package to the device using the file `copy ftp://username@hostname.net/filename /var/tmp/filename` command.

We recommend that you copy the package to the `/var/tmp` directory, which is a large file system on the hard disk.

```
{master}
user@host> file copy ftp://myid@myhost.mydomain.net/jinstall64-14.1R4.10-domestic-signed.tgz
/var/tmp/jinstall64-14.1R4.10-domestic-signed.tgz
```



**BEST PRACTICE:** When you access the Download Software web page for your device, record the md5 checksum. After downloading the software package to your device, confirm that it is not modified in any way by using the `file checksum md5` command. For more information about verifying the md5 checksum, see <https://kb.juniper.net/InfoCenter/index?page=content&id=KB17665>.

Table 31 on page 553 shows the Routing Engine status prior to starting the unified ISSU.

**Table 31: Routing Engine Status Before Upgrading and Manually Rebooting the Backup Routing Engine**

RE0	RE1
Primary	Backup
Old software version installed	Old software version installed
Old software version running	Old software version running

- On the primary Routing Engine, start the upgrade by using the `request system software in-service-upgrade package-name` command without the `reboot` option.

```
{master}
user@host> request system software in-service-upgrade
/var/tmp/jinstall64-14.1R4.10-domestic-signed.tgz
Chassis ISSU Check Done
ISSU: Validating Image
FPC 0 will be offlined (In-Service-Upgrade not supported)
PIC 0/0 will be offlined (In-Service-Upgrade not supported)
PIC 0/1 will be offlined (In-Service-Upgrade not supported)
```

Do you want to continue with these actions being taken ? [yes,no] (no) yes

Checking compatibility with configuration

Initializing...

Using jbase-13.3R6.5

Verified manifest signed by PackageProductionEc\_2015

Using /var/tmp/jinstall64-14.1R4.10-domestic-signed.tgz

Verified jinstall64-14.1R4.10-domestic.tgz signed by PackageProductionEc\_2015

Using jinstall64-14.1R4.10-domestic.tgz

Using jbundle64-14.1R4.10-domestic.tgz

Checking jbundle requirements on /

Using jbase-14.1R4.10.tgz

Verified manifest signed by PackageProductionEc\_2015

Verified jbase-14.1R4.10 signed by PackageProductionEc\_2015

Using /var/v/c/tmp/jbundle/jboot-14.1R4.10.tgz

Using jcrypto64-14.1R4.10.tgz

Verified manifest signed by PackageProductionEc\_2015

Verified jcrypto64-14.1R4.10 signed by PackageProductionEc\_2015

Using jdocs-14.1R4.10.tgz

Verified manifest signed by PackageProductionEc\_2015

Verified jdocs-14.1R4.10 signed by PackageProductionEc\_2015

Using jkernel64-14.1R4.10.tgz

Using jpfe-14.1R4.10.tgz

Verified SHA1 checksum of jpfe-M10-14.1R4.10.tgz

Verified SHA1 checksum of jpfe-M120-14.1R4.10.tgz

Verified SHA1 checksum of jpfe-M160-14.1R4.10.tgz

Verified SHA1 checksum of jpfe-M320-14.1R4.10.tgz

Verified SHA1 checksum of jpfe-M40-14.1R4.10.tgz

Verified SHA1 checksum of jpfe-M7i-14.1R4.10.tgz

Verified SHA1 checksum of jpfe-T-14.1R4.10.tgz

Verified SHA1 checksum of jpfe-X2000-14.1R4.10.tgz

Verified SHA1 checksum of jpfe-X960-14.1R4.10.tgz

Verified SHA1 checksum of jpfe-common-14.1R4.10.tgz

Using jplatform-14.1R4.10.tgz

Verified manifest signed by PackageProductionEc\_2015

Verified jplatform-14.1R4.10 signed by PackageProductionEc\_2015

Using jroute-14.1R4.10.tgz

Verified manifest signed by PackageProductionEc\_2015

Verified jroute-14.1R4.10 signed by PackageProductionEc\_2015

Using jruntime-14.1R4.10.tgz

Verified manifest signed by PackageProductionEc\_2015

Verified jruntime-14.1R4.10 signed by PackageProductionEc\_2015

```

Using jruntime64-14.1R4.10.tgz
Verified manifest signed by PackageProductionEc_2015
Verified jruntime64-14.1R4.10 signed by PackageProductionEc_2015
Using jservices-14.1R4.10.tgz
Using jservices-crypto-14.1R4.10.tgz
Hardware Database regeneration succeeded
Validating against /config/juniper.conf.gz
mgd: commit complete
Validation succeeded
ISSU: Preparing Backup RE
Pushing /var/tmp/jinstall64-14.1R4.10-domestic-signed.tgz to re1:/var/tmp/
jinstall64-14.1R4.10-domestic-signed.tgz
Installing package '/var/tmp/jinstall64-14.1R4.10-domestic-signed.tgz' ...
Verified jinstall64-14.1R4.10-domestic.tgz signed by PackageProductionEc_2015
Verified jinstall64-14.1R4.10-domestic.tgz signed by PackageProductionRSA_2015
Adding jinstall64...
Verified manifest signed by PackageProductionEc_2015

WARNING:      This package will load JUNOS 14.1R4.10 software.
WARNING:      It will save JUNOS configuration files, and SSH keys
WARNING:      (if configured), but erase all other files and information
WARNING:      stored on this machine. It will attempt to preserve dumps
WARNING:      and log files, but this can not be guaranteed. This is the
WARNING:      pre-installation stage and all the software is loaded when
WARNING:      you reboot the system.

Saving the config files ...
NOTICE: uncommitted changes have been saved in /var/db/config/juniper.conf.pre-install
Installing the bootstrap installer ...

WARNING:      A REBOOT IS REQUIRED TO LOAD THIS SOFTWARE CORRECTLY. Use the
WARNING:      'request system reboot' command when software installation is
WARNING:      complete. To abort the installation, do not reboot your system,
WARNING:      instead use the 'request system software delete jinstall'
WARNING:      command as soon as this operation completes.

Saving state for rollback ...
Backup upgrade done
Rebooting Backup RE

Rebooting re1
ISSU: Backup RE Prepare Done
Waiting for Backup RE reboot

```

```

GRES operational
Initiating Chassis In-Service-Upgrade
Chassis ISSU Started
ISSU: Preparing Daemons
ISSU: Daemons Ready for ISSU
ISSU: Starting Upgrade for FRUs
ISSU: Preparing for Switchover
ISSU: Ready for Switchover
Checking In-Service-Upgrade status
  Item          Status          Reason
  FPC 0          Offline          Offlined by cli command
Resolving mastership...
Complete. The other routing engine becomes the master.
ISSU: RE switchover Done
ISSU: Upgrading Old Master RE
Installing package '/var/tmp/jinstall64-14.1R4.10-domestic-signed.tgz' ...
Verified jinstall64-14.1R4.10-domestic.tgz signed by PackageProductionEc_2015
Verified jinstall64-14.1R4.10-domestic.tgz signed by PackageProductionRSA_2015
Adding jinstall64...
Verified manifest signed by PackageProductionEc_2015

WARNING:      This package will load JUNOS 14.1R4.10 software.
WARNING:      It will save JUNOS configuration files, and SSH keys
WARNING:      (if configured), but erase all other files and information
WARNING:      stored on this machine. It will attempt to preserve dumps
WARNING:      and log files, but this can not be guaranteed. This is the
WARNING:      pre-installation stage and all the software is loaded when
WARNING:      you reboot the system.

Saving the config files ...
NOTICE: uncommitted changes have been saved in /var/db/config/juniper.conf.pre-install
Installing the bootstrap installer ...

WARNING:      A REBOOT IS REQUIRED TO LOAD THIS SOFTWARE CORRECTLY. Use the
WARNING:      'request system reboot' command when software installation is
WARNING:      complete. To abort the installation, do not reboot your system,
WARNING:      instead use the 'request system software delete jinstall'
WARNING:      command as soon as this operation completes.

Saving package file in /var/sw/pkg/jinstall64-14.1R4.10-domestic-signed.tgz ...
Saving state for rollback ...

```

ISSU: Old Master Upgrade Done  
ISSU: IDLE

Table 32 on page 557 shows the Routing Engine status after the unified ISSU and before manually rebooting the backup Routing Engine.

**Table 32: Routing Engine Status After Upgrading and Before Manually Rebooting the Backup Routing Engine**

RE0	RE1
Backup	Primary
New software version installed	New software version installed
Old software version running	New software version running

6. Verify that the new backup, (old primary) Routing Engine (re0), is still running the previous software image and that the new primary Routing Engine (re1) is running the new software image, by using the `show version` command.

```
{backup}
user@host> show version invoke-on all-routing-engines
re0:
-----
Hostname: host
Model: mx480
Junos: 13.3R6.5
JUNOS Base OS boot [13.3R6.5]
JUNOS Base OS Software Suite [13.3R6.5]
JUNOS 64-bit Kernel Software Suite [13.3R6.5]
JUNOS Crypto Software Suite [13.3R6.5]
JUNOS Packet Forwarding Engine Support (M/T/EX Common) [13.3R6.5]
JUNOS Packet Forwarding Engine Support (MX Common) [13.3R6.5]
JUNOS Online Documentation [13.3R6.5]

re1:
-----
Hostname: host
Model: mx480
```

```

Junos: 14.1R4.10
JUNOS Base OS boot [14.1R4.10]
JUNOS Base OS Software Suite [14.1R4.10]
JUNOS Packet Forwarding Engine Support (M/T/EX Common) [14.1R4.10]
JUNOS Packet Forwarding Engine Support (MX Common) [14.1R4.10]
JUNOS platform Software Suite [14.1R4.10]
JUNOS Runtime Software Suite [14.1R4.10]
JUNOS Online Documentation [14.1R4.10]

```

7. At this point, if you do not want to install the newer software version on the new backup Routing Engine (re0), issue the request system software delete *package-name* command on it.

Otherwise, to complete the upgrade, go to the next step.

8. Reboot the new backup Routing Engine (re0) by issuing the request system reboot command.

```

{backup}
user@host> request system reboot
Reboot the system ? [yes,no] (no) yes

*** FINAL System shutdown message from remote@host ***

System going down IMMEDIATELY

Shutdown NOW!
[pid 38432]

{backup}
user@home> Connection closed by foreign host.

```

If you are not on the console port, you are disconnected from the device session.

[Table 33 on page 559](#) shows the Routing Engine status after the unified ISSU, after rebooting the backup Routing Engine, but before switching primary role.



**Table 33: Routing Engine Status After Upgrading, Manually Rebooting, and Before Switching Primary Role**

RE0	RE1
Backup	Primary
New software version installed	New software version installed
New software version running	New software version running

9. Wait a few minutes, then log in to the device again.

You are logged in to the new backup Routing Engine (re0).

10. Verify that both Routing Engines have been upgraded by using the `show version` command.

```
{backup}
user@host> show version invoke-on all-routing-engines
re0:
-----
Hostname: host
Model: mx480
Junos: 14.1R4.10
JUNOS Base OS boot [14.1R4.10]
JUNOS Base OS Software Suite [14.1R4.10]
JUNOS Packet Forwarding Engine Support (M/T/EX Common) [14.1R4.10]
JUNOS Packet Forwarding Engine Support (MX Common) [14.1R4.10]
JUNOS platform Software Suite [14.1R4.10]
JUNOS Runtime Software Suite [14.1R4.10]
JUNOS Online Documentation [14.1R4.10]

re1:
-----
Hostname: host
Model: mx480
Junos: 14.1R4.10
JUNOS Base OS boot [14.1R4.10]
JUNOS Base OS Software Suite [14.1R4.10]
JUNOS Packet Forwarding Engine Support (M/T/EX Common) [14.1R4.10]
```

JUNOS Packet Forwarding Engine Support (MX Common) [14.1R4.10]  
JUNOS platform Software Suite [14.1R4.10]  
JUNOS Runtime Software Suite [14.1R4.10]  
JUNOS Online Documentation [14.1R4.10]

- 11. If you want to, you can optionally display the unified ISSU log messages by using the `show log messages` command.
- 12. If you want to, you can optionally make `re0` the primary Routing Engine by using the `request chassis routing-engine master acquire` command:

```
{backup}  
user@host> request chassis routing-engine master  
acquire  
Attempt to become the master routing engine ? [yes,no] (no) yes  
  
Resolving mastership...  
Complete. The local routing engine becomes the master.  
  
{master}  
user@host>
```

[Table 34 on page 560](#) shows the Routing Engine status after the unified ISSU, after rebooting the backup Routing Engine, and after switching primary role.

**Table 34: Routing Engine Status After Upgrading, Manually Rebooting, and Switching Primary Role**

RE0	RE1
Primary	Backup
New software version installed	New software version installed
New software version running	New software version running

- 13. Perform the applicable steps in ["Restoring Feature-Specific Configuration" on page 550](#).
- 14. If you are satisfied with the results of your testing, you can optionally back up the system software to the device's hard disk by using the `request system snapshot` command on *each* Routing Engine.

**NOTE:** The root file system is backed up to `/altroot`, and `/config` is backed up to `/altconfig`. After you issue the `request system snapshot` command, you cannot easily return to the previous version of the software, because the device flash and hard disks are identical. To return to the previous version of the software, you must boot the device from removable media.

```
{master}
user@host> request system snapshot
user@host> request routing-engine login re1
{backup}
user@host> request system snapshot
```

Upgrading and Rebooting Only One Routing Engine

- IN THIS SECTION
- Procedure | 561

Procedure

Step-by-Step Procedure

In certain circumstances you might want to install the new software on only one Routing Engine. The advantage is if the results of your testing requires you to downgrade the software, you can switch Routing Engines to run the old software on one Routing Engine and then install the old software on the other Routing Engine. This is not the typical scenario.

[Table 35 on page 561](#) shows the Routing Engine status prior to starting the unified ISSU.

Table 35: Routing Engine Status Before Upgrading and Rebooting One Routing Engine

RE0	RE1
Primary	Backup

Table 35: Routing Engine Status Before Upgrading and Rebooting One Routing Engine (*Continued*)

RE0	RE1
Old software version installed	Old software version installed
Old software version running	Old software version running

To upgrade and rebooting only one Routing Engine:

1. Perform the steps in ["Verifying Dual Routing Engines and Enabling GRES and NSR" on page 536](#).
2. Perform the steps in ["Verifying the Software Versions and Backing Up the Device Software" on page 539](#).
3. Perform the applicable steps in ["Adjusting Timers and Changing Feature-Specific Configuration" on page 540](#).
4. Copy the Junos OS software package to the device by using the file `copy ftp://username@hostname.net/filename /var/tmp/filename` command.

We recommend that you copy the package to the `/var/tmp` directory, which is a large file system on the hard disk.

```
{master}
user@host> file copy ftp://myid@myhost.mydomain.net/jinstall64-14.1R4.10-domestic-signed.tgz
/var/tmp/jinstall64-14.1R4.10-domestic-signed.tgz
```

**BEST PRACTICE:** When you access the Download Software web page for your device, record the md5 checksum. After downloading the software package to your device, confirm that it is not modified in any way by using the `file checksum md5` command. For more information about verifying the md5 checksum, see <https://kb.juniper.net/InfoCenter/index?page=content&id=KB17665>.

5. On the primary Routing Engine, start the upgrade by using the request `system software in-service-upgrade package-name no-old-master-upgrade` command.

```
{master}
user@host> request system software in-service-upgrade
```

```

/var/tmp/jinstall64-14.1R4.10-domestic-signed.tgz no-old-master-upgrade
Chassis ISSU Check Done
ISSU: Validating Image
FPC 0 will be offlined (In-Service-Upgrade not supported)
PIC 0/0 will be offlined (In-Service-Upgrade not supported)
PIC 0/1 will be offlined (In-Service-Upgrade not supported)
Do you want to continue with these actions being taken ? [yes,no] (no) yes

Checking compatibility with configuration
Initializing...
Using jbase-13.3R6.5
Verified manifest signed by PackageProductionEc_2015
Using /var/tmp/jinstall64-14.1R4.10-domestic-signed.tgz
Verified jinstall64-14.1R4.10-domestic.tgz signed by PackageProductionEc_2015
Using jinstall64-14.1R4.10-domestic.tgz
Using jbundle64-14.1R4.10-domestic.tgz
Checking jbundle requirements on /
Using jbase-14.1R4.10.tgz
Verified manifest signed by PackageProductionEc_2015
Verified jbase-14.1R4.10 signed by PackageProductionEc_2015
Using /var/v/c/tmp/jbundle/jboot-14.1R4.10.tgz
Using jcrypto64-14.1R4.10.tgz
Verified manifest signed by PackageProductionEc_2015
Verified jcrypto64-14.1R4.10 signed by PackageProductionEc_2015
Using jdocs-14.1R4.10.tgz
Verified manifest signed by PackageProductionEc_2015
Verified jdocs-14.1R4.10 signed by PackageProductionEc_2015
Using jkernel64-14.1R4.10.tgz
Using jpfe-14.1R4.10.tgz
Verified SHA1 checksum of jpfe-M10-14.1R4.10.tgz
Verified SHA1 checksum of jpfe-M120-14.1R4.10.tgz
Verified SHA1 checksum of jpfe-M160-14.1R4.10.tgz
Verified SHA1 checksum of jpfe-M320-14.1R4.10.tgz
Verified SHA1 checksum of jpfe-M40-14.1R4.10.tgz
Verified SHA1 checksum of jpfe-M7i-14.1R4.10.tgz
Verified SHA1 checksum of jpfe-T-14.1R4.10.tgz
Verified SHA1 checksum of jpfe-X2000-14.1R4.10.tgz
Verified SHA1 checksum of jpfe-X960-14.1R4.10.tgz
Verified SHA1 checksum of jpfe-common-14.1R4.10.tgz
Using jplatform-14.1R4.10.tgz
Verified manifest signed by PackageProductionEc_2015
Verified jplatform-14.1R4.10 signed by PackageProductionEc_2015
Using jroute-14.1R4.10.tgz

```

```

Verified manifest signed by PackageProductionEc_2015
Verified jroute-14.1R4.10 signed by PackageProductionEc_2015
Using jruntime-14.1R4.10.tgz
Verified manifest signed by PackageProductionEc_2015
Verified jruntime-14.1R4.10 signed by PackageProductionEc_2015
Using jruntime64-14.1R4.10.tgz
Verified manifest signed by PackageProductionEc_2015
Verified jruntime64-14.1R4.10 signed by PackageProductionEc_2015
Using jservices-14.1R4.10.tgz
Using jservices-crypto-14.1R4.10.tgz
Hardware Database regeneration succeeded
Validating against /config/juniper.conf.gz
mgd: commit complete
Validation succeeded
ISSU: Preparing Backup RE
Pushing /var/tmp/jinstall64-14.1R4.10-domestic-signed.tgz to re1:/var/tmp/
jinstall64-14.1R4.10-domestic-signed.tgz
Installing package '/var/tmp/jinstall64-14.1R4.10-domestic-signed.tgz' ...
Verified jinstall64-14.1R4.10-domestic.tgz signed by PackageProductionEc_2015
Verified jinstall64-14.1R4.10-domestic.tgz signed by PackageProductionRSA_2015
Adding jinstall64...
Verified manifest signed by PackageProductionEc_2015

WARNING:      This package will load JUNOS 14.1R4.10 software.
WARNING:      It will save JUNOS configuration files, and SSH keys
WARNING:      (if configured), but erase all other files and information
WARNING:      stored on this machine. It will attempt to preserve dumps
WARNING:      and log files, but this can not be guaranteed. This is the
WARNING:      pre-installation stage and all the software is loaded when
WARNING:      you reboot the system.

Saving the config files ...
NOTICE: uncommitted changes have been saved in /var/db/config/juniper.conf.pre-install
Installing the bootstrap installer ...

WARNING:      A REBOOT IS REQUIRED TO LOAD THIS SOFTWARE CORRECTLY. Use the
WARNING:      'request system reboot' command when software installation is
WARNING:      complete. To abort the installation, do not reboot your system,
WARNING:      instead use the 'request system software delete jinstall'
WARNING:      command as soon as this operation completes.

Saving state for rollback ...
Backup upgrade done

```

```
Rebooting Backup RE

Rebooting re1
ISSU: Backup RE Prepare Done
Waiting for Backup RE reboot
GRES operational
Initiating Chassis In-Service-Upgrade
Chassis ISSU Started
ISSU: Preparing Daemons
ISSU: Daemons Ready for ISSU
ISSU: Starting Upgrade for FRUs
ISSU: Preparing for Switchover
ISSU: Ready for Switchover
Checking In-Service-Upgrade status
  Item          Status          Reason
  FPC 0         Offline         Offlined by cli command
Resolving mastership...
Complete. The other routing engine becomes the master.
ISSU: RE switchover Done
Skipping Old Master Upgrade
ISSU: IDLE
```

Table 36 on page 565 shows the Routing Engine status after the unified ISSU upgrades the primary Routing Engine but before the backup Routing Engine is upgraded.

**Table 36: Routing Engine Status After Upgrading One Routing Engine and Before Upgrading the Other Routing Engine**

RE0	RE1
Backup	Primary
Old software version installed	New software version installed
Old software version running	New software version running

6. Verify that the new backup, (old primary) Routing Engine (re0), is still running the previous software image and that the new primary Routing Engine (re1) is running the new software image, by using the `show version` command.

```
{backup}
user@host> show version invoke-on all-routing-engines
re0:
-----
Hostname: host
Model: mx480
Junos: 13.3R6.5
JUNOS Base OS boot [13.3R6.5]
JUNOS Base OS Software Suite [13.3R6.5]
JUNOS 64-bit Kernel Software Suite [13.3R6.5]
JUNOS Crypto Software Suite [13.3R6.5]
JUNOS Packet Forwarding Engine Support (M/T/EX Common) [13.3R6.5]
JUNOS Packet Forwarding Engine Support (MX Common) [13.3R6.5]
JUNOS Online Documentation [13.3R6.5]

re1:
-----
Hostname: host
Model: mx480
Junos: 14.1R4.10
JUNOS Base OS boot [14.1R4.10]
JUNOS Base OS Software Suite [14.1R4.10]
JUNOS Packet Forwarding Engine Support (M/T/EX Common) [14.1R4.10]
JUNOS Packet Forwarding Engine Support (MX Common) [14.1R4.10]
JUNOS platform Software Suite [14.1R4.10]
JUNOS Runtime Software Suite [14.1R4.10]
JUNOS Online Documentation [14.1R4.10]
```

7. If your testing is complete and you want to install the new software on the backup Routing Engine, you must first disable GRES and NSR on both Routing Engines and commit the configuration.

```
{backup} [edit ]
user@host# delete chassis redundancy graceful-switchover
user@host# delete routing-options nonstop-routing
user@host# commit
warning: Graceful-switchover is enabled, commit on backup is not recommended
Continue commit on backup RE? [yes,no] (no) yes
```



```

re0:
configuration check succeeds
re1:
commit complete
re0:
commit complete
[edit ]
user@host#

```

8. Install the new software on the backup Routing Engine (re0) by using the request system software add /var/tmp/jinstall64-14.1R4.10-domestic-signed.tgz command.

```

user@host> request system software add /var/tmp/jinstall64-14.1R4.10-domestic-signed.tgz
NOTICE: Validating configuration against jinstall64-14.1R4.10-domestic-signed.tgz.
NOTICE: Use the 'no-validate' option to skip this if desired.
Checking compatibility with configuration
Initializing...
Using jbase-13.3R6.5
Verified manifest signed by PackageProductionEc_2015
Using /var/tmp/jinstall64-14.1R4.10-domestic-signed.tgz
Verified jinstall64-14.1R4.10-domestic.tgz signed by PackageProductionEc_2015
Using jinstall64-14.1R4.10-domestic.tgz
Using jbundle64-14.1R4.10-domestic.tgz
Checking jbundle requirements on /
Using jbase-14.1R4.10.tgz
Verified manifest signed by PackageProductionEc_2015
Verified jbase-14.1R4.10 signed by PackageProductionEc_2015
Using /var/v/c/tmp/jbundle/jboot-14.1R4.10.tgz
Using jcrypto64-14.1R4.10.tgz
Verified manifest signed by PackageProductionEc_2015
Verified jcrypto64-14.1R4.10 signed by PackageProductionEc_2015
Using jdocs-14.1R4.10.tgz
Verified manifest signed by PackageProductionEc_2015
Verified jdocs-14.1R4.10 signed by PackageProductionEc_2015
Using jkernel64-14.1R4.10.tgz
Using jpfe-14.1R4.10.tgz
Verified SHA1 checksum of jpfe-M10-14.1R4.10.tgz
Verified SHA1 checksum of jpfe-M120-14.1R4.10.tgz
Verified SHA1 checksum of jpfe-M160-14.1R4.10.tgz
Verified SHA1 checksum of jpfe-M320-14.1R4.10.tgz
Verified SHA1 checksum of jpfe-M40-14.1R4.10.tgz
Verified SHA1 checksum of jpfe-M7i-14.1R4.10.tgz

```

```

Verified SHA1 checksum of jpfe-T-14.1R4.10.tgz
Verified SHA1 checksum of jpfe-X2000-14.1R4.10.tgz
Verified SHA1 checksum of jpfe-X960-14.1R4.10.tgz
Verified SHA1 checksum of jpfe-common-14.1R4.10.tgz
Using jplatform-14.1R4.10.tgz
Verified manifest signed by PackageProductionEc_2015
Verified jplatform-14.1R4.10 signed by PackageProductionEc_2015
Using jroute-14.1R4.10.tgz
Verified manifest signed by PackageProductionEc_2015
Verified jroute-14.1R4.10 signed by PackageProductionEc_2015
Using jruntime-14.1R4.10.tgz
Verified manifest signed by PackageProductionEc_2015
Verified jruntime-14.1R4.10 signed by PackageProductionEc_2015
Using jruntime64-14.1R4.10.tgz
Verified manifest signed by PackageProductionEc_2015
Verified jruntime64-14.1R4.10 signed by PackageProductionEc_2015
Using jservices-14.1R4.10.tgz
Using jservices-crypto-14.1R4.10.tgz
Hardware Database regeneration succeeded
Validating against /config/juniper.conf.gz
mgd: commit complete
Validation succeeded
Installing package '/var/tmp/jinstall64-14.1R4.10-domestic-signed.tgz' ...
Verified jinstall64-14.1R4.10-domestic.tgz signed by PackageProductionEc_2015
Verified jinstall64-14.1R4.10-domestic.tgz signed by PackageProductionRSA_2015
Adding jinstall64...
Verified manifest signed by PackageProductionEc_2015

WARNING:      This package will load JUNOS 14.1R4.10 software.
WARNING:      It will save JUNOS configuration files, and SSH keys
WARNING:      (if configured), but erase all other files and information
WARNING:      stored on this machine. It will attempt to preserve dumps
WARNING:      and log files, but this can not be guaranteed. This is the
WARNING:      pre-installation stage and all the software is loaded when
WARNING:      you reboot the system.

Saving the config files ...
NOTICE: uncommitted changes have been saved in /var/db/config/juniper.conf.pre-install
Installing the bootstrap installer ...

WARNING:      A REBOOT IS REQUIRED TO LOAD THIS SOFTWARE CORRECTLY. Use the
WARNING:      'request system reboot' command when software installation is
WARNING:      complete. To abort the installation, do not reboot your system,

```

```

WARNING:      instead use the 'request system software delete jinstall'
WARNING:      command as soon as this operation completes.

Saving package file in /var/sw/pkg/jinstall64-14.1R4.10-domestic-signed.tgz ...
Saving state for rollback ...

```

9. Reboot `re0` by using the `request system reboot` command.

```

user@host> request system reboot
Reboot the system ? [yes,no] (no) yes

*** FINAL System shutdown message from user@host ***

System going down IMMEDIATELY

Shutdown NOW!
[pid 22857]

user@host> Connection closed by foreign host.

```

If you are not on the console port, you are disconnected from the router session.

10. After waiting a few minutes, log in to the device again.

You are logged in to the backup Routing Engine (`re0`).

11. Verify that both Routing Engines are running the new software image by using the `show version` command.

```

{backup}
user@host> show version invoke-on all-routing-engines
Hostname: host
Model: mx480
Junos: 14.1R4.10
JUNOS Base OS boot [14.1R4.10]
JUNOS Base OS Software Suite [14.1R4.10]
JUNOS Packet Forwarding Engine Support (M/T/EX Common) [14.1R4.10]
JUNOS Packet Forwarding Engine Support (MX Common) [14.1R4.10]
JUNOS platform Software Suite [14.1R4.10]
JUNOS Runtime Software Suite [14.1R4.10]

```

```
JUNOS Online Documentation [14.1R4.10]

re1:
-----
Hostname: host
Model: mx480
Junos: 14.1R4.10
JUNOS Base OS boot [14.1R4.10]
JUNOS Base OS Software Suite [14.1R4.10]
JUNOS Packet Forwarding Engine Support (M/T/EX Common) [14.1R4.10]
JUNOS Packet Forwarding Engine Support (MX Common) [14.1R4.10]
JUNOS platform Software Suite [14.1R4.10]
JUNOS Runtime Software Suite [14.1R4.10]
JUNOS Online Documentation [14.1R4.10]
```

- 12. If you want to, you can optionally display the unified ISSU log messages by using the `show log messages` command.
- 13. If you want to, make `re0` the primary Routing Engine by using the `request chassis routing-engine master acquire` command.

```
{backup}
user@host> request chassis routing-engine master
acquire
Attempt to become the master routing engine ? [yes,no] (no) yes

Resolving mastership...
Complete. The local routing engine becomes the master.

user@host>
```

Table 37 on page 570 shows the Routing Engine status after the unified ISSU, after rebooting the backup Routing Engine, and after switching primary role.

Table 37: Routing Engine Status After Upgrading, Manually Rebooting, and Switching Primary Role

RE0	RE1
Primary	Backup

**Table 37: Routing Engine Status After Upgrading, Manually Rebooting, and Switching Primary Role**  
*(Continued)*

RE0	RE1
New software version installed	New software version installed
New software version running	New software version running

14. Enable GRES and NSR again by performing the steps in ["Verifying Dual Routing Engines and Enabling GRES and NSR" on page 536](#).
15. Perform the applicable steps in ["Restoring Feature-Specific Configuration" on page 550](#).
16. If you are satisfied with the results of your testing, you can optionally back up the system software to the device's hard disk by using the `request system snapshot` command on *each* Routing Engine.

**NOTE:** The root file system is backed up to `/altroot`, and `/config` is backed up to `/altconfig`. After you issue the `request system snapshot` command, you cannot easily return to the previous version of the software, because the device flash and hard disks are identical. To return to the previous version of the software, you must boot the device from removable media.

```
{master}
user@host> request system snapshot
user@host> request routing-engine login re1
{backup}
user@host> request system snapshot
```

## SEE ALSO

- Getting Started with Unified In-Service Software Upgrade
- Understanding the Unified ISSU Process
- [Unified ISSU System Requirements | 504](#)
- Best Practices for Performing a Unified ISSU
- Verifying a Unified ISSU
- Troubleshooting Unified ISSU Problems

## Performing an In-Service Software Upgrade (ISSU) with Non-Stop Routing

### IN THIS SECTION

- [Preparing the Switch for Software Installation | 572](#)
- [Upgrading the Software Using ISSU | 573](#)

You can use an in-service software upgrade with non-stop routing to upgrade the software running on the switch with minimal traffic disruption during the upgrade.

**NOTE:** Starting with Junos OS Release 18.2R1 on the QFX5200 switch, we recommend that you wait at least five minutes between in-service software upgrades.

**NOTE:** Starting with Junos OS Release 17.1R1, on QFX5100 and EX4600 switches, you cannot perform an ISSU from a Junos OS Release earlier than 17.1R1 to Junos OS Release 17.1R1.

This topic covers:

### Preparing the Switch for Software Installation

Before you begin software installation using ISSU:

**NOTE:** Before you perform an in-service software upgrade, if applicable, remove the `set system internet-options no-tcp-reset drop-all-tcp` command from the configuration, otherwise the upgrade will fail and an error message will be displayed.

NSB and non-stop routing enable NSB-supported Layer 2 protocols to synchronize protocol information between the primary and backup Routing Engines.

- Enable non-stop routing. See [Configuring Nonstop Active Routing on Switches](#) for information on how to enable it.
- Enable nonstop bridging (NSB). See [Configuring Nonstop Bridging on Switches \(CLI Procedure\)](#) for information on how to enable it.

- Configure the Bidirectional Forwarding Detection Protocol (BFD) timeout to be more than one second, otherwise you will receive an error.

## Upgrading the Software Using ISSU

This procedure describes how to upgrade the software running on a standalone switch:

**NOTE:** If the Host OS software needs to be updated, you cannot perform an ISSU. Instead, perform a standard software upgrade.

To upgrade the switch using ISSU:

1. Download the software package by following the procedure in the Downloading Software Files with a Browser section in [Installing Software Packages on QFX Series Devices](#).
2. Copy the software package or packages to the switch. We recommend that you copy the file to the `/var/tmp` directory.
3. Log in to the console connection. Using a console connection allows you to monitor the progress of the upgrade.
4. Start the ISSU:
  - On the switch, enter:

```
user@switch> request system software in-service-upgrade /var/tmp/package-name.tgz
```

where `package-name.tgz` is, for example, `jinstall-host-qfx-5e-18.1R1-secured-signed.tgz`.

**NOTE:** During the upgrade, you will not be able to access the Junos OS CLI.

The switch displays status messages similar to the following messages as the upgrade executes:

```
ISSU: Validating Image

PRE ISSU CHECK:
-----
PFE Status                : Online
Member Id zero            : Valid
VC not in mixed or fabric mode : Valid
```

```

Member is single node vc          : Valid
BFD minimum-interval check done   : Valid
GRES enabled                      : Valid
GR enabled                        : Valid
drop-all-tcp not configured      : Valid
Ready for ISSU                    : Valid

```

warning: Do NOT use /user during ISSU. Changes to /user during ISSU may get lost!

Pushing Junos image package to the host...

Installing /var/tmp/install-media-qfx-5e-junos-2018-secure.tgz

Extracting the package ...

total 1110328

```
-rw-r--r-- 1 18735 758 237044439 Oct 26 05:11 jinstall-qfx-5e-junos-2018-secure-linux.tgz
```

```
-rw-r--r-- 1 18735 758 899918118 Oct 26 05:11 jinstall-qfx-5e-junos-2018-secure-app.tgz
```

=====

Current Host kernel version : 3.14.52-rt50-WR7.0.0.9\_ovp

Package Host kernel version : 3.14.52-rt50-WR7.0.0.9\_ovp

Current Host version : 3.0.7

Package Host version : 3.0.7

Min host version required for applications: 3.0.7

Min host version required for in-service-upgrade: 3.0.7

=====

Setting up Junos host applications for in-service-upgrade ...

-----

Running Junos application installer for in-service-upgrade

-----

-----

Installing /var/sw/applications/qfx-5e-flex-2018.tgz

-----

pkg\_install\_rpms: qfx-5e-base-1.0-0-2018.x86\_64.rpm

Installing qfx-5e-control-plane-flex-1.0-0-2018.x86\_64.rpm ...

=====

Loading cache...

Updating cache... ##### [100%]

Committing transaction...

Preparing... ##### [ 0%]

1:Installing qfx-5e-contro.. ##### [100%]



Output from qfx-5e-control-plane-flex-1.0-0@x86\_64:

-----

Installing JUNOS image: jinstall-jcp-i386-flex-18.12018.img.gz

-----

Extracting jinstall-jcp-i386-flex-18.12018.img.gz to /recovery/junos/jinstall-jcp-i386-flex-18.12018-2018.img

Prepare host for virtfs...

Integrity check passed for hash-control-plane.md5.

Installing packages (1):

qfx-5e-control-plane-flex-1.0-0@x86\_64

812.9MB of package files are needed. 821.5MB will be used.

Saving cache...

=====

Application installed.

Waiting to sync newly setup VM disk

VM ready after 200 seconds

[Oct 26 05:19:22]:ISSU: Preparing Backup RE

Prepare for ISSU

[Oct 26 05:19:27]:ISSU: Backup RE Prepare Done

Spawning the backup RE

Spawn backup RE, index 0 successful

Starting secondary dataplane

Second dataplane container started

GRES in progress

Waiting for backup RE switchover ready

GRES operational

Copying home directories

Copying home directories successful

Initiating Chassis In-Service-Upgrade

Chassis ISSU Started

[Oct 26 05:28:33]:ISSU: Preparing Daemons

[Oct 26 05:28:39]:ISSU: Daemons Ready for ISSU

[Oct 26 05:28:43]:ISSU: Starting Upgrade for FRUs

[Oct 26 05:28:54]:ISSU: FPC Warm Booting

[Oct 26 05:29:59]:ISSU: FPC Warm Booted

[Oct 26 05:30:10]:ISSU: Preparing for Switchover

```
[Oct 26 05:30:14]:ISSU: Ready for Switchover
Checking In-Service-Upgrade status
  Item           Status           Reason
  FPC 0         Online (ISSU)
Send ISSU done to chassisd on backup RE
Chassis ISSU Completed
Removing dcpfe1 eth1 128.0.0.16 IP
Bringing down bme01
Post Chassis ISSU processing done
[Oct 26 05:30:17]:ISSU: IDLE
Stopping primary dataplane
Clearing ISSU states
Console and management sessions will be disconnected. Please login again.
```

**NOTE:** If the ISSU process stops, you can look at the CLI output when you issue the request system software in-service-upgrade command to diagnose the problem. You can also look at syslog files for more information.

5. Log in after the reboot of the switch completes. To verify that the software has been upgraded, enter the following command:

```
user@switch> show version
```

RELATED DOCUMENTATION

Understanding In-Service Software Upgrade (ISSU)
<a href="#">request system software in-service-upgrade</a>   1270

Performing an In-Service Software Upgrade (ISSU) in ACX5000 Series Routers

IN THIS SECTION

- [Preparing the Router for Software Installation](#) | 577
- [Upgrading the Software Using ISSU](#) | 578
- [Verifying a Unified ISSU](#) | 581

You can use an in-service software upgrade to upgrade the software running on the router with minimal traffic disruption during the upgrade.

**NOTE:** ISSU is supported in Junos OS Release 15.1X54-D60 and later on ACX5000 Series routers.

This topic covers:

## Preparing the Router for Software Installation

Before you begin software installation using ISSU:

**NOTE:** Before you perform an in-service software upgrade, if applicable, remove the `set system internet-options no-tcp-reset drop-all-tcp` command from the configuration, otherwise the upgrade will fail and an error message will be displayed.

- Ensure that nonstop active routing (NSR) and nonstop bridging (NSB) are enabled. If enabled, disable graceful restart (GR), because NSR and GR cannot be enabled simultaneously. NSB and GR enable NSB-supported Layer 2 protocols to synchronize protocol information between the primary and backup Routing Engines.
- If NSR is not enabled (Stateful Replication is Disabled), then enable NSR. NSR requires you to configure graceful Routing Engine switchover (GRES). By default, NSR is disabled.
  - To enable graceful Routing Engine switchover, include the `graceful-switchover` statement at the `[edit chassis redundancy]` hierarchy level as `user@host#set chassis redundancy graceful-switchover`.
  - To enable NSR, include the `nonstop-routing` statement at the `[edit routing-options]` hierarchy level as `user@host#set routing-options nonstop-routing`.
- Enable nonstop bridging (NSB). Nonstop bridging requires you to configure graceful Routing Engine switchover (GRES). By default, NSB is disabled.
  - To enable graceful Routing Engine switchover, include the `graceful-switchover` statement at the `[edit chassis redundancy]` hierarchy level as `user@host#set chassis redundancy graceful-switchover`.
  - To enable NSB, include the `nonstop-bridging` statement at the `[edit protocols layer2-control]` hierarchy level as `user@host#set protocols layer2-control nonstop-bridging`.
- (Optional) Back up the system software—Junos OS, the active configuration, and log files—on the router to an external storage device with the `request system snapshot` command.

On ACX5000 line of routers, you need to consider the following feature before performing ISSU:

- ISSU supports link fault management (LFM) timeout sessions of 1 second interval. During ISSU, you may notice LFM flaps for sessions having timeout interval of less than 1 second.
- Bidirectional Forwarding Detection (BFD) sessions having timeout interval of less than 1 second need to be reconfigured to 1 second before starting the ISSU process. You can restore the timeout interval to its original value after completing the ISSU process.
- ISSU supports interval slow (every 30 seconds) for periodic transmission of Link Aggregation Control Protocol (LACP) packets.
- ISSU supports Virtual Router Redundancy Protocol (VRRP) version 3.

ISSU do not support the following ACX5000 features:

- Downgrade to an earlier version of Junos OS software. If you want to install an earlier version of Junos OS software, use the request system software add CLI command.
- Upgrade of Host OS software.
- Connectivity fault management (CFM).
- TWAMP, RPF, RFC2544, and clocksyncd daemon (timing functionality).
- Mirroring and pseudowire cross connect.
- IPv6 firewall, IPv6 COS (classification and rewrite), IPv6 VPN, and VPLS mesh group.
- Virtual Router Redundancy Protocol (VRRP) version 1 and 2.
- Interval fast (every second) for periodic transmission of Link Aggregation Control Protocol (LACP) packets. If the periodic interval fast is configured, then you may notice traffic drops because of LACP links going down during ISSU. ACX5000 line of routers can support LACP with fast hello by configuring the fast-hello-issu option (**user@host# set protocols lacp fast-hello-issu**) on the main router and peer routers before starting ISSU.

**NOTE:** The peer router must have Junos OS software to support this functionality.

## Upgrading the Software Using ISSU

This procedure describes how to upgrade the software running on a standalone router:

**NOTE:** If the Host OS software needs to be updated, you cannot perform an ISSU. Instead, perform a standard software upgrade.

It is recommended to cleanup any unwanted data from the `/var` directory (`/var/log`, `/var/tmp`) before initiating the ISSU process.

To upgrade the router using ISSU:

1. Download the software package from the Juniper Networks Support website <https://www.juniper.net/support/downloads/junos.html>.

**NOTE:** To access the download site, you must have a service contract with Juniper Networks and an access account. If you need help obtaining an account, complete the registration form at the Juniper Networks website <https://www.juniper.net/registration/Register.jsp>.

2. Go to ACX Series section and select the ACX5000 Series platform software you want to download.
3. Copy the software package or packages to the router. We recommend that you copy the file to the `/var/tmp` directory.
4. Log in to the console connection. Using a console connection allows you to monitor the progress of the upgrade.
5. Start the ISSU:
  - On the router, enter:

```
user@host> request system software in-service-upgrade /var/tmp/package-name.tgz
```

where `package-name.tgz` is, for example, `jinstall-acx5k-15.1X54-D60.9-domestic-signed.tgz`.

**NOTE:** During the upgrade, you will not be able to access the Junos OS CLI.

The router displays status messages similar to the following messages as the upgrade executes:

```
PRE ISSU CHECK:
-----
```

```

PFE Status                : Online
BFD minimum-interval check done : Valid
GRES enabled              : Valid
NSR enabled               : Valid
drop-all-tcp not configured : Valid
OVSDDB not configured      : Valid

```

warning: Do NOT use /user during ISSU. Changes to /user during ISSU may get lost!

[Oct 24 00:25:37]:ISSU: Validating Image

[Oct 24 00:25:44]:ISSU: Preparing Backup RE

Prepare for ISSU

[Oct 24 00:25:49]:ISSU: Backup RE Prepare Done

Extracting jinstall-acx5k-15.1X54-D60.3-domestic ...

Install jinstall-acx5k-15.1X54-D60.3-domestic completed

Spawning the backup RE

Spawn backup RE, index 0 successful

GRES in progress

GRES done in 0 seconds

Waiting for backup RE switchover ready

GRES operational

Copying home directories

Copying home directories successful

Initiating Chassis In-Service-Upgrade

Chassis ISSU Started

[Oct 24 00:31:56]:ISSU: Preparing Daemons

[Oct 24 00:32:57]:ISSU: Daemons Ready for ISSU

[Oct 24 00:33:02]:ISSU: Starting Upgrade for FRUs

[Oct 24 00:33:23]:ISSU: FPC Warm Booting

[Oct 24 00:34:41]:ISSU: FPC Warm Booted

[Oct 24 00:34:51]:ISSU: Preparing for Switchover

[Oct 24 00:34:57]:ISSU: Ready for Switchover

Checking In-Service-Upgrade status

Item	Status	Reason
FPC 0	Online (ISSU)	

Send ISSU done to chassisd on backup RE

Chassis ISSU Completed

[Oct 24 00:35:18]:ISSU: IDLE

Console and management sessions will be disconnected. Please login again.

**NOTE:** An ISSU might stop instead of terminate if the FPC is at the warm boot stage. Also, any links that go down and up will not be detected during a warm boot of the Packet Forwarding Engine (PFE).

**NOTE:** If the ISSU process stops, you can look at the log files to diagnose the problem. The log files are located at `/var/log/vjunos-log.tgz`.

6. Log in after the router reboots. To verify that the software has been upgraded, enter the following command:

```
user@host> show version
```

7. Disable or delete the configuration done to enable the ISSU. This includes disabling nonstop active routing (NSR), nonstop bridging (NBR) and graceful Routing Engine (GRES).

### Verifying a Unified ISSU

Verify the status of FPCs and their corresponding PICs after the most recent unified ISSU.

Issue the `show chassis in-service-upgrade` command on the primary Routing Engine.

```
user@host> show chassis in-service-upgrade
```

Item	Status	Reason
FPC 0	Online	

Display the unified ISSU process messages by using the `show log messages` command.

### How to Use Unified ISSU with Enhanced Mode

#### IN THIS SECTION

- [Unified ISSU with Enhanced Mode Overview | 582](#)
- [Benefits of Unified ISSU with Enhanced Mode | 582](#)
- [Prerequisites for Performing Unified ISSU with Enhanced Mode | 582](#)
- [Performing Unified ISSU with Enhanced Mode | 583](#)

## Unified ISSU with Enhanced Mode Overview

Enhanced mode is an in-service software upgrade (ISSU) option available on MPC8E, MPC9E, and MPC11E line cards that eliminates packet loss during the unified ISSU process. This is achieved by taking advantage of new line card architecture improvements that make it possible to have a second copy of the Junos OS software running on the line card in standby mode ready to take over while software moves from an old image to a new one during unified ISSU. You can enable enhanced mode by adding the `enhanced-mode` option to the `request system software in-service-upgrade` CLI command.

Use this document to learn about unified ISSU with enhanced mode and how to use it.

## Benefits of Unified ISSU with Enhanced Mode

Unified ISSU with enhanced mode provides the following benefits:

- Upgrades to a new software version with no loss of transit or host bound traffic
- Reduces packet loss to zero or several milliseconds depending on configuration and network conditions
- Allows software upgrades to be performed without the need for maintenance windows
- Uses the existing unified ISSU process and doesn't require any special configuration

## Prerequisites for Performing Unified ISSU with Enhanced Mode

Before you begin a unified ISSU with enhanced mode, there are several prerequisites to keep in mind:

- The device running unified ISSU with enhanced mode must use an MPC8E, MPC9E, or MPC11E line card.

**NOTE:** If you are performing unified ISSU with enhanced mode on a device that has a mix of supported and unsupported line cards, there will be sub-second traffic loss for traffic passing through the unsupported line cards.

**NOTE:** If you are performing unified ISSU with enhanced mode on guest network functions (GNFs), then all GNFs should be using MPC8E, MPC9E, or MPC11E line cards to avoid traffic loss.

- The Linux version running on your Flexible PIC Concentrator (FPC) and the line card Linux version in the target release need to be compatible.



- Enhanced mode won't work if the target release carries changes that require the ASIC blocks to be reset.
- Forwarding memory usage should be below 75 percent to ensure no packet loss during the unified ISSU process

**NOTE:** Unified ISSU with enhanced mode will still work if forwarding memory usage is above 75 percent, but it might introduce several milliseconds of packet loss.

- All prerequisites for unified ISSU also apply to enhanced mode. See [Unified ISSU System Requirements](#) for more information.

You can check to see if your device can use unified ISSU with enhanced mode to upgrade to a specific release by using the `request system software validate in-service-upgrade package-name.tgz enhanced-mode` command. If your device and the target release are not compatible with enhanced mode, you can still use regular unified ISSU to upgrade with minimal disruption of traffic.

### Performing Unified ISSU with Enhanced Mode

To perform a unified ISSU with enhanced mode, follow these steps:

1. Download the software package by following the procedure in [Downloading Software](#).
2. Copy the software package or packages to the device. We recommend that you copy the file to the `/var/tmp` directory.
3. Log in to the console connection. Using a console connection allows you to monitor the progress of the upgrade.
4. Verify that you can use unified ISSU with enhanced mode for your desired release.
  - a. On the device, enter:

```
user@host> request system software validate in-service-upgrade /var/tmp/package-name.tgz enhanced-mode
```

where *package-name*.tgz is the name of the software package you downloaded in Step 1.

5. Start the unified ISSU with enhanced mode:

- a. On the device, enter:

```
user@host> request system software in-service-upgrade /var/tmp/package-name.tgz enhanced-mode
reboot
```

where *package-name.tgz* is the name of the software package you downloaded in Step 1.

**NOTE:** During the upgrade, you will not be able to access the Junos OS CLI.

The device displays status messages similar to the following messages as the upgrade executes:

```
Chassis ISSU enhanced-mode
ISSU: set chassis enhanced-mode
Chassis ISSU Check Done
ISSU: Validating Image
..
mgd: commit complete
Validation succeeded
Validating Image Done
Preparing Backup RE
Pushing /var/tmp/junos-install-mx-x86-32-20.1.tgz to re1:/var/tmp/junos-install-mx-
x86-32-20.1.tgz
Pushing package /var/tmp/junos-install-mx-x86-32-20.1.tgz to re1 done
Installing package /var/tmp/junos-install-mx-x86-32-20.1.tgz on re1
...
Verified sflow-mx signed by PackageDevelopmentEc_2019 method ECDSA256+SHA256
NOTICE: 'pending' set will be activated at next reboot...
ISSU: Installing package /var/tmp/junos-install-mx-x86-32-20.1.tgz on re1 done
ISSU: Rebooting Backup RE

Rebooting re1
Backup RE Prepare Done
Waiting for Backup RE reboot
Backup RE reboot done. Backup RE is up
Waiting for Backup RE state synchronization
Backup RE state synchronization done
GRES operational
"Initiating Chassis In-Service-Upgrade"
Chassis ISSU Started
ISSU: Preparing Daemons
```

```

ISSU: Daemons Ready for ISSU
ISSU: Offline Incompatible FRUs
ISSU: Starting Upgrade for FRUs
...

ISSU: Preparing for Switchover
ISSU: Ready for Switchover
Checking In-Service-Upgrade status
  Item           Status           Reason
  FPC 1          Online (ISSU)
  FPC 2          Offline           Configured power off
Resolving mastership...
Complete. The other routing engine becomes the master.

```

**NOTE:** If the unified ISSU process stops, you can look at the CLI output by using the request system software in-service-upgrade command to diagnose the problem. You can also look at syslog files for more information.

6. Log in after the reboot of the device is completed. To verify that the software has been upgraded, enter the following command:

```

user@host> show version

```

**NOTE:** When using unified ISSU with enhanced mode, the base Linux OS on your FPC cannot be upgraded as part of the ISSU process. Linux can be updated with an upgrade done through regular unified ISSU or a reboot of the FPC.

## Verifying a Unified ISSU

IN THIS SECTION

● Purpose | 586

● Action | 586

● Meaning | 586

**Purpose**

Verify the status of FPCs and their corresponding PICs after the most recent unified ISSU.

**Action**

Issue the `show chassis in-service-upgrade` command on the primary Routing Engine.

```
user@host> show chassis in-service-upgrade
Item           Status           Reason
FPC 0          Online
FPC 1          Online
FPC 2          Online
  PIC 0        Online
  PIC 1        Online
FPC 3          Offline          Offlined by CLI command
FPC 4          Online
  PIC 1        Online
FPC 5          Online
  PIC 0        Online
FPC 6          Online
  PIC 3        Online
FPC 7          Online
```

Display the unified ISSU process messages by using the `show log messages` command.

**Meaning**

See ["show chassis in-service-upgrade" on page 1389](#) for more information.

**SEE ALSO**

Example: Performing a Unified ISSU
Troubleshooting Unified ISSU Problems
Understanding the Unified ISSU Process
<a href="#">Unified ISSU System Requirements   504</a>
Managing and Tracing BFD Sessions During Unified ISSU Procedures

## Troubleshooting Unified ISSU Problems

If the unified ISSU procedure stops progressing:

1. Open a new session on the primary Routing Engine and issue the `request system software abort in-service-upgrade` command.
2. Check the existing router session to verify that the upgrade has been terminated.

An “ISSU: terminated!” message is provided. Additional system messages provide you with information about where the upgrade stopped and recommendations for the next step to take.

See [request chassis cluster in-service-upgrade abort \(ISSU\)](#) for more information.

### SEE ALSO

Understanding the Unified ISSU Process
<a href="#">Unified ISSU System Requirements   504</a>
Best Practices for Performing a Unified ISSU
Example: Performing a Unified ISSU
Verifying a Unified ISSU
Managing and Tracing BFD Sessions During Unified ISSU Procedures


## Managing and Tracing BFD Sessions During Unified ISSU Procedures

Bidirectional Forwarding Detection (BFD) sessions temporarily increase their detection and transmission timers during unified ISSU procedures. After the upgrade, these timers revert to the values in use before the unified ISSU started. The BFD process replicates the unified ISSU state and timer values to the backup Routing Engine for each session.

No additional configuration is necessary to enable unified ISSU for BFD. However, you can disable the BFD timer negotiation during the unified ISSU by including the `no-issu-timer-negotiation` statement at the `[edit protocols bfd]` hierarchy level.

```
[edit protocols bfd]
no-issu-timer-negotiation;
```

If you include this statement, the BFD timers maintain their original values during unified ISSU.



**CAUTION:** The BFD sessions might flap during unified ISSU or Routing Engine switchover, depending on the detection intervals.

For more information about BFD, see the [Junos OS Routing Protocols Library](#).

To configure unified ISSU trace options for BFD sessions, include the `issu` statement at the `[edit protocols bfd traceoptions flag]` hierarchy level.

```
[edit protocols]
bfd {
  traceoptions {
    flag issu;
  }
}
```

SEE ALSO

Getting Started with Unified In-Service Software Upgrade
Understanding the Unified ISSU Process
<a href="#">Unified ISSU System Requirements   504</a>
Best Practices for Performing a Unified ISSU
Example: Performing a Unified ISSU
Verifying a Unified ISSU
Troubleshooting Unified ISSU Problems

Release History Table

Release	Description
18.1R1	Starting with Junos OS Release 18.2R1 on the QFX5200 switch, we recommend that you wait at least five minutes between in-service software upgrades.
17.1R1	Starting with Junos OS Release 17.1R1, on QFX5100 and EX4600 switches, you cannot perform an ISSU from a Junos OS Release earlier than 17.1R1 to Junos OS Release 17.1R1.

# Performing an ISSR

## IN THIS CHAPTER

- [Performing an In-Service Software Reboot | 589](#)

## Performing an In-Service Software Reboot

### SUMMARY

You can perform an in-service software reboot (ISSR) by following these steps.

**NOTE:** We recommend that you wait at least five minutes between in-service software reboots.

When you request an in-service software reboot (ISSR) on a standalone device:

1. The management process (MGD) verifies that graceful restart (GR) or non-stop routing and graceful Routing Engine switchover (GRES) are enabled.
2. The ISSU state machine spawns the backup Routing Engine (RE) with the existing software version.
3. The ISSU state machine checks to see if the backup RE has synchronized all of the data with the primary RE.
4. The ISSU state machine requests the routing protocol process (RPD) to notify its readiness for switchover.
5. RPD initiates the GR or non-stop routing procedures by notifying all of the registered protocols.
6. RPD notifies the ISSU state machine that its ready for switchover.

7. The primary role is switched between the REs, so the backup RE becomes the primary RE.
8. The old primary RE is shut down.
9. RPD is spawned on the new primary and continues the GR or non-stop routing procedure and exits either GR or non-stop routing after the protocol state synchronizes.

To perform an ISSR:

Issue the `request system reboot in-service` command.

For example:

```
user@switch> request system reboot in-service
Reboot the system ? [yes,no]
[Feb 22 02:37:04]:ISSU: Validating Image

PRE ISSR CHECK:
-----
PFE Status                : Online
Member Id zero             : Valid
VC not in mixed or fabric mode : Valid
Member is single node vc   : Valid
BFD minimum-interval check done : Valid
GRES enabled               : Valid
NSR enabled                : Valid
drop-all-tcp not configured : Valid
Ready for ISSR             : Valid

warning: Do NOT use /user during ISSR. Changes to /user during ISSR may get lost!
Current image is jinstall-jcp-i386-flex-18.1.img
[Feb 22 02:37:14]:ISSU: Preparing Backup RE
Prepare for ISSR
[Feb 22 02:37:19]:ISSU: Backup RE Prepare Done
Spawning the backup RE
Spawn backup RE, index 1 successful
Starting secondary dataplane
Second dataplane container started
GRES in progress
Waiting for backup RE switchover ready
GRES operational
Copying home directories
Copying home directories successful
Initiating Chassis In-Service-Upgrade for ISSR
```



```

Chassis ISSU Started
[Feb 22 02:42:55]:ISSU: Preparing Daemons
[Feb 22 02:43:00]:ISSU: Daemons Ready for ISSU
[Feb 22 02:43:05]:ISSU: Starting Upgrade for FRUs
[Feb 22 02:43:15]:ISSU: FPC Warm Booting
[Feb 22 02:44:16]:ISSU: FPC Warm Booted
[Feb 22 02:44:27]:ISSU: Preparing for Switchover
[Feb 22 02:44:31]:ISSU: Ready for Switchover
Checking In-Service-Upgrade status
  Item           Status           Reason
  FPC 0          Online (ISSU)
Send ISSR done to chassisd on backup RE
Chassis ISSU Completed
Removing dcpfe0 eth1 128.168.0.16 IP
Bringing down bme00
Post Chassis ISSU processing done
[Feb 22 02:44:33]:ISSU: IDLE
Stopping primary dataplane
Clearing ISSU states
Console and management sessions will be disconnected. Please login again.
device_handoff successful ret: 0
Shutdown NOW!
[pid 14305]

*** FINAL System shutdown message from root@sw-duckhorn-01 ***

System going down IMMEDIATELY

```

## RELATED DOCUMENTATION

| *request system reboot*

# 14

PART

## Performing Nonstop Software Upgrade (NSSU)

---

[Getting Started with NSSU and Understanding How NSSU Works | 593](#)

[Performing a NSSU | 603](#)

---

# Getting Started with NSSU and Understanding How NSSU Works

## IN THIS CHAPTER

- [Understanding Nonstop Software Upgrade on EX Series Switches | 593](#)

## Understanding Nonstop Software Upgrade on EX Series Switches

### SUMMARY

Nonstop software upgrade (NSSU) is a feature that enables the upgrade of all supported EX Series switches in a network with a single command.

### IN THIS SECTION

- [Requirements for Performing an NSSU | 595](#)
- [How an NSSU Works | 597](#)
- [NSSU Limitations | 600](#)
- [NSSU and Junos OS Release Support | 600](#)
- [Overview of NSSU Configuration and Operation | 602](#)

Nonstop software upgrade (NSSU) enables you to upgrade the software running on Juniper Networks EX Series Ethernet Switches with redundant Routing Engines and all member switches in EX Series Virtual Chassis using a single command. During the upgrade there might be minimal network traffic disruption during primary-role switchover, and the extent of disruption could be dependent on the network topology, configuration, network traffic, and other environment factors .

**NOTE:** When an EX Series switch in a mixed Virtual Chassis is upgraded to Junos OS Release 15.1 or later from a release earlier than Release 15.1, there might be a drop in traffic for up to 60 seconds.

The following EX Series Virtual Chassis support NSSU:

- EX3300 Virtual Chassis
- EX3400 Virtual Chassis
- EX4200 Virtual Chassis
- EX4300 Virtual Chassis
- EX4400 Virtual Chassis
- EX4500 Virtual Chassis
- EX4550 Virtual Chassis
- All mixed Virtual Chassis composed of EX4200, EX4500, and EX4550 switches
- EX4600 Virtual Chassis
- EX4650 Virtual Chassis

**NOTE:** An EX4650 Virtual Chassis operates the same as a QFX5120 Virtual Chassis, so for details on upgrading an EX4650 Virtual Chassis using NSSU, see [Understanding Nonstop Software Upgrade on a Virtual Chassis and Mixed Virtual Chassis](#) and [Upgrading Software on a Virtual Chassis and Mixed Virtual Chassis Using Nonstop Software Upgrade](#) instead of this topic.

- EX6200 switches
- EX8200 switches
- EX8200 Virtual Chassis

Performing an NSSU provides these benefits:

- No disruption to the control plane—An NSSU takes advantage of *graceful Routing Engine switchover* (GRES) and *nonstop active routing* (NSR) to ensure no disruption to the control plane. During the upgrade process, interface, kernel, and routing protocol information is preserved.

- Minimal disruption to network traffic—An NSSU minimizes network traffic disruption by:
  - Upgrading line cards one at a time in an EX6200 switch, EX8200 switch, or EX8200 Virtual Chassis while permitting traffic to continue to flow through the line cards that are not being upgraded.
  - Upgrading member switches one at a time in other EX Series Virtual Chassis while permitting traffic to continue to flow through the members that are not being upgraded.

To achieve minimal disruption to traffic, you must configure link aggregation groups (LAGs) such that the member links of each LAG reside on different line cards or Virtual Chassis members. When one member link of a LAG is down, the remaining links are up, and traffic continues to flow through the LAG.

**NOTE:** Because NSSU upgrades the software on each line card or on each Virtual Chassis member one at a time, an upgrade using NSSU can take longer than an upgrade using the request system software add command.

In releases prior to Junos OS Release 16.1, for EX6200 switches, EX8200 switches, and EX8200 Virtual Chassis, you can reduce the amount of time an upgrade takes by configuring line-card upgrade groups. The line cards in an upgrade group are upgraded simultaneously, reducing the amount of time it takes to complete an upgrade. See *Configuring Line-Card Upgrade Groups for Nonstop Software Upgrade*.

## Requirements for Performing an NSSU

The following requirements apply to all switches and Virtual Chassis:

**NOTE:** NSSU can only upgrade up to three major releases ahead of the current release on a device. To upgrade to a release more than three releases ahead of the current release on a device, use the NSSU process to upgrade the switch to one or more intermediate releases until the switch is within three major releases of the target release.

- All Virtual Chassis members and all Routing Engines must be running the same Junos OS release.
- Graceful Routing Engine switchover (GRES) must be enabled.
- Nonstop active routing (NSR) must be enabled.

**NOTE:** Although nonstop bridging (NSB) does not have to be enabled to perform an NSSU, we recommend enabling NSB before performing an NSSU. Enabling NSB ensures that all NSB-supported Layer 2 protocols operate seamlessly during the Routing Engine switchover that is part of the NSSU. In releases prior to Junos OS Release 16.1, see [Configuring Nonstop Bridging on Switches \(CLI Procedure\)](#).

- For minimal traffic disruption, you must define link aggregation groups (LAGs) such that the member links reside on different Virtual Chassis members or on different line cards.

**NOTE:** During an NSSU operation, if you try to view LAG interface status on the primary Routing Engine member using the `show interfaces ae-ae-interface-number` CLI command, you might see incorrect or zero traffic counts. To work around this problem, run the command on the backup Routing Engine member instead if that member is already loaded and running.

The following are requirements for performing NSSU on an EX Series Virtual Chassis (excluding EX6200 or EX8200 Virtual Chassis):

- The Virtual Chassis members must be connected in a ring topology so that no member is isolated as a result of another member being rebooted. This topology prevents the Virtual Chassis from splitting during an NSSU.
- The Virtual Chassis primary and backup must be adjacent to each other in the ring topology. Adjacency permits the primary and backup to always be in sync, even when the switches in linecard roles are rebooting.
- The Virtual Chassis must be preprovisioned so that the linecard role has been explicitly assigned to member switches acting in a linecard role. During an NSSU, the Virtual Chassis members must maintain their roles—the primary and backup must maintain their primary and backup roles (although primary role will change), and the remaining switches must maintain their linecard roles.
- A two-member Virtual Chassis must have `no-split-detection` configured so that the Virtual Chassis does not split when an NSSU upgrades a member.

**NOTE:** For the EX4300 Virtual Chassis, you should enable the `vcp-no-hold-time` statement at the `[edit virtual-chassis]` hierarchy level before performing a software upgrade using NSSU. If you do not enable the `vcp-no-hold-time` statement, the Virtual Chassis might split during the upgrade. A split Virtual Chassis can cause disruptions to your network, and you might have to manually reconfigure your Virtual Chassis after the NSSU if the split and merge feature was disabled. For

more information about a split Virtual Chassis, see [Understanding Split and Merge in a Virtual Chassis](#)

## How an NSSU Works

This section describes what happens when you request an NSSU on EX Series switches and Virtual Chassis.

**NOTE:** An EX4650 Virtual Chassis operates the same as a QFX5120 Virtual Chassis, so for details on upgrading an EX4650 Virtual Chassis using NSSU, see [Understanding Nonstop Software Upgrade on a Virtual Chassis and Mixed Virtual Chassis](#) and [Upgrading Software on a Virtual Chassis and Mixed Virtual Chassis Using Nonstop Software Upgrade](#) instead of this topic.

### EX3300, EX3400, EX4200, EX4300, EX4400, EX4500, EX4600, and Mixed Virtual Chassis

When you request an NSSU on an EX3300, EX3400, EX4200, EX4300, EX4400, EX4500, or mixed Virtual Chassis:

1. The Virtual Chassis primary verifies that:
  - The backup is online and running the same software version.
  - Graceful Routing Engine switchover (GRES) and nonstop active routing (NSR) are enabled.
  - The Virtual Chassis has a preprovisioned configuration.
2. The primary installs the new software image on the backup and reboots it.
3. The primary resynchronizes the backup.
4. The primary installs the new software image on member switches that are in the linecard role and reboots them, one at a time. The primary waits for each member to become online and active before starting the software upgrade on the next member.
5. When all members that are in the linecard role have been upgraded, the primary performs a graceful Routing Engine switchover, and the upgraded backup becomes the primary.
6. The software on the original primary is upgraded and the original primary is automatically rebooted. After the original primary has rejoined the Virtual Chassis, you can optionally return control to it by requesting a graceful Routing Engine switchover.

## EX6200 and EX8200 Switches

When you request an NSSU on a standalone switch with redundant Routing Engines:

1. The switch verifies that:
  - Both Routing Engines are online and running the same software version.
  - Both Routing Engines have sufficient storage space for the new software image.
  - Graceful Routing Engine switchover and nonstop active routing are enabled.
2. The switch installs the new software image on the backup Routing Engine and reboots it.
3. The switch resynchronizes the backup Routing Engine to the primary Routing Engine.
4. The line cards in the first upgrade group (or the line card in slot 0, if no upgrade groups are defined) download the new image and then restart. Traffic continues to flow through the line cards in the other upgrade groups during this process.
5. When line cards restarted in Step 4 are online again, the line cards in the next upgrade group download the new image and restart. This process continues until all online line cards have restarted with the new software.

**NOTE:** If you have taken a line card offline with the CLI before you start the NSSU, the line card is not restarted and remains offline.

6. The switch performs a graceful Routing Engine switchover, so that the upgraded backup Routing Engine becomes the primary.
7. The switch installs the new software on the original primary Routing Engine.

To complete the upgrade process, the original primary Routing Engine must be rebooted. You can do so manually or have the switch perform an automatic reboot by including the `reboot` option when you request the NSSU. After the original primary has been rebooted, you can optionally return control to it by requesting a graceful Routing Engine switchover.

8. (EX6200 switch only) The original primary Routing Engine reboots to complete the software upgrade.

**NOTE:** To complete the upgrade process on an EX8200 switch, you must intervene to reboot the original primary Routing Engine. You can reboot the original primary Routing Engine



manually or have the switch perform an automatic reboot by including the `reboot` option when you request the NSSU.

9. (Optional) After the original primary has been rebooted, you can return control to it by requesting a graceful Routing Engine switchover.

The switch can maintain normal operations with either Routing Engine acting as the primary Routing Engine after the software upgrade, so you only have to perform this switchover if you want to return Routing Engine control to the original primary Routing Engine.

## EX8200 Virtual Chassis

When you request an NSSU on an EX8200 Virtual Chassis:

1. The primary external Routing Engine verifies that:
  - It has a backup external Routing Engine that is online.
  - All Virtual Chassis members have redundant Routing Engines and the Routing Engines are online.
  - All Routing Engines are running the same software version.
  - All Routing Engines have sufficient storage space for the new software image.
  - Graceful Routing Engine switchover and nonstop active routing (NSR) are enabled.
2. The primary external Routing Engine installs the new software image on the backup external Routing Engine and reboots it.
3. The backup external Routing Engine resynchronizes with the primary external Routing Engine.
4. The primary external Routing Engine installs the new software on the backup Routing Engines in the member switches and reboots the backup Routing Engines.
5. When the reboot of the backup Routing Engines complete, the line cards in the first upgrade group download the new image and then restart. (If no upgrade groups are defined, the line card in slot 0 of member 0 downloads the new image and restarts.) Traffic continues to flow through the line cards in the other upgrade groups during this process.
6. When line cards restarted in Step 5 are online again, the line cards in the next upgrade group (or the next sequential line card) download the new image and restart. This process continues until all online line cards have restarted with the new software.

**NOTE:** If you have taken a line card offline with the CLI before you start the NSSU, the line card is not restarted and remains offline.

7. The new software image is installed on the primary Routing Engines, both external and internal.
8. The member switches perform a graceful Routing Engine switchover, so that the upgraded backup Routing Engines become primaries.
9. The primary external Routing Engine performs a graceful Routing Engine switchover so that the backup external Routing Engine is now the primary.

To complete the upgrade process, the original primary Routing Engines, both external and internal, must be rebooted. You can do so manually by establishing a console connection to each Routing Engine or have the reboot performed automatically by including the `reboot` option when you request the NSSU. After the original primary external Routing Engine has been rebooted, you can optionally return control to it by requesting a graceful Routing Engine switchover.

### NSSU Limitations

You cannot use an NSSU to downgrade the software—that is, to install an earlier version of the software than is currently running on the switch. To install an earlier software version, use the `request system software add` command.

You cannot roll back to the previous software version after you perform an upgrade using NSSU. If you need to roll back to the previous software version, you can do so by rebooting from the alternate root partition if you have not already copied the new software version into the alternate root partition.

### NSSU and Junos OS Release Support

A Virtual Chassis must be running a Junos OS release that supports NSSU before you can perform an NSSU. If a Virtual Chassis is running a software version that does not support NSSU, use the `request system software add` command.

[Table 38 on page 600](#) lists the EX Series switches and Virtual Chassis that support NSSU and the Junos OS release at which they began supporting it.

**Table 38: Platform and Release Support for NSSU**

Platform	Junos OS Release
EX3300 Virtual Chassis	12.2 or later

**Table 38: Platform and Release Support for NSSU (Continued)**

Platform	Junos OS Release
EX3400 Virtual Chassis	15.1X53-D55
EX4200 Virtual Chassis	12.1 or later
EX4300 Virtual Chassis	13.2X51-D20 or later
EX4300 Multigigabit Virtual Chassis	18.2R1 or later
EX4400 Virtual Chassis	21.1 or later
EX4400 Multigigabit Virtual Chassis	21.2 or later
EX4500 Virtual Chassis	12.1 or later
EX4550 Virtual Chassis	12.2 or later
Mixed EX4200 and EX4500 Virtual Chassis	12.1 or later
Mixed EX4200 and EX4550 Virtual Chassis	12.2 or later
Mixed EX4200, EX4500, and EX4550 Virtual Chassis	12.2 or later
Mixed EX4500 and EX4550 Virtual Chassis	12.2 or later
Mixed EX4300 and EX4600 Virtual Chassis	13.2X51-D25 or later
EX6200 switch	12.2 or later
EX8200 switch	10.4 or later
EX8200 Virtual Chassis	11.1 or later

## Overview of NSSU Configuration and Operation

You must ensure that the configuration of the switch or Virtual Chassis meets the requirements described in ["Requirements for Performing an NSSU" on page 595](#). NSSU requires no additional configuration.

In releases prior to Junos OS Release 16.1, for EX6200 switches, EX8200 switches, and EX8200 Virtual Chassis, you can optionally configure line-card upgrade groups using the CLI. See ["Example: Configuring Line-Card Upgrade Groups for Nonstop Software Upgrade on EX Series Switches" on page 593](#).

You perform an NSSU by executing the `request system software nonstop-upgrade` command. For detailed instructions on how to perform an NSSU, see the topics in Related Documentation.

Release History Table

Release	Description
16.1	In releases prior to Junos OS Release 16.1, for EX6200 switches, EX8200 switches, and EX8200 Virtual Chassis, you can reduce the amount of time an upgrade takes by configuring line-card upgrade groups.

### RELATED DOCUMENTATION

<a href="#">Upgrading Software Using Nonstop Software Upgrade on EX Series Virtual Chassis and Mixed Virtual Chassis (CLI Procedure)   1215</a>
<a href="#">Upgrading Software on an EX6200 or EX8200 Standalone Switch Using Nonstop Software Upgrade (CLI Procedure)</a>
<a href="#">Upgrading Software on an EX8200 Virtual Chassis Using Nonstop Software Upgrade (CLI Procedure)   1209</a>
<a href="#">Configuring Nonstop Active Routing on Switches</a>
<a href="#">Configuring Graceful Routing Engine Switchover in a Virtual Chassis</a>
<a href="#">Understanding Nonstop Software Upgrade on EX Series Switches   593</a>

# Performing a NSSU

## IN THIS CHAPTER

- [Performing a NSSU | 603](#)

## Performing a NSSU

### SUMMARY

Follow the steps below to perform a nonstop software upgrade (NSSU) on your device.

### IN THIS SECTION

- [Configuring Line-Card Upgrade Groups for Nonstop Software Upgrade | 603](#)
- [Example: Configuring Line-Card Upgrade Groups for Nonstop Software Upgrade on EX Series Switches | 608](#)

## Configuring Line-Card Upgrade Groups for Nonstop Software Upgrade

### IN THIS SECTION

- [How Line-card Upgrade Groups Work with Nonstop Software Upgrade | 604](#)
- [Line-card Upgrade Groups Support | 604](#)
- [Configure Line-Card Upgrade Groups on an EX4650 Virtual Chassis, a QFX Series Virtual Chassis or a QFX5100 VCF | 605](#)
- [Configure Line-Card Upgrade Groups on Standalone EX6200 or EX8200 Switches | 605](#)
- [Configure Line-Card Upgrade Groups on an EX8200 Virtual Chassis | 606](#)

You can configure line-card upgrade groups for nonstop software upgrade (NSSU) operations on supporting platforms. Line-card upgrade groups can reduce the total time required to complete an NSSU operation and enable you to control the upgrade sequence among the switches being upgraded.

### How Line-card Upgrade Groups Work with Nonstop Software Upgrade

With NSSU, you can upgrade software on supporting switches with redundant Routing Engines, a Virtual Chassis, or a Virtual Chassis Fabric (VCF) using a single command with minimal disruption to network traffic.

In its default configuration, NSSU upgrades each line card in a switch or linecard role member in a Virtual Chassis or VCF one at a time. Traffic continues to flow through the other line cards or members while each one is being restarted as part of the upgrade. This behavior minimizes traffic disruption if you configure link aggregation groups (LAGs) such that the member links of each LAG reside on different line cards or members. As a result, when one member link of a LAG is down, the remaining links are up, and traffic continues to flow through the LAG.

When you configure line-card upgrade groups for NSSU, NSSU upgrades all of the devices in each upgrade group at the same time instead of sequentially, reducing the total time needed to complete the upgrade on all line cards or members.

To achieve minimal traffic disruption during an NSSU operation, you must define the line-card upgrade groups such that the member links of the LAGs reside on line cards or members that are in different upgrade groups. For information on how to configure LAGs, see [Configuring Aggregated Ethernet Links \(CLI Procedure\)](#).

NSSU upgrades the groups in the order that they appear in the configuration (in other words, in the order you configure them). As a result, you can also define upgrade groups to control the upgrade sequence during an NSSU operation.

To configure upgrade groups, use the `upgrade-group` configuration statement in the `[edit chassis nssu]` hierarchy.

### Line-card Upgrade Groups Support

The following platforms support NSSU line-card upgrade groups:

- EX4650 Virtual Chassis with more than three member switches
- QFX3500, QFX3600, and QFX5100 Virtual Chassis
- QFX5100 Virtual Chassis Fabric (VCF)
- EX6200 or EX8200 switches with redundant Routing Engines
- EX8200 Virtual Chassis

## Configure Line-Card Upgrade Groups on an EX4650 Virtual Chassis, a QFX Series Virtual Chassis or a QFX5100 VCF

When you configure line-card upgrade groups on an EX4650 Virtual Chassis, a QFX Series Virtual Chassis, or a QFX5100 VCF, whose switches do not have separate line cards, you use only the `fpcs` option to specify the Virtual Chassis or VCF member IDs that you want to include in an upgrade group. You don't need to use the `member` option.

- To create an upgrade group and add a Virtual Chassis or VCF member switch to the upgrade group, configure the upgrade group name and specify the member number using the `fpcs` option:

```
[edit chassis]
user@switch# set nssu upgrade-group group-name fpcs member-number
```

For example, to create an upgrade group called `vcf` and add linecard role member 2 to that group:

```
[edit chassis]
user@switch# set nssu upgrade-group vcf fpcs 2
```

If `vcf` already exists, this command adds member 2 to `vcf`.

- To create an upgrade group that contains multiple members in a Virtual Chassis or VCF, specify multiple member numbers enclosed in square brackets after the `fpcs` option:

```
[edit chassis]
user@switch# set nssu upgrade-group group-name fpcs [list-of-member-numbers]
```

For example, to create an upgrade group called `vc1` that contains members 1 and 2:

```
[edit chassis]
user@switch# set nssu upgrade-group vc1 fpcs [1 2]
```

Make sure you commit the configuration before starting an NSSU operation.

## Configure Line-Card Upgrade Groups on Standalone EX6200 or EX8200 Switches

To configure line-card upgrade groups on a standalone EX6200 or EX8200 switch:

- To create an upgrade group and add a line card to it:

```
[edit chassis]
user@switch# set nssu upgrade-group group-name fpcs slot-number
```

For example, to create an upgrade group called `group3` and add the line card in slot 5 to it:

```
[edit chassis]
user@switch# set nssu upgrade-group group3 fpcs 5
```

If `group3` already exists, this command adds line card 5 to `group3`.

- To create an upgrade group and add multiple line cards to it:

```
[edit chassis]
user@switch# set nssu upgrade-group group-name fpcs [list-of-slot-numbers]
```

For example, to create an upgrade group called `primary` and add line cards in slots 1, 4, and 7 to it:

```
[edit chassis]
user@switch# set nssu upgrade-group primary fpcs [1 4 7]
```

If `primary` already exists, this command adds line cards in slots 1, 4, and 7 to `primary`.

## SEE ALSO

[Upgrading Software on an EX6200 or EX8200 Standalone Switch Using Nonstop Software Upgrade \(CLI Procedure\)](#)

## Configure Line-Card Upgrade Groups on an EX8200 Virtual Chassis

To configure line-card upgrade groups on an EX8200 Virtual Chassis:

- To create an upgrade group and add a line card on a Virtual Chassis member to it:

```
[edit chassis]
user@switch# set nssu upgrade-group group-name member member-id fpcs slot-number
```



For example, to create an upgrade group called `primary-ny` and add the line card on member 1 in slot 5 to it:

```
[edit chassis]
user@switch# set nssu upgrade-group primary-ny member 1 fpcs 5
```

If `primary-ny` already exists, this command adds line card 5 on member 1 to `primary-ny`.

- To create an upgrade group that contains multiple line cards on a Virtual Chassis member:

```
[edit chassis]
user@switch# set nssu upgrade-group group-name member member-id fpcs [list-of-slot-numbers]
```

For example, to create an upgrade group called `primary-ny` that contains the line cards in slots 1 and 2 on member 0 and in slots 3 and 4 on member 1:

```
[edit chassis]
user@switch# set nssu upgrade-group primary-ny member 0 fpcs [1 2]

[edit chassis]
user@switch# set nssu upgrade-group primary-ny member 1 fpcs [3 4]
```

## SEE ALSO

[Upgrading Software on an EX8200 Virtual Chassis Using Nonstop Software Upgrade \(CLI Procedure\)](#)

## RELATED DOCUMENTATION

[Understanding Nonstop Software Upgrade on a Virtual Chassis and Mixed Virtual Chassis](#)

[Upgrading Software on a Virtual Chassis and Mixed Virtual Chassis Using Nonstop Software Upgrade](#)

[Understanding Nonstop Software Upgrade on a Virtual Chassis Fabric](#)

[Upgrading Software on a Virtual Chassis Fabric Using Nonstop Software Upgrade](#)

[Understanding Nonstop Software Upgrade on EX Series Switches](#)

[Upgrading Software Using Nonstop Software Upgrade on EX Series Virtual Chassis and Mixed Virtual Chassis \(CLI Procedure\)](#)

[Example: Configuring Line-Card Upgrade Groups for Nonstop Software Upgrade on EX Series Switches](#)

## Example: Configuring Line-Card Upgrade Groups for Nonstop Software Upgrade on EX Series Switches

### IN THIS SECTION

- [Requirements](#) | 608
- [Overview and Topology](#) | 608
- [Configuration](#) | 610

Nonstop software upgrade (NSSU) enables you to upgrade the software running on an EX Series switch with redundant Routing Engines or on most EX Series Virtual Chassis by using a single command and with minimal disruption to network traffic. By default, NSSU upgrades the software running on line cards one line card at a time.

To reduce the time an NSSU takes, you can configure line-card upgrade groups on an EX6200 or EX8200 switch with redundant Routing Engines or on an EX8200 Virtual Chassis.

This example shows how to configure NSSU to use line-card upgrade groups:

### Requirements

This example uses the following hardware and software components:

- An EX8200 switch with redundant Routing Engines
- Junos OS Release 10.4 or later for EX Series switches

Before you begin to configure line-card upgrade groups, ensure that you have configured the link aggregation groups (LAGs) as described in [Configuring Aggregated Ethernet Links \(CLI Procedure\)](#). See ["Overview and Topology" on page 608](#) for details about the LAG configurations for this example.

### Overview and Topology

### IN THIS SECTION

- [Topology](#) | 609

In its default configuration, NSSU upgrades each line card in a switch or Virtual Chassis one at a time. Traffic continues to flow through the other line cards while a line card is being restarted as part of the upgrade. This behavior allows you minimize disruption to traffic by configuring link aggregation groups (LAGs) such that the member links of each LAG reside on different line cards. When one member link of a LAG is down, the remaining links are up, and traffic continues to flow through the LAG.

Because the default configuration upgrades each line card one at a time, the upgrade can take some time to complete. You can reduce the time it takes to perform an NSSU by configuring line-card upgrade groups. Instead of being upgraded sequentially, the line cards in an upgrade group are upgraded simultaneously. To achieve minimal traffic disruption, you must define the line-card upgrade groups such that the member links of the LAGs reside on line cards that are in different upgrade groups.

**NOTE:** NSSU upgrades the groups in the order that they appear in the configuration (in other words, in the order you configure them).

### *Topology*

This example uses an EX8200 switch that has five line cards installed in slots 0 through 4. Two LAGs have been configured:

- ae0—Has two member links, one on the line card in slot 0 and one on the line card in slot 1.
- ae1—Has two member links, one on the line card in slot 2 and one on the line card in slot 3.

The interfaces on the line card in slot 4 are not part of either LAG.

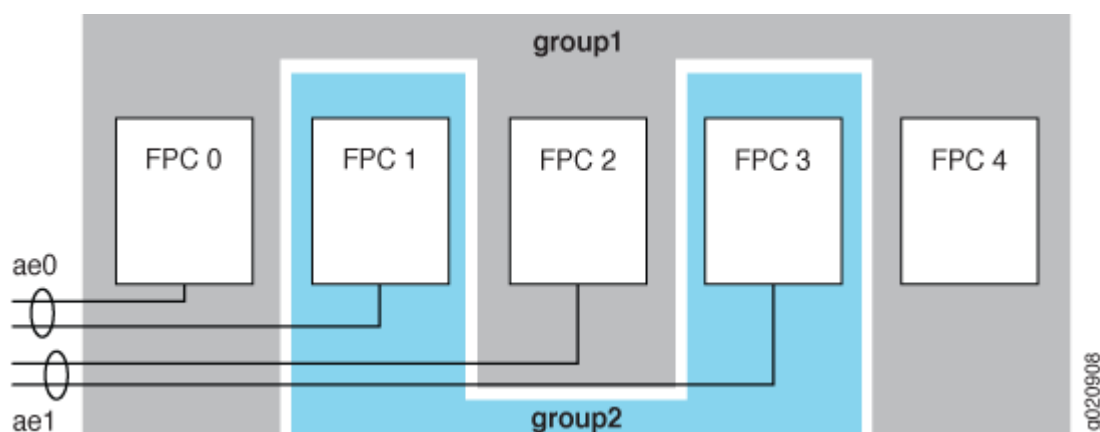
To minimize the time an upgrade takes and to ensure that the member links of each LAG are in different upgrade groups, this example configures the following two line-card upgrade groups:

- group1—Contains the line cards in slots 0, 2, and 4.
- group2—Contains the line cards in slots 1 and 3.

The line card in slot 4 could be put in either group. It could also be left out of an upgrade group entirely, and it would be upgraded separately after the line cards in the upgrade groups have been upgraded. However, it is more efficient to include it in an upgrade group.

[Figure 36 on page 610](#) illustrates the topology.

Figure 36: Example Line-Card Upgrade Group Topology



## Configuration

### IN THIS SECTION

- [CLI Quick Configuration | 610](#)
- [Procedure | 610](#)

To create line-card upgrade groups, perform these tasks:

### *CLI Quick Configuration*

To quickly create the line-card upgrade groups, copy the following commands and paste them into the switch terminal window:

```
[edit]
set chassis nssu upgrade-group group1 fpcs [0 2 4]
set chassis nssu upgrade-group group2 fpcs [1 3]
```

### *Procedure*

### Step-by-Step Procedure

To create the line-card upgrade groups for an NSSU:

1. Create the first line-card upgrade group:

```
[edit chassis]
user@switch# set nssu upgrade-group group1 fpcs [0 2 4]
```

2. Create the second line-card upgrade group:

```
[edit chassis]
user@switch# set nssu upgrade-group group2 fpcs (NSSU Upgrade Groups) [1
3]
```

## Results

Display the results of the configuration:

```
[edit chassis]
user@switch# show
nssu {
    upgrade-group group1 {
        fpcs [ 0 2 4 ];
    }
    upgrade-group group2 {
        fpcs [ 1 3 ];
    }
}
```

## SEE ALSO

Configuring Line-Card Upgrade Groups for Nonstop Software Upgrade

[Upgrading Software on an EX6200 or EX8200 Standalone Switch Using Nonstop Software Upgrade \(CLI Procedure\)](#)

[Upgrading Software on an EX8200 Virtual Chassis Using Nonstop Software Upgrade \(CLI Procedure\) | 1209](#)

# 15

PART

## Multinode High Availability

---

[Overview](#) | [613](#)

[Multinode High Availability Configuration](#) | [672](#)

[Hardware and Software Upgrades](#) | [885](#)

[Multinode High Availability Support for vSRX](#) | [908](#)

---

## CHAPTER 31

# Overview

**IN THIS CHAPTER**

- [Multinode High Availability | 613](#)
- [Prepare Your Environment for Multinode High Availability Deployment | 654](#)
- [Multinode High Availability Services | 658](#)
- [IPsec VPN Support in Multinode High Availability | 664](#)

## Multinode High Availability

**SUMMARY**

Learn about the Multinode High Availability solution and how you can use it in simple and reliable deployment models. Currently, we support two nodes in any Multinode High Availability deployment.

**IN THIS SECTION**

- [Overview | 613](#)
- [How Multinode High Availability Works | 627](#)
- [Multinode High Availability Monitoring | 645](#)

### Overview

Business continuity is an important requirement of the modern network. Downtime of even a few seconds might cause disruption and inconvenience apart from affecting the OpEx and CapEx. Modern networks also have data centers spread across multiple geographical areas. In such scenarios, achieving high availability can be very challenging.

Juniper Networks® SRX Series Firewalls support a new solution, Multinode High Availability, to address high availability requirements for modern data centers. In this solution, both the control plane and the data plane of the participating devices (nodes) are active at the same time. Thus, the solution provides interchassis resiliency.

The participating devices could be co-located or physically separated across geographical areas or other locations such as different rooms or buildings. Having nodes with high availability across geographical locations ensures resilient service. If a disaster affects one physical location, Multinode High Availability can fail over to a node in another physical location, thereby ensuring continuity.

### Benefits of Multinode High Availability

- **Reduced CapEx and OpEx**—Eliminates the need for a switched network surrounding the firewall complex and the need for a direct Layer 2 (L2) connectivity between nodes
- **Network flexibility**—Provides greater network flexibility by supporting high availability across Layer 3 (L3) and switched network segments.
- **Stateful resilient solution**—Supports active control plane and data plane at the same time on both nodes.
- **Business continuity and disaster recovery**—Maximizes availability, increasing redundancy within and across data centers and geographies.
- **Smooth upgrades**—Supports different versions of Junos OS on two nodes to ensure smooth upgrades between the Junos OS releases, also allows to run two different version of Junos.

We support two nodes in Multinode High Availability solution.

### Active/Backup Multinode High Availability

We support active/backup Multinode High Availability on:

- SRX5800, SRX5600, SRX5400 with SPC3, IOC3, IOC4, SCB3, SCB4, and RE3 (in Junos OS Release 20.4R1)
- SRX4600, SRX4200, SRX4100, and SRX1500 (in Junos OS Release 22.3R1)
- vSRX3.0 virtual firewalls (in Junos OS Release 22.3R1) for the following private and public cloud platforms:
  - KVM (kernel-based virtual machine)
  - VMWare ESXi
  - Amazon Web Services (AWS)



## Active/Active Multinode High Availability

Starting in Junos OS Release 22.4R1, you can operate Multinode High Availability in active-active mode with support of multiple services redundancy groups (SRGs).

Multi SRG support is available on SRX5400, SRX5600, and SRX5800 with SPC3, IOC3, SCB3, SCB4, and RE3.

## Supported Features

SRX Series devices with Multinode High Availability support the firewall and advanced security services —such as application security, unified threat management (UTM), intrusion prevention system (IPS), firewall user authentication, NAT, ALG.

For the complete list of features supported with Multinode High Availability, see [Feature Explorer](#).

Multinode High Availability does not support transparent mode high availability (HA)

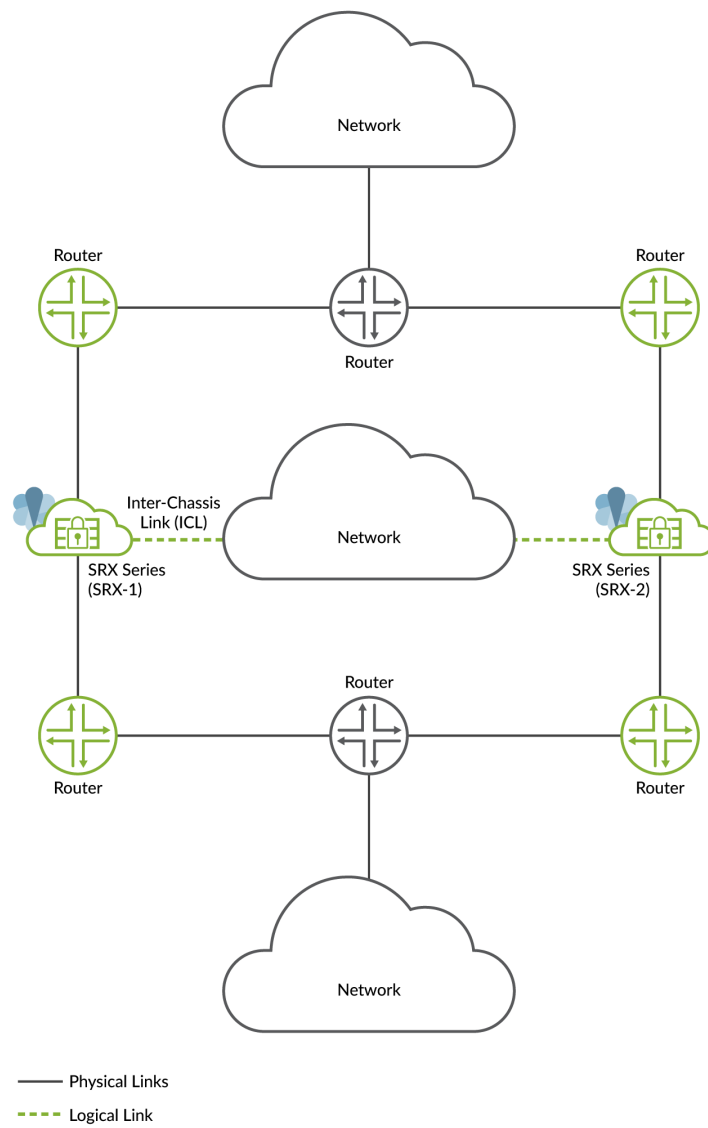
## Deployment Scenarios

Multinode High Availability supports two SRX Series devices presenting themselves as independent nodes to the rest of the network. The nodes are connected to adjacent infrastructure belonging to the same or different networks, all depending on the deployment mode. The nodes are connected to adjacent infrastructure belonging to different networks. These nodes can either be collocated or separated across geographies. Participating nodes back up each other to ensure a fast synchronized failover in case of system or hardware failure.

We support the following types of network deployment models for Multinode High Availability:

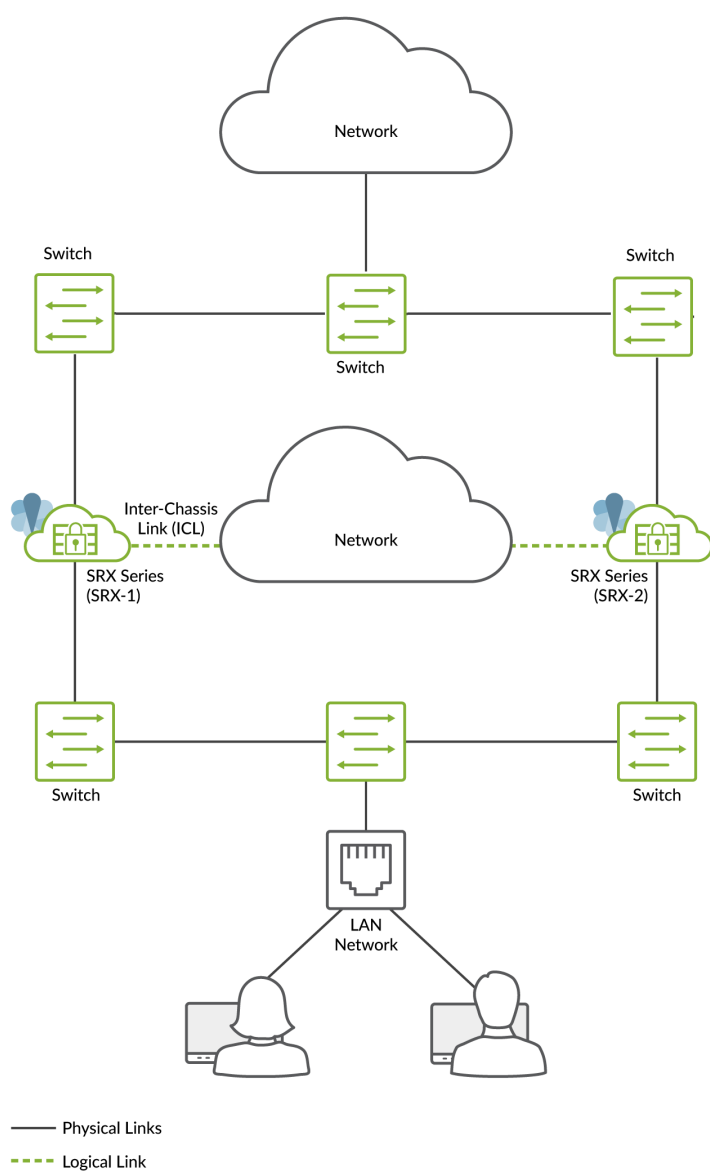
- Route mode (all interfaces connected using a Layer 3 topology)

Figure 37: Layer 3 Mode



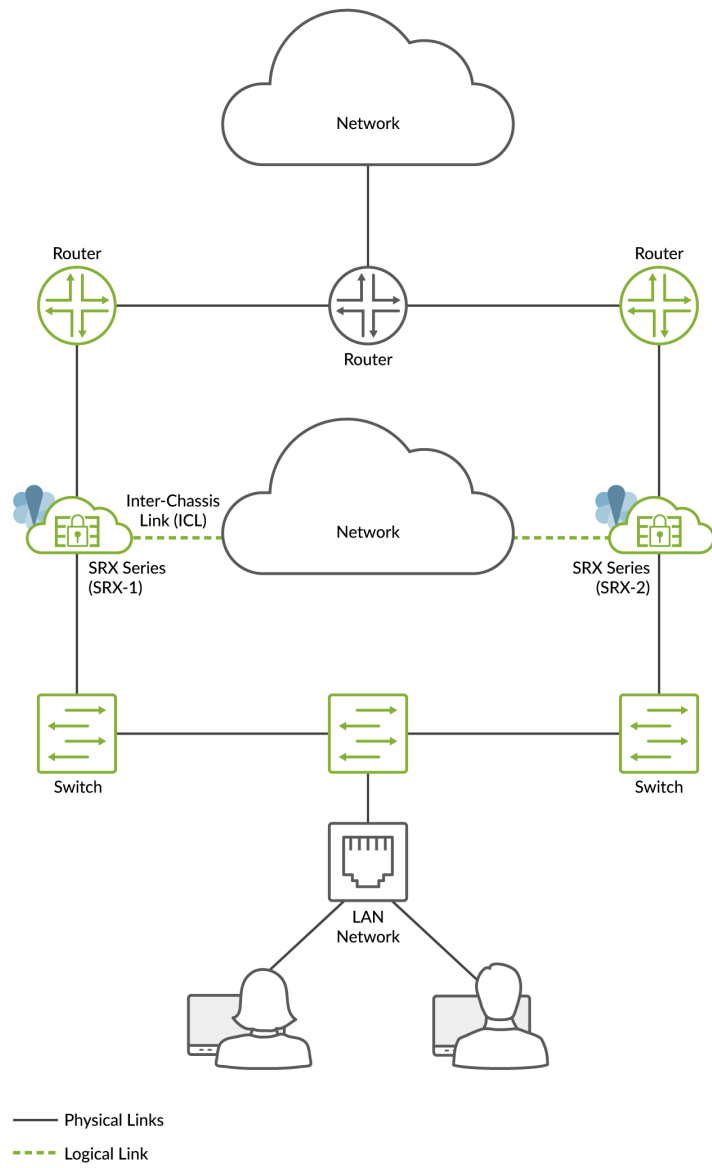
- Default gateway mode (all interfaces connected using an Layer 2 topology) used in more traditional environments. Common deployment of DMZ networks where the firewall devices act as the default gateway for the hosts and applications on the same segment.

Figure 38: Default Gateway Mode



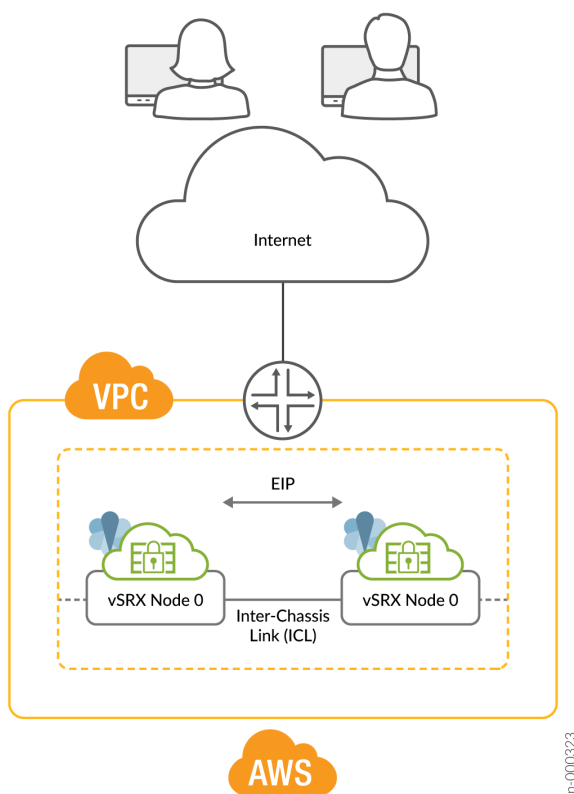
- Hybrid mode (one or more interfaces are connected using a Layer 3 topology and one or more interfaces are connected using a Layer 2 topology)

Figure 39: Hybrid Mode



- AWS deployment

Figure 40: Public Cloud Deployment



### How Is Multinode High Availability Different from Chassis Cluster?

A chassis cluster operates in Layer 2 network environment and requires two links between the nodes (control link and fabric link). These links connect both nodes over dedicated VLANs using back-to-back cabling or over dark fiber. Control links and fabric links use dedicated physical ports on the SRX Series device.

Multinode High Availability uses an encrypted logical interchassis link (ICL). The ICL connects the nodes over a routed path instead of a dedicated Layer 2 network. This routed path can use one or more revenue ports for best resiliency, it's even possible to dedicate its own routing instance to these ports and paths to ensure total isolation which maximizes the resiliency of the solution.

[Figure 41 on page 620](#) and [Figure 42 on page 621](#) show two architectures.

Figure 41: Chassis Cluster Topology in a Layer 2 Network

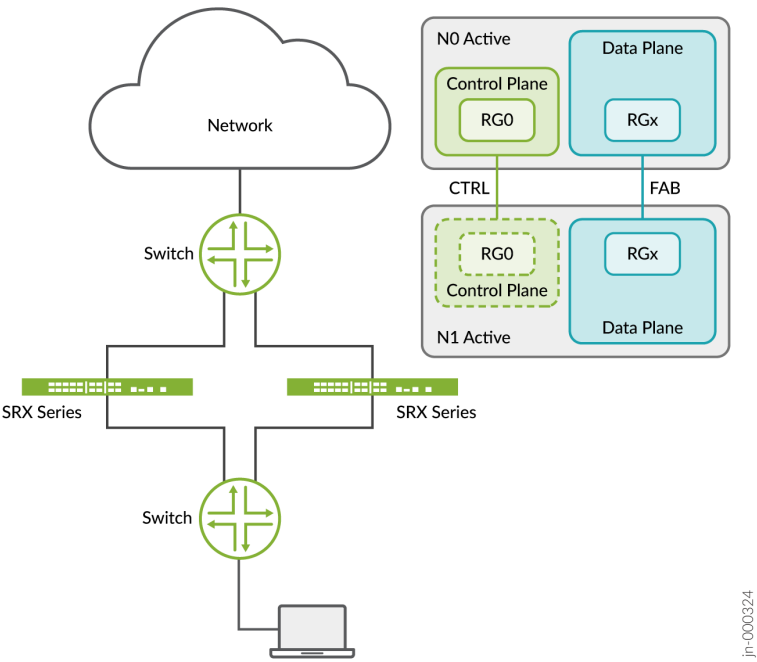
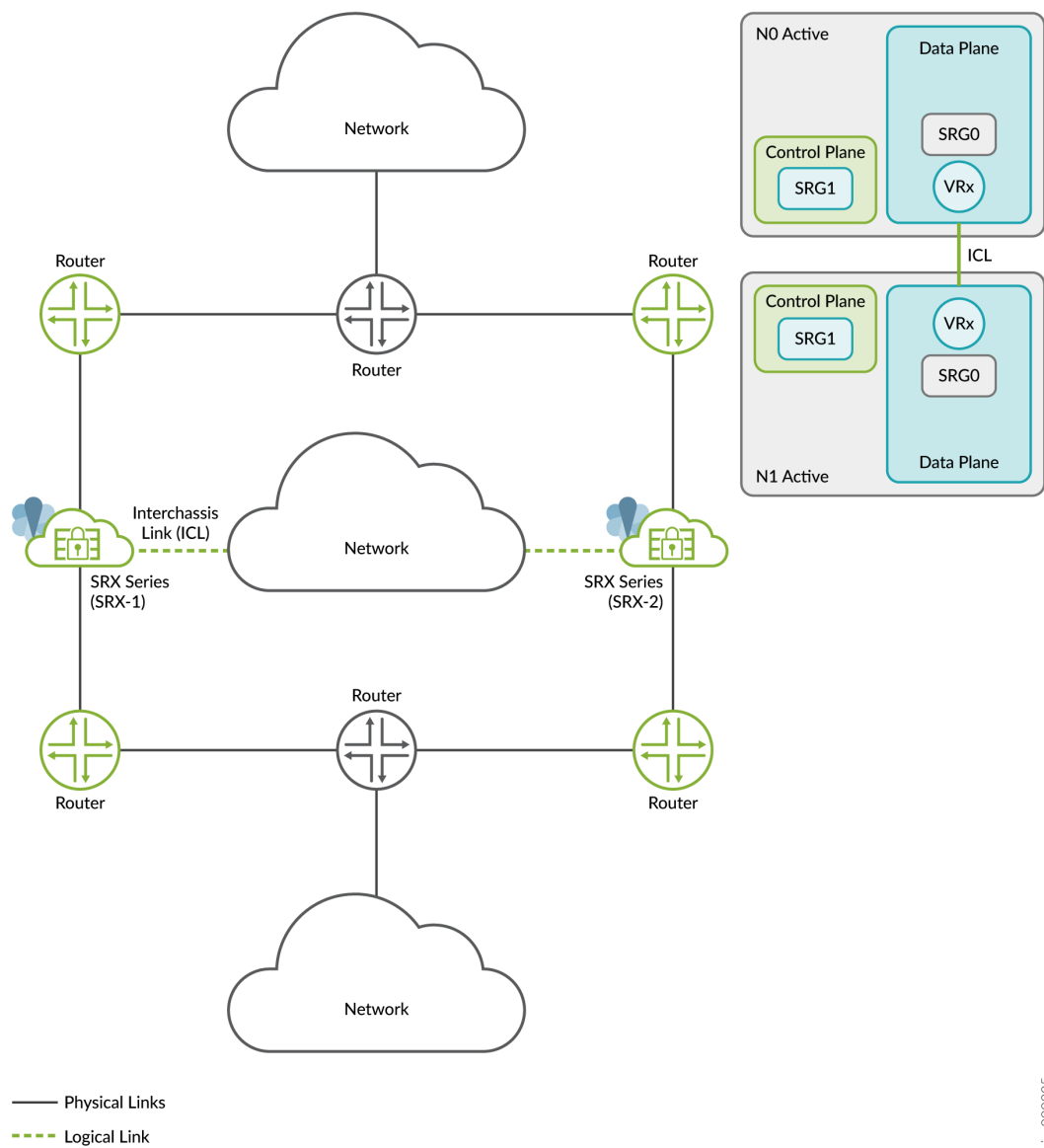


Figure 42: Multinode High Availability in a Layer 3 Network



jn-000325

Table 39 on page 622 lists the differences between the two architectures

Table 39: Comparing Chassis Cluster and Multinode High Availability

Parameters	Chassis Cluster	Multinode High Availability
Network topology	Nodes connect to a broadcast domain	<p>Nodes connect to a router, a broadcast domain, or a combination of both.</p> <ul style="list-style-type: none"> <li>• Nodes connect to a router</li> <li>• Broadcast domain</li> <li>• Combination of both above</li> </ul>
Network environment	Layer 2	<ul style="list-style-type: none"> <li>• Layer 3 (Route mode)</li> <li>• Layer 2 (default gateway mode)</li> <li>• Combination of Layer 3 and Layer 2 (hybrid mode)</li> <li>• Public cloud (AWS) deployments</li> </ul>
Traffic switchover approach	SRX Series device sends GARP to the switch	<p>Switchover using IP path selection by a peer Layer 3 router or Layer 2 GARP from an SRX Series device to a peer Layer 2 switch</p> <ul style="list-style-type: none"> <li>• Route mode: Switchover using IP path selection (route updates)</li> <li>• Hybrid mode: Switchover using IP path selection (route updates) in route and hybrid mode</li> <li>• Default gateway mode: SRX Series device sends GARP to the switch</li> </ul>
Public cloud	Not supported	Supported



Table 39: Comparing Chassis Cluster and Multinode High Availability (*Continued*)

Parameters	Chassis Cluster	Multinode High Availability
Dynamic routing function	Routing process active on the SRX Series where the control plane (RG0) is active	Routing process active on each SRX Series device participating in Multinode High Availability
Connection between SRX Series devices	<ul style="list-style-type: none"> <li>Control link (Layer 2 path)</li> <li>Fabric link (Layer 2 path)</li> </ul>	Interchassis link (Layer 3 path)
Connectivity / Geo-redundance	Requires a dedicated Layer 2 stretch between the SRX Series nodes for the control link and fabric link.	Uses any routed path between the nodes for the Interchassis link.
IP monitoring to detect network failure	<ul style="list-style-type: none"> <li>Interfaces</li> <li>IP monitoring using IPv4 addresses</li> </ul>	<ul style="list-style-type: none"> <li>Interfaces</li> <li>IP monitoring using IPv4 and IPv6 addresses</li> <li>Bidirectional Forwarding Detection (BFD) using IPv4 addresses</li> </ul>

## Multinode High Availability Glossary

Let's begin by getting familiar with Multinode High Availability terms used in this documentation.

Table 40: Multinode High Availability Glossary

Term	Description
active/active state (SRG0)	All security services/flows are inspected at each node and backed up on the other node. Security flows must be symmetric.

Table 40: Multinode High Availability Glossary (*Continued*)

Term	Description
active/backup state (SRG1+)	SRG1+ remains active on one node at any given time and remains in backed up state on the other node. SRG1+ in the backup state is ready to take over traffic from the active SRG1 in case on a failure.
device priority	Priority value determines whether a node can act as the active node in a Multinode High Availability setup. The node with a lower numerical value has a higher priority and, therefore, acts as the active node while the other node acts as the backup node.
device preemption	Preemptive behavior allows the device with the higher priority (lower numerical value) to resume as active node after it recovers from a failure. If you need to use a specific device in Multinode High Availability as active node, then you must enable the preemptive behavior on both the devices and assign a device priority value for each device.
failover	A failover happens when one node detects a failure (hardware/software and so on) and traffic transitions to the other node in a stateful manner. As result, the backup node in a high availability system takes over the task of the active node when the active node fails.
floating IP address or activeness probing IP address	An IP address that moves from an active node to the backup node during failover in a Multinode High Availability setup. This mechanism enables clients to communicate with the nodes using a single IP address.
high availability/resiliency	Ability of a system to eliminate single points of failure to ensure continuous operations over an extended period of time.

Table 40: Multinode High Availability Glossary (*Continued*)

Term	Description
interchassis link	<p>IP-based link (logical link) that connects nodes over a routed network in a Multinode High Availability deployment. The ICL link is normally bound to the loopback interfaces for most flexible deployments. Connectivity can be any routed or switched path as long as the connectivity is reachable between the two IP addresses.</p> <p>The security device uses the ICL to synchronize and maintain state information and to handle device failover scenarios.</p>
Interchassis link encryption	Link encryption provides data privacy for messages traversing over the network. As the ICL link transmits private data, it is important to encrypt the link. You must encrypt the ICL using IPsec VPN.
monitoring (BFD)	Monitoring of one or more links using Bidirectional Forwarding Detection (BFD). BFD monitoring triggers a routing path change or a system failover, depending on system configuration.
monitoring (IP)	Monitoring of a reliable IP address and system state in case of loss of communication with the peer node.
monitoring (path)	Method that uses ICMP to verify the reachability of the IP address. The default interval for ICMP ping probes is 1 second.
monitoring (system)	Monitoring of key hardware and software resources and infrastructures by triggering failover when a failure is detected on a node.
probing	Mechanism used to exchange messages between active and backup nodes in the high availability setup. The messages determine the status and health of the application on each individual node.

Table 40: Multinode High Availability Glossary (*Continued*)

Term	Description
real-time object (RTO)	Special payload packet that contains the necessary information to synchronize the data from one node to the other node.
split-brain detection (also known as control plane detection or activeness conflict detection)	Event where the ICL between two Multinode High Availability nodes is down, and both nodes initiate an activeness determination probe (split-brain probe). Based on the response to the probe, subsequent failover to a new role is triggered
services redundancy group (SRG)	Failover unit that includes and manages a collection of objects on the participating nodes. The SRG on one node switches over to the other node when a failover is detected.
SRG0	Manages all control plane stateless services such as firewall, NAT, and ALG. SRG0 is active on all participating nodes and handles symmetric security flows.
SRG1+	Manages control plane stateful service (IPsec VPN or virtual IPs in hybrid or default gateway mode.).
synchronization	Process where controls and data plane states are synchronized across the nodes.
virtual IP (VIP) address	Virtual IP addresses in hybrid or default gateway mode are used for activeness determination and enforcement on the switching side in a Multinode High Availability setup. The virtual IP is controlled by the SRG1+.
virtual MAC (VMAC) address	(For hybrid and default gateway deployments). Virtual MAC address dynamically assigned to the interface on active node that faces the switching side.

Now we are that familiar with Multinode High Availability features and terminology, let's proceed to understand how Multinode High Availability works.

## How Multinode High Availability Works

### IN THIS SECTION

- [Services Redundancy Groups | 631](#)
- [Activeness Determination and Enforcement | 634](#)
- [Resiliency and Failover | 637](#)
- [Interchassis Link \(ICL\) Encryption | 638](#)
- [Split-Brain Detection and Prevention | 641](#)

**NOTE:** We support a two-node configuration for the Multinode High Availability solution.

In a Multinode High Availability setup, you connect two SRX Series devices to adjacent upstream and downstream routers (for Layer 3 deployments), routers and switches (hybrid deployment), or switches (default gateway deployment) using the revenue interfaces.

The nodes communicate with each other using an interchassis link (ICL). The ICL link uses Layer 3 connectivity to communicate with each other. This communication can take place over a routed network (Layer 3), or a directly connected Layer 2 path. It is recommended to bind the ICL to the loopback interface and have more than one physical link (LAG/LACP) to ensure path diversity for the highest resiliency.

Multinode High Availability operates in active/active mode for data plane and active/backup mode for control plane services. The active SRX Series device hosts the floating IP address and steers traffic towards it using the floating IP address.

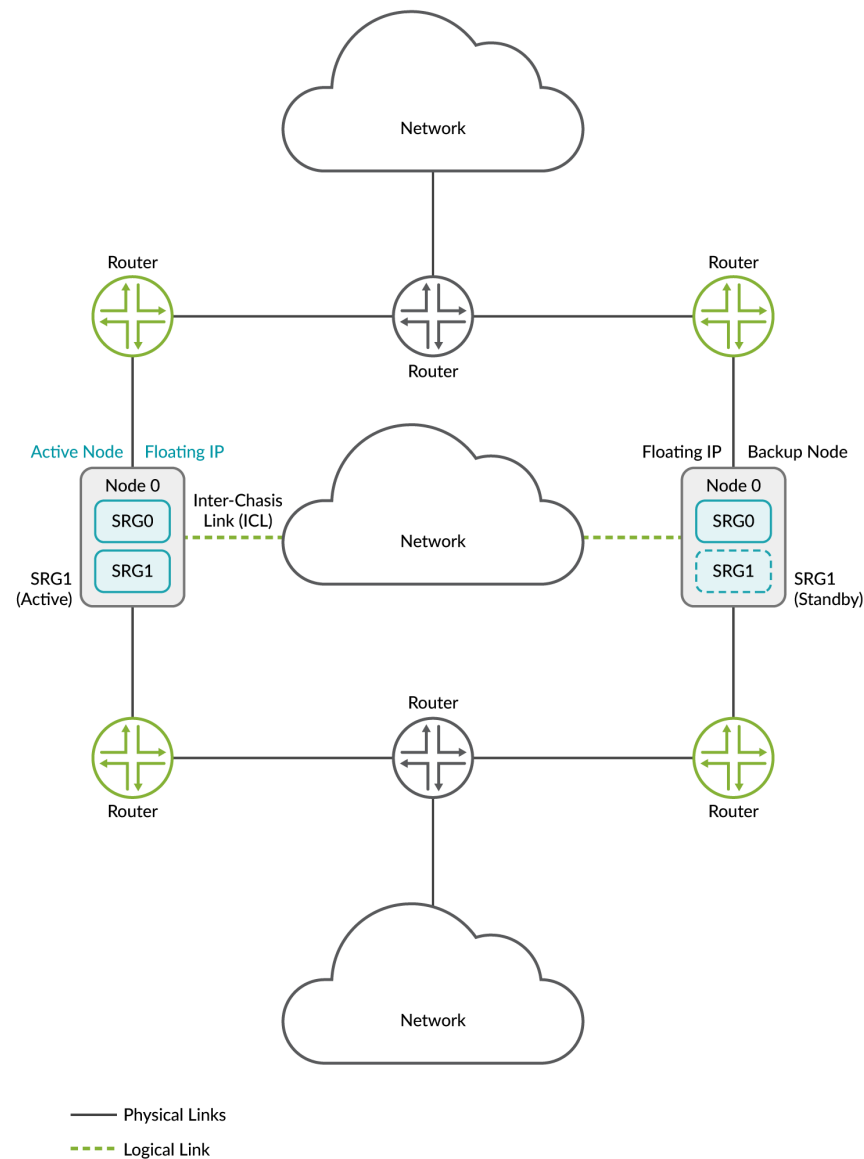
Multinode High Availability operates in:

- Active/active mode (SRG0) for the security services
- Active/backup mode (SRG1 and above) for security and system services

Floating IP addresses controlled by SRG1 or above moves between the nodes. Active SRG1+ hosts and controls the floating IP address. In failover scenarios, this IP address 'floats' to another active SRG1 based on configuration, system health, or path monitoring decisions. The newly active SRG1+ can take on the function of a now-standby SRG1 and starts responding to incoming requests.

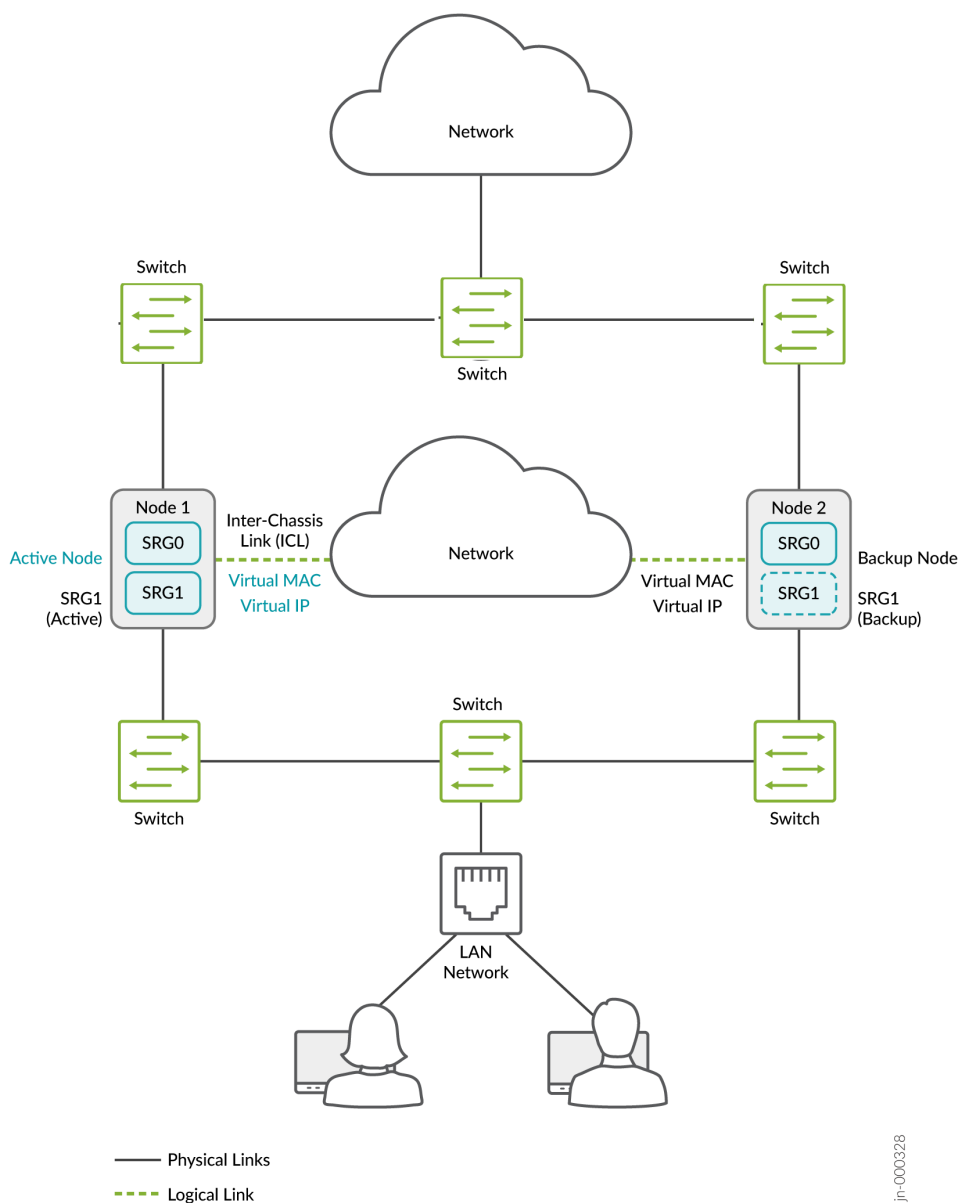
[Figure 43 on page 628](#), [Figure 44 on page 629](#), and [Figure 45 on page 630](#) show deployments in Layer 3, hybrid, and default gateway modes.

Figure 43: Layer 3 Deployment



In this topology, two SRX Series devices are part of a Multinode High Availability setup. The setup has Layer 3 connectivity between SRX Series devices and neighboring routers. The devices are running on separate physical Layer 3 networks and are operating as two independent nodes. The nodes shown in the illustration are co-located in the topology. The nodes can also be geographically separated.

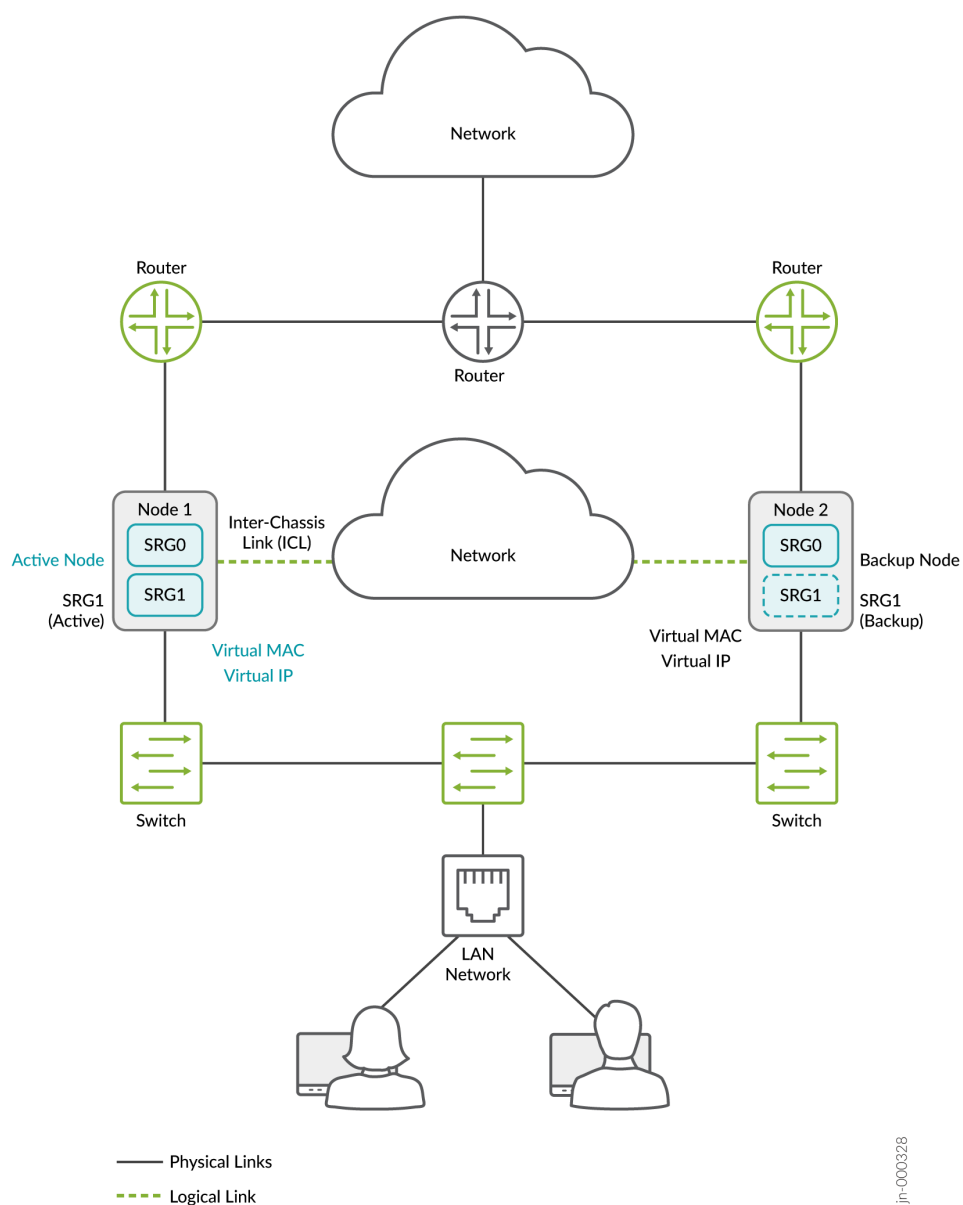
Figure 44: Default Gateway Deployment



In a typical default gateway deployment, hosts and servers in a LAN are configured with a default gateway of the security device. So the security device must host a virtual IP (VIP) address that moves between nodes based on the activeness. The configuration on hosts remains static, and security device failover is seamless from the hosts' perspective.

You must create static routes or dynamic routing on SRX Series devices to reach other networks not directly connected.

### Figure 45: Hybrid Deployment



In hybrid mode, an SRX Series device uses a VIP address on the Layer 2 side to draw traffic toward it. You can optionally configure the static ARP for the VIP using the VMAC address to ensure no change in the IP address during the failover

Let's now understand the components and functionality of Multinode High Availability in detail.



## Services Redundancy Groups

A services redundancy group (SRG) is a failover unit in a Multinode High Availability setup. There are two types of SRGs:

- SRG0—Manages security service from Layer 4-Layer 7 except IPsec VPN services. The SRG0 operates in active mode on both nodes at any point in time. On SRG0, each security session must traverse the node in a symmetric flow, Backup of these flows are fully state-synchronized to the other node,
- SRG1+—Manages IPsec services and virtual IPs for hybrid and default gateway mode and are backed up to the other node. The SRG1 operates in active mode on one node and in backup node on another node.

Figure 46 on page 631 shows SRG0 and SRG1 in a Multinode High Availability setup.

**Figure 46: Single SRG Support in Multinode High Availability (Active-Backup Mode)**

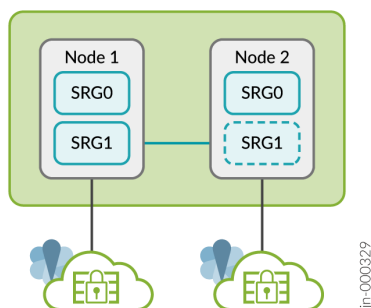
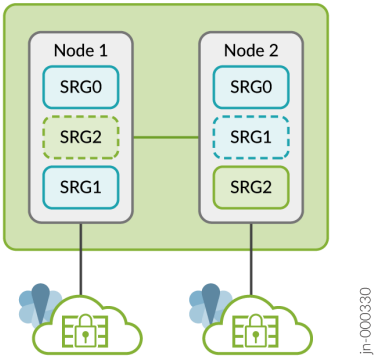


Figure 47 on page 632 shows SRG0 and SRG1+ in a Multinode High Availability setup.

**Figure 47: Multi SRG Support in Multinode High Availability (Active-Active Mode)**



Starting in Junos OS Release 22.4R1, you can configure Multinode High Availability to operate in active-active mode with support of multi SRG1s (SRG1+). In this mode, some SRGs remain active on one node and some SRGs remain active on another node. A particular SRG always operates in active-backup mode; it operates in active mode on one node and backup mode on another node. In this case, both the nodes can have the active SRG1 forwarding stateful services. Each node has a different set of floating IP addresses assigned to SRG1+.

**NOTE:** Starting in Junos OS Release 22.4R1, you can configure upto 20 SRGs in a Multinode Highavailability setup.

Table 41 on page 632 explains the behavior of SRGs in a Multinode High Availability setup.

**Table 41: Services Redundancy Group Details in Multinode High Availability**

Related Services Redundancy Group (SRG)	Managed Services	Operates in	Synchronization Type	When Active Node Fails	Configuration Options
SRG0	Manages security service L4-L7 except IPsec VPN.	Active/active mode	Stateful synchronization of security services	Traffic processed on the failed node will transition to the healthy node in a stateful manner.	<ul style="list-style-type: none"> <li>Shutdown on failure option</li> <li>Install on failure route options</li> </ul>

Table 41: Services Redundancy Group Details in Multinode High Availability *(Continued)*

Related Services Redundancy Group (SRG)	Managed Services	Operates in	Synchronization Type	When Active Node Fails	Configuration Options
SRG1+	Manages IPsec and virtual-IP addresses with associated security services	Active/backup mode	Stateful synchronization of security services	Traffic processed on the failed node will transition to the healthy node in a stateful manner.	<ul style="list-style-type: none"> <li>• Active/backup signal route</li> <li>• Deployment type</li> <li>• Activeness priority and preemption</li> <li>• Virtual IP address (for default gateway deployments )</li> <li>• Activeness probing</li> <li>• Process packet on backup option</li> <li>• BFD monitoring</li> <li>• IP monitoring</li> <li>• Interface monitoring</li> </ul>

**NOTE:** When you configure monitoring (BFD or IP or Interface) options on SRG1+, we recommend not to configure the shutdown-on-failure option on SRG0.

## Activeness Determination and Enforcement

In a Multinode High Availability setup, activeness is determined at the service level, not at the node level. The active/backup state is at the SRG level and the traffic is steered toward the active SRG. SRG0 remains active on both the nodes, whereas SRG1 can remain in active or in backup state in each node

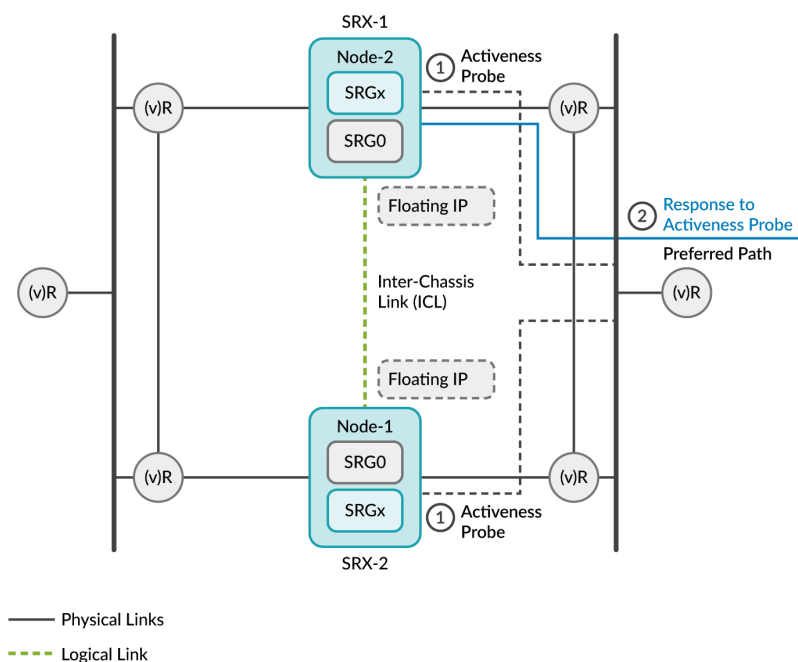
If you prefer a certain node to take over as the active node on boot, you can do one of the followings:

- Configure the upstream routers to include preferences for the path where the node is located.
- Configure activeness priority.
- Allow the node with higher node ID (in case the above two options not configured) to take the active role.

In a Multinode High Availability setup, both the SRX Series devices initially advertise the route for the floating IP address to the upstream routers. There isn't a specific preference between the two paths advertised by SRX Series devices. However, the router can have its own preferences on one of the paths depending on the configured metrics.

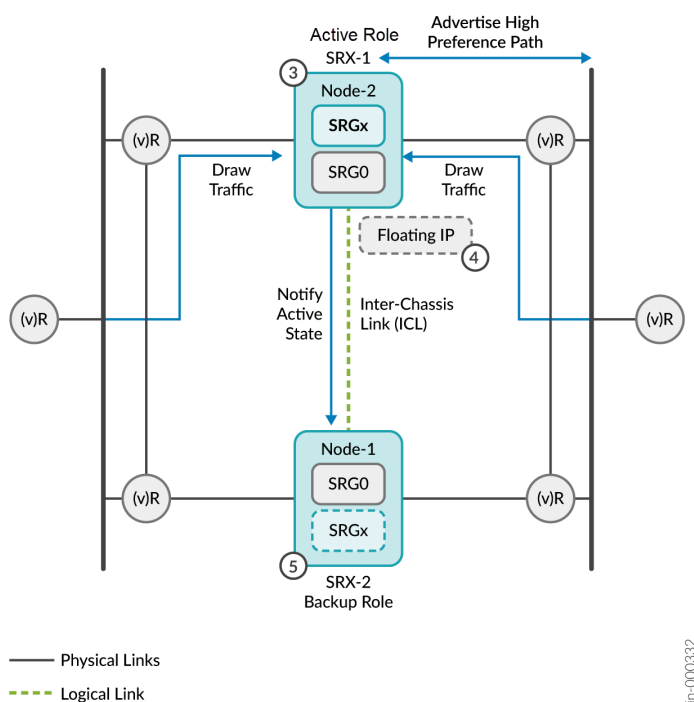
Figure 48 on page 634 represents the sequence of events for activeness determination and activeness enforcement.

**Figure 48: Activeness Determination and Enforcement**



1. On boot, devices enter the hold state and start probing continuously. The devices use the floating IP address (activeness-probing source IP address) as the source IP address and IP addresses of the upstream routers as the destination IP address for the activeness determination probe.
2. The router hosting the probe destination IP address replies to the SRX Series device that is available on its preferred routing path. In the following example, SRX-1 gets the response from the upstream router.

**Figure 49: Activeness Determination and Enforcement**



3. SRX-1 promotes itself to the active role since it got the probe reply. SRX-1 communicates its role change to the other device and takes up the active role.
4. After the activeness is determined, the active node (SRX-1):
  - Hosts the floating IP address assigned to it.
  - Advertises the high-preference path to adjacent BGP neighbors.
  - Continues to advertise the active (higher) preference path for all remote and local routes to draw the traffic.
  - Notifies the active node status to the other node through the ICL.

5. The other device (SRX-2) stops probing and takes over the backup role. The backup node advertises the default (lower) priority, ensuring that the upstream routers do not forward any packets to the backup node.

The Multinode High Availability module adds active and backup signal routes for the SRG to the routing table when the node moves to the active role. In case of node failures, the ICL goes down and the current active node releases its active role and removes the active signal route. Now the backup node detects the condition through its probes and transitions to the active role. The route preference is swapped to drive all the traffic towards the new active node.

The switch in the route preference advertisement is part of routing policies configured on SRX Series devices. You must configure the routing policy to include the active signal route with the `if-route-exists` condition.

### For Default Gateway Deployments

If both the nodes are booting up at the same time, then the Multinode High Availability system uses the configured priority value of an SRG to determine activeness. Activeness enforcement takes place when the node with an active SRG1+ owns the virtual IP (VIP) address and the virtual MAC (VMAC) address. This action triggers Gratuitous ARP (GARP) toward the switches on both sides and results in updating the MAC tables on the switches.

### For Hybrid Deployments

Activeness enforcement takes place on the Layer 3 side, when the configured signal route enforces activeness with the corresponding route advertisements. On the Layer 2 side, the SRX Series device triggers a Gratuitous ARP (GARP) to the switch layer and owns the VIP and VMAC addresses.

When the failover happens and the old backup node transitions to the active role, the route preference is swapped to drive all the traffic to the new active node.

### Activeness Priority and Preemption

Configure the preemption priority (1-254) for SRG1+. You must configure the preemption value on both nodes. The preempt option ensures that the traffic always falls back to the specified node, when the node recovers from a failover.

You can configure activeness priority and preemption for an SRG1+ as in the following sample:

```
[edit]
user@host# show chassis high-availability
services-redundancy-group 1 {
    preemption;
```

```
activeness-priority 200;
}
```

See ["Configuring Multinode High Availability In a Layer 3 Network" on page 672](#) for the complete configuration example.

As long as the nodes can communicate with each other through the ICL, the activeness priority is honored.

## Configuring Activeness Probe Settings

Starting in Junos OS 22.4R1, default gateway (switching) and in hybrid deployments of Multinode High Availability, you can optionally configure activeness probe parameters using the following statements:

```
[edit]
user@host# set chassis high-availability services-redundancy-group 1 activeness-probe multiplier
<>
user@host# set chassis high-availability services-redundancy-group 1 activeness-probe minimal-
interval <>
```

The probe interval sets the time period between the probes sent to the destination IP addresses. You can set the probe interval as 1000 milliseconds.

The multiplier value determines the time period, after which the backup node transitions to active state, if the backup node fails to receive response to the activeness-probes from the peer node.

The default is 2, and the minimum value is 2, and the maximum is 15.

Example: If you configure the multiplier value to two, the backup node will transition to the active state if it does not receive a response to activeness probing request from the peer node after two seconds.

You can configure `multiplier` and `minimal-interval` in switching and hybrid deployments.

In hybrid mode deployments, if you've configured the probe destination IP details for activeness determination (by using the `activeness-probe dest-ip` statement), then do not configure the `multiplier` and `minimal-interval` values. Configure these parameters when you are using VIP-based activeness probing.

## Resiliency and Failover

The Multinode High Availability solution supports redundancy at the service level. Service-level redundancy minimizes the effort needed to synchronize the control plane across the nodes.

After the Multinode High Availability setup determines activeness, it negotiates subsequent high availability (HA) state through the ICL. The backup node sends ICMP probes using the floating IP

address. If the ICL is up, the node gets the response to its probe and remains as the backup node. If the ICL is down, and there are no probe response, the backup node transitions into the active node.

The SRG1 of the previous backup node now transitions to the active state and continues to operate seamlessly. When the transition happens, the floating IP address is assigned to the active SRG1. In this way, the IP address floats between the active and backup nodes and remains reachable to all the connected hosts. Thus, traffic continues to flow without any disruption.

Services, such as IPsec VPN, that require both control plane and data plane states are synchronized across the nodes. Whenever an active node fails for this service function, both control plane and data plane fail over to the backup node at the same time.

The nodes use the following messages to synchronize data:

- Routing Engine to Routing Engine control application messages
- Routing Engine configuration-related messages
- Data plane RTO messages

### Interchassis Link (ICL) Encryption

In Multinode High Availability, the active and backup nodes communicate with each other using an interchassis link (ICL) connected over a routed network or connected directly. The ICL is a logical IP link and it is established using IP addresses that are routable in the network.

Nodes use the ICL to synchronize control plane and data plane states between them. ICL communication could go over a shared or untrusted network and packets sent over the ICL may traverse a path that is not always trusted. Therefore, you must secure the packets traversing the ICL by encrypting the traffic using IPsec standards.

IPsec protects traffic by establishing an encryption tunnel for the ICL. When you apply HA link encryption, the HA traffic flows between the nodes only through the secure, encrypted tunnel. Without HA link encryption, communication between the nodes may not be secure.

To encrypt the HA link for the ICL:

- Install the Junos IKE package on your SRX Series device by using the following command:  
`request system software add optional://junos-ike.tgz .`
- Configure a VPN profile for the HA traffic and apply the profile for both the nodes. The IPsec tunnel negotiated between the SRX Series devices uses the IKEv2 protocol.
- Ensure you have included the statement `ha-link-encryption` in your IPsec VPN configuration.  
 Example: `user@host# set security ipsec vpn vpn-name ha-link-encryption.`

We recommend following for setting up an ICL:



- Use ports and network which is less likely to be saturated
- Not to use the dedicated HA ports (control and fabric ports, if available on your SRX Series device)
- Bind the ICL to the loopback interface (lo0) or an aggregated Ethernet interface (ae0) and have more than one physical link (LAG/LACP) that ensure path diversity for highest resiliency.
- You can use a revenue Ethernet port on the SRX Series devices to setup an ICL connection. Ensure that you separate the transit traffic in revenue interfaces from the high availability (HA) traffic.

See ["Configuring Multinode High Availability" on page 672](#) for more details.

**PKI-Based Link Encryption for ICL**

Starting in Junos OS Release 22.3R1, we support PKI-based link encryption for interchassis link (ICL) in Multinode High Availability. As a part of this support, you can now generate and store node-specific PKI objects such as local keypairs, local certificates, and certificate-signing requests on both nodes. The objects are specific to local nodes and are stored in the specific locations on both nodes.

The node local objects enable you to distinguish between PKI objects that are used for ICL encryption and PKI objects used for IPsec VPN tunnel created between two endpoints.

You can use the following commands run on local node to work with node-specific PKI objects.

Generating a private/public key pair for a local node	<a href="#">"request security pki node-local generate-key-pair" on page 1264</a>
---	--

---

Generating and enrolling a local digital certificate in a local node	<ul style="list-style-type: none"> <li>• <a href="#">"request security pki node-local generate-certificate-request" on page 1267</a></li> <li>• <a href="#">"request security pki node-local key-pair export" on page 1262</a></li> <li>• <a href="#">"request security pki node-local local-certificate verify" on page 1252</a></li> <li>• <a href="#">"request security pki node-local local-certificate re-enroll" on page 1254</a></li> <li>• <a href="#">"request security pki node-local local-certificate load" on page 1255</a></li> <li>• <a href="#">request security pki node-local local-certificate export</a></li> <li>• <a href="#">"request security pki node-local local-certificate enroll" on page 1259</a></li> </ul>
Clear node-specific certificates	<ul style="list-style-type: none"> <li>• <a href="#">"clear security pki node-local certificate-request" on page 1229</a></li> <li>• <a href="#">"clear security pki node-local local-certificate" on page 1230</a></li> <li>• <a href="#">"clear security pki node-local key-pair" on page 1232</a></li> </ul>
Display node-specific local certificates and certificate requests.	<ul style="list-style-type: none"> <li>• <a href="#">"show security pki node-local local-certificate" on page 1501</a></li> <li>• <a href="#">"show security pki node-local certificate-request" on page 1507</a></li> </ul>

On your security device in Multinode High Availability, if you've configured the automatic re-enrollment option and if the ICL goes down at the time of re-enrollment trigger, both the devices start enrolling the same certificate separately with the CA server and download the same CRL file. Once Multinode High Availability re-establishes the ICL, the setup uses only one local certificate. You must synchronize the certificates from the active node to backup node using the `user@host> request security pki sync-from-peer` command on the backup node.

If you don't synchronize the certificates, the certificate mismatch issue between peer nodes persists till the next re-enrollment.

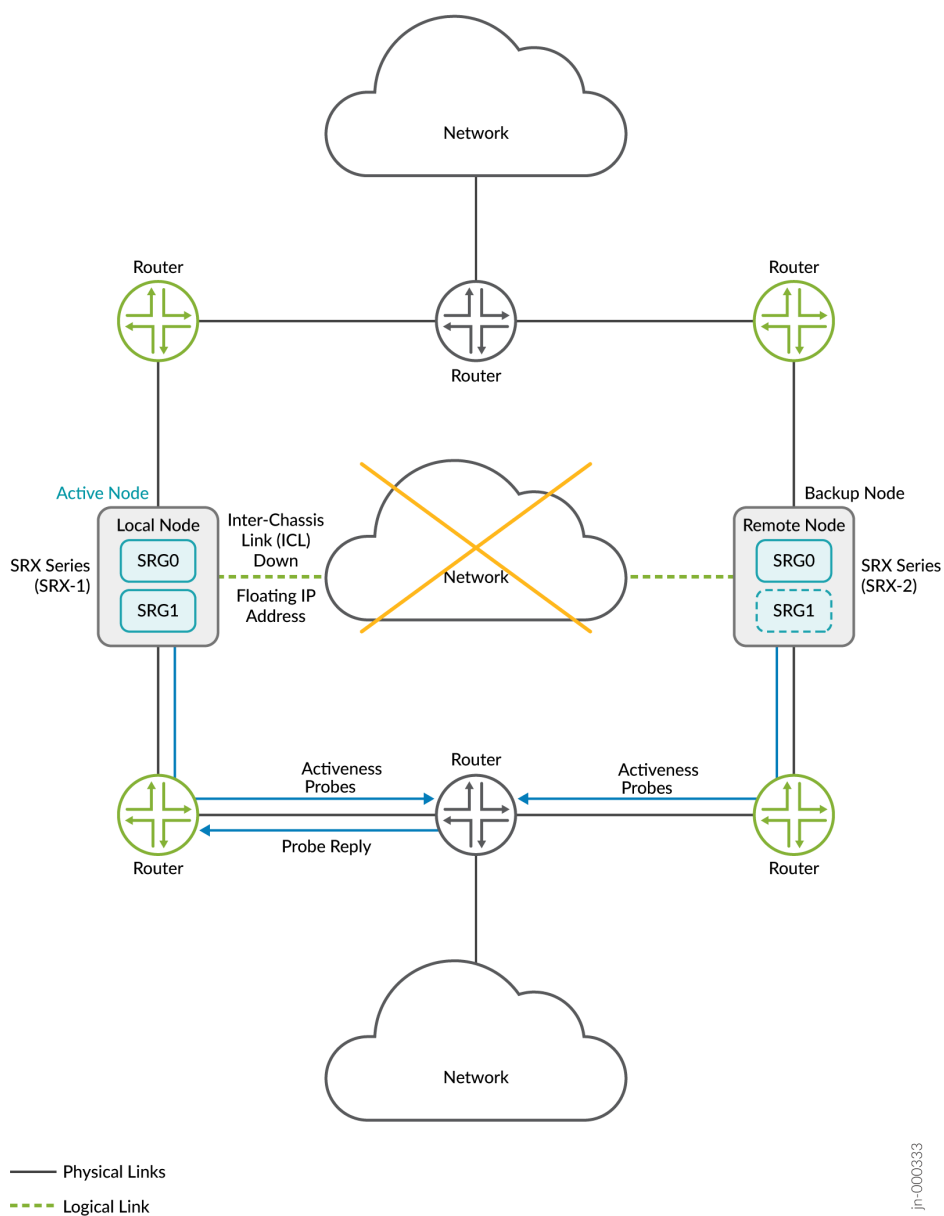
Optionally you can enable TPM (Trusted Platform module) on both nodes before generating any keypairs on the nodes. See [Using Trusted Platform Module to Bind Secrets on SRX Series devices](#).

### **Split-Brain Detection and Prevention**

Split-brain detection or activeness conflict happens when the ICL between two Multinode High Availability nodes is down and both nodes cannot reach each other to gather the status of peer node anymore.

Consider a scenario where two SRX Series devices are part of Multinode High Availability setup. Lets consider SRX-1 as a local node and SRX-2 a remote node. The local node is currently in active role and the upstream router has higher priority path for the local node.

#### **Case 1: Active Node is Up**

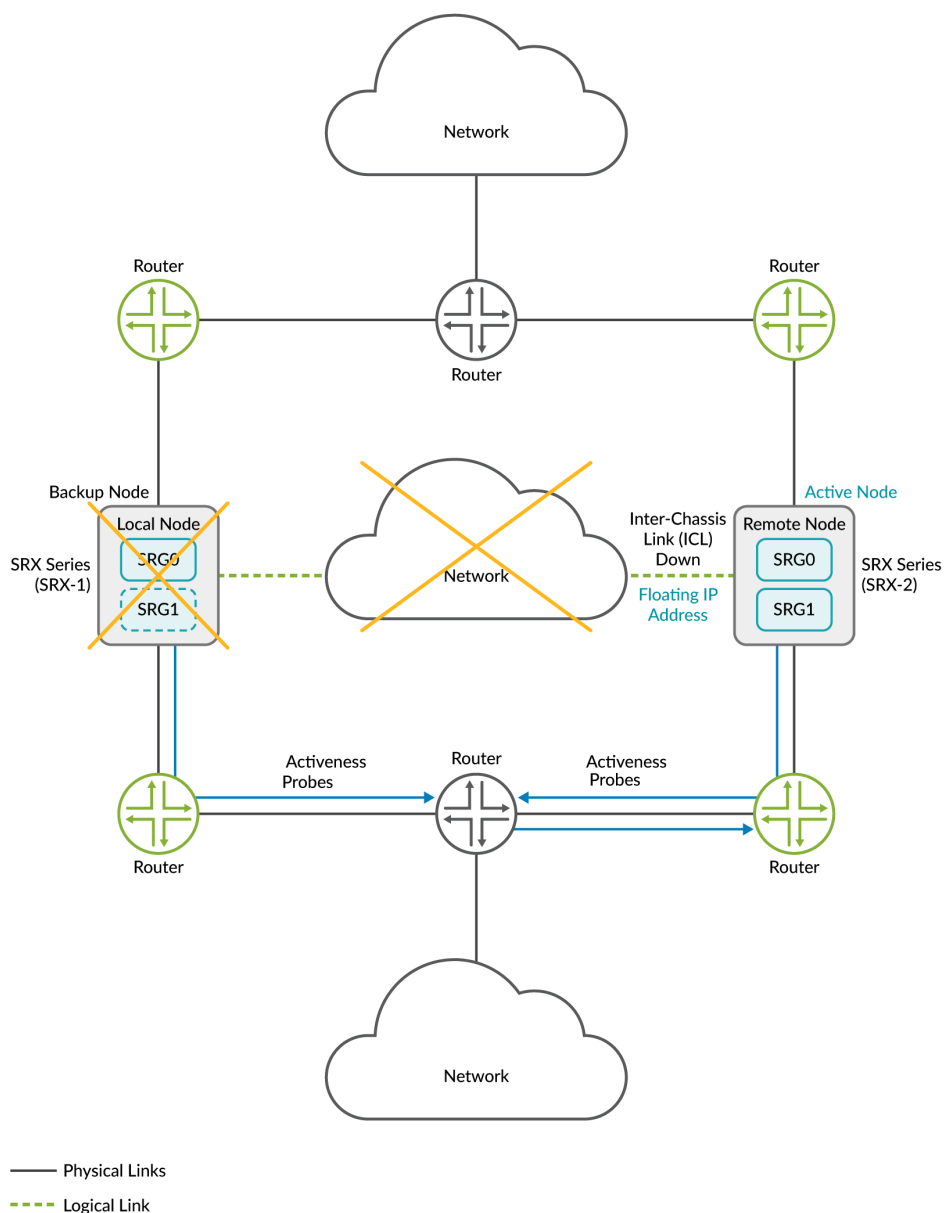


jin-000333

- The upstream router, that hosts the probe destination IP address, receives the ICMP probes from both nodes.
- Upstream router replies to only to the active node; because it's configuration has the higher preference path for the active node
- The active node retains the active role.

#### If Active Node is Down

When the ICL between the nodes goes down, both nodes initiate an activeness determination probe (ICMP probe). The nodes use the floating IP address (activeness determination IP address) as source IP address and IP addresses of the upstream routers as destination IP address for the probes.



- The remote node restarts the activeness determination probes.
- The router hosting the probe destination IP address has lost its higher preference path (of former active node) and replies to the remote node.
- The probe result is a success for the remote node and the remote node transitions to the active state.

As demonstrated in the above cases, activeness determination probes and the configuration of higher path preference in the upstream router ensures one node always stays in the active role and prevents split-brain taking place.

You must also ensure that ICMP packets can be reached and allowed all the way to the router hosting the probe destination IP address.

See ["Configuring Multinode High Availability In a Layer 3" on page 672](#) for details.

## Default Gateway Deployments

In a default gateway deployments, when the ICL connection is down, SRX Series devices are not able to communicate with each other. In such case, there is a possibility of both devices could claim active role. To prevent this, Multinode High Availability probes using ICMP-based ping to the virtual IP from the backup node. Following two scenarios are possible:

- **ICL Down and Active Node Up**

The active node owns the virtual IP address and hence when active node pings to the virtual IP using ICMP probes, the probe succeeds. The backup node remains in backup state.

- **ICL and Active Node Down**

The backup node pings the virtual IP using ICMP probes. Because the active node is down, it does not host VIP, and does not respond to the IP-based probes. So after a specified number of failures, the backup node transitions to active state.

See ["Configuring Multinode High Availability In a Default Gateway Deployment" on page 717](#) for details.

## Hybrid Deployments

You can use Layer 3 side or Layer 2 side for the split brain prevention, You can use only one method at the same time. If you use the Layer 2 side, then Multinode High Availability uses the VIP probing method described in "default gateway mode deployment". If you use Layer 3 side, then the activeness determination probe (ICMP probe) method described in "Route Mode" is used.

See ["Configuring Multinode High Availability In a Default Gateway Deployment" on page 717](#) or ["Configuring Multinode High Availability In a Layer 3" on page 672](#).

In spite of the split brain prevention mechanism, theoretically the nodes can still get in to a active-active state. This happens when the ICL is down and there are other network issues on the probe router at the same time. Because of this, the probe router replies to probe requests from both the nodes. In this case, once the situation improves and the ICL is up, one of the nodes takes up the active role based on your

activeness-priority configuration. In case the activeness-priority configuration is not available, the node with lower local ID takes up the backup role.

Multinode High Availability Monitoring

IN THIS SECTION

Multinode High Availability Failure Scenarios | 646

Node Failure | 647

Network/Connectivity Failure | 649

A high availability failure detection monitors both system, software, and hardware for internal failures. The system can also monitor network connectivity problems or link connectivity using interface monitoring, BFD path monitoring and IP monitoring to detect reachability of targets further away.

Table 42 on page 645 provides details on different monitoring types used in Multinode High Availability.

Table 42: Multinode High Availability Monitoring Types

Montitoring Type	What is Does	Detection Type	Scope
BFD Monitoring	Monitors reachability to the next hop by examining the link layer along with the actual link,	<ul style="list-style-type: none"><li>• Path failures</li><li>• Link failures</li></ul>	<ul style="list-style-type: none"><li>• Detects failure within its routing connectivity</li><li>• Not intended to detect failures beyond direct connections/ next-hops.</li></ul>

Table 42: Multinode High Availability Monitoring Types *(Continued)*

Monitoring Type	What it Does	Detection Type	Scope
IP monitoring	Monitors the connectivity to hosts or services located beyond directly connected interfaces or next-hops.	<ul style="list-style-type: none"> <li>• Path failures</li> <li>• Link failures</li> </ul>	<ul style="list-style-type: none"> <li>• Detects failure occurring at more distant hosts or services.</li> <li>• Not intended for detecting failures occurring in directly connected links or next-hop failures.</li> </ul>
Interface monitoring	Examines whether the link layer is operational or not,	Link failures	<ul style="list-style-type: none"> <li>• Detects failure in directly connected links or next-hops, and connectivity to hosts or services located farther away.</li> <li>• Not intended for monitoring path</li> </ul>

In Multinode High Availability, when monitoring detects a connectivity failure to a host or service, it marks the affected path as down/unavailable, and marks the corresponding Service Route Groups (SRGs) at the impacted node as Ineligible. The affected SRGs will transition in a stateful manner to the other node without causing any disruption to traffic.

To prevent any traffic from being lost, Multinode High Availability takes following precautions:

- Layer 3 mode—Routes will be redrawn so that the traffic is redirected correctly
- Default gateway or hybrid mode—The new active node for the SRG sends a GARP (Gratuitous ARP) to the connected switch to ensure the re-routing of traffic

### Multinode High Availability Failure Scenarios

The following sections describe possible failure scenarios: how a failure is detected, what recovery action to take, and if applicable, the impact on the system caused by the failure.

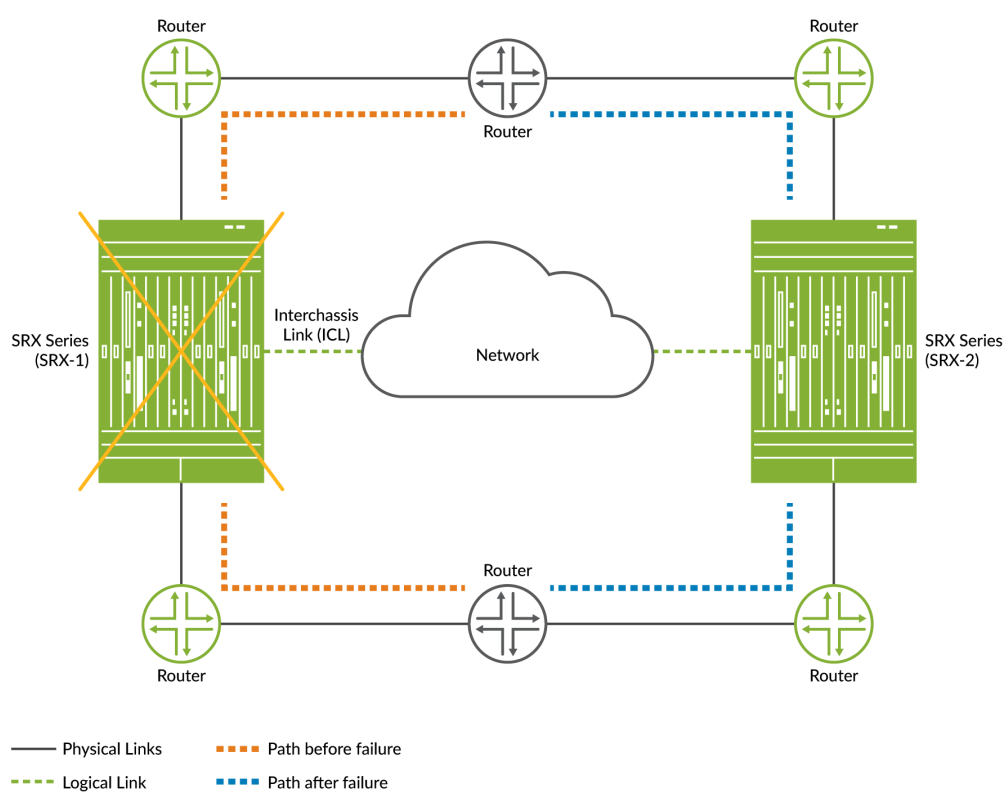


## Node Failure

### Hardware Failure

- **Cause**—A failed hardware component or an environmental issue such as a power failure.
- **Detection**— In Multinode High Availability
  - Affected device/node not accessible
  - SRG1 status changes to INELIGIBLE on the node with hardware failure.
- **Impact** —Traffic will failover to the other node (if healthy) as shown in [Figure 50 on page 647](#).

Figure 50: Hardware Failure in Multinode High Availability



jn-000398

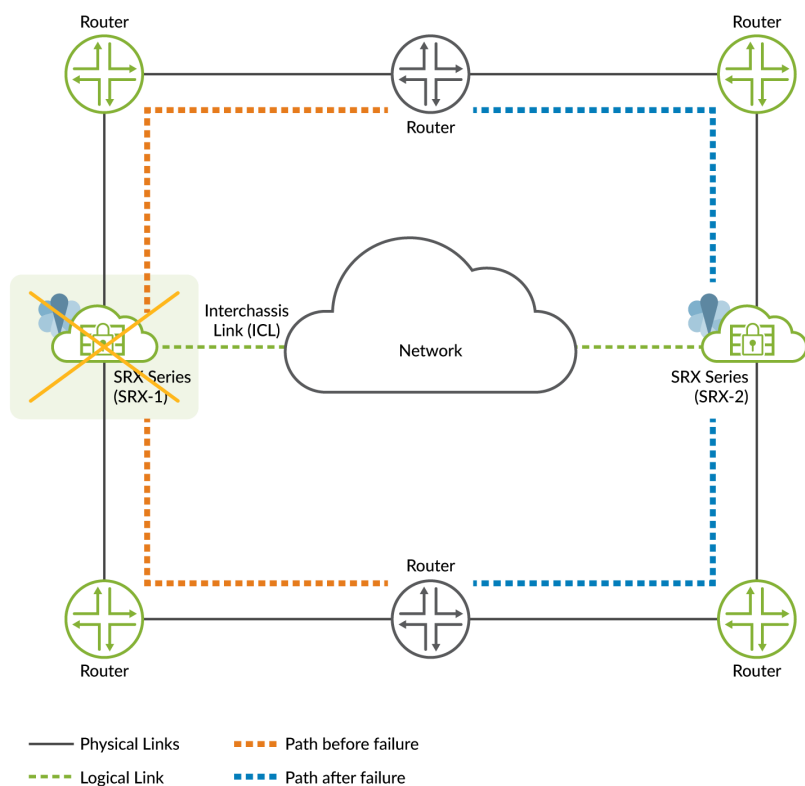
- **Recovery**—Recovery of failure takes place when you clear chassis hardware failure (ex: replace or repair the failed hardware component).
- **Results**—Check status using the following commands:
  - ["show chassis high-availability information detail" on page 1406](#)

- `show chassis hardware`
- `show chassis alarms`

## System/Software Failure

- **Cause**—A failure in software process or service or issues with operating system.
- **Detection**— In Multinode High Availability
  - Affected device/node not accessible
  - Changes system state to INELIGIBLE on the affected node with system/software failure.
- **Impact** —Traffic will failover to the other node if healthy as shown in [Figure 51 on page 648](#)

Figure 51: Software Failure in Multinode High Availability



- **Recovery**—Automatically and gracefully recovers from the outage once the issue is addressed. The backup node that has taken the active role, continues to remain active. The formerly active node remains as the backup node.

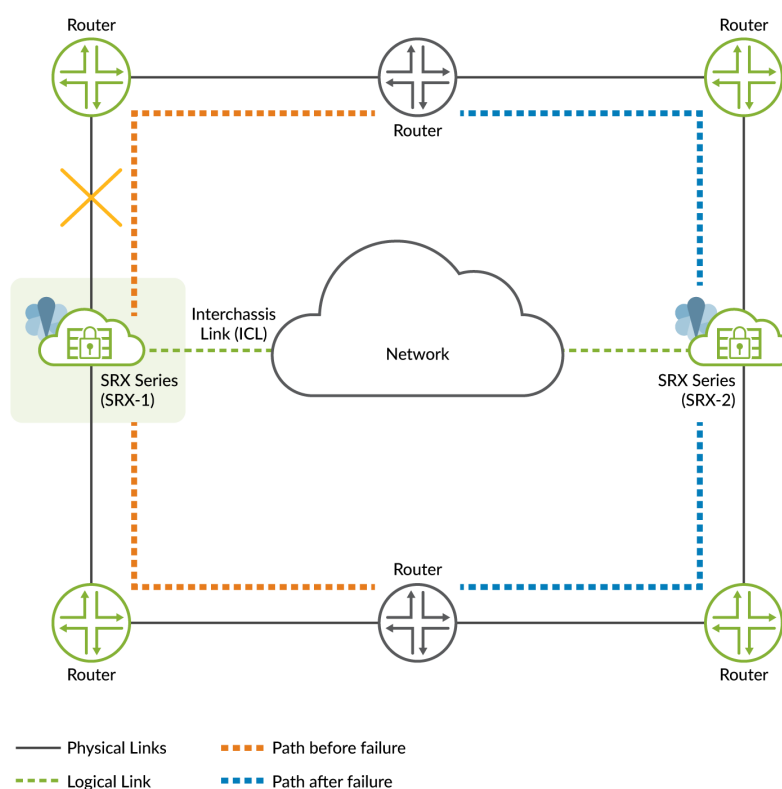
- **Results**—Check status using the ["show chassis high-availability information detail"](#) on page 1406 command.

## Network/Connectivity Failure

### Physical Interfaces (Link) Failure

- **Cause**—A failure in interfaces could be due to network equipment outages, or disruption with physical cable or inconsistent configurations.
- **Detection**— In Multinode High Availability
  - Affected device/node is not accessible.
  - SRG1 status changes to INELIGIBLE on the affected node with network or connectivity failure (if the interface-monitor is configured). Path connectivity could also be detected with BFD or IP-monitoring and trigger an event based on configured action.
- **Impact**—A change in the link state of the interfaces triggers a failover. The backup node takes up the active role, and services that were running on the failed node are migrated to other node as shown in [Figure 52 on page 650](#).

Figure 52: Interface Failure



- **Configuration**—To configure BFD monitoring and interface monitoring, use the following configuration statement:

```
set chassis high-availability services-redundancy-group <1> monitor bfd-liveliness <source-ip-address> <destination-ip-address> routing-instance <routing-instance-name> <single-hop|multihop> <interface-name>
```

```
set chassis high-availability services-redundancy-group <1> monitor interface <interface-name>
```

All links critical to traffic flow should be monitored.

Checkout *Configuring Multinode High Availability In a Layer 3 Network* or *Configuring Multinode High Availability In a Default Gateway Deployment* for complete configuration details.

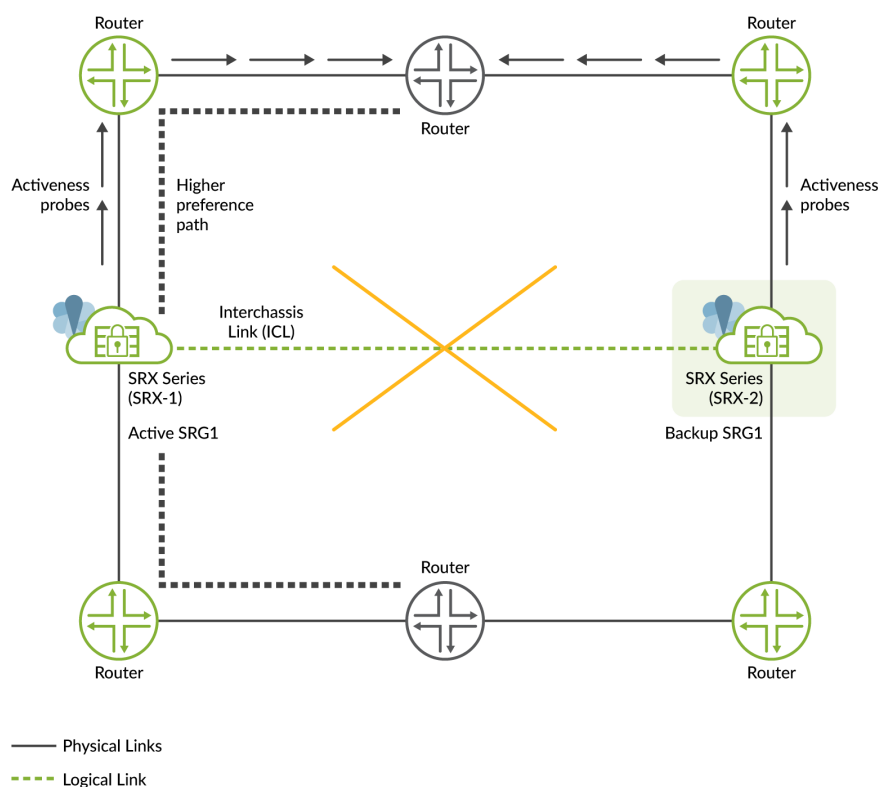
- **Recovery**—Recovers when you repair/replace the failed interface. After the network/connectivity failure recovers, SRG1 moves from the INELIGIBLE state to the BACKUP state. The new-active node continues advertise better metrics to its upstream router and processes traffic.

- **Results**—Check status using the following commands:
  - `show chassis high-availability information detail`
  - `monitor interfaces`
  - `show interfaces terse`
- For information on configuring interfaces, see *Configuring Multinode High Availability In a Layer 3 Network*, *Configuring Multinode High Availability In a Hybrid Deployment*, *Configuring Multinode High Availability In a Default Gateway Deployment*, [Troubleshooting Interfaces](#).

### Interchassis Link (ICL) Failure

- **Cause**—A failure in ICL could be due to network outages, or inconsistent configurations.
- **Detection**— In Multinode High Availability, nodes cannot reach each other and they initiate a activeness determination probe (ICMP probe).
- **Impact**— In a Multinode High Availability system, ICL connects active and backup nodes; if the ICL goes down, both devices will notice this change and start the activeness probe (ICMP probe). Activeness probe is done to determine the node that can take active role for each SRG1+. Based on the probe result, one of the node transitions to the active state.  
As shown in [Figure 53 on page 652](#), the ICL between SRX-1 and SRX-2 goes down. Both devices cannot reach each other and start sending activeness probes to the upstream router. Since SRX-1 is on higher preferred path in the router configuration, it takes up active role and continues to process traffic and advertises higher preference path. The other takes up backup role.

Figure 53: ICL Failure in Multinode High Availability



- **Configuration**—To configure the activeness probing, use the following configuration statement:

```
set chassis high-availability services-redundancy-group <1> activeness-probe <destination-ip-address> routing-instance <routing-instance-name>
```

Checkout *Configuring Multinode High Availability In a Layer 3 Network* for complete configuration details.

- **Results**—Check status using the following commands:
  - `show chassis high-availability information detail`
  - `show chassis high-availability services-redundancy-group 1`
  - Check ICMP packet reply from the upstream router using ping option. Example: `ping <activeness-probe-dest-ip> source <activeness-probe-source-ip> routing-instance <routing-instance-name>`.

- **Recovery**—Once one of the nodes assumes active role, Multinode High Availability restarts cold synchronization process and resynchronizes control-plane services (IPSec VPN). SRG state information is re-exchanged between the nodes.

### Node Remains in Isolated State

- **Cause**—In a Multinode High Availability setup, the node remains in isolated state after a reboot and associated interfaces continue to remain down when:
  - Inter chassis link (ICL) has no connectivity to the other node after booting up until the cold-sync complete
  - and
  - The shutdown-on-failure option is configured on SRG0

**NOTE:** The above cause could also happen if the other device is out of service.

- **Detection**—SRG0 status displayed as ISOLATED in command output.
- **Recovery**—The node automatically recovers when the other node comes online and the ICL can exchange system information or when you remove the shutdown-on-failure statement and commit the configuration.

Use the `delete chassis high-availability services-redundancy-group 0 shutdown-on-failure` to remove the statement.

If the above solution is not suitable for your environment, you can use the `install-on-failure-route` option. In this option, the Multinode High Availability setup uses a defined signal route for more graceful handling of the above situation using routing policy options, which is similar to `active-signal-route` and `backup-signal-route` approach available in SRG1+.

### SEE ALSO

[Prepare Your Environment for Multinode High Availability Deployment | 654](#)

[Multinode High Availability Services | 658](#)

[Example: Configure Multinode High Availability in a Default Gateway Deployment | 717](#)

[Example: Configure Multinode High Availability in a Layer 3 Network | 672](#)

[Example: Configure Multinode High Availability in a Hybrid Deployment | 752](#)

[Insert Additional SRX5K-SPC3 in a Multinode High Availability Setup | 904](#)

[Software Upgrade in Multinode High Availability | 885](#)

[Multinode High Availability Support for vSRX Instances in Public Cloud Deployments | 908](#)

## Prepare Your Environment for Multinode High Availability Deployment

### IN THIS SECTION

- [Using IP Address Pools in Multinode High Availability Configuration | 656](#)

This topic provides details to prepare the environment for Multinode High Availability deployment.

### Device Model

In Multinode High Availability, you must use the same SRX Series device model as your nodes. For example, if you use the SRX5600 as one node, you must use another SRX5600 as the other node.

In case of the SRX5000 line of devices, ensure that SPCs, NPCs, and IOCs have the same slot placement and type.

We support Multinode High Availability on the following devices:

- SRX5800, SRX5600, SRX5400 with the following components running Junos OS Release 20.4R1 or later:
  - Services Processing Card SPC3
  - I/O card IOC3
  - Switch Control Boards SCB3 and SCB4
  - Routing Engine RE3
- SRX4600, SRX4200, SRX4100, and SRX1500 running Junos OS Release 22.3R1 or later
- vSRX running Junos OS Release 22.3R1 or later

### Software Version

Install the compatible version of Junos OS on the participating security devices.



## Latest Junos IKE Package

You must install IKE package for enabling ICL encryption in Multinode High Availability solution.

By default, when your SRX Series device boots up, the legacy IKE architecture is executed. To enable the new IKE architecture, you must install the new Junos IKE package. This is an optional package included in the Junos OS software download image.

Use the following command to install the IKE package:

```
user@host> request system software add optional://junos-ike.tgz
```

After you install the Junos IKE package, for subsequent software upgrades of the instance, the Junos IKE package is upgraded automatically from the new Junos OS releases installed on your device.

## Software Licenses

You do not need any specific license for the Multinode High Availability feature. However, licenses are unique to each SRX Series and cannot be shared between the nodes in a Multinode High Availability setup. Therefore, you must use identical licenses on both the nodes. If both SRX Series devices do not have an identical set of licenses, the system is not ready for the deployment.

## Network Accessibility

Both the nodes in the Multinode High Availability setup must be able to reach each other using the ICL path. This path uses (whether the ICL is encrypted or not) IP address, protocol, and port details. You must ensure that this communication is allowed between the nodes if any firewall or other inspection is in place.

The floating IP address that you use for each node must be routable IP (logical routed path) across the network.

We recommend to bind the ICL to the loopback interface (lo0) or an aggregated Ethernet interface (ae0) and have more than one physical link (LAG/LACP) that ensure path diversity for highest resiliency. You can also use a revenue Ethernet port on the SRX Series devices to setup an ICL connection. Ensure that you separate the transit traffic in revenue interfaces from the high availability (HA) traffic.

## IP Address Consideration

[Table 43 on page 656](#) provides details on IPv4 and IPv6 address support for Multinode High Availability deployments.

Table 43: IP Address Consideration For Multinode High Availability

MNHA Deployment Type	Layer 3 Network (Routers at Both Ends)	Hybrid Network (Router at One End and Switch at the Other End)	Default Gateway (Switches at Both Ends)
IPv4 and IPv6 addresses for IP monitoring	Yes	Yes	Yes
IPv4 and IPv6 addresses for activeness probing	Yes	Yes	Yes
Virtual IPv4 and IPv6 addresses	Not applicable	Yes	Yes

**NOTE:** Configure only one VIP per logical interface (IFL) in a Multinode High Availability setup. Support for using multiple VIPs or dual-stack is not available.

## Using IP Address Pools in Multinode High Availability Configuration

When you configure multiple SRGs (active-active mode) in Multinode High Availability, ensure that address pools used by SRGs in an access profile must not overlap. Also ensure that address and address pool configured in the RADIUS server for the hosts connected to different SRGs must be unique.

Example: Following sample shows address pool configurations with access profile localpool and localpool2 for SRG1 and SRG2 respectively:

```

user@host# set groups manha_config_group access profile localpool address-assignment pool v4-
pool1
user@host# set groups manha_config_group access profile localpool2 authentication-order none
user@host# set groups manha_config_group access profile localpool2 address-assignment pool v4-
pool2
user@host# set groups manha_config_group access address-assignment pool v4-pool1 family inet
network 192.0.2.0/24
user@host# set groups manha_config_group access address-assignment pool v4-pool1 family inet
range v41 low 192.0.2.1
user@host# set groups manha_config_group access address-assignment pool v4-pool1 family inet

```

```

range v41 high 192.0.2.127
user@host# set groups manha_config_group access address-assignment pool v4-pool2 family inet
network 192.0.2.0/24
user@host# set groups manha_config_group access address-assignment pool v4-pool2 family inet
range v41 low 192.0.2.128
user@host# set groups manha_config_group access address-assignment pool v4-pool2 family inet
range v41 high 192.0.2.255

```

In this example, Services Redundancy Groups - SRG1 and SRG2 - are in the same network (192.0.2.0/24). However, IP addresses in address pools are distributed to avoid overlapping (192.0.2.1/24—192.0.2.127 for SRG1 and 192.0.2.128—192.0.2.255 for SRG2).

Similarly you must use unique IP address and address pools for user configurations in the RADIUS server.

In case you assign same address for hosts in two SRGs, then Multinode High Availability deletes the new host and halts IKE negotiations with the following message:

```
AUTHENTICATION_FAILED as the AUTH response
```

System Log displays the following message:

```
Duplicate assigned IPv4 received, delete new peer
```

## RELATED DOCUMENTATION

[Multinode High Availability | 613](#)

[Example: Configure Multinode High Availability in a Default Gateway Deployment | 717](#)

[Example: Configure Multinode High Availability in a Layer 3 Network | 672](#)

[Example: Configure Multinode High Availability in a Hybrid Deployment | 752](#)

[Multinode High Availability Services | 658](#)

## Multinode High Availability Services

### IN THIS SECTION

- [Control Plane Stateless Services | 658](#)
- [Network Address Translation | 659](#)
- [Firewall User Authentication | 659](#)
- [Configuration Synchronization Between Multinode High Availability Nodes | 660](#)

Multinode High Availability supports active/active mode for data plane and active/backup mode for control plane services. Lets learn about control plane stateless and stateful services in the following sections:

### Control Plane Stateless Services

SRG0 manages services without control plane state, such as application security, IDP, UTM, firewall, NAT, policies, ALG, and so on. Failover for these services is required at data plane level only and some of these services are pass through (not terminating on the device except NAT, firewall authentication).

SRG0 remains active on both nodes and forwards traffic from both the nodes. These feature works independently on both SRX Series devices in Multinode High Availability.

To configure the control plane stateless services:

- Configure the features as you configure them on a stand-alone SRX Series device.
- Install the same Junos OS version on the participating security devices (Junos OS Release 22.3R1 or later)
- Install identical licenses on both the nodes
- Download and install same versions of application signature package or IPS package on both nodes (if you are using application security and IDP)
- Configure conditional route advertisement, routing policy, and static routes as per your requirements.
- In Multinode High Availability, configuration synchronization does not happen by default. You need to configure applications as part of groups and then synchronize the configuration using the peer synchronization option or manage configuration independently on each node.

## Network Address Translation

Services such as Firewall, ALG, NAT do not have control plane state. For such services, only data plane state needs to be synchronized across the nodes.

In a Multinode High Availability setup, one device handles a NAT session at a time, and the other device takes over the active role when failover happens. So, a session remains active on one device, and on the other device, the session will be in warm (standby) state till failover happens.

NAT sessions and ALG state objects gets synchronized between the nodes. If one node fails, the second node continues to process traffic for the synchronized sessions from the failed device, including NAT translations.

You must create NAT rules and pools with the same parameters on both the SRX Series devices. To steer the response path for the NAT traffic (destined to NAT pool IP address) to the correct SRX Series device (active device), you must have the required routing configuration on both active/backup devices. That is, the configuration must specify what routes are advertised via the routing protocols to the adjacent routing devices. Accordingly, you must also configure policy-option and route configuration.

When you run NAT-specific operational commands on both devices, you can see the same output. However, there could be instances where NAT rule / pool internal numerical IDs can be different between the nodes. Different numerical IDs don't impact the session sync/ NAT translations upon failover.

## Firewall User Authentication

With firewall authentication, you can restrict or permit users individually or in groups. Users can be authenticated using a local password database or using an external password database.

Multinode High Availability supports following authentication methods:

- Pass-through authentication
- Pass-through with web-redirect authentication
- Web authentication

Firewall user authentication is service with a active control plane state and requires control and data plane states synchronization across the nodes. While working in Multinode High Availability setup, the firewall user authentication feature works independently on both SRX Series devices and synchronizes the authentication table between the nodes. When a user authenticates successfully, authentication entry gets synced to the other node and is visible on both the nodes when you run show command (example: `show security firewall-authentication users` ).

Multinode High Availability supports Juniper Identity Management Service (JIMS) to obtain user identity information. Each node fetches the authentication entries from JIMS server and process them independently. Because of this,

You must run firewall user authentication commands separately on each node. For example, when you display the auth entries using the show commands, each node displays only those auth entries that it is handling currently (as if working independently in standalone mode):

- `show services user-identification authentication-table`
- `show service user-identification identity-management`

## Configuration Synchronization Between Multinode High Availability Nodes

In Multinode High Availability, two SRX Series devices act as independent devices. These devices have unique hostname and the IP address on fxp0 interface. You can configure control plane stateless services such as ALG, firewall, NAT independently on these devices. Node-specific packets are always processed on the respective nodes.

Following packets/services are node-specific (local) in Multinode High Availability:

- Routing protocols packets to Routing Engine
- Management services, such as SNMP, and operational commands (show, request)
- Processes, such as the authentication service process (authd), integrated with RADIUS and LDAP servers
- ICL encryption specific tunnel control and data packets

The configuration synchronization in Multinode High Availability is not by default. If you want certain configurations to synchronize to the other node, you need to:

- Configure the feature/function as part of groups
- Synchronize the configuration using the `[edit system commit peers-synchronize]` option

When you enable configuration synchronization (by using the `peers-synchronize` option) on both the devices in a Multinode High Availability, configuration settings you configure on one peer under `[groups]` will automatically sync to the other peer upon the **commit** action.

The local peer on which you enable the `peers-synchronize` statement copies and loads its configuration to the remote peer. Each peer then performs a syntax check on the configuration file being committed. If no errors are found, the configuration is activated and becomes the current operational configuration on both peers.

The following configuration snippet shows VPN configuration under `avpn_config_group` on `host-mnha-01`. We'll synchronize the configuration to the other peer device `host-mnha-02`.

1. Configure the hostname and IP address of the participating peer device (`host-mnha-02`), authentication details, and include the `peers-synchronization` statement.

```
[edit]
user@host-mnha-01# set system commit peers-synchronize
user@host-mnha-01# set system commit peers host-mnha-02 user user-02
user@host-mnha-01# set system commit peers host-mnha-02 authentication "$ABC"
user@host-mnha-01# set system services netconf ssh
user@host-mnha-01# set system static-host-mapping host-mnha-02 inet 10.157.75.129
```

2. Configure the group (`avpn_config_group`) and specify apply conditions (when peers `host-mnha-01` and `host-mnha-02`)

```
user@host-mnha-01# set groups avpn_config_group when peers host-mnha-01
user@host-mnha-01# set groups avpn_config_group when peers host-mnha-02
user@host-mnha-01# set groups avpn_config_group security ike proposal avpn_IKE_PROP
authentication-method rsa-signatures
user@host-mnha-01# set groups avpn_config_group security ike proposal avpn_IKE_PROP dh-group
group14
user@host-mnha-01# set groups avpn_config_group security ike proposal avpn_IKE_PROP
authentication-algorithm sha1
user@host-mnha-01# set groups avpn_config_group security ike proposal avpn_IKE_PROP
encryption-algorithm aes-128-cbc
user@host-mnha-01# set groups avpn_config_group security ike proposal avpn_IKE_PROP lifetime-
seconds 3600
user@host-mnha-01# set groups avpn_config_group security ike policy avpn_IKE_POL proposals
avpn_IKE_PROP
user@host-mnha-01# set groups avpn_config_group security ike policy avpn_IKE_POL certificate
local-certificate crt2k
user@host-mnha-01# set groups avpn_config_group security ike gateway avpn_ike_gw ike-policy
avpn_IKE_POL
user@host-mnha-01# set groups avpn_config_group security ike gateway avpn_ike_gw dynamic
distinguished-name wildcard C=us,O=ixia
user@host-mnha-01# set groups avpn_config_group security ike gateway avpn_ike_gw dynamic ike-
user-type group-ike-id
user@host-mnha-01# set groups avpn_config_group security ike gateway avpn_ike_gw dead-peer-
detection probe-idle-tunnel
user@host-mnha-01# set groups avpn_config_group security ike gateway avpn_ike_gw dead-peer-
```

```

detection interval 60
user@host-mnha-01# set groups avpn_config_group security ike gateway avpn_ike_gw dead-peer-
detection threshold 5
user@host-mnha-01# set groups avpn_config_group security ike gateway avpn_ike_gw local-
identity hostname srx.juniper.net
user@host-mnha-01# set groups avpn_config_group security ike gateway avpn_ike_gw external-
interface lo0.0
user@host-mnha-01# set groups avpn_config_group security ike gateway avpn_ike_gw local-
address 10.11.0.1
user@host-mnha-01# set groups avpn_config_group security ike gateway avpn_ike_gw version v2-
only
user@host-mnha-01# set groups avpn_config_group security ipsec proposal avpn_IPSEC_PROP
protocol esp
user@host-mnha-01# set groups avpn_config_group security ipsec proposal avpn_IPSEC_PROP
authentication-algorithm hmac-sha1-96
user@host-mnha-01# set groups avpn_config_group security ipsec proposal avpn_IPSEC_PROP
encryption-algorithm aes-128-cbc
user@host-mnha-01# set groups avpn_config_group security ipsec proposal avpn_IPSEC_PROP
lifetime-seconds 1800
user@host-mnha-01# set groups avpn_config_group security ipsec policy avpn_IPSEC_POL perfect-
forward-secrecy keys group14
user@host-mnha-01# set groups avpn_config_group security ipsec policy avpn_IPSEC_POL
proposals avpn_IPSEC_PROP
user@host-mnha-01# set groups avpn_config_group security ipsec vpn avpn_ipsec_vpn bind-
interface st0.15001
user@host-mnha-01# set groups avpn_config_group security ipsec vpn avpn_ipsec_vpn ike gateway
avpn_ike_gw
user@host-mnha-01# set groups avpn_config_group security ipsec vpn avpn_ipsec_vpn ike ipsec-
policy avpn_IPSEC_POL
user@host-mnha-01# set groups avpn_config_group security ipsec vpn avpn_ipsec_vpn traffic-
selector ts local-ip 10.19.0.0/8
user@host-mnha-01# set groups avpn_config_group security ipsec vpn avpn_ipsec_vpn traffic-
selector ts remote-ip 10.4.0.0/8
user@host-mnha-01# set groups avpn_config_group security zones security-zone vpn host-inbound-
traffic system-services all
user@host-mnha-01# set groups avpn_config_group security zones security-zone vpn host-inbound-
traffic protocols all
user@host-mnha-01# set groups avpn_config_group security zones security-zone vpn interfaces
st0.15001
user@host-mnha-01# set groups avpn_config_group interfaces st0 description vpn
user@host-mnha-01# set groups avpn_config_group interfaces st0 unit 15001 family inet

```



3. Use the `apply-groups` command at the root of the configuration.

```
user@host-mnha-01# set apply-groups avpn_config_group
```

When you commit the configuration, Junos checks the command and merge the correct group to match the node name.

4. Verify the synchronization status using the `show configuration system` command from the operational mode.

```
user@host-mnha-01> show configuration system
.....
commit {
  peers {
    host-mnha-02 {
      user user user-02;
      authentication "$ABC123";
    }
  }
}

static-host-mapping {
  host-mnha-02 inet 10.157.75.129;
}
.....
```

The command output displays the details of the peer SRX Series device under the **peers** option.

**NOTE:** The configuration synchronization happens dynamically and if any configuration change done when only one node is available or when the connectivity breaks between the nodes, you must issue one more commit to synchronize the configuration to the other node. Otherwise, it will lead to inconsistent configurations across nodes for the applications.

## RELATED DOCUMENTATION

[Multinode High Availability | 613](#)

---

[Prepare Your Environment for Multinode High Availability Deployment | 654](#)

---

[Example: Configure Multinode High Availability in a Default Gateway Deployment | 717](#)

---

[Example: Configure Multinode High Availability in a Layer 3 Network | 672](#)

---

[Example: Configure Multinode High Availability in a Hybrid Deployment | 752](#)

---

## IPsec VPN Support in Multinode High Availability

### IN THIS SECTION

- [IPsec VPN in Active-Backup Mode | 664](#)
- [IPsec VPN in Active-Active Mode | 665](#)

### IPsec VPN in Active-Backup Mode

SRX Series devices support IPsec VPN tunnels in a Multinode High Availability setup. Prior Junos OS Release 22.4R1, IPsec VPN tunnel anchors at SRG1, where SRG1 acts in stateful active / backup mode. In this mode, all VPN tunnels terminate on the same device where SRG1 is active.

Multinode High Availability establishes IPsec tunnel and performs key exchanges by:

- Dynamically associating the floating IP address of the active SRG1 for the termination IP in routing deployment and assigns the termination IP, the virtual IP(VIP), which floats between the two devices in switching mode.
- Generating the CA profile, when there is a need for a dynamic CA profile to authenticate the tunnel establishment, on the node where SRG1 is active.
- Performing new authentication and loading the dynamic profile on the newly active node and clearing on the old node.

Although you can run the `show` commands on both active and backup nodes to display the status of IKE and IPsec security associations, you can delete the IKE and IPsec security associations only on the active node.

VPN service is automatically enabled when you enable the active/backup mode using the `set chassis high-availability services-redundancy-group 1` command. See the configuration example for more details.

**NOTE:** PKI files are synchronized to the peer node only if you enable link encryption for the ICL.

**TIP:** We recommend following sequence when you configure VPN with Multinode High Availability on your security device:

- On the backup node, configure security IKE gateway, IPsec VPN, interfaces st0.x, and security zones and then commit the configuration.
- On the active node, configure security IKE gateway, IPsec VPN, st0.x interface, security zones, and static route and commit the configuration.

You must commit the configuration on the backup node before committing configuration on the active node if you don't use the commit synchronize option.

## Process Packets on Backup Node

When you use the process-packet-on-backup option in Multinode High Availability, the Packet Forward Engine forwards packets on backup node for the corresponding SRG. This configuration processes VPN packets on the backup node even when the node is not in active mode; thus, eliminating the delay when backup node transitions to the active role after a failover. The packet process continues even during the transition period.

You can configure the process packet on backup on an SRG1 using the `[set chassis high-availability services-redundancy-group name process-packet-on-backup]` statement.

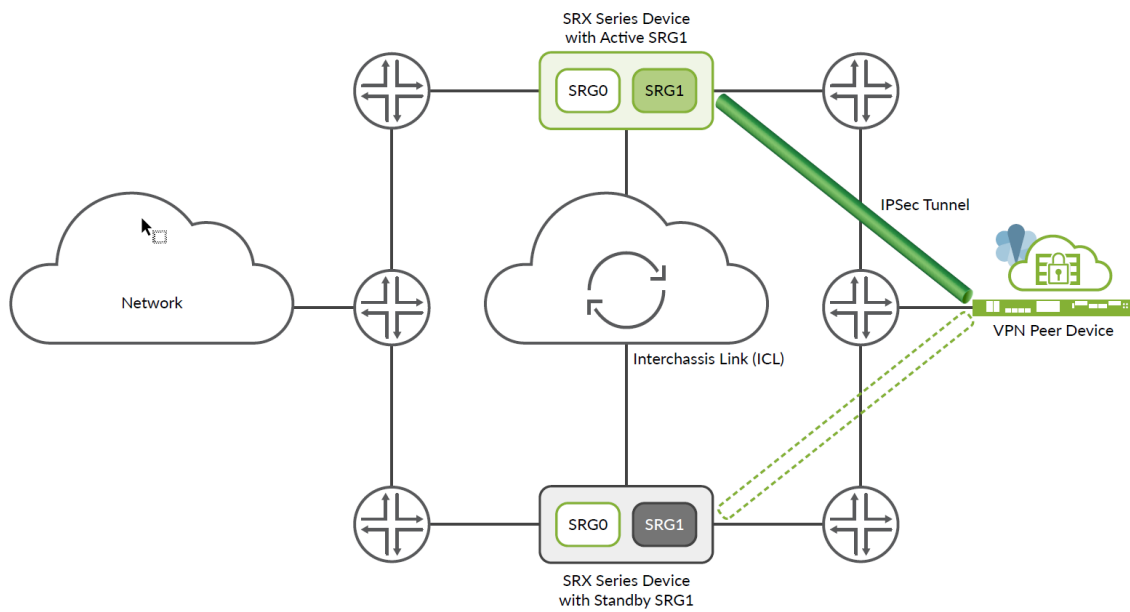
## IPsec VPN in Active-Active Mode

Starting in Junos OS Release 22.4R1, you can configure Multinode High Availability to operate in active-active mode with support of multi SRG1s (SRG1+) for IPsec VPN. In this mode, some SRGs remain active on one node and some SRGs remain active on another node. A particular SRG always operates in active-backup mode; it operates in active mode on one node and backup mode on another node.

Multinode High Availability supports IPsec VPN in active-active mode with multiple SRGs (SRG1+). In this mode, you can establish multiple active tunnels from both the nodes, based on SRG activeness. Since different SRGs can be active on different nodes, tunnels belonging to these SRGs come up on both nodes independently. Having active tunnels on both the nodes enables encrypting/decrypting data traffic on both the nodes resulting in efficient use of bandwidth.

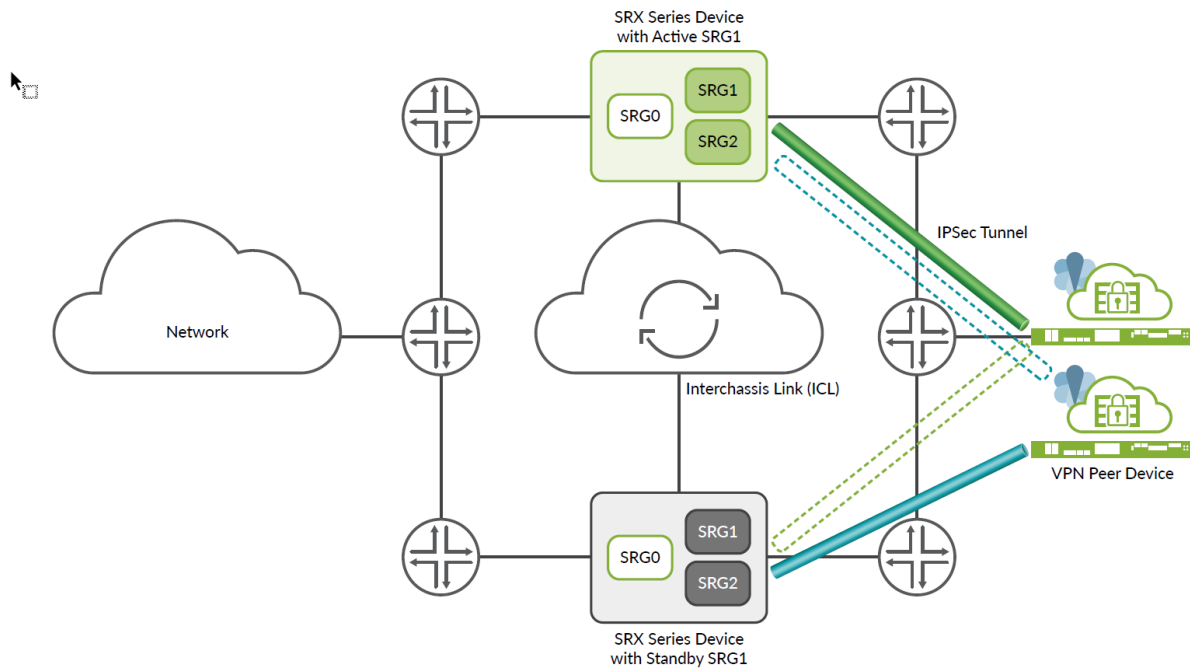
[Figure 54 on page 666](#) and [Figure 55 on page 666](#) show differences in active-backup and active-active Multinode High Availability IPsec VPN tunnels.

Figure 54: Active-Backup IPsec VPN Tunnel in Multinode High Availability



jn-000503

Figure 55: Active-Active IPsec VPN Tunnel in Multinode High Availability



jn-000504

Multinode High Availability establishes IPsec tunnel and performs key exchanges by associating termination IP address (which also identifies the tunnels ending on it) to the SRG. Since different SRG1+ can be in active state or in backup state on each of the devices, Multinode High Availability steers the matching traffic effectively to the corresponding active SRG1. Multinode High Availability also maintains the SRG ID and IP prefix mapping information.

[Table 44 on page 667](#) and [Table 45 on page 667](#) provide details on impact on IPsec VPN tunnels due to change in SRG1+ changes.

**Table 44: Impact on IPsec VPN Tunnels Due to SRG1+ Modification**

SRG1 Changes	Impact on IPsec VPN Tunnels
SRG addition	No impact on existing tunnels
SRG deletion	Deletes all routes associated with the SRG.
SRG attribute (other than prefix-list) modification	No impact on existing tunnels
SRG ID modification	Deletes all existing tunnels associated with the SRG.
IP-prefix in prefix-list modification	Deletes all tunnels mapping to that particular IP prefix.  No impact if there is no existing tunnel mapping to the modified IP prefix.

**Table 45: Impact on IPsec VPN Tunnels Due to SRG1+ State Changes**

SRG State Changes	Action from Multinode High Availability
Active to Backup	Deletes all data corresponding to that SRG, and resynchronizes from new the active SRG
Active to Ineligible	Deletes all data corresponding to that SRG, and resynchronizes from new the active SRG
Active to Hold	Not applicable
Backup to Active	No action

**Table 45: Impact on IPsec VPN Tunnels Due to SRG1+ State Changes (Continued)**

SRG State Changes	Action from Multinode High Availability
Ineligible to Active	No action
Hold to Active	No action
Hold to Backup	No action (possible state transition; if Active state is not involved in either pre or post state, no action is required)
Ineligible to Backup	No action (possible state transition; if Active state is not involved in either pre or post state, no action is required)
Hold to Ineligible	No action (possible state transition; if Active state is not involved in either pre or post state, no action is required)

## Associate IPsec VPN Service to an SRG

Releases before 22.4R1 supported only SRG0 and SRG1, and SRG1 was associated to IPsec VPN by default. In 22.4R1, an SRG is not associated to the IPsec VPN service by default. You must associate the IPsec VPN service to any of the multiple SRGs by:

- Specifying IPsec as managed service  
Ex: [set chassis high-availability services-redundancy-group <id> managed-services ipsec]
- Creating an IP prefix list  
Ex: [set chassis high-availability services-redundancy-group <id> prefix-list <name>]  
  
[set policy-options prefix-list <name> <IP address>

When you have multiple SRGs in your Multinode High Availability setup, some SRGs are in active state on one node and some SRGs are active on another node. You can anchor certain IPsec tunnels to particular node (SRX Series firewall) by configuring an IP prefix list.

In IPsec VPN configuration, an IKE gateway initiates and terminates network connections between two security devices. The local end (local IKE gateway) is the SRX Series interface that initiates IKE negotiations. Local IKE gateway has a local IP address, a publicly routable IP address on the firewall, which the VPN connection uses as the endpoint.

IP prefix list includes a list of IPv4 or IPv6 address prefixes, which are used as local address of an IKE gateway. You can associate these IP prefixes (prefix-list) with a specified SRG1 to advertise local address of IKE gateway with a higher preference according to state of the SRG.

To anchor a certain IPsec VPN tunnel to a particular security device, then you must:

- Create an IP prefix list by including the local address of IKE gateway and associate the IP prefix list to the SRG:

Example:

```
user@host# set chassis high-availability services-redundancy-group 1 prefix-list lo0_1
user@host# set chassis high-availability services-redundancy-group 2 prefix-list lo0_2
user@host# set policy-options prefix-list lo0_1 10.11.0.1/32
user@host# set policy-options prefix-list lo0_2 10.11.1.1/32
user@host# set interfaces lo0 description untrust
user@host# set interfaces lo0 unit 0 family inet address 10.11.0.1/32
user@host# set interfaces lo0 unit 0 family inet address 10.11.1.1/32
```

- Associate/enable IPsec VPN to the SRG.

Example:

```
user@host# set chassis high-availability services-redundancy-group 1 managed-services ipsec
user@host# set chassis high-availability services-redundancy-group 2 managed-services ipsec
```

This configuration allows you to selectively and flexibly associate IPsec VPN to one of the multiple SRGs configured on SRX Series device in a Multinode High Availability setup.

You can check the mapping of IKE/IPsec objects to the SRG by using the following command:

```
user@host# show chassis high-availability information detail
.....
Services Redundancy Group: 1
  Deployment Type: SWITCHING
  Status: BACKUP
  Activeness Priority: 200
  Hold Timer: 1
  Services: [ IPSEC ]
  Process Packet In Backup State: NO
```

```

Control Plane State: NOT READY
System Integrity Check: COMPLETE
Peer Information:
Failure Events: NONE
  Peer Id: 2
  Last Advertised HA Status: ACTIVE
  Last Advertised Health Status: HEALTHY
  Failover Readiness: N/A

```

```

.....

```

You can check the mapping of SRGs and IP prefix list by using the following command:

```

user@host> show chassis high-availability prefix-srgid-table
IP SRGID Table:

```

SRGID	IP Prefix	Routing Table
1	10.11.0.1/32	rt-vr
1	10.19.0.1/32	rt-vr
1	10.20.0.1/32	rt-vr
2	10.11.1.1/32	rt-vr
2	10.19.1.1/32	rt-vr
2	10.20.1.1/32	rt-vr

If you do not configure a prefix list, you'll get the following warning message:

```

user@host> show chassis high-availability prefix-srgid-table
Warning: prefix list not configured

```

See ["Example: Configure IPSec VPN in Active-Active Multinode High Availability in a Layer 3 Network" on page 795](#) for details.

## RELATED DOCUMENTATION

[Example: Configure IPSec VPN in Active-Active Multinode High Availability in a Layer 3 Network | 795](#)



---

Multinode High Availability | **613**

---

Example: Configure IPSec VPN in Active-Active Multinode High Availability in a Layer 3 Network | **795**

# Multinode High Availability Configuration

## IN THIS CHAPTER

- [Example: Configure Multinode High Availability in a Layer 3 Network | 672](#)
- [Example: Configure Multinode High Availability in a Default Gateway Deployment | 717](#)
- [Example: Configure Multinode High Availability in a Hybrid Deployment | 752](#)
- [Example: Configure IPSec VPN in Active-Active Multinode High Availability in a Layer 3 Network | 795](#)

## Example: Configure Multinode High Availability in a Layer 3 Network

### SUMMARY

Read this topic to understand how to configure the Multinode High Availability solution on SRX Series devices. The example covers configuration in active/backup mode when SRX Series devices are connected to routers on both sides.

### IN THIS SECTION

- [Overview | 672](#)
- [Requirements | 673](#)
- [Topology | 673](#)
- [Configuration | 676](#)
- [Verification | 703](#)

### Overview

In Multi-Node High Availability, participating SRX Series devices operate as independent nodes in a Layer 3 network. The nodes are connected to adjacent infrastructure belonging to different networks. An encrypted logical interchassis link (ICL) connects the nodes over a routed network. Participating nodes backup each other to ensure a fast synchronized failover in case of system or hardware failure.

In Multinode High Availability, activeness is determined at the services redundancy group (SRG) level. The SRX Series device, on which the SRG1 is active, hosts the floating IP address and steers traffic towards it using the floating IP address. During a failover, the floating IP address moves from the old active node to the new active node and continues the communication client devices.

**NOTE:** As of Junos OS Release 22.3R1, we support a two-node configuration in the Multinode High Availability solution.

## Requirements

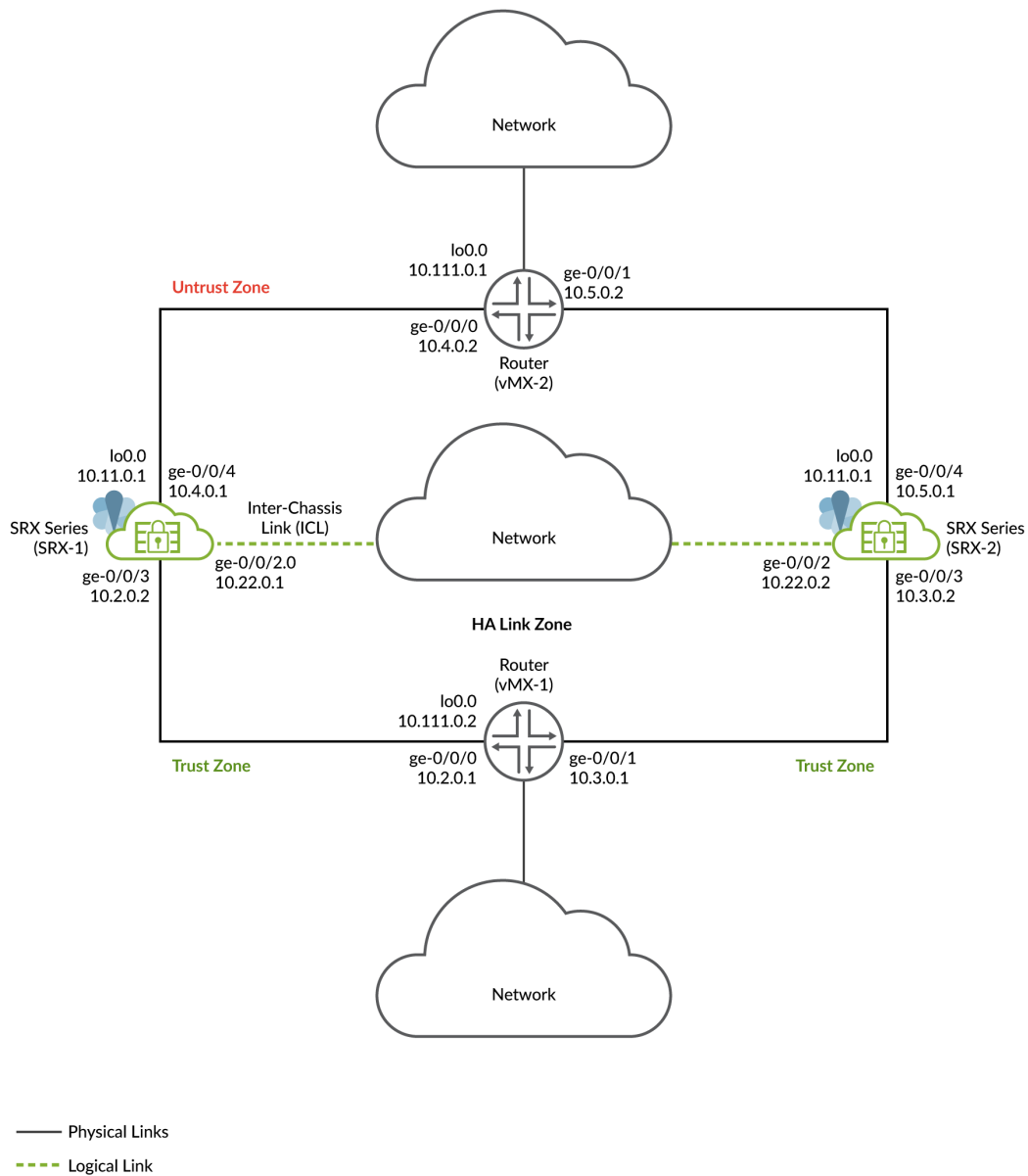
This example uses the following hardware and software components:

- Two SRX Series devices or vSRX instances
- Two Juniper Networks(R) MX960 Universal Routing Platform
- Junos OS Release 22.3R1

## Topology

[Figure 56 on page 674](#) shows the topology used in this example.

Figure 56: Multinode High Availability in Layer 3 Network



As shown in the topology, two SRX Series devices are connected to adjacent routers on trust and untrust side forming a BGP neighborship. An encrypted logical interchassis link (ICL) connects the nodes over a routed network. The nodes communicate with each other using a routable IP address (floating IP address) over the network. Loopback interfaces are used to host the IP addresses on SRX Series and routers.

In general, you can use Aggregated Ethernet (AE) or a revenue Ethernet port on the SRX Series devices to setup an ICL connection. In this example, we've used GE ports for the ICL. We've also configured a routing instance for the ICL path to ensure maximum segmentation.

In a typical high availability deployment, you have multiple routers and switches on the northbound and southbound sides of the network. For this example, we are using two routers on both sides of SRX Series devices.

In this example, you'll establish high availability between the SRX Series devices and secure the tunnel traffic by enabling HA link encryption.

You'll perform the following tasks to build a Multinode High Availability setup:

- Configure a pair of SRX Series devices as local and peer nodes by assigning IDs.
- Configure services redundancy groups.
- Configure a loopback interface (lo0.0) to host the floating IP address.
- Configure IP probes for the activeness determination and enforcement
- Configure a signal route required for activeness enforcement and use it along with the route exists policy.
- Configure a VPN profile for the high availability (ICL) traffic using IKEv2.
- Configure BFD monitoring options
- Configure a routing policy and routing options
- Configure appropriate security policies to manage traffic in your network
- Configure stateless firewall filtering and quality of service (QoS) as per your network requirements.
- Configure interfaces and zones according to your network requirement. You must allow services such as IKE for link encryption and SSH for configuration synchronization as host-inbound system services on the security zone that is associated with the ICL.

You can configure the following options on SRG0 and SRG1:

- SRG1: Active/backup signal route, deployment type, activeness priority, preemption, virtual IP address (for default gateway deployments), activeness probing and process packet on backup.
- SRG1: BFD monitoring, IP monitoring, and interface monitoring options on SRG1.
- SRG0: shutdown on failure and install on failure route options.

When you configure monitoring (BFD or IP or Interface) options under SRG1, we recommend not to configure the shutdown-on-failure option under SRG0.

For interchassis link (ICL), we recommend the following configuration settings:

- Use a loopback (lo0) interface using an aggregated Ethernet interface (ae0), or any revenue Ethernet interface to establish the ICL. Do not to use the dedicated HA ports (control and fabric ports) if available on your SRX Series device).
- Set MTU of 1514
- Allow the following services on the security zone associated with interfaces used for ICL
  - IKE, high-availability, SSH
  - Protocols depending on the routing protocol you need.
  - BFD to monitor the neighboring routes.

A secure tunnel interface (st0) from st0.16000 to st0.16385 is reserved for Multinode High Availability. These interfaces are not user configurable interfaces. You can only use interfaces from st0.0 to st0.15999.

## Configuration

### IN THIS SECTION

- [Before You Begin | 676](#)
- [CLI Quick Configuration | 677](#)
- [Configuration | 683](#)
- [Results \(SRX-1\) | 691](#)
- [Results \(SRX-2\) | 697](#)

### Before You Begin

Install the Junos IKE package on your SRX Series. You require this step for ICL encryption.

```
user@host> request system software add optional://junos-ike.tgz
Verified junos-ike signed by PackageProductionECP256_2022 method ECDSA256+SHA256
Rebuilding schema and Activating configuration...
mgd: commit complete
Restarting MGD ...
```

WARNING: cli has been replaced by an updated version:

CLI release 20220208.163814\_builder.r1239105 built by builder on 2022-02-08 17:07:55 UTC

Restart cli using the new version ? [yes,no] (yes)

## CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the [edit] hierarchy level, and then enter `commit` from configuration mode.

These configurations are captured from a lab environment, and are provided for reference only. Actual configurations may vary based on the specific requirements of your environment.

### On SRX-1 Device

```
set chassis high-availability local-id 1
set chassis high-availability local-id local-ip 10.22.0.1
set chassis high-availability peer-id 2 peer-ip 10.22.0.2
set chassis high-availability peer-id 2 interface ge-0/0/2.0
set chassis high-availability peer-id 2 vpn-profile IPSEC_VPN_ICL
set chassis high-availability peer-id 2 liveness-detection minimum-interval 400
set chassis high-availability peer-id 2 liveness-detection multiplier 5
set chassis high-availability services-redundancy-group 0 peer-id 2
set chassis high-availability services-redundancy-group 1 deployment-type routing
set chassis high-availability services-redundancy-group 1 peer-id 2
set chassis high-availability services-redundancy-group 1 activeness-probe dest-ip 10.111.0.1
set chassis high-availability services-redundancy-group 1 activeness-probe dest-ip src-ip
10.11.0.1
set chassis high-availability services-redundancy-group 1 monitor bfd-liveliness 10.4.0.2 src-ip
10.4.0.1
set chassis high-availability services-redundancy-group 1 monitor bfd-liveliness 10.4.0.2
session-type singlehop
set chassis high-availability services-redundancy-group 1 monitor bfd-liveliness 10.4.0.2
interface ge-0/0/4.0
set chassis high-availability services-redundancy-group 1 active-signal-route 10.39.1.1
set chassis high-availability services-redundancy-group 1 backup-signal-route 10.39.1.2
set chassis high-availability services-redundancy-group 1 preemption
set chassis high-availability services-redundancy-group 1 activeness-priority 200
set interfaces ge-0/0/3 description "trust" unit 0 family inet address 10.2.0.2/16
set interfaces ge-0/0/4 description "untrust" unit 0 family inet address 10.4.0.1/16
set interfaces ge-0/0/2 description "ha_link" unit 0 family inet address 10.22.0.1/24
set interfaces lo0 description "untrust" unit 0 family inet address 10.11.0.1/32
set interfaces lo0 description "untrust" unit 0 family inet address 10.11.0.2/32
```

```

set interfaces lo0 description "untrust" unit 0 family inet address 10.11.0.3/32
set routing-options autonomous-system 100
set routing-options static route 10.1.0.0/16 next-hop 10.2.0.1
set routing-options static route 10.6.0.0/16 next-hop 10.4.0.2
set routing-options static route 10.111.0.1 next-hop 10.2.0.1
set routing-options static route 10.111.0.2 next-hop 10.4.0.2
set security zones security-zone untrust host-inbound-traffic system-services ike
set security zones security-zone untrust host-inbound-traffic system-services ping
set security zones security-zone untrust host-inbound-traffic protocols bfd
set security zones security-zone untrust host-inbound-traffic protocols bgp
set security zones security-zone untrust interfaces ge-0/0/4
set security zones security-zone untrust interfaces lo0.0
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 ge-0/0/3
set security zones security-zone halink host-inbound-traffic system-services ike
set security zones security-zone halink host-inbound-traffic system-services ping
set security zones security-zone halink host-inbound-traffic system-services high-availability
set security zones security-zone halink host-inbound-traffic system-services ssh
set security zones security-zone halink host-inbound-traffic protocols bfd
set security zones security-zone halink host-inbound-traffic protocols bgp
set security zones security-zone halink interfaces ge-0/0/2
set security policies default-policy permit-all
set security pki ca-profile Root-CA ca-identity Root-CA
set security pki ca-profile Root-CA enrollment url http://10.157.69.204/certsrv/mscep/mscep.dll
set security pki ca-profile Root-CA revocation-check disable
set system syslog file vpn_syslog any info
set system syslog file vpn_syslog match "iked|pkid|kmd|ikemd|authd|jsrpd|chassisd|bfd"
set system services netconf ssh
set security ike proposal MNHA_IKE_PROP description mnha_link_encr_tunnel
set security ike proposal MNHA_IKE_PROP authentication-method pre-shared-keys
set security ike proposal MNHA_IKE_PROP dh-group group14
set security ike proposal MNHA_IKE_PROP authentication-algorithm sha-256
set security ike proposal MNHA_IKE_PROP encryption-algorithm aes-256-cbc
set security ike proposal MNHA_IKE_PROP lifetime-seconds 3600
set security ike policy MNHA_IKE_POL description mnha_link_encr_tunnel
set security ike policy MNHA_IKE_POL proposals MNHA_IKE_PROP
set security ike policy MNHA_IKE_POL pre-shared-key ascii-text "$ABC123"
set security ike gateway MNHA_IKE_GW ike-policy MNHA_IKE_POL
set security ike gateway MNHA_IKE_GW version v2-only
set security ipsec proposal MNHA_IPSEC_PROP description mnha_link_encr_tunnel
set security ipsec proposal MNHA_IPSEC_PROP protocol esp
set security ipsec proposal MNHA_IPSEC_PROP encryption-algorithm aes-256-gcm

```



```

set security ipsec proposal MNHA_IPSEC_PROP lifetime-seconds 3600
set security ipsec policy MNHA_IPSEC_POL description mnha_link_encr_tunnel
set security ipsec policy MNHA_IPSEC_POL proposals MNHA_IPSEC_PROP
set security ipsec vpn IPSEC_VPN_ICL ha-link-encryption
set security ipsec vpn IPSEC_VPN_ICL ike gateway MNHA_IKE_GW
set security ipsec vpn IPSEC_VPN_ICL ike ipsec-policy MNHA_IPSEC_POL
set policy-options condition active_route_exists if-route-exists address-family inet 10.39.1.1
table inet.0
set policy-options condition backup_route_exists if-route-exists address-family inet 10.39.1.2
table inet.0
set policy-options policy-statement mnha-route-policy term 1 from protocol static
set policy-options policy-statement mnha-route-policy term 1 from protocol direct
set policy-options policy-statement mnha-route-policy term 1 from condition active_route_exists
set policy-options policy-statement mnha-route-policy term 1 then accept metric 10
set policy-options policy-statement mnha-route-policy term 2 from protocol static
set policy-options policy-statement mnha-route-policy term 2 from protocol direct
set policy-options policy-statement mnha-route-policy term 2 from condition backup_route_exists
set policy-options policy-statement mnha-route-policy term 2 then accept metric 20
set policy-options policy-statement mnha-route-policy term 3 from protocol static
set policy-options policy-statement mnha-route-policy term 3 from protocol direct
set policy-options policy-statement mnha-route-policy term 3 then accept metric 30
set policy-options policy-statement mnha-route-policy term default then reject
set protocols bgp group trust type internal
set protocols bgp group trust local-address 10.2.0.2
set protocols bgp group trust export mnha-route-policy
set protocols bgp group trust neighbor 10.2.0.1
set protocols bgp group trust bfd-liveness-detection minimum-interval 500
set protocols bgp group trust bfd-liveness-detection minimum-receive-interval 500
set protocols bgp group trust bfd-liveness-detection multiplier 3
set protocols bgp group trust local-as 100
set protocols bgp group untrust type internal
set protocols bgp group untrust local-address 10.4.0.1
set protocols bgp group untrust export mnha-route-policy
set protocols bgp group untrust neighbor 10.4.0.2
set protocols bgp group untrust bfd-liveness-detection minimum-interval 500
set protocols bgp group untrust bfd-liveness-detection minimum-receive-interval 500
set protocols bgp group untrust bfd-liveness-detection multiplier 3
set protocols bgp group untrust local-as 100

```

## On SRX-2 Device

```

set chassis high-availability local-id 2
set chassis high-availability local-id local-ip 10.22.0.2
set chassis high-availability peer-id 1 peer-ip 10.22.0.1
set chassis high-availability peer-id 1 interface ge-0/0/2.0
set chassis high-availability peer-id 1 vpn-profile IPSEC_VPN_ICL
set chassis high-availability peer-id 1 liveness-detection minimum-interval 400
set chassis high-availability peer-id 1 liveness-detection multiplier 5
set chassis high-availability services-redundancy-group 0 peer-id 1
set chassis high-availability services-redundancy-group 1 deployment-type routing
set chassis high-availability services-redundancy-group 1 peer-id 1
set chassis high-availability services-redundancy-group 1 activeness-probe dest-ip 10.111.0.1
set chassis high-availability services-redundancy-group 1 activeness-probe dest-ip src-ip
10.11.0.1
set chassis high-availability services-redundancy-group 1 monitor bfd-liveliness 10.5.0.2 src-ip
10.5.0.1
set chassis high-availability services-redundancy-group 1 monitor bfd-liveliness 10.5.0.2
session-type singlehop
set chassis high-availability services-redundancy-group 1 monitor bfd-liveliness 10.5.0.2
interface ge-0/0/4.0
set chassis high-availability services-redundancy-group 1 active-signal-route 10.39.1.1
set chassis high-availability services-redundancy-group 1 backup-signal-route 10.39.1.2
set chassis high-availability services-redundancy-group 1 activeness-priority 1
set security ike proposal MNHA_IKE_PROP description mnha_link_encr_tunnel
set security ike proposal MNHA_IKE_PROP authentication-method pre-shared-keys
set security ike proposal MNHA_IKE_PROP dh-group group14
set security ike proposal MNHA_IKE_PROP authentication-algorithm sha-256
set security ike proposal MNHA_IKE_PROP encryption-algorithm aes-256-cbc
set security ike proposal MNHA_IKE_PROP lifetime-seconds 3600
set security ike policy MNHA_IKE_POL description mnha_link_encr_tunnel
set security ike policy MNHA_IKE_POL proposals MNHA_IKE_PROP
set security ike policy MNHA_IKE_POL pre-shared-key ascii-text "$ABC123"
set security ike gateway MNHA_IKE_GW ike-policy MNHA_IKE_POL
set security ike gateway MNHA_IKE_GW version v2-only
set security ipsec proposal MNHA_IPSEC_PROP description mnha_link_encr_tunnel
set security ipsec proposal MNHA_IPSEC_PROP protocol esp
set security ipsec proposal MNHA_IPSEC_PROP encryption-algorithm aes-256-gcm
set security ipsec proposal MNHA_IPSEC_PROP lifetime-seconds 3600
set security ipsec policy MNHA_IPSEC_POL description mnha_link_encr_tunnel
set security ipsec policy MNHA_IPSEC_POL proposals MNHA_IPSEC_PROP
set security ipsec vpn IPSEC_VPN_ICL ha-link-encryption

```

```

set security ipsec vpn IPSEC_VPN_ICL ike gateway MNHA_IKE_GW
set security ipsec vpn IPSEC_VPN_ICL ike ipsec-policy MNHA_IPSEC_POL
set interfaces ge-0/0/3 description "trust" unit 0 family inet address 10.3.0.2/16
set interfaces ge-0/0/4 description "untrust" unit 0 family inet address 10.5.0.1/16
set interfaces ge-0/0/2 description "ha_link" unit 0 family inet address 10.22.0.2/24
set interfaces lo0 description "untrust" unit 0 family inet address 10.11.0.1/32
set interfaces lo0 description "untrust" unit 0 family inet address 10.11.0.2/32
set interfaces lo0 description "untrust" unit 0 family inet address 10.11.0.3/32
set routing-options autonomous-system 100
set routing-options static route 10.1.0.0/16 next-hop 10.3.0.1
set routing-options static route 10.6.0.0/16 next-hop 10.5.0.2
set routing-options static route 10.111.0.1 next-hop 10.3.0.1
set routing-options static route 10.111.0.2 next-hop 10.5.0.2
set security zones security-zone untrust host-inbound-traffic system-services ike
set security zones security-zone untrust host-inbound-traffic system-services ping
set security zones security-zone untrust host-inbound-traffic protocols bfd
set security zones security-zone untrust host-inbound-traffic protocols bgp
set security zones security-zone untrust interfaces ge-0/0/4
set security zones security-zone untrust interfaces lo0.0
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 ge-0/0/3
set security zones security-zone halink host-inbound-traffic system-services ike
set security zones security-zone halink host-inbound-traffic system-services ping
set security zones security-zone halink host-inbound-traffic system-services high-availability
set security zones security-zone halink host-inbound-traffic system-services ssh
set security zones security-zone halink host-inbound-traffic protocols bfd
set security zones security-zone halink host-inbound-traffic protocols bgp
set security zones security-zone halink interfaces ge-0/0/2
set security policies default-policy permit-all
set security pki ca-profile Root-CA ca-identity Root-CA
set security pki ca-profile Root-CA enrollment url http://10.157.69.204/certsrv/mscep/mscep.dll
set security pki ca-profile Root-CA revocation-check disable
set system syslog file vpn_syslog any info
set system syslog file vpn_syslog match "iked|pkid|kmd|ikemd|authd|jsrpd|chassisd|bfd"
set system services netconf ssh
set policy-options route-filter-list loopback 10.11.0.0/24 orlonger
set policy-options route-filter-list ipsec 10.6.0.0/16 orlonger
set policy-options condition active_route_exists if-route-exists address-family inet 10.39.1.1
table inet.0
set policy-options condition backup_route_exists if-route-exists address-family inet 10.39.1.2
table inet.0
set policy-options policy-statement mnha-route-policy term 1 from protocol static

```

```

set policy-options policy-statement mnha-route-policy term 1 from protocol direct
set policy-options policy-statement mnha-route-policy term 1 from condition active_route_exists
set policy-options policy-statement mnha-route-policy term 1 then accept metric 10
set policy-options policy-statement mnha-route-policy term 2 from protocol static
set policy-options policy-statement mnha-route-policy term 2 from protocol direct
set policy-options policy-statement mnha-route-policy term 2 from condition backup_route_exists
set policy-options policy-statement mnha-route-policy term 2 then accept metric 20
set policy-options policy-statement mnha-route-policy term 3 from protocol static
set policy-options policy-statement mnha-route-policy term 3 from protocol direct
set policy-options policy-statement mnha-route-policy term 3 then accept metric 30
set policy-options policy-statement mnha-route-policy term default then reject
set protocols bgp group trust type internal
set protocols bgp group trust local-address 10.3.0.2
set protocols bgp group trust export mnha-route-policy
set protocols bgp group trust neighbor 10.3.0.1
set protocols bgp group trust bfd-liveness-detection minimum-interval 500
set protocols bgp group trust bfd-liveness-detection minimum-receive-interval 500
set protocols bgp group trust bfd-liveness-detection multiplier 3
set protocols bgp group trust local-as 100
set protocols bgp group untrust type internal
set protocols bgp group untrust local-address 10.5.0.1
set protocols bgp group untrust export mnha-route-policy
set protocols bgp group untrust neighbor 10.5.0.2
set protocols bgp group untrust bfd-liveness-detection minimum-interval 500
set protocols bgp group untrust bfd-liveness-detection minimum-receive-interval 500
set protocols bgp group untrust bfd-liveness-detection multiplier 3
set protocols bgp group untrust local-as 100

```

The following sections show configuration snippets on the routers required for setting up Multinode High Availability setup in the network.

### Router (VMX-1)

```

set interfaces ge-0/0/2 description lan unit 0 family inet address 10.1.0.1/16
set interfaces ge-0/0/0 description ha unit 0 family inet address 10.2.0.1/16
set interfaces ge-0/0/1 description ha unit 0 family inet address 10.3.0.1/16
set interfaces lo0 description "loopback" unit 0 family inet address 10.111.0.1 primary preferred
set routing-options autonomous-system 100
set protocols bgp group mnha_r0 type internal
set protocols bgp group mnha_r0 local-address 10.2.0.1
set protocols bgp group mnha_r0 neighbor 10.2.0.2
set protocols bgp group mnha_r0 bfd-liveness-detection minimum-interval 500

```

```

set protocols bgp group mnha_r0 bfd-liveness-detection minimum-receive-interval 500
set protocols bgp group mnha_r0 bfd-liveness-detection multiplier 3
set protocols bgp group mnha_r0 local-as 100
set protocols bgp group mnha_r0_b type internal
set protocols bgp group mnha_r0_b local-address 10.3.0.1
set protocols bgp group mnha_r0_b neighbor 10.3.0.2
set protocols bgp group mnha_r0_b bfd-liveness-detection minimum-interval 500
set protocols bgp group mnha_r0_b bfd-liveness-detection minimum-receive-interval 500
set protocols bgp group mnha_r0_b bfd-liveness-detection multiplier 3
set protocols bgp group mnha_r0_b local-as 100

```

## Router (VMX-2)

```

set interfaces ge-0/0/0 description HA unit 0 family inet address 10.4.0.2/16
set interfaces ge-0/0/1 description HA unit 0 family inet address 10.5.0.2/16
set interfaces ge-0/0/2 description trust unit 0 family inet address 10.6.0.1/16
set interfaces lo0 description "loopback" unit 0 family inet address 10.111.0.2 primary preferred
set routing-options autonomous-system 100
set protocols bgp group mnha_r0 type internal
set protocols bgp group mnha_r0 local-address 10.4.0.2
set protocols bgp group mnha_r0 neighbor 10.4.0.1
set protocols bgp group mnha_r0 bfd-liveness-detection minimum-interval 500
set protocols bgp group mnha_r0 bfd-liveness-detection minimum-receive-interval 500
set protocols bgp group mnha_r0 bfd-liveness-detection multiplier 3
set protocols bgp group mnha_r0 local-as 100
set protocols bgp group mnha_r0_b type internal
set protocols bgp group mnha_r0_b local-address 10.5.0.2
set protocols bgp group mnha_r0_b neighbor 10.5.0.1
set protocols bgp group mnha_r0_b bfd-liveness-detection minimum-interval 500
set protocols bgp group mnha_r0_b bfd-liveness-detection minimum-receive-interval 500
set protocols bgp group mnha_r0_b bfd-liveness-detection multiplier 3
set protocols bgp group mnha_r0_b local-as 100

```

## Configuration

### Step-by-Step Procedure

We're showing the configuration of SRX-01 in the step-by-step procedure.

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see [Using the CLI Editor in Configuration Mode](#) in the [CLI User Guide](#).

## 1. Configure Interfaces.

```
[edit]
user@host# set interfaces ge-0/0/3 description "trust" unit 0 family inet address
10.2.0.2/16
user@host# set interfaces ge-0/0/4 description "untrust" unit 0 family inet address
10.4.0.1/16
user@host# set interfaces ge-0/0/2 description "ha_link" unit 0 family inet address
10.22.0.1/24
```

We're using ge-0/0/3 and ge-0/0/4 interfaces to connect to the upstream and downstream routers and using ge-0/0/2 interface to setup the ICL.

## 2. Configure the loopback interfaces.

```
[edit]
user@host# set interfaces lo0 description "untrust" unit 0 family inet address 10.11.0.1/32
user@host# set interfaces lo0 description "untrust" unit 0 family inet address 10.11.0.2/32
user@host# set interfaces lo0 description "untrust" unit 0 family inet address 10.11.0.3/32
```

The IP address (10.11.0.1) assigned to the loopback interface will be used as the floating IP address.

Using the loopback interface ensures that at any given point, traffic from the adjacent routers will be steered toward the floating IP address (that is, toward the active node).

## 3. Configure security zones, assign interfaces to the zones, and specify the allowed system services for the security zones.

```
[edit]
user@host# set security zones security-zone untrust host-inbound-traffic system-services ike
user@host# set security zones security-zone untrust host-inbound-traffic system-services
ping
user@host# set security zones security-zone untrust host-inbound-traffic protocols bfd
user@host# set security zones security-zone untrust host-inbound-traffic protocols bgp
user@host# set security zones security-zone untrust interfaces ge-0/0/4
user@host# set security zones security-zone untrust interfaces lo0.0
user@host# set security zones security-zone trust host-inbound-traffic system-services all
user@host# set security zones security-zone trust host-inbound-traffic protocols all
user@host# set security zones security-zone trust interfaces ge-0/0/3
user@host# set security zones security-zone halink host-inbound-traffic system-services ike
user@host# set security zones security-zone halink host-inbound-traffic system-services ping
user@host# set security zones security-zone halink host-inbound-traffic system-services
```

```

high-availability
user@host# set security zones security-zone halink host-inbound-traffic system-services ssh
user@host# set security zones security-zone halink host-inbound-traffic protocols bfd
user@host# set security zones security-zone halink host-inbound-traffic protocols bgp
user@host# set security zones security-zone halink interfaces ge-0/0/2

```

Assign the interfaces ge-0/0/3 and ge-0/0/4 the trust and untrust zones respectively. Assign the lo0.0 interface to the untrust zone to connect over the public IP network. Assign the interface ge-0/0/2 to the halink zone. You use this zone to set up the ICL.

4. Configure routing options.

```

[edit]
user@host# set routing-options autonomous-system 100
user@host# set routing-options static route 10.1.0.0/16 next-hop 10.2.0.1
user@host# set routing-options static route 10.6.0.0/16 next-hop 10.4.0.2
user@host# set routing-options static route 10.111.0.1 next-hop 10.2.0.1
user@host# set routing-options static route 10.111.0.2 next-hop 10.4.0.2

```

5. Configure both local node and peer node details such as node ID, IP addresses of local node and peer node, and the interface for the peer node.

```

[edit]
user@host# set chassis high-availability local-id 1
user@host# set chassis high-availability local-id local-ip 10.22.0.1
user@host# set chassis high-availability peer-id 2 peer-ip 10.22.0.2
user@host# set chassis high-availability peer-id 2 interface ge-0/0/2.0
user@host# set chassis high-availability peer-id 2 vpn-profile IPSEC_VPN_ICL

```

You'll use the ge-0/0/2 interface for communicating with the peer node using the ICL.

6. Attach the IPsec VPN profile IPSEC\_VPN\_ICL to the peer node.

```

[edit]
user@host# set chassis high-availability peer-id 2 vpn-profile IPSEC_VPN_ICL

```

You'll need this configuration to establish a secure ICL link between the nodes.

7. Configure Bidirectional Forwarding Detection (BFD) protocol options for the peer node.

```
[edit]
user@host# set chassis high-availability peer-id 2 liveness-detection minimum-interval 400
user@host# set chassis high-availability peer-id 2 liveness-detection multiplier 5
```

8. Associate the peer node ID 2 to the services redundancy group 0 (SRG0).

```
[edit]
user@host# set chassis high-availability services-redundancy-group 0 peer-id 2
```

9. Configure the services redundancy group 1 (SRG1).

```
[edit]
user@host# set chassis high-availability services-redundancy-group 0 peer-id 2
user@host# set chassis high-availability services-redundancy-group 1 deployment-type routing
user@host# set chassis high-availability services-redundancy-group 1 peer-id 2
```

In this step, you are specifying deployment type as routing because you are setting up Multinode High Availability in a Layer 3 network.

.

10. Setup activeness determination parameters for SRG1.

```
[edit]
user@host# set chassis high-availability services-redundancy-group 1 activeness-probe dest-
ip 10.111.0.1
user@host# set chassis high-availability services-redundancy-group 1 activeness-probe dest-
ip src-ip 10.11.0.1
```

Use the floating IP address as source IP address (10.11.0.1) and IP addresses of the upstream routers as the destination IP address (10.111.0.1) for the activeness determination probe.

You can configure up to 64 IP addresses for IP monitoring and activeness probing. The total 64 IP addresses is sum of the number of IPv4 and IPv6 addresses)

11. Configure BFD monitoring parameters for the SRG1 to detect failures in network.

```
[edit]
user@host# set chassis high-availability services-redundancy-group 1 monitor bfd-liveliness
```



```

10.4.0.2 src-ip 10.4.0.1
user@host# set chassis high-availability services-redundancy-group 1 monitor bfd-liveliness
10.4.0.2 session-type singlehop
user@host# set chassis high-availability services-redundancy-group 1 monitor bfd-liveliness
10.4.0.2 interface ge-0/0/4.0

```

**12. Configure an active signal route required for activeness enforcement.**

```

[edit]
user@host# set chassis high-availability services-redundancy-group 1 active-signal-route
10.39.1.1
user@host# set chassis high-availability services-redundancy-group 1 backup-signal-route
10.39.1.2
user@host# set chassis high-availability services-redundancy-group 1 preemption
user@host# set chassis high-availability services-redundancy-group 1 activeness-priority 200

```

The active signal route IP address you assign is used for route preference advertisement. You must specify the active signal route along with the route-exists policy in the policy-options statement.

**13. Configure the security policy.**

```

[edit]
user@host# set security policies default-policy permit-all

```

Ensure you have configured security policies as per your network requirements.

**14. Configure CA certificates as per your requirements.**

```

[edit]
user@host# set security pki ca-profile Root-CA ca-identity Root-CA
user@host# set security pki ca-profile Root-CA enrollment url http://10.157.69.204/certsrv/
mscep/mscep.dll
user@host# set security pki ca-profile Root-CA revocation-check disable

```

**15. Define Internet Key Exchange (IKE) configuration for Multinode High Availability. An IKE configuration defines the algorithms and keys used to establish a secure connection.**

```

[edit]
user@host# set security ike proposal MNHA_IKE_PROP description mnha_link_encr_tunnel
user@host# set security ike proposal MNHA_IKE_PROP authentication-method pre-shared-keys

```

```

user@host# set security ike proposal MNHA_IKE_PROP dh-group group14
user@host# set security ike proposal MNHA_IKE_PROP authentication-algorithm sha-256
user@host# set security ike proposal MNHA_IKE_PROP encryption-algorithm aes-256-cbc
user@host# set security ike proposal MNHA_IKE_PROP lifetime-seconds 3600
user@host# set security ike policy MNHA_IKE_POL description mnha_link_encr_tunnel
user@host# set security ike policy MNHA_IKE_POL proposals MNHA_IKE_PROP
user@host# set security ike policy MNHA_IKE_POL pre-shared-key ascii-text "$ABC123"
user@host# set security ike gateway MNHA_IKE_GW ike-policy MNHA_IKE_POL
user@host# set security ike gateway MNHA_IKE_GW version v2-only

```

For the Multinode High availability feature, you must configure the IKE version as v2-only

16. Specify the IPsec proposal protocol and encryption algorithm. Specify IPsec options to create a IPsec tunnel between two participant devices to secure VPN communication.

```

[edit]
user@host# set security ipsec proposal MNHA_IPSEC_PROP description mnha_link_encr_tunnel
user@host# set security ipsec proposal MNHA_IPSEC_PROP protocol esp
user@host# set security ipsec proposal MNHA_IPSEC_PROP encryption-algorithm aes-256-gcm
user@host# set security ipsec proposal MNHA_IPSEC_PROP lifetime-seconds 3600
user@host# set security ipsec policy MNHA_IPSEC_POL description mnha_link_encr_tunnel
user@host# set security ipsec policy MNHA_IPSEC_POL proposals MNHA_IPSEC_PROP
user@host# set security ipsec vpn IPSEC_VPN_ICL ha-link-encryption
user@host# set security ipsec vpn IPSEC_VPN_ICL ike gateway MNHA_IKE_GW
user@host# set security ipsec vpn IPSEC_VPN_ICL ike ipsec-policy MNHA_IPSEC_POL

```

Specifying the ha-link-encryption option encrypts the ICL to secure high availability traffic flow between the nodes.

The same VPN name IPSEC\_VPN\_ICL must be mentioned for *vpn\_profile* in chassis high availability configuration.

17. Configure policy options.

```

[edit]
user@host# set policy-options condition active_route_exists if-route-exists address-family
inet 10.39.1.1 table inet.0
user@host# set policy-options condition backup_route_exists if-route-exists address-family
inet 10.39.1.2 table inet.0
user@host# set policy-options policy-statement mnha-route-policy term 1 from protocol static
user@host# set policy-options policy-statement mnha-route-policy term 1 from protocol direct
user@host# set policy-options policy-statement mnha-route-policy term 1 from condition
active_route_exists

```

```

user@host# set policy-options policy-statement mnha-route-policy term 1 then accept metric
10
user@host# set policy-options policy-statement mnha-route-policy term 2 from protocol static
user@host# set policy-options policy-statement mnha-route-policy term 2 from protocol
directuser@host# set policy-options policy-statement mnha-route-policy term 2 from
condition backup_route_exists
user@host# set policy-options policy-statement mnha-route-policy term 2 then accept metric
20
user@host# set policy-options policy-statement mnha-route-policy term 3 from protocol static
user@host# set policy-options policy-statement mnha-route-policy term 3 from protocol direct
user@host# set policy-options policy-statement mnha-route-policy term 3 then accept metric
30
user@host# set policy-options policy-statement mnha-route-policy term default then reject

```

Configure the active signal route 10.39.1.1 with the route match condition (if-route-exists). The Multinode High Availability adds this route to the routing table when the node moves to the active role. The node also starts advertising the higher preference route. Configure the back up signal route (10.39.1.2) to advertise the backup node with a medium priority. In case of any failures, the high availability link goes down and the current active node releases it's primary role and removes the active-signal-route. Now the backup node detects the condition through it's probes and transitions to the active role. The route preference is swapped to drive all the traffic to the new active node

#### 18. Configure BFD peering sessions options and specify liveness detection timers.

```

[edit]
user@host# set protocols bgp group trust type internal
user@host# set protocols bgp group trust local-address 10.2.0.2
user@host# set protocols bgp group trust export mnha-route-policy
user@host# set protocols bgp group trust neighbor 10.2.0.1
user@host# set protocols bgp group trust bfd-liveness-detection minimum-interval 500
user@host# set protocols bgp group trust bfd-liveness-detection minimum-receive-interval 500
user@host# set protocols bgp group trust bfd-liveness-detection multiplier 3
user@host# set protocols bgp group trust local-as 100
user@host# set protocols bgp group untrust type internal
user@host# set protocols bgp group untrust local-address 10.4.0.1
user@host# set protocols bgp group untrust export mnha-route-policy
user@host# set protocols bgp group untrust neighbor 10.4.0.2
user@host# set protocols bgp group untrust bfd-liveness-detection minimum-interval 500
user@host# set protocols bgp group untrust bfd-liveness-detection minimum-receive-interval
500

```

```
user@host# set protocols bgp group untrust bfd-liveness-detection multiplier 3
user@host# set protocols bgp group untrust local-as
```

## Configuration Option for Software Upgrades (Optional)

In Multinode High Availability, during software upgrades, you can divert the traffic by changing the route. Use the following steps to add install route on failure configuration. Here, traffic can still go through the node and interface remains up.

Check ["Software Upgrade in Multinode High Availability" on page 885](#) for details.

1. Create a dedicated custom virtual router for the route used for diverting traffic during the upgrade.

```
user@host# set routing-instances MNHA-signal-routes instance-type virtual-router
```

2. Configure install route on failure statement for the SRG0.

```
user@host# set chassis high-availability services-redundancy-group 0 install-on-failure-route
10.39.1.3 routing-instance MNHA-signal-routes
user@host# set chassis high-availability services-redundancy-group 1 active-signal-route
10.39.1.1 routing-instance MNHA-signal-routes
user@host# set chassis high-availability services-redundancy-group 1 backup-signal-route
10.39.1.2 routing-instance MNHA-signal-routes
```

The routing table installs the route mentioned in the statement when the node fails.

3. Create a matching routing policy which refers the route as condition with the `route-exists` attribute.  
Example: Following configuration snippets show that you have configured the route with IP address 10.39.1.3 for SRG0 as install on failure route. The routing policy statement includes the route 10.39.1.3 as the `if-route-exists` condition and the policy statement refers the condition as one of the matching term.

```
user@host# set policy-options condition active_route_exists if-route-exists address-family
inet 10.39.1.1/32
user@host# set policy-options condition active_route_exists if-route-exists address-family
inet table MNHA-signal-routes.inet.0
user@host# set policy-options condition backup_route_exists if-route-exists address-family
inet 10.39.1.2/32
user@host# set policy-options condition backup_route_exists if-route-exists address-family
```

```

inet table MNHA-signal-routes.inet.0
user@host# set policy-options condition failure_route_exists if-route-exists address-family
inet 10.39.1.3/32
user@host# set policy-options condition failure_route_exists if-route-exists address-family
inet table MNHA-signal-routes.inet.0

```

```

user@host# set policy-options policy-statement mnha-route-policy term 4 from protocol static
user@host# set policy-options policy-statement mnha-route-policy term 4 from protocol direct
user@host# set policy-options policy-statement mnha-route-policy term 4 from condition
failure_route_exists
user@host# set policy-options policy-statement mnha-route-policy term 4 then metric 100
user@host# set policy-options policy-statement mnha-route-policy term 4 then accept

```

## Results (SRX-1)

From configuration mode, confirm your configuration by entering the following commands.

If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```

[edit]
user@host# show chassis high-availability
local-id 1 local-ip 10.22.0.1;
peer-id 2 {
    peer-ip 10.22.0.2;
    interface ge-0/0/2.0;
    vpn-profile IPSEC_VPN_ICL;
    liveness-detection {
        minimum-interval 400;
        multiplier 5;
    }
}
services-redundancy-group 0 {
    peer-id {
        2;
    }
}
services-redundancy-group 1 {
    deployment-type routing;
}

```

```

peer-id {
    2;
}
activeness-probe {
    dest-ip {
        10.111.0.1;
        src-ip 10.11.0.1;
    }
}
monitor {
    bfd-liveliness 10.4.0.2 {
        src-ip 10.4.0.1;
        session-type singlehop;
        interface ge-0/0/4.0;
    }
}
active-signal-route {
    10.39.1.1;
}
backup-signal-route {
    10.39.1.2;
}
preemption;
activeness-priority 200;
}

```

```

[edit]
user@host# show security ike
proposal MNHA_IKE_PROP {
    description mnha_link_encr_tunnel;
    authentication-method pre-shared-keys;
    dh-group group14;
    authentication-algorithm sha-256;
    encryption-algorithm aes-256-cbc;
    lifetime-seconds 3600;
}
policy MNHA_IKE_POL {
    description mnha_link_encr_tunnel;
    proposals MNHA_IKE_PROP ;
    pre-shared-key ascii-text "$ABC123"; ## SECRET-DATA
}

```

```

gateway MNHA_IKE_GW {
    ike-policy MNHA_IKE_POL ;
    version v2-only;
}

```

```

[edit]
user@host# show security ipsec
proposal MNHA_IPSEC_PROP {
    description mnha_link_encr_tunnel;
    protocol esp;
    encryption-algorithm aes-256-gcm;
    lifetime-seconds 3600;
}
policy MNHA_IPSEC_POL {
    description mnha_link_encr_tunnel;
    proposals MNHA_IPSEC_PROP;
}
vpn IPSEC_VPN_ICL {
    ha-link-encryption;
    ike {
        gateway MNHA_IKE_GW;
        ipsec-policy MNHA_IPSEC_POL;
    }
}

```

```

[edit]
user@host# show policy-options
policy-statement mnha-route-policy {
    term 1 {
        from {
            protocol [ static direct ];
            condition active_route_exists;
        }
        then {
            metric 10;
            accept;
        }
    }
    term 2 {

```

```

        from {
            protocol [ static direct ];
            condition backup_route_exists;
        }
        then {
            metric 20;
            accept;
        }
    }
    term 3 {
        from protocol [ static direct ];
        then {
            metric 30;
            accept;
        }
    }
    term default {
        then reject;
    }
}

condition active_route_exists {
    if-route-exists {
        address-family {
            inet {
                10.39.1.1/32;
                table inet.0;
            }
        }
    }
}

condition backup_route_exists {
    if-route-exists {
        address-family {
            inet {
                10.39.1.2/32;
                table inet.0;
            }
        }
    }
}

```



```
}
```

```
[edit]
user@host# show routing-options
autonomous-system 100;
static {
    route 10.1.0.0/16 next-hop 10.2.0.1;
    route 10.6.0.0/16 next-hop 10.4.0.2;
    route 10.111.0.1/32 next-hop 10.2.0.1;
    route 10.111.0.2/32 next-hop 10.4.0.2;
}
```

```
[edit]
user@host# show security zones security-zone
security-zone untrust {
    host-inbound-traffic {
        system-services {
            ike;
            ping;
        }
        protocols {
            bfd;
            bgp;
        }
    }
    interfaces {
        ge-0/0/4.0;
        lo0.0;
    }
}
security-zone trust {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            all;
        }
    }
}
```

```

    interfaces {
        ge-0/0/3.0;
    }
}
security-zone halink {
    host-inbound-traffic {
        system-services {
            ike;
            ping;
            high-availability;
            ssh;
        }
        protocols {
            bfd;
            bgp;
        }
    }
    interfaces {
        ge-0/0/2.0;
    }
}
}

```

```

[edit]
user@host# show interfaces
ge-0/0/2 {
    description ha_link;
    unit 0 {
        family inet {
            address 10.22.0.1/24;
        }
    }
}
ge-0/0/3 {
    description trust;
    unit 0 {
        family inet {
            address 10.2.0.2/16;
        }
    }
}
}

```

```

ge-0/0/4 {
    description untrust;
    unit 0 {
        family inet {
            address 10.4.0.1/16;
        }
    }
}
lo0 {
    description untrust;
    unit 0 {
        family inet {
            address 10.11.0.1/32;
            address 10.11.0.2/32;
            address 10.11.0.3/32;
        }
    }
}

```

If you are done configuring the device, enter `commit` from configuration mode.

## Results (SRX-2)

From configuration mode, confirm your configuration by entering the following commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```

[edit]
user@host# show chassis high-availability
local-id 2 local-ip 10.22.0.2;
peer-id 1 {
    peer-ip 10.22.0.1;
    interface ge-0/0/2.0;
    vpn-profile IPSEC_VPN_ICL;
    liveness-detection {
        minimum-interval 400;
        multiplier 5;
    }
}
services-redundancy-group 0 {
    peer-id {
        1;
    }
}

```

```

    }
}
services-redundancy-group 1 {
    deployment-type routing;
    peer-id {
        1;
    }
    activeness-probe {
        dest-ip {
            10.111.0.1;
            src-ip 10.11.0.1;
        }
    }
}
monitor {
    bfd-liveliness 10.5.0.2 {
        src-ip 10.5.0.1;
        session-type singlehop;
        interface ge-0/0/4.0;
    }
}
active-signal-route {
    10.39.1.1;
}
backup-signal-route {
    10.39.1.2;
}
activeness-priority 1;
}

```

```

[edit]
user@host# show security ike
proposal MNHA_IKE_PROP {
    description mnha_link_encr_tunnel;
    authentication-method pre-shared-keys;
    dh-group group14;
    authentication-algorithm sha-256;
    encryption-algorithm aes-256-cbc;
    lifetime-seconds 3600;
}
policy MNHA_IKE_POL {
    description mnha_link_encr_tunnel;

```

```

    proposals MNHA_IKE_PROP ;
    pre-shared-key ascii-text "$ABC123"; ## SECRET-DATA
}
gateway MNHA_IKE_GW {
    ike-policy MNHA_IKE_POL ;
    version v2-only;
}

```

```

[edit]
user@host# show security ipsec
proposal MNHA_IPSEC_PROP {
    description mnha_link_encr_tunnel;
    protocol esp;
    encryption-algorithm aes-256-gcm;
    lifetime-seconds 3600;
}
policy MNHA_IPSEC_POL {
    description mnha_link_encr_tunnel;
    proposals MNHA_IPSEC_PROP;
}
vpn IPSEC_VPN_ICL {
    ha-link-encryption;
    ike {
        gateway MNHA_IKE_GW;
        ipsec-policy MNHA_IPSEC_POL;
    }
}

```

```

[edit]
user@host# show policy-options

route-filter-list loopback {
    10.11.0.0/24 orlonger;
}
route-filter-list ipsec {
    10.6.0.0/16 orlonger;
}
policy-statement mnha-route-policy {
    term 1 {
        from {

```

```

        protocol [ static direct ];
        condition active_route_exists;
    }
    then {
        metric 10;
        accept;
    }
}
term 2 {
    from {
        protocol [ static direct ];
        condition backup_route_exists;
    }
    then {
        metric 20;
        accept;
    }
}
term 3 {
    from protocol [ static direct ];
    then {
        metric 30;
        accept;
    }
}
term default {
    then reject;
}
}
condition active_route_exists {
    if-route-exists {
        address-family {
            inet {
                10.39.1.1/32;
                table inet.0;
            }
        }
    }
}
condition backup_route_exists {
    if-route-exists {
        address-family {
            inet {

```

```

        10.39.1.2/32;
        table inet.0;
    }
}
}
}
}

```

```

[edit]
user@host# show routing-options
autonomous-system 100;
static {
    route 10.1.0.0/16 next-hop 10.3.0.1;
    route 10.6.0.0/16 next-hop 10.5.0.2;
    route 10.111.0.1/32 next-hop 10.3.0.1;
    route 10.111.0.2/32 next-hop 10.5.0.2;
}

```

```

[edit]
user@host# show security zones
security-zone untrust {
    host-inbound-traffic {
        system-services {
            ike;
            ping;
        }
        protocols {
            bfd;
            bgp;
        }
    }
    interfaces {
        ge-0/0/4.0;
        lo0.0;
    }
}
security-zone trust {
    host-inbound-traffic {
        system-services {
            all;
        }
    }
}

```

```

        protocols {
            all;
        }
    }
    interfaces {
        ge-0/0/3.0;
    }
}
security-zone halink {
    host-inbound-traffic {
        system-services {
            ike;
            ping;
            high-availability;
            ssh;
        }
        protocols {
            bfd;
            bgp;
        }
    }
    interfaces {
        ge-0/0/2.0;
    }
}
}

```

```

[edit]
user@host# show interfaces
root@10.52.45.4# show interfaces
ge-0/0/2 {
    description ha_link;
    unit 0 {
        family inet {
            address 10.22.0.2/24;
        }
    }
}
ge-0/0/3 {
    description trust;
    unit 0 {
        family inet {

```



```

        address 10.3.0.2/16;
    }
}
ge-0/0/4 {
    description untrust;
    unit 0 {
        family inet {
            address 10.5.0.1/16;
        }
    }
}
lo0 {
    description untrust;
    unit 0 {
        family inet {
            address 10.11.0.1/32;
            address 10.11.0.2/32;
            address 10.11.0.3/32;
        }
    }
}
}

```

If you are done configuring the device, enter `commit` from configuration mode.

On your security devices, you'll get the following message that asks you to reboot the device:

```

user@host# commit
warning: High Availability Mode changed, please reboot the device to avoid undesirable behavior
commit complete

```

## Verification

### IN THIS SECTION

- [Check Multinode High Availability Details | 704](#)
- [Check Multinode High Availability Peer Node Status | 707](#)
- [Check Multinode High Availability Service Redundancy Groups | 709](#)
- [Verify the Multinode High Availability Status Before and After Failover | 711](#)

- [Verify Interchassis Link \(ICL\) Encryption Status | 713](#)
- [Verify Link Encryption Tunnel Statistics | 715](#)
- [Verify Interchassis Link Active Peers | 716](#)

Confirm that the configuration is working properly.

## Check Multinode High Availability Details

### Purpose

View and verify the details of the Multinode High Availability setup configured on your security device.

### Action

From operational mode, run the following command:

On SRX-1

```
user@host> show chassis high-availability information
Node failure codes:
  HW  Hardware monitoring    LB  Loopback monitoring
  MB  Mbuf monitoring        SP  SPU monitoring
  CS  Cold Sync monitoring   SU  Software Upgrade

Node Status: ONLINE
Local-id: 1
Local-IP: 10.22.0.1
HA Peer Information:

  Peer Id: 2      IP address: 10.22.0.2    Interface: ge-0/0/2.0
  Routing Instance: default
  Encrypted: YES   Conn State: UP
  Cold Sync Status: COMPLETE

Services Redundancy Group: 0
  Current State: ONLINE
  Peer Information:
    Peer Id: 2
```

SRG failure event codes:

BF BFD monitoring  
 IP IP monitoring  
 IF Interface monitoring  
 CP Control Plane monitoring

Services Redundancy Group: 1

Deployment Type: ROUTING  
 Status: ACTIVE  
 Activeness Priority: 200  
 Preemption: ENABLED  
 Process Packet In Backup State: NO  
 Control Plane State: READY  
 System Integrity Check: N/A  
 Failure Events: NONE  
 Peer Information:  
 Peer Id: 2  
 Status : BACKUP  
 Health Status: HEALTHY  
 Failover Readiness: READY

## On SRX-2

user@host> **show chassis high-availability information**

Node failure codes:

HW	Hardware monitoring	LB	Loopback monitoring
MB	Mbuf monitoring	SP	SPU monitoring
CS	Cold Sync monitoring	SU	Software Upgrade

Node Status: ONLINE

Local-id: 2

Local-IP: 10.22.0.2

HA Peer Information:

Peer Id: 1	IP address: 10.22.0.1	Interface: ge-0/0/2.0
Routing Instance: default		
Encrypted: YES	Conn State: UP	
Cold Sync Status: COMPLETE		

Services Redundancy Group: 0

Current State: ONLINE

Peer Information:

Peer Id: 1

SRG failure event codes:

BF BFD monitoring

IP IP monitoring

IF Interface monitoring

CP Control Plane monitoring

Services Redundancy Group: 1

Deployment Type: ROUTING

Status: BACKUP

Activeness Priority: 1

Preemption: DISABLED

Process Packet In Backup State: NO

Control Plane State: READY

System Integrity Check: COMPLETE

Failure Events: NONE

Peer Information:

Peer Id: 1

Status : ACTIVE

Health Status: HEALTHY

Failover Readiness: N/A

## Meaning

Verify these details from the command output:

- Local node and peer node details such as IP address and ID.
- The field Encrypted: YES indicates that the traffic is protected.
- The field Deployment Type: ROUTING indicates a Layer 3 mode configuration—that is, the network has routers on both sides.
- The field Services Redundancy Group: 1 indicates the status of the SRG1 (ACTIVE or BACKUP) on that node.

Check Multinode High Availability Peer Node Status

Purpose

View and verify the peer node details.

Action

From operational mode, run the following command:

SRX-1

```
user@host> user@host> show chassis high-availability peer-info
HA Peer Information:

Peer-ID: 2      IP address: 10.22.0.2      Interface: ge-0/0/2.0
Routing Instance: default
Encrypted: YES   Conn State: UP
Cold Sync Status: COMPLETE
Internal Interface: st0.16000
Internal Local-IP: 180.100.1.1
Internal Peer-IP: 180.100.1.2
Internal Routing-instance: __juniper_private1__
Packet Statistics:
    Receive Error : 0      Send Error : 0

    Packet-type      Sent      Received

    SRG Status Msg      4          4

    SRG Status Ack      4          3

    Attribute Msg      4          2

    Attribute Ack      2          2
```

## SRX-2

```

user@host> show chassis high-availability peer-info
HA Peer Information:

Peer-ID: 1      IP address: 10.22.0.1      Interface: ge-0/0/2.0
Routing Instance: default
Encrypted: YES   Conn State: UP
Cold Sync Status: COMPLETE
Internal Interface: st0.16000
Internal Local-IP: 180.100.1.2
Internal Peer-IP: 180.100.1.1
Internal Routing-instance: __juniper_private1__

Packet Statistics:
    Receive Error : 0      Send Error : 0

    Packet-type      Sent      Received

    SRG Status Msg      4          3

    SRG Status Ack      3          4

    Attribute Msg      3          2

    Attribute Ack      2          2

```

**Meaning**

Verify these details from the command output:

- Peer node details such as interface used, IP address, and ID
- Encryption status, connection status, and cold synchronization status
- Packet statistics across the node.

## Check Multinode High Availability Service Redundancy Groups

### Purpose

Verify that the SRGs are configured and working correctly.

### Action

From operational mode, run the following command:

For SRG0:

```
user@host> show chassis high-availability services-redundancy-group 0
Services Redundancy Group: 0
    Current State: ONLINE
    Peer Information:
        Peer Id: 2
```

For SRG1:

```
user@host> show chassis high-availability services-redundancy-group 1
SRG failure event codes:
    BF  BFD monitoring
    IP  IP monitoring
    IF  Interface monitoring
    CP  Control Plane monitoring

Services Redundancy Group: 1
    Deployment Type: ROUTING
    Status: ACTIVE
    Activeness Priority: 200
    Preemption: ENABLED
    Process Packet In Backup State: NO
    Control Plane State: READY
    System Integrity Check: N/A
    Failure Events: NONE
    Peer Information:
        Peer Id: 2
        Status : BACKUP
        Health Status: HEALTHY
        Failover Readiness: READY
```

## Signal Route Info:

Active Signal Route:

IP: 10.39.1.1

Routing Instance: default

Status: INSTALLED

Backup Signal Route:

IP: 10.39.1.2

Routing Instance: default

Status: NOT INSTALLED

## Split-brain Prevention Probe Info:

DST-IP: 10.111.0.1

SRC-IP: 10.11.0.1

Routing Instance: default

Status: NOT RUNNING

Result: N/A

Reason: N/A

## BFD Monitoring:

Status: UP

SRC-IP: 10.4.0.1      DST-IP: 10.4.0.2

Routing Instance: default

Type: SINGLE-HOP

IFL Name: ge-0/0/4.0

State: UP

**Meaning**

Verify these details from the command output:

- Peer node details such as deployment type, status, and active and back up signal routes.
- Virtual IP Information such as IP address and virtual MAC address.
- IP monitoring and BFD monitoring status.



## Verify the Multinode High Availability Status Before and After Failover

### Purpose

Check the change in node status before and after failover in a Multinode High Availability setup.

### Action

To check the Multinode High Availability status on the backup node (SRX-2), run the following command from operational mode:

```
user@host> show chassis high-availability information
Node failure codes:
    HW  Hardware monitoring    LB  Loopback monitoring
    MB  Mbuf monitoring        SP  SPU monitoring
    CS  Cold Sync monitoring    SU  Software Upgrade

Node Status: ONLINE
Local-id: 2
Local-IP: 10.22.0.2
HA Peer Information:

    Peer Id: 1      IP address: 10.22.0.1    Interface: ge-0/0/2.0
    Routing Instance: default
    Encrypted: YES   Conn State: UP
    Cold Sync Status: COMPLETE

Services Redundancy Group: 0
    Current State: ONLINE
    Peer Information:
        Peer Id: 1

SRG failure event codes:
    BF  BFD monitoring
    IP  IP monitoring
    IF  Interface monitoring
    CP  Control Plane monitoring

Services Redundancy Group: 1
    Deployment Type: ROUTING
    Status: BACKUP
    Activeness Priority: 1
```

```

Preemption: DISABLED
Process Packet In Backup State: NO
Control Plane State: READY
System Integrity Check: COMPLETE
Failure Events: NONE
Peer Information:
  Peer Id: 1
  Status : ACTIVE
  Health Status: HEALTHY
  Failover Readiness: N/A

```

Under the Services Redundancy Group: 1 section, you can see the Status: BACKUP field. This field value indicates that the status of SRG 1 is backup.

Initiate the failover on the active node (SRX-1 device) and again run the command on the backup node (SRX-2 device).

```

user@host> show chassis high-availability information
Node failure codes:
  HW  Hardware monitoring   LB  Loopback monitoring
  MB  Mbuf monitoring       SP  SPU monitoring
  CS  Cold Sync monitoring  SU  Software Upgrade

Node Status: ONLINE
Local-id: 2
Local-IP: 10.22.0.2
HA Peer Information:

  Peer Id: 1      IP address: 10.22.0.1   Interface: ge-0/0/2.0
  Routing Instance: default
  Encrypted: YES   Conn State: DOWN
  Cold Sync Status: IN PROGRESS

Services Redundancy Group: 0
  Current State: ONLINE
  Peer Information:
    Peer Id: 1

SRG failure event codes:
  BF  BFD monitoring
  IP  IP monitoring
  IF  Interface monitoring

```

```
CP Control Plane monitoring
```

```
Services Redundancy Group: 1
```

```
Deployment Type: ROUTING
```

```
Status: ACTIVE
```

```
Activeness Priority: 1
```

```
Preemption: DISABLED
```

```
Process Packet In Backup State: NO
```

```
Control Plane State: READY
```

```
System Integrity Check: N/A
```

```
Failure Events: NONE
```

```
Peer Information:
```

```
Peer Id: 1
```

```
Status : BACKUP
```

```
Health Status: HEALTHY
```

```
Failover Readiness: READY
```

Note that under the Services Redundancy Group: 1 section, the status of SRG1 has changed from **BACKUP** to **ACTIVE**.

You can also see peer node details under the Peer Information section. The output shows the status of peer as **BACKUP**.

## Verify Interchassis Link (ICL) Encryption Status

### Purpose

Verify the interchassis link (ICL) status.

### Action

From operational mode, run the following command:

```
user@host> show security ipsec security-associations ha-link-encryption detail
```

```
ID: 495001 Virtual-system: root, VPN Name: IPSEC_VPN_ICL
```

```
Local Gateway: 10.22.0.1, Remote Gateway: 10.22.0.2
```

```
Traffic Selector Name: __IPSEC_VPN_ICL__multi_node__
```

```
Local Identity: ipv4(180.100.1.1-180.100.1.1)
```

```
Remote Identity: ipv4(180.100.1.2-180.100.1.2)
```

```
TS Type: traffic-selector
```

```
Version: IKEv2
```

```
PFS group: N/A
```

```

DF-bit: clear, Copy-Outer-DSCP Disabled, Bind-interface: st0.16000, Tunnel MTU: 0, Policy-
name: MNHA_IPSEC_POL
Port: 500, Nego#: 0, Fail#: 0, Def-Del#: 0 Flag: 0
Multi-sa, Configured SAs# 0, Negotiated SAs#: 0
HA Link Encryption Mode: Multi-Node
Location: FPC -, PIC -, KMD-Instance -
Anchorship: Thread -
Distribution-Profile: default-profile
Direction: inbound, SPI: 0x0005a7ec, AUX-SPI: 0
                , VPN Monitoring: -
    Hard lifetime: Expires in 3597 seconds
    Lifesize Remaining: Unlimited
    Soft lifetime: Expires in 2900 seconds
    Mode: Tunnel(0 0), Type: dynamic, State: installed
    Protocol: ESP, Authentication: aes256-gcm, Encryption: aes-gcm (256 bits)
    Anti-replay service: counter-based enabled, Replay window size: 64
    Extended-Sequence-Number: Disabled
    tunnel-establishment: establish-tunnels-immediately
    Location: FPC 0, PIC 0, KMD-Instance 0
    Anchorship: Thread 0
    IKE SA Index: 4294966273
Direction: outbound, SPI: 0x000a2aba, AUX-SPI: 0
                , VPN Monitoring: -
    Hard lifetime: Expires in 3597 seconds
    Lifesize Remaining: Unlimited
    Soft lifetime: Expires in 2900 seconds
    Mode: Tunnel(0 0), Type: dynamic, State: installed
    Protocol: ESP, Authentication: aes256-gcm, Encryption: aes-gcm (256 bits)
    Anti-replay service: counter-based enabled, Replay window size: 64
    Extended-Sequence-Number: Disabled
    tunnel-establishment: establish-tunnels-immediately
    Location: FPC 0, PIC 0, KMD-Instance 0
    Anchorship: Thread 0
    IKE SA Index: 4294966273

```

## Meaning

The command output provides the following information:

- The local gateway and remote gateway details.
- The IPsec SA pair for each threads in PIC.

- HA link encryption mode (as shown in the following line):

```
HA Link Encryption Mode: Multi-Node
```

- Authentication and encryption algorithms used

## Verify Link Encryption Tunnel Statistics

### Purpose

Verify link encryption tunnel statistics on both active and backup nodes.

### Action

From operational mode, run the following command:

```
user@host> show security ipsec statistics ha-link-encryption
```

ESP Statistics:

Encrypted bytes: 984248

Decrypted bytes: 462519

Encrypted packets: 9067

Decrypted packets: 8797

AH Statistics:

Input bytes: 0

Output bytes: 0

Input packets: 0

Output packets: 0

Errors:

AH authentication failures: 0, Replay errors: 0

ESP authentication failures: 0, ESP decryption failures: 0

Bad headers: 0, Bad trailers: 0

Invalid SPI: 0, TS check fail: 0

Exceeds tunnel MTU: 0

Discarded: 0

### Meaning

If you see packet loss issues across a VPN, you can run the `show security ipsec statistics ha-link-encryption` command several times to verify that the encrypted and decrypted packet counters are incrementing. You should also check whether the other error counters are incrementing.

Use the `clear security ipsec security-associations ha-link-encryption` command to clear all IPsec statistics.

Verify Interchassis Link Active Peers

Purpose

View only ICL active peers, but not regular IKE active peers.

Action

From operational mode, run the following command:

SRX-1

```
user@host> show security ike active-peer ha-link-encryption
```

Remote Address	Port	Peer IKE-ID	AAA username	Assigned IP
10.22.0.2	500	10.22.0.2	not available	0.0.0.0

SRX-2

```
user@host> show security ike active-peer ha-link-encryption
```

Remote Address	Port	Peer IKE-ID	AAA username	Assigned IP
10.22.0.1	500	10.22.0.1	not available	0.0.0.0

Meaning

Command output displays only the active peer of the ICL with details such as the peer addresses and ports the active peer is using.

SEE ALSO

- [Multinode High Availability | 613](#)
- [Multinode High Availability Services | 658](#)
- [Prepare Your Environment for Multinode High Availability Deployment | 654](#)
- [Example: Configure Multinode High Availability in a Default Gateway Deployment | 717](#)
- [Example: Configure Multinode High Availability in a Hybrid Deployment | 752](#)

## Example: Configure Multinode High Availability in a Default Gateway Deployment

### SUMMARY

In this example, you'll establish Multinode High Availability between SRX Series devices in a default gateway (Layer 2 network) deployment.

### IN THIS SECTION

- [Overview | 717](#)
- [Requirements | 717](#)
- [Topology | 718](#)
- [Configuration | 720](#)
- [Verification | 740](#)

### Overview

In Multi-Node High Availability, participating SRX Series devices operate as independent nodes in a Layer 2 network. An encrypted logical interchassis link (ICL) connects the nodes over a routed network. Participating nodes backup each other to ensure a fast synchronized failover in case of system or hardware failure.

In Multinode High Availability, activeness is determined at the services redundancy group (SRG) level. The SRX Series device, on which the SRG1 is active, hosts the floating IP address and steers traffic towards it using the floating IP address. During a failover, the floating IP address moves from the old active node to the new active node and continues the communication client devices.

**NOTE:** As of Junos OS Release 22.3R1, we support a two-node configuration in the Multinode High Availability solution.

Lets start with an overview about the topology you'll be using in this example.

### Requirements

This example uses the following hardware and software components:

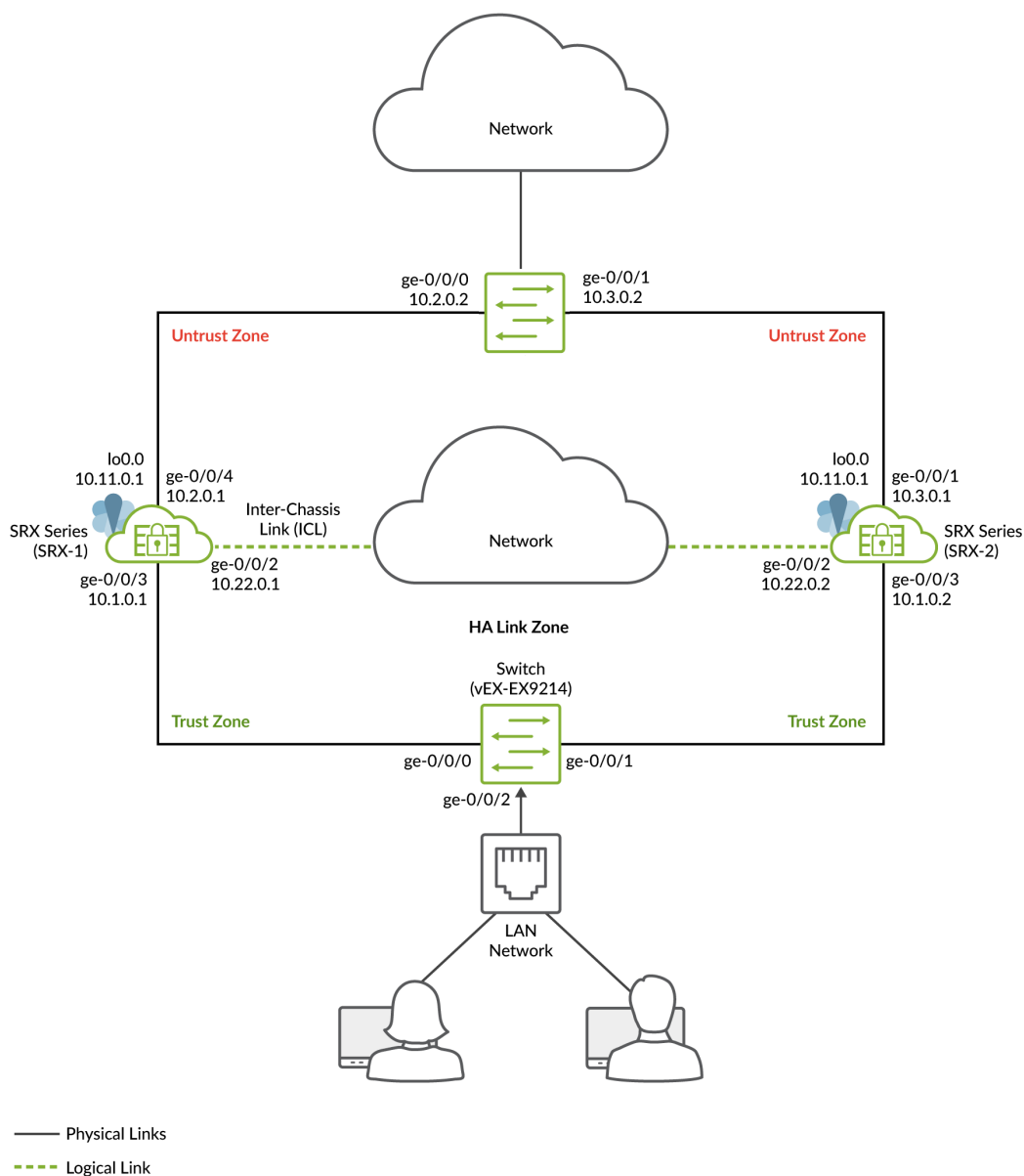
- Two SRX Series devices or vSRX instances
- Two Juniper Networks EX9214 Ethernet Switches

- Junos OS Release 22.3R1

## Topology

Figure 1 shows the topology used in this example.

**Figure 57: Multinode High Availability in Default Gateway Deployment**



As shown in the topology, two SRX Series devices are connected to switches on trust and untrust side. An encrypted logical interchassis link (ICL) connects the nodes over a routed network. The nodes



communicate with each other using a routable IP address (floating IP address) over the network. Loopback interfaces are used to host the IP addresses on SRX Series devices.

In general, you can use Aggregated Ethernet (AE) or a revenue Ethernet port on the SRX Series devices to setup an ICL connection. In this example, we've used GE ports for the ICL. We've also configured a routing instance for the ICL path to ensure maximum segmentation.

In a typical high availability deployment, you have multiple routers and switches on the northbound and southbound sides of the network. For this example, we are using two switches on both sides of SRX Series devices.

You'll perform the following tasks to build a Multinode High Availability setup:

- Configure a pair of SRX Series devices as local and peer nodes by assigning IDs.
- Configure services redundancy groups (SRGs).
- Configure virtual IP addresses for activeness determination and enforcement.
- Configure a VPN profile for the high availability (ICL) traffic using IKEv2.
- Configure appropriate security policies to manage traffic in your network.
- Configure stateless firewall filtering and quality of service (QoS) as per your network requirements.
- Configure interfaces and zones according your network requirement. You must allow services such as IKE for link encryption and SSH for configuration synchronization as host inbound system services on the security zone that is associated with the ICL.

You can configure the following options on SRG0 and SRG1:

- SRG1: Active/backup signal route, deployment type, activeness priority, preemption, virtual IP address (for default gateway deployments), activeness probing and process packet on backup.
- SRG1: BFD monitoring, IP monitoring, and interface monitoring options on SRG1.
- SRG0: shutdown on failure and install on failure route options.

When you configure monitoring (BFD or IP or Interface) options under SRG1, we recommend not to configure the shutdown-on-failure option under SRG0.

For interchassis link (ICL), we recommend the following configuration settings:

- Use a loopback (lo0) interface using an aggregated Ethernet interface (ae0), or any revenue Ethernet interface to establish the ICL. Do not to use the dedicated HA ports (control and fabric ports) if available on your SRX Series device).
- Set MTU of 1514
- Allow the following services on the security zone associated with interfaces used for ICL

- IKE, high-availability, SSH
- Protocols depends on the routing protocols you need
- BFD to monitor the neighboring routes

## Configuration

### IN THIS SECTION

- [Before You Begin | 720](#)
- [CLI Quick Configuration | 720](#)
- [Configuration | 725](#)
- [Results \(SRX-1\) | 730](#)
- [Results \(SRX-2\) | 735](#)

### Before You Begin

Install the Junos IKE package on your SRX Series. You require this step for ICL encryption.

```
user@host> request system software add optional://junos-ike.tgz
```

```
Verified junos-ike signed by PackageProductionECP256_2022 method ECDSA256+SHA256  
Rebuilding schema and Activating configuration...  
mgd: commit complete  
Restarting MGD ...
```

```
WARNING: cli has been replaced by an updated version:  
CLI release 20220208.163814_builder.r1239105 built by builder on 2022-02-08 17:07:55 UTC  
Restart cli using the new version ? [yes,no] (yes)
```

### CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the `[edit]` hierarchy level, and then enter `commit` from configuration mode.

These configurations are captured from a lab environment, and are provided for reference only. Actual configurations may vary based on the specific requirements of your environment.

## On SRX-1 Device

```

set chassis high-availability local-id 1
set chassis high-availability local-id local-ip 10.22.0.1
set chassis high-availability peer-id 2 peer-ip 10.22.0.2
set chassis high-availability peer-id 2 interface ge-0/0/2.0
set chassis high-availability peer-id 2 vpn-profile IPSEC_VPN_ICL
set chassis high-availability peer-id 2 liveness-detection minimum-interval 400
set chassis high-availability peer-id 2 liveness-detection multiplier 5
set chassis high-availability services-redundancy-group 0 peer-id 2
set chassis high-availability services-redundancy-group 1 deployment-type switching
set chassis high-availability services-redundancy-group 1 peer-id 2
set chassis high-availability services-redundancy-group 1 virtual-ip 1 ip 10.1.0.200/16
set chassis high-availability services-redundancy-group 1 virtual-ip 1 interface ge-0/0/3.0
set chassis high-availability services-redundancy-group 1 virtual-ip 1 use-virtual-mac
set chassis high-availability services-redundancy-group 1 virtual-ip 2 ip 10.2.0.200/16
set chassis high-availability services-redundancy-group 1 virtual-ip 2 interface ge-0/0/4.0
set chassis high-availability services-redundancy-group 1 virtual-ip 2 use-virtual-mac
set chassis high-availability services-redundancy-group 1 monitor interface ge-0/0/3
set chassis high-availability services-redundancy-group 1 monitor interface ge-0/0/4
set chassis high-availability services-redundancy-group 1 preemption
set chassis high-availability services-redundancy-group 1 activeness-priority 200
set security ike proposal MNHA_IKE_PROP description mnha_link_encr_tunnel
set security ike proposal MNHA_IKE_PROP authentication-method pre-shared-keys
set security ike proposal MNHA_IKE_PROP dh-group group14
set security ike proposal MNHA_IKE_PROP authentication-algorithm sha-256
set security ike proposal MNHA_IKE_PROP encryption-algorithm aes-256-cbc
set security ike proposal MNHA_IKE_PROP lifetime-seconds 3600
set security ike policy MNHA_IKE_POL description mnha_link_encr_tunnel
set security ike policy MNHA_IKE_POL proposals MNHA_IKE_PROP
set security ike policy MNHA_IKE_POL pre-shared-key ascii-text "$ABC123"
set security ike gateway MNHA_IKE_GW ike-policy MNHA_IKE_POL
set security ike gateway MNHA_IKE_GW version v2-only
set security ipsec proposal MNHA_IPSEC_PROP description mnha_link_encr_tunnel
set security ipsec proposal MNHA_IPSEC_PROP protocol esp
set security ipsec proposal MNHA_IPSEC_PROP encryption-algorithm aes-256-gcm
set security ipsec proposal MNHA_IPSEC_PROP lifetime-seconds 3600
set security ipsec policy MNHA_IPSEC_POL description mnha_link_encr_tunnel
set security ipsec policy MNHA_IPSEC_POL proposals MNHA_IPSEC_PROP
set security ipsec vpn IPSEC_VPN_ICL ha-link-encryption
set security ipsec vpn IPSEC_VPN_ICL ike gateway MNHA_IKE_GW
set security ipsec vpn IPSEC_VPN_ICL ike ipsec-policy MNHA_IPSEC_POL

```

```

set interfaces ge-0/0/3 description "trust" unit 0 family inet address 10.1.0.1/16
set interfaces ge-0/0/4 description "untrust" unit 0 family inet address 10.2.0.1/16
set interfaces ge-0/0/2 description "ha_link" unit 0 family inet address 10.22.0.1/24
set interfaces lo0 description "untrust" unit 0 family inet address 10.11.0.1/32
set routing-options autonomous-system 100
set routing-options static route 10.2.0.0/16 next-hop 10.2.0.1
set routing-options static route 10.111.0.2 next-hop 10.2.0.1
set security zones security-zone untrust host-inbound-traffic system-services ike
set security zones security-zone untrust host-inbound-traffic system-services ping
set security zones security-zone untrust host-inbound-traffic protocols bfd
set security zones security-zone untrust host-inbound-traffic protocols bgp
set security zones security-zone untrust interfaces ge-0/0/4
set security zones security-zone untrust interfaces lo0.0
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 ge-0/0/3
set security zones security-zone halink host-inbound-traffic system-services ike
set security zones security-zone halink host-inbound-traffic system-services ping
set security zones security-zone halink host-inbound-traffic system-services high-availability
set security zones security-zone halink host-inbound-traffic system-services ssh
set security zones security-zone halink host-inbound-traffic protocols bfd
set security zones security-zone halink host-inbound-traffic protocols bgp
set security zones security-zone halink interfaces ge-0/0/2
set security policies default-policy permit-all
set security pki ca-profile Root-CA ca-identity Root-CA
set security pki ca-profile Root-CA enrollment url http://10.157.69.204/certsrv/mscep/mscep.dll
set security pki ca-profile Root-CA revocation-check disable
set system syslog file vpn_syslog any info
set system syslog file vpn_syslog match "iked|pkid|kmd|ikemd|authd|jsrpd|chassisd|bfd"
set system services netconf ssh

```

## On SRX-2 Device

```

set chassis high-availability local-id 2
set chassis high-availability local-id local-ip 10.22.0.2
set chassis high-availability peer-id 1 peer-ip 10.22.0.1
set chassis high-availability peer-id 1 interface ge-0/0/2.0
set chassis high-availability peer-id 1 vpn-profile IPSEC_VPN_ICL
set chassis high-availability peer-id 1 liveness-detection minimum-interval 400
set chassis high-availability peer-id 1 liveness-detection multiplier 5
set chassis high-availability services-redundancy-group 0 peer-id 1
set chassis high-availability services-redundancy-group 1 deployment-type switching

```

```

set chassis high-availability services-redundancy-group 1 peer-id 1
set chassis high-availability services-redundancy-group 1 virtual-ip 1 ip 10.1.0.200/16
set chassis high-availability services-redundancy-group 1 virtual-ip 1 interface ge-0/0/3.0
set chassis high-availability services-redundancy-group 1 virtual-ip 2 ip 10.2.0.200/16
set chassis high-availability services-redundancy-group 1 virtual-ip 2 interface ge-0/0/4.0
set chassis high-availability services-redundancy-group 1 monitor interface ge-0/0/3
set chassis high-availability services-redundancy-group 1 monitor interface ge-0/0/4
set chassis high-availability services-redundancy-group 1 activeness-priority 1
set security ike proposal MNHA_IKE_PROP description mnha_link_encr_tunnel
set security ike proposal MNHA_IKE_PROP authentication-method pre-shared-keys
set security ike proposal MNHA_IKE_PROP dh-group group14
set security ike proposal MNHA_IKE_PROP authentication-algorithm sha-256
set security ike proposal MNHA_IKE_PROP encryption-algorithm aes-256-cbc
set security ike proposal MNHA_IKE_PROP lifetime-seconds 3600
set security ike policy MNHA_IKE_POL description mnha_link_encr_tunnel
set security ike policy MNHA_IKE_POL proposals MNHA_IKE_PROP
set security ike policy MNHA_IKE_POL pre-shared-key ascii-text "$ABC123"
set security ike gateway MNHA_IKE_GW ike-policy MNHA_IKE_POL
set security ike gateway MNHA_IKE_GW version v2-only
set security ipsec proposal MNHA_IPSEC_PROP description mnha_link_encr_tunnel
set security ipsec proposal MNHA_IPSEC_PROP protocol esp
set security ipsec proposal MNHA_IPSEC_PROP encryption-algorithm aes-256-gcm
set security ipsec proposal MNHA_IPSEC_PROP lifetime-seconds 3600
set security ipsec policy MNHA_IPSEC_POL description mnha_link_encr_tunnel
set security ipsec policy MNHA_IPSEC_POL proposals MNHA_IPSEC_PROP
set security ipsec vpn IPSEC_VPN_ICL ha-link-encryption
set security ipsec vpn IPSEC_VPN_ICL ike gateway MNHA_IKE_GW
set security ipsec vpn IPSEC_VPN_ICL ike ipsec-policy MNHA_IPSEC_POL
set interfaces ge-0/0/3 description "trust" unit 0 family inet address 10.1.0.2/16
set interfaces ge-0/0/4 description "untrust" unit 0 family inet address 10.2.0.2/16
set interfaces ge-0/0/2 description "ha_link" unit 0 family inet address 10.22.0.2/24
set interfaces lo0 description "untrust" unit 0 family inet address 10.11.0.1/32
set interfaces lo0 description "untrust" unit 0 family inet address 10.11.0.2/32
set interfaces lo0 description "untrust" unit 0 family inet address 10.11.0.3/32
set routing-options autonomous-system 100
set routing-options static route 10.2.0.0/16 next-hop 10.2.0.2
set routing-options static route 10.111.0.2 next-hop 10.2.0.2
set security zones security-zone untrust host-inbound-traffic system-services ike
set security zones security-zone untrust host-inbound-traffic system-services ping
set security zones security-zone untrust host-inbound-traffic protocols bfd
set security zones security-zone untrust host-inbound-traffic protocols bgp
set security zones security-zone untrust interfaces ge-0/0/4
set security zones security-zone untrust interfaces lo0.0

```

```

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 ge-0/0/3
set security zones security-zone halink host-inbound-traffic system-services ike
set security zones security-zone halink host-inbound-traffic system-services ping
set security zones security-zone halink host-inbound-traffic system-services high-availability
set security zones security-zone halink host-inbound-traffic system-services ssh
set security zones security-zone halink host-inbound-traffic protocols bfd
set security zones security-zone halink host-inbound-traffic protocols bgp
set security zones security-zone halink interfaces ge-0/0/2
set security policies default-policy permit-all
set security pki ca-profile Root-CA ca-identity Root-CA
set security pki ca-profile Root-CA enrollment url http://10.157.69.204/certsrv/mscep/mscep.dll
set security pki ca-profile Root-CA revocation-check disable
set system syslog file vpn_syslog any info
set system syslog file vpn_syslog match "iked|pkid|kmd|ikemd|authd|jsrpd|chassisd|bfd"
set system services netconf ssh

```

The following sections show configuration snippets on the switches required for setting up Multinode High Availability setup in the network.

#### On Switch (EX9214 Ethernet Switch)

```

set interfaces ge-0/0/2 description lan
set interfaces ge-0/0/2 mtu 9192
set interfaces ge-0/0/2 unit 0 family ethernet-switching interface-mode access
set interfaces ge-0/0/2 unit 0 family ethernet-switching vlan members lan
set interfaces ge-0/0/0 mtu 9192
set interfaces ge-0/0/0 description lan unit 0 family ethernet-switching interface-mode access
set interfaces ge-0/0/0 unit 0 family ethernet-switching vlan members lan
set interfaces ge-0/0/1 mtu 9192
set interfaces ge-0/0/1 description lan unit 0 family ethernet-switching interface-mode access
set interfaces ge-0/0/1 unit 0 family ethernet-switching vlan members lan
set vlans lan vlan-id 1001

```

#### On Switch (EX9214 Ethernet Switch)

```

set interfaces ge-0/0/2 description lan
set interfaces ge-0/0/2 mtu 9192
set interfaces ge-0/0/2 unit 0 family ethernet-switching interface-mode access
set interfaces ge-0/0/2 unit 0 family ethernet-switching vlan members lan

```

```

set interfaces ge-0/0/0 mtu 9192
set interfaces ge-0/0/0 description lan unit 0 family ethernet-switching interface-mode access
set interfaces ge-0/0/0 unit 0 family ethernet-switching vlan members lan
set interfaces ge-0/0/1 mtu 9192
set interfaces ge-0/0/1 description lan unit 0 family ethernet-switching interface-mode access
set interfaces ge-0/0/1 unit 0 family ethernet-switching vlan members lan
set vlans lan vlan-id 1001

```

## Configuration

### Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see [Using the CLI Editor in Configuration Mode](#) in the [CLI User Guide](#).

#### 1. Configure Interfaces.

```

[edit]
user@host# set interfaces ge-0/0/3 description "trust" unit 0 family inet address
10.1.0.1/16
user@host# set interfaces ge-0/0/4 description "untrust" unit 0 family inet address
10.2.0.1/16
user@host# set interfaces ge-0/0/2 description "ha_link" unit 0 family inet address
10.22.0.1/24

```

We're using the interfaces ge-0/0/3 and ge-0/0/4 to connect to the switches, and using the ge-0/0/2 interface for ICL.

#### 2. Configure the loopback interface.

```

[edit]
user@host# set interfaces lo0 description "untrust" unit 0 family inet address 10.11.0.1/32

```

Assign the IP address (10.11.0.1) to the loopback interface. This IP address acts as the floating IP address.

Using the loopback interface ensures that at any given point, traffic from the adjacent devices will be steered toward the floating IP address (that is toward the active node).

### 3. Configure the security policy.

```
[edit]
user@host# set security policies default-policy permit-all
```

Ensure you have configured security policies as per your network requirements. In this example, you'll configure a policy to permit all traffic.

### 4. Configure security zones, assign interfaces to the zones, and specify the allowed system services for the security zones.

```
[edit]
user@host# set security zones security-zone untrust host-inbound-traffic system-services ike
user@host# set security zones security-zone untrust host-inbound-traffic system-services ping
user@host# set security zones security-zone untrust host-inbound-traffic protocols bfd
user@host# set security zones security-zone untrust host-inbound-traffic protocols bgp
user@host# set security zones security-zone untrust interfaces ge-0/0/4
user@host# set security zones security-zone untrust interfaces lo0.0
user@host# set security zones security-zone trust host-inbound-traffic system-services all
user@host# set security zones security-zone trust host-inbound-traffic protocols all
user@host# set security zones security-zone trust interfaces ge-0/0/3
user@host# set security zones security-zone halink host-inbound-traffic system-services ike
user@host# set security zones security-zone halink host-inbound-traffic system-services ping
user@host# set security zones security-zone halink host-inbound-traffic system-services high-availability
user@host# set security zones security-zone halink host-inbound-traffic system-services ssh
user@host# set security zones security-zone halink host-inbound-traffic protocols bfd
user@host# set security zones security-zone halink host-inbound-traffic protocols bgp
user@host# set security zones security-zone halink interfaces ge-0/0/2
```

Assign the interfaces ge-0/0/3 and ge-0/0/4 to the trust and untrust zones respectively. Assign the lo0.0 interface to the untrust zone to connect over the public IP network. Assign the interface ge-0/0/2 to the halink zone. You use this zone to setup the ICL.

### 5. Configure routing options.

```
[edit]
user@host# set routing-options autonomous-system 100
user@host# set routing-options static route 10.2.0.0/16 next-hop 10.2.0.1
user@host# set routing-options static route 10.111.0.2 next-hop 10.2.0.1
```



6. Configure both local node and peer node details such as node ID, IP addresses of the local node and peer node, and the interface for the peer node.

```
[edit]
user@host# set chassis high-availability local-id 1
user@host# set chassis high-availability local-id local-ip 10.22.0.1
user@host# set chassis high-availability peer-id 2 peer-ip 10.22.0.2
user@host# set chassis high-availability peer-id 2 interface ge-0/0/2.0
```

You'll use the ge-0/0/2 interface for communicating with the peer node using the ICL.

7. Attach the IPsec VPN profile IPSEC\_VPN\_ICL to the peer node.

```
[edit]
user@host# set chassis high-availability peer-id 2 vpn-profile IPSEC_VPN_ICL
```

You'll need this configuration to establish a secure ICL link between the nodes.

8. Configure Bidirectional Forwarding Detection (BFD) protocol options for the peer node.

```
[edit]
user@host# set chassis high-availability peer-id 2 liveness-detection minimum-interval 400
user@host# set chassis high-availability peer-id 2 liveness-detection multiplier 5
```

9. Associate the peer node ID 2 to the services redundancy group 0 (SRG0).

```
[edit]
user@host# set chassis high-availability services-redundancy-group 0 peer-id 2
```

10. Configure the services redundancy group 1 (SRG1).

```
[edit]
user@host# set chassis high-availability services-redundancy-group 1 deployment-type
switching
user@host# set chassis high-availability services-redundancy-group 1 peer-id 2
user@host# set chassis high-availability services-redundancy-group 1 virtual-ip 1 ip
10.1.0.200/16
user@host# set chassis high-availability services-redundancy-group 1 virtual-ip 1 interface
ge-0/0/3.0
```

```

user@host# set chassis high-availability services-redundancy-group 1 virtual-ip 1 use-
virtual-mac
user@host# set chassis high-availability services-redundancy-group 1 virtual-ip 2 ip
10.2.0.200/16
user@host# set chassis high-availability services-redundancy-group 1 virtual-ip 2 interface
ge-0/0/4.0
user@host# set chassis high-availability services-redundancy-group 1 virtual-ip 2 use-
virtual-mac

```

In this step, you are specifying the deployment type as switching because you are setting up Multinode High Availability as default gateway (Layer 2 network).

Assign a virtual IP (VIP) address and an interface for SRG1.

11. Configure IP and BFD monitoring parameters for SRG1 to check the reachability of an IP address and to detect failures in network.

```

[edit]
user@host# set chassis high-availability services-redundancy-group 1 monitor interface
ge-0/0/3
user@host# set chassis high-availability services-redundancy-group 1 monitor interface
ge-0/0/4
user@host# set chassis high-availability services-redundancy-group 1 preemption

```

12. Configure an active signal route required for activeness enforcement.

```

[edit]
user@host# set chassis high-availability services-redundancy-group 1 activeness-priority 200

```

The active signal route IP address you assign is used for route preference advertisement. You must specify the active signal route along with the route-exists policy in the policy-options statement.

13. Configure CA certificates as per your requirements.

```

[edit]
user@host# set security pki ca-profile Root-CA ca-identity Root-CA
user@host# set security pki ca-profile Root-CA enrollment url http://10.157.69.204/certsrv/
mscep/mscep.dll
user@host# set security pki ca-profile Root-CA revocation-check disable

```

14. Define Internet Key Exchange (IKE) configuration for Multinode High Availability. An IKE configuration defines the algorithms and keys used to establish a secure connection.

```
[edit]
user@host# set security ike proposal MNHA_IKE_PROP description mnha_link_encr_tunnel
user@host# set security ike proposal MNHA_IKE_PROP authentication-method pre-shared-keys
user@host# set security ike proposal MNHA_IKE_PROP dh-group group14
user@host# set security ike proposal MNHA_IKE_PROP authentication-algorithm sha-256
user@host# set security ike proposal MNHA_IKE_PROP encryption-algorithm aes-256-cbc
user@host# set security ike proposal MNHA_IKE_PROP lifetime-seconds 3600
user@host# set security ike policy MNHA_IKE_POL description mnha_link_encr_tunnel
user@host# set security ike policy MNHA_IKE_POL proposals MNHA_IKE_PROP
user@host# set security ike policy MNHA_IKE_POL pre-shared-key ascii-text "$ABC123"
user@host# set security ike gateway MNHA_IKE_GW ike-policy MNHA_IKE_POL
user@host# set security ike gateway MNHA_IKE_GW version v2-only
```

For the Multinode High availability feature, you must configure the IKE version as v2-only

15. Specify the IPsec proposal protocol and encryption algorithm. Specify IPsec options to create a IPsec tunnel between two participant devices to secure VPN communication.

```
[edit]
user@host# set security ipsec proposal MNHA_IPSEC_PROP description mnha_link_encr_tunnel
user@host# set security ipsec proposal MNHA_IPSEC_PROP protocol esp
user@host# set security ipsec proposal MNHA_IPSEC_PROP encryption-algorithm aes-256-gcm
user@host# set security ipsec proposal MNHA_IPSEC_PROP lifetime-seconds 3600
user@host# set security ipsec policy MNHA_IPSEC_POL description mnha_link_encr_tunnel
user@host# set security ipsec policy MNHA_IPSEC_POL proposals MNHA_IPSEC_PROP
user@host# set security ipsec vpn IPSEC_VPN_ICL ha-link-encryption
user@host# set security ipsec vpn IPSEC_VPN_ICL ike gateway MNHA_IKE_GW
user@host# set security ipsec vpn IPSEC_VPN_ICL ike ipsec-policy MNHA_IPSEC_POL
```

Specifying the ha-link-encryption option encrypts the ICL to secure high availability traffic flow between the nodes.

The same VPN name IPSEC\_VPN\_ICL must be mentioned for *vpn\_profile* in chassis high availability configuration.

## Configuration Options for Software Upgrades

In Multinode High Availability, during software upgrade, you can divert the traffic by closing down interfaces on the node. Here, traffic cannot pass through the nodes. Check ["Software Upgrade in Multinode High Availability" on page 885](#) for details.

1. Configure all traffic interfaces under “shutdown-on-failure” option.

```
user@srx-02# set chassis high-availability services-redundancy-group 0 shutdown-on-failure
<interface-name>
```

Example:

```
[edit]
user@srx-02# set chassis high-availability services-redundancy-group 0 shutdown-on-failure
ge-0/0/3
user@srx-02# set chassis high-availability services-redundancy-group 0 shutdown-on-failure
ge-0/0/4
```



**CAUTION:** Donot use interfaces assigned for the interchassis link (ICL).

## Results (SRX-1)

From configuration mode, confirm your configuration by entering the following commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show chassis high-availability
local-id 1 local-ip 10.22.0.1;
peer-id 2 {
  peer-ip 10.22.0.2;
  interface ge-0/0/2.0;
  vpn-profile IPSEC_VPN_ICL;
  liveness-detection {
    minimum-interval 400;
    multiplier 5;
  }
}
```

```

}
services-redundancy-group 0 {
    peer-id {
        2;
    }
}
services-redundancy-group 1 {
    deployment-type switching;
    peer-id {
        2;
    }
    virtual-ip 1 {
        ip 10.1.0.200/16;
        interface ge-0/0/3.0;
        use-virtual-mac;
    }
    virtual-ip 2 {
        ip 10.2.0.200/16;
        interface ge-0/0/4.0;
        use-virtual-mac;
    }
    monitor {
        interface {
            ge-0/0/3;
            ge-0/0/4;
        }
    }
    preemption;
    activeness-priority 200;
}

```

```

[edit]
user@host# show security ike
proposal MNHA_IKE_PROP {
    description mnha_link_encr_tunnel;
    authentication-method pre-shared-keys;
    dh-group group14;
    authentication-algorithm sha-256;
    encryption-algorithm aes-256-cbc;
    lifetime-seconds 3600;
}

```

```

policy MNHA_IKE_POL {
    description mnha_link_encr_tunnel;
    proposals MNHA_IKE_PROP ;
    pre-shared-key ascii-text "$ABC123"; ## SECRET-DATA
}
gateway MNHA_IKE_GW {
    ike-policy MNHA_IKE_POL ;
    version v2-only;
}

```

```

[edit]
user@host# show security ipsec
proposal MNHA_IPSEC_PROP {
    description mnha_link_encr_tunnel;
    protocol esp;
    encryption-algorithm aes-256-gcm;
    lifetime-seconds 3600;
}
policy MNHA_IPSEC_POL {
    description mnha_link_encr_tunnel;
    proposals MNHA_IPSEC_PROP;
}
vpn IPSEC_VPN_ICL {
    ha-link-encryption;
    ike {
        gateway MNHA_IKE_GW;
        ipsec-policy MNHA_IPSEC_POL;
    }
}

```

```

[edit]
user@host# show routing-options
autonomous-system 100;
static {
    route 10.2.0.0/16 next-hop 10.2.0.1;
    route 10.111.0.2/32 next-hop 10.2.0.1;
}

```

```
}
```

```
[edit]
user@host# show security zones
security-zone untrust {
    host-inbound-traffic {
        system-services {
            ike;
            ping;
        }
        protocols {
            bfd;
            bgp;
        }
    }
    interfaces {
        ge-0/0/4.0;
        lo0.0;
    }
}
security-zone trust {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            all;
        }
    }
    interfaces {
        ge-0/0/3.0;
    }
}
security-zone halink {
    host-inbound-traffic {
        system-services {
            ike;
            ping;
            high-availability;
            ssh;
```

```

    }
    protocols {
        bfd;
        bgp;
    }
}
interfaces {
    ge-0/0/2.0;
}
}

```

```

[edit]
user@host# show interfaces

ge-0/0/2 {
    description ha_link;
    unit 0 {
        family inet {
            address 10.22.0.1/24;
        }
    }
}

ge-0/0/3 {
    description trust;
    unit 0 {
        family inet {
            address 10.1.0.1/16;
        }
    }
}

ge-0/0/4 {
    description untrust;
    unit 0 {
        family inet {
            address 10.2.0.1/16;
        }
    }
}

lo0 {

```



```

description untrust;
unit 0 {
    family inet {
        address 10.11.0.1/32;
    }
}
}

```

If you are done configuring the device, enter `commit` from configuration mode.

## Results (SRX-2)

From configuration mode, confirm your configuration by entering the following commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```

[edit]
user@host# show chassis high-availability
local-id 2 local-ip 10.22.0.2;
peer-id 1 {
    peer-ip 10.22.0.1;
    interface ge-0/0/2.0;
    vpn-profile IPSEC_VPN_ICL;
    liveness-detection {
        minimum-interval 400;
        multiplier 5;
    }
}
services-redundancy-group 0 {
    peer-id {
        1;
    }
}
services-redundancy-group 1 {
    deployment-type switching;
    peer-id {
        1;
    }
    virtual-ip 1 {
        ip 10.1.0.200/16;
        interface ge-0/0/3.0;
    }
}

```

```

virtual-ip 2 {
    ip 10.2.0.200/16;
    interface ge-0/0/4.0;
}
monitor {
    interface {
        ge-0/0/3;
        ge-0/0/4;
    }
}
activeness-priority 1;
}

```

```

[edit]
user@host# show security ike
proposal MNHA_IKE_PROP {
    description mnha_link_encr_tunnel;
    authentication-method pre-shared-keys;
    dh-group group14;
    authentication-algorithm sha-256;
    encryption-algorithm aes-256-cbc;
    lifetime-seconds 3600;
}
policy MNHA_IKE_POL {
    description mnha_link_encr_tunnel;
    proposals MNHA_IKE_PROP ;
    pre-shared-key ascii-text "$ABC123"; ## SECRET-DATA
}
gateway MNHA_IKE_GW {
    ike-policy MNHA_IKE_POL ;
    version v2-only;
}

```

```

[edit]
user@host# show security ipsec

proposal MNHA_IPSEC_PROP {
    description mnha_link_encr_tunnel;
    protocol esp;
    encryption-algorithm aes-256-gcm;
}

```

```

        lifetime-seconds 3600;
    }
    policy MNHA_IPSEC_POL {
        description mnha_link_encr_tunnel;
        proposals MNHA_IPSEC_PROP;
    }
    vpn IPSEC_VPN_ICL {
        ha-link-encryption;
        ike {
            gateway MNHA_IKE_GW;
            ipsec-policy MNHA_IPSEC_POL;
        }
    }
}

```

```

[edit]
user@host# show routing-options
autonomous-system 100;
static {
    route 10.2.0.0/16 next-hop 10.2.0.2;
    route 10.111.0.2/32 next-hop 10.2.0.2;
}

```

```

[edit]
user@host# show security zones
security-zone untrust {
    host-inbound-traffic {
        system-services {
            ike;
            ping;
        }
        protocols {
            bfd;
            bgp;
        }
    }
    interfaces {
        ge-0/0/4.0;
        lo0.0;
    }
}

```

```

security-zone trust {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            all;
        }
    }
    interfaces {
        ge-0/0/3.0;
    }
}
security-zone halink {
    host-inbound-traffic {
        system-services {
            ike;
            ping;
            high-availability;
            ssh;
        }
        protocols {
            bfd;
            bgp;
        }
    }
    interfaces {
        ge-0/0/2.0;
    }
}

```

[edit]

user@host# **show interfaces**

```

ge-0/0/2 {
    description ha_link;
    unit 0 {
        family inet {
            address 10.22.0.2/24;
        }
    }
}

```

```

    }
}
ge-0/0/3 {
    description trust;
    unit 0 {
        family inet {
            address 10.1.0.2/16;
        }
    }
}
ge-0/0/4 {
    description untrust;
    unit 0 {
        family inet {
            address 10.2.0.2/16;
        }
    }
}
lo0 {
    description untrust;
    unit 0 {
        family inet {
            address 10.11.0.1/32;
            address 10.11.0.2/32;
            address 10.11.0.3/32;
        }
    }
}
}

```

If you are done configuring the device, enter `commit` from configuration mode.

On your security devices, you'll get the following message that asks you to reboot the device:

```

user@host# commit
warning: High Availability Mode changed, please reboot the device to avoid undesirable behavior
commit complete

```

## Verification

### IN THIS SECTION

- [Check Multinode High Availability Details | 740](#)
- [Check Multinode High Availability Peer Node Status | 743](#)
- [Check Multinode High Availability Service Redundancy Groups | 744](#)
- [Verify the Multinode High Availability Status Before and After Failover | 746](#)
- [Verify Interchassis Link \(ICL\) Encryption Status | 749](#)
- [Verify Link Encryption Tunnel Statistics | 751](#)

Confirm that the configuration is working properly.

### Check Multinode High Availability Details

#### Purpose

View and verify the details of the Multinode High Availability setup configured on your security device.

#### Action

From operational mode, run the following command:

On SRX-1

```
user@host> show chassis high-availability information
Node failure codes:
  HW  Hardware monitoring   LB  Loopback monitoring
  MB  Mbuf monitoring       SP  SPU monitoring
  CS  Cold Sync monitoring  SU  Software Upgrade

Node Status: ONLINE
Local-id: 1
Local-IP: 10.22.0.1
HA Peer Information:

Peer Id: 2      IP address: 10.22.0.2   Interface: ge-0/0/2.0
Routing Instance: default
```

```

Encrypted: YES    Conn State: UP
Cold Sync Status: COMPLETE

```

```

Services Redundancy Group: 0
    Current State: ONLINE
    Peer Information:
        Peer Id: 2

```

```

SRG failure event codes:
    BF  BFD monitoring
    IP  IP monitoring
    IF  Interface monitoring
    CP  Control Plane monitoring

```

```

Services Redundancy Group: 1
    Deployment Type: SWITCHING
    Status: ACTIVE
    Activeness Priority: 200
    Preemption: ENABLED
    Process Packet In Backup State: NO
    Control Plane State: READY
    System Integrity Check: N/A
    Failure Events: NONE
    Peer Information:
        Peer Id: 2
        Status : BACKUP
        Health Status: HEALTHY
        Failover Readiness: READY

```

## On SRX-2

```

user@host> show chassis high-availability information

```

```

Node failure codes:

```

```

    HW  Hardware monitoring    LB  Loopback monitoring
    MB  Mbuf monitoring        SP  SPU monitoring
    CS  Cold Sync monitoring    SU  Software Upgrade

```

```

Node Status: ONLINE

```

```

Local-id: 2

```

```

Local-IP: 10.22.0.2

```

```

HA Peer Information:

```

```

Peer Id: 1      IP address: 10.22.0.1      Interface: ge-0/0/2.0
Routing Instance: default
Encrypted: YES  Conn State: UP
Cold Sync Status: COMPLETE

```

```

Services Redundancy Group: 0
  Current State: ONLINE
  Peer Information:
    Peer Id: 1

```

```

SRG failure event codes:
  BF  BFD monitoring
  IP  IP monitoring
  IF  Interface monitoring
  CP  Control Plane monitoring

```

```

Services Redundancy Group: 1
  Deployment Type: SWITCHING
  Status: BACKUP
  Activeness Priority: 1
  Preemption: DISABLED
  Process Packet In Backup State: NO
  Control Plane State: READY
  System Integrity Check: COMPLETE
  Failure Events: NONE
  Peer Information:
    Peer Id: 1
    Status : ACTIVE
    Health Status: HEALTHY
    Failover Readiness: N/A

```

## Meaning

Verify these details from the command output:

- Local node and peer node details such as IP address and ID.
- The field Encrypted: YES indicates that the traffic is protected.
- The field Deployment Type: SWITCHING indicates a default gateway (switching) mode configuration—that is, the network has switches connected at both ends (Layer 2 network).



- The field Services Redundancy Group: 1 indicates the status of the SRG1 (ACTIVE or BACKUP) on that node.

**Check Multinode High Availability Peer Node Status**

**Purpose**

View and verify the peer node details.

**Action**

From operational mode, run the following command:

SRX-1

```
user@host> show chassis high-availability peer-info
HA Peer Information:

Peer-ID: 2      IP address: 10.22.0.2      Interface: ge-0/0/2.0
Routing Instance: default
Encrypted: YES   Conn State: UP
Cold Sync Status: COMPLETE
Internal Interface: st0.16000
Internal Local-IP: 180.100.1.1
Internal Peer-IP: 180.100.1.2
Internal Routing-instance: __juniper_private1__
Packet Statistics:
    Receive Error : 0      Send Error : 0

    Packet-type      Sent      Received

    SRG Status Msg   3         4

    SRG Status Ack   4         3

    Attribute Msg     3         2

    Attribute Ack     2         2
```

## SRX-2

```

user@host> show chassis high-availability peer-info
HA Peer Information:

Peer-ID: 1      IP address: 10.22.0.1      Interface: ge-0/0/2.0
Routing Instance: default
Encrypted: YES   Conn State: UP
Cold Sync Status: COMPLETE
Internal Interface: st0.16000
Internal Local-IP: 180.100.1.2
Internal Peer-IP: 180.100.1.1
Internal Routing-instance: __juniper_private1__
Packet Statistics:
    Receive Error : 0      Send Error : 0

    Packet-type      Sent      Received

    SRG Status Msg   10        8

    SRG Status Ack    8         8

    Attribute Msg     8         4

    Attribute Ack     4         4

```

**Meaning**

Verify these details from the command output:

- Peer node details such as interface used, IP address, and ID.
- Encryption status, connection status, and cold synchronization status
- Packet statistics across the node.

**Check Multinode High Availability Service Redundancy Groups****Purpose**

Verify that the SRGs are configured and working correctly.

## Action

From operational mode, run the following command:

For SRG0:

```
user@host> show chassis high-availability services-redundancy-group 0
```

```
Services Redundancy Group: 0
  Current State: ONLINE
  Peer Information:
    Peer Id: 2
```

For SRG1:

```
user@host> show chassis high-availability services-redundancy-group 1 >
```

```
SRG failure event codes:
```

```
BF  BFD monitoring
IP  IP monitoring
IF  Interface monitoring
CP  Control Plane monitoring
```

```
Services Redundancy Group: 1
```

```
  Deployment Type: SWITCHING
  Status: ACTIVE
  Activeness Priority: 200
  Preemption: ENABLED
  Process Packet In Backup State: NO
  Control Plane State: READY
  System Integrity Check: N/A
  Failure Events: NONE
  Peer Information:
    Peer Id: 2
    Status : BACKUP
    Health Status: HEALTHY
    Failover Readiness: READY
```

```
Virtual IP Info:
```

```
  Index: 2
  IP: 10.2.0.200/16
  VMAC: N/A
```

Interface: ge-0/0/4.0

Status: INSTALLED

Index: 1

IP: 10.1.0.200/16

VMAC: N/A

Interface: ge-0/0/3.0

Status: INSTALLED

Split-brain Prevention Probe Info:

DST-IP: 10.1.0.200

Routing Instance: default

Status: NOT RUNNING

Result: N/A Reason: N/A

Interface Monitoring:

Status: UP

IF Name: ge-0/0/4 State: Up

IF Name: ge-0/0/3 State: Up

## Meaning

Verify these details from the command output:

- Peer node details such as deployment type, status, and active and back up signal routes.
- Virtual IP Information such as IP address and virtual MAC address.
- IP monitoring and BFD monitoring status.

## Verify the Multinode High Availability Status Before and After Failover

### Purpose

Check the change in node status before and after failover in a Multinode High Availability setup.

## Action

To check the Multinode High Availability status on the backup node (SRX-2), run the following command from operational mode:

```
user@host> show chassis high-availability information
Node failure codes:
  HW  Hardware monitoring    LB  Loopback monitoring
  MB  Mbuf monitoring        SP  SPU monitoring
  CS  Cold Sync monitoring    SU  Software Upgrade

Node Status: ONLINE
Local-id: 2
Local-IP: 10.22.0.2
HA Peer Information:

  Peer Id: 1      IP address: 10.22.0.1    Interface: ge-0/0/2.0
  Routing Instance: default
  Encrypted: YES   Conn State: UP
  Cold Sync Status: COMPLETE

Services Redundancy Group: 0
  Current State: ONLINE
  Peer Information:
    Peer Id: 1

SRG failure event codes:
  BF  BFD monitoring
  IP  IP monitoring
  IF  Interface monitoring
  CP  Control Plane monitoring

Services Redundancy Group: 1
  Deployment Type: SWITCHING
  Status: BACKUP
  Activeness Priority: 1
  Preemption: DISABLED
  Process Packet In Backup State: NO
  Control Plane State: READY
  System Integrity Check: COMPLETE
  Failure Events: NONE
  Peer Information:
```

```

Peer Id: 1
Status : ACTIVE
Health Status: HEALTHY
Failover Readiness: N/A

```

Under the Services Redundancy Group: 1 section, you can see the Status: BACKUP field. This field value indicates that the status of SRG 1 is backup.

Initiate the failover on the active node (SRX-1 device) and again run the command on the backup node (SRX-2).

```

user@host> show chassis high-availability information
Node failure codes:
  HW  Hardware monitoring   LB  Loopback monitoring
  MB  Mbuf monitoring       SP  SPU monitoring
  CS  Cold Sync monitoring   SU  Software Upgrade

Node Status: ONLINE
Local-id: 2
Local-IP: 10.22.0.2
HA Peer Information:

  Peer Id: 1      IP address: 10.22.0.1    Interface: ge-0/0/2.0
  Routing Instance: default
  Encrypted: YES   Conn State: DOWN
  Cold Sync Status: IN PROGRESS

Services Redundancy Group: 0
  Current State: ONLINE
  Peer Information:
    Peer Id: 1

SRG failure event codes:
  BF  BFD monitoring
  IP  IP monitoring
  IF  Interface monitoring
  CP  Control Plane monitoring

Services Redundancy Group: 1
  Deployment Type: SWITCHING
  Status: ACTIVE
  Activeness Priority: 1

```

```

Preemption: DISABLED
Process Packet In Backup State: NO
Control Plane State: READY
System Integrity Check: N/A
Failure Events: NONE
Peer Information:
  Peer Id: 1
  Status : BACKUP
  Health Status: HEALTHY
  Failover Readiness: READY

```

Note that under the Services Redundancy Group: 1 section, the status of SRG1 has changed from **BACKUP** to **ACTIVE**.

You can also see peer node details under the Peer Information section. The output shows the status of peer as **BACKUP**.

## Verify Interchassis Link (ICL) Encryption Status

### Purpose

Verify the interchassis link (ICL) status.

### Action

From operational mode, run the following command:

```

user@host> show security ipsec security-associations ha-link-encryption detail
ID: 495002 Virtual-system: root, VPN Name: IPSEC_VPN_ICL
  Local Gateway: 10.22.0.1, Remote Gateway: 10.22.0.2
  Traffic Selector Name: __IPSEC_VPN_ICL__multi_node__
  Local Identity: ipv4(180.100.1.1-180.100.1.1)
  Remote Identity: ipv4(180.100.1.2-180.100.1.2)
  TS Type: traffic-selector
  Version: IKEv2
  PFS group: N/A
  DF-bit: clear, Copy-Outer-DSCP Disabled, Bind-interface: st0.16000, Tunnel MTU: 0, Policy-
name: MNHA_IPSEC_POL
  Port: 500, Nego#: 0, Fail#: 0, Def-Del#: 0 Flag: 0
  Multi-sa, Configured SAs# 0, Negotiated SAs#: 0
  HA Link Encryption Mode: Multi-Node
  Location: FPC -, PIC -, KMD-Instance -

```

```

Anchorship: Thread -
Distribution-Profile: default-profile
Direction: inbound, SPI: 0x000afc7f, AUX-SPI: 0
                , VPN Monitoring: -
    Hard lifetime: Expires in 1888 seconds
    Lifesize Remaining: Unlimited
    Soft lifetime: Expires in 1248 seconds
    Mode: Tunnel(0 0), Type: dynamic, State: installed
    Protocol: ESP, Authentication: aes256-gcm, Encryption: aes-gcm (256 bits)
    Anti-replay service: counter-based enabled, Replay window size: 64
    Extended-Sequence-Number: Disabled
    tunnel-establishment: establish-tunnels-immediately
    Location: FPC 0, PIC 0, KMD-Instance 0
    Anchorship: Thread 0
    IKE SA Index: 4294966274
Direction: outbound, SPI: 0x000079a0, AUX-SPI: 0
                , VPN Monitoring: -
    Hard lifetime: Expires in 1888 seconds
    Lifesize Remaining: Unlimited
    Soft lifetime: Expires in 1248 seconds
    Mode: Tunnel(0 0), Type: dynamic, State: installed
    Protocol: ESP, Authentication: aes256-gcm, Encryption: aes-gcm (256 bits)
    Anti-replay service: counter-based enabled, Replay window size: 64
    Extended-Sequence-Number: Disabled
    tunnel-establishment: establish-tunnels-immediately
    Location: FPC 0, PIC 0, KMD-Instance 0
    Anchorship: Thread 0
    IKE SA Index: 4294966274

```

## Meaning

The command output provides the following information:

- The local gateway and remote gateway details.
- The IPsec SA pair for each threads in PIC.
- HA link encryption mode (as shown in the following line):

```
HA Link Encryption Mode: Multi-Node
```

- Authentication and encryption algorithms used



## Verify Link Encryption Tunnel Statistics

### Purpose

Verify link encryption tunnel statistics on both active and backup nodes.

### Action

From operational mode, run the following command:

```
user@host> show security ipsec statistics ha-link-encryption
```

#### ESP Statistics:

Encrypted bytes:	2455540
Decrypted bytes:	1186957
Encrypted packets:	22673
Decrypted packets:	22694

#### AH Statistics:

Input bytes:	0
Output bytes:	0
Input packets:	0
Output packets:	0

#### Errors:

AH authentication failures: 0, Replay errors: 0  
ESP authentication failures: 0, ESP decryption failures: 0  
Bad headers: 0, Bad trailers: 0  
Invalid SPI: 0, TS check fail: 0  
Exceeds tunnel MTU: 0  
Discarded: 0

### Meaning

If you see packet loss issues across a VPN, you can run the `show security ipsec statistics ha-link-encryption` command several times to verify that the encrypted and decrypted packet counters are incrementing. You should also check whether the other error counters are incrementing.

Use the `show security ike active-peer ha-link-encryption` command to display details of ICL on the active peer node.

Use the `clear security ipsec statistics ha-link-encryption` command to clear all IPsec statistics.

## SEE ALSO

[Multinode High Availability | 613](#)

[Prepare Your Environment for Multinode High Availability Deployment | 654](#)

[Multinode High Availability Services | 658](#)

[Example: Configure Multinode High Availability in a Layer 3 Network | 672](#)

[Example: Configure Multinode High Availability in a Hybrid Deployment | 752](#)

## Example: Configure Multinode High Availability in a Hybrid Deployment

### SUMMARY

Read this topic to learn how to configure Multinode High Availability solution on SRX Series devices. The example covers configuration in active/backup mode when SRX Series devices are connected to a router on one side and switch on the other side.

### IN THIS SECTION

- [Overview | 752](#)
- [Requirements | 753](#)
- [Topology | 753](#)
- [Configuration | 756](#)
- [Verification | 782](#)

### Overview

In a hybrid deployments, participating SRX Series devices operate as independent nodes in a mixed mode of routed networks on one side and locally connected networks on the other side. An encrypted logical interchassis link (ICL) connects the nodes over a routed network.

In Multinode High Availability, activeness is determined at the services redundancy group (SRG) level. The SRX Series device, on which the SRG1 is active, hosts the floating IP address and steers traffic towards it using the floating IP address. During a failover, the floating IP address moves from the old active node to the new active node and continues the communication client devices.

**NOTE:** As of Junos OS Release 22.3R1, we support a two-node configuration in the Multinode High Availability solution.

In this example, you'll establish high availability between the SRX Series devices and secure the tunnel traffic by enabling HA link encryption.

## Requirements

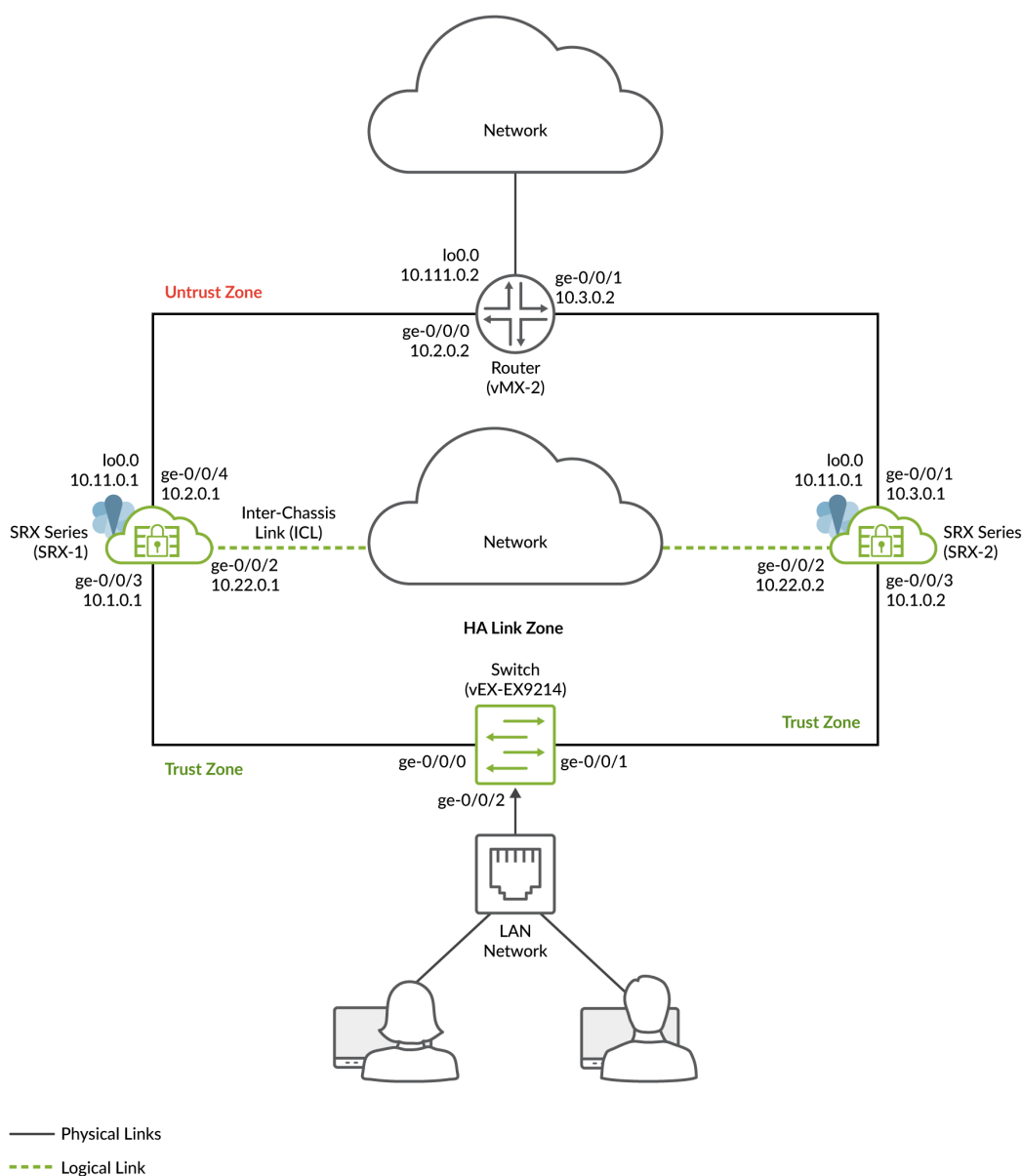
This example uses the following hardware and software components:

- Two SRX Series devices or vSRX Instances
- A Juniper Networks(R) MX960 Universal Routing Platform at one end
- A Juniper Networks(R) EX9214 Ethernet Switch at the other end
- Junos OS Release 22.3R1

## Topology

Figure 1 shows the topology used in this example.

Figure 58: Multinode High Availability In Hybrid Network



As shown in the topology, two SRX Series devices connected to routers on untrust side and to a switch trust side of the network. The nodes communicate with each other using a routable IP address (floating IP address) over the network. Loopback interfaces are used to host the IP addresses on SRX Series and upstream router.

In general, you can use Aggregated Ethernet (AE) or a revenue Ethernet port on the SRX Series devices to setup an ICL connection. In this example, we've used GE ports for the ICL. We've also configured a routing instance for the ICL path to ensure maximum segmentation.

In a typical high availability deployment, you have multiple routers and switches on the northbound and southbound sides of the network. For this example, we are using one routers and one switch.

You'll perform the following tasks to build a Multinode High Availability setup:

- Configure a pair of SRX Series devices as local and peer nodes by assigning IDs.
- Configure services redundancy groups (SRGs).
- Configure a loopback interface (lo0.0) to host a floating IP address on the Layer 3 side.
- Configure virtual IP addresses for activeness determination and enforcement on the Layer 2 side.
- Configure a signal route required for activeness enforcement and use it along with the route exists policy.
- Configure a VPN profile for the high availability (ICL) traffic using IKEv2.
- Configure BFD monitoring options.
- Configure a routing policy and routing options.
- Configure appropriate security policies to manage traffic in your network.
- Configure stateless firewall filtering and quality of service (QoS) as per your network requirements.
- Configure interfaces and zones according to your network requirement. You must allow services such as IKE for link encryption and SSH for configuration synchronization as host-inbound system services on the security zone that is associated with the ICL.

You can configure the following options on SRG0 and SRG1:

- SRG1: Active/backup signal route, deployment type, activeness priority, preemption, virtual IP address (for default gateway deployments), activeness probing and process packet on backup.
- SRG1: BFD monitoring, IP monitoring, and interface monitoring options on SRG1.
- SRG0: shutdown on failure and install on failure route options.

When you configure monitoring (BFD or IP or Interface) options under SRG1, we recommend not to configure the shutdown-on-failure option under SRG0.

For interchassis link (ICL), we recommend the following configuration settings:

- Use a loopback (lo0) interface using an aggregated Ethernet interface (ae0), or any revenue Ethernet interface to establish the ICL. Do not to use the dedicated HA ports (control and fabric ports) if available on your SRX Series device).
- Set MTU of 1514
- Allow the following services on the security zone associated with interfaces used for ICL

- IKE, high-availability, SSH
- Protocols depends on routing protocol you need
- BFD to monitor the neighboring routes

## Configuration

### IN THIS SECTION

- [Before You Begin | 756](#)
- [CLI Quick Configuration | 756](#)
- [Configuration | 763](#)
- [Results \(SRX-1\) | 770](#)
- [Results \(SRX-2\) | 776](#)

### Before You Begin

Install the Junos IKE package on your SRX Series. You require this step for ICL encryption.

```
user@host> request system software add optional://junos-ike.tgz
Verified junos-ike signed by PackageProductionECP256_2022 method ECDSA256+SHA256
Rebuilding schema and Activating configuration...
mgd: commit complete
Restarting MGD ...

WARNING: cli has been replaced by an updated version:
CLI release 20220208.163814_builder.r1239105 built by builder on 2022-02-08 17:07:55 UTC
Restart cli using the new version ? [yes,no] (yes)
```

### CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the [edit] hierarchy level, and then enter `commit` from configuration mode.

These configurations are captured from a lab environment, and are provided for reference only. Actual configurations may vary based on the specific requirements of your environment.

## On SRX-1 Device

```

set chassis high-availability local-id 1
set chassis high-availability local-id local-ip 10.22.0.1
set chassis high-availability peer-id 2 peer-ip 10.22.0.2
set chassis high-availability peer-id 2 interface ge-0/0/2.0
set chassis high-availability peer-id 2 vpn-profile IPSEC_VPN_ICL
set chassis high-availability peer-id 2 liveness-detection minimum-interval 400
set chassis high-availability peer-id 2 liveness-detection multiplier 5
set chassis high-availability services-redundancy-group 0 peer-id 2
set chassis high-availability services-redundancy-group 1 deployment-type hybrid
set chassis high-availability services-redundancy-group 1 peer-id 2
set chassis high-availability services-redundancy-group 1 virtual-ip 1 ip 10.1.0.200/16
set chassis high-availability services-redundancy-group 1 virtual-ip 1 interface ge-0/0/3.0
set chassis high-availability services-redundancy-group 1 virtual-ip 1 use-virtual-mac
set chassis high-availability services-redundancy-group 1 monitor bfd-liveliness 10.2.0.1 src-ip
10.2.0.2
set chassis high-availability services-redundancy-group 1 monitor bfd-liveliness 10.2.0.1
session-type singlehop
set chassis high-availability services-redundancy-group 1 monitor bfd-liveliness 10.2.0.1
interface ge-0/0/4.0
set chassis high-availability services-redundancy-group 1 monitor interface ge-0/0/3
set chassis high-availability services-redundancy-group 1 monitor interface ge-0/0/4
set chassis high-availability services-redundancy-group 1 active-signal-route 10.39.1.1
set chassis high-availability services-redundancy-group 1 backup-signal-route 10.39.1.2
set chassis high-availability services-redundancy-group 1 preemption
set chassis high-availability services-redundancy-group 1 activeness-priority 200
set security pki ca-profile Root-CA ca-identity Root-CA
set security pki ca-profile Root-CA enrollment url http://10.157.69.204/certsrv/mscep/mscep.dll
set security pki ca-profile Root-CA revocation-check disable
set security ike proposal MNHA_IKE_PROP description mnha_link_encr_tunnel
set security ike proposal MNHA_IKE_PROP authentication-method pre-shared-keys
set security ike proposal MNHA_IKE_PROP dh-group group14
set security ike proposal MNHA_IKE_PROP authentication-algorithm sha-256
set security ike proposal MNHA_IKE_PROP encryption-algorithm aes-256-cbc
set security ike proposal MNHA_IKE_PROP lifetime-seconds 3600
set security ike policy MNHA_IKE_POL description mnha_link_encr_tunnel
set security ike policy MNHA_IKE_POL proposals MNHA_IKE_PROP
set security ike policy MNHA_IKE_POL pre-shared-key ascii-text "$ABC123"
set security ike gateway MNHA_IKE_GW ike-policy MNHA_IKE_POL
set security ike gateway MNHA_IKE_GW version v2-only
set security ipsec proposal MNHA_IPSEC_PROP description mnha_link_encr_tunnel

```

```

set security ipsec proposal MNHA_IPSEC_PROP protocol esp
set security ipsec proposal MNHA_IPSEC_PROP encryption-algorithm aes-256-gcm
set security ipsec proposal MNHA_IPSEC_PROP lifetime-seconds 3600
set security ipsec policy MNHA_IPSEC_POL description mnha_link_encr_tunnel
set security ipsec policy MNHA_IPSEC_POL proposals MNHA_IPSEC_PROP
set security ipsec vpn IPSEC_VPN_ICL ha-link-encryption
set security ipsec vpn IPSEC_VPN_ICL ike gateway MNHA_IKE_GW
set security ipsec vpn IPSEC_VPN_ICL ike ipsec-policy MNHA_IPSEC_POL
set security policies default-policy permit-all
set security zones security-zone untrust host-inbound-traffic system-services ike
set security zones security-zone untrust host-inbound-traffic system-services ping
set security zones security-zone untrust host-inbound-traffic protocols bfd
set security zones security-zone untrust host-inbound-traffic protocols bgp
set security zones security-zone untrust interfaces ge-0/0/4.0
set security zones security-zone untrust interfaces lo0.0
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 ge-0/0/3.0
set security zones security-zone halink host-inbound-traffic system-services ike
set security zones security-zone halink host-inbound-traffic system-services ping
set security zones security-zone halink host-inbound-traffic system-services high-availability
set security zones security-zone halink host-inbound-traffic system-services ssh
set security zones security-zone halink host-inbound-traffic protocols bfd
set security zones security-zone halink host-inbound-traffic protocols bgp
set security zones security-zone halink interfaces ge-0/0/2.0
set interfaces ge-0/0/2 description ha_link
set interfaces ge-0/0/2 unit 0 family inet address 10.22.0.1/24
set interfaces ge-0/0/3 description trust
set interfaces ge-0/0/3 unit 0 family inet address 10.1.0.1/16
set interfaces ge-0/0/4 description untrust
set interfaces ge-0/0/4 unit 0 family inet address 10.2.0.1/16
set interfaces lo0 description untrust
set interfaces lo0 unit 0 family inet address 10.11.0.1/32
set interfaces lo0 unit 0 family inet address 10.11.0.2/32
set interfaces lo0 unit 0 family inet address 10.11.0.3/32
set policy-options policy-statement mnha-route-policy term 1 from protocol static
set policy-options policy-statement mnha-route-policy term 1 from protocol direct
set policy-options policy-statement mnha-route-policy term 1 from condition active_route_exists
set policy-options policy-statement mnha-route-policy term 1 then metric 10
set policy-options policy-statement mnha-route-policy term 1 then accept
set policy-options policy-statement mnha-route-policy term 2 from protocol static
set policy-options policy-statement mnha-route-policy term 2 from protocol direct
set policy-options policy-statement mnha-route-policy term 2 from condition backup_route_exists

```



```

set policy-options policy-statement mnha-route-policy term 2 then metric 20
set policy-options policy-statement mnha-route-policy term 2 then accept
set policy-options policy-statement mnha-route-policy term 3 from protocol static
set policy-options policy-statement mnha-route-policy term 3 from protocol direct
set policy-options policy-statement mnha-route-policy term 3 then metric 30
set policy-options policy-statement mnha-route-policy term 3 then accept
set policy-options policy-statement mnha-route-policy term default then reject
set policy-options condition active_route_exists if-route-exists address-family inet 10.39.1.1/32
set policy-options condition active_route_exists if-route-exists address-family inet table inet.0
set policy-options condition backup_route_exists if-route-exists address-family inet 10.39.1.2/32
set policy-options condition backup_route_exists if-route-exists address-family inet table inet.0
set protocols bgp group untrust type internal
set protocols bgp group untrust local-address 10.2.0.1
set protocols bgp group untrust export mnha-route-policy
set protocols bgp group untrust local-as 100
set protocols bgp group untrust bfd-liveness-detection minimum-interval 500
set protocols bgp group untrust bfd-liveness-detection minimum-receive-interval 500
set protocols bgp group untrust bfd-liveness-detection multiplier 3
set protocols bgp group untrust neighbor 10.2.0.2
set routing-options autonomous-system 100
set routing-options static route 10.4.0.0/16 next-hop 10.2.0.2
set routing-options static route 10.111.0.2/32 next-hop 10.2.0.2

```

## On SRX-2 Device

```

set chassis high-availability local-id 2
set chassis high-availability local-id local-ip 10.22.0.2
set chassis high-availability peer-id 1 peer-ip 10.22.0.1
set chassis high-availability peer-id 1 interface ge-0/0/2.0
set chassis high-availability peer-id 1 vpn-profile IPSEC_VPN_ICL
set chassis high-availability peer-id 1 liveness-detection minimum-interval 400
set chassis high-availability peer-id 1 liveness-detection multiplier 5
set chassis high-availability services-redundancy-group 0 peer-id 1
set chassis high-availability services-redundancy-group 1 deployment-type hybrid
set chassis high-availability services-redundancy-group 1 peer-id 1
set chassis high-availability services-redundancy-group 1 virtual-ip 1 ip 10.1.0.200/16
set chassis high-availability services-redundancy-group 1 virtual-ip 1 interface ge-0/0/3.0
set chassis high-availability services-redundancy-group 1 virtual-ip 1 use-virtual-mac
set chassis high-availability services-redundancy-group 1 monitor bfd-liveliness 10.3.0.1 src-ip 10.3.0.2
set chassis high-availability services-redundancy-group 1 monitor bfd-liveliness 10.3.0.1
session-type singlehop

```

```

set chassis high-availability services-redundancy-group 1 monitor bfd-liveliness 10.3.0.1
interface ge-0/0/4.0
set chassis high-availability services-redundancy-group 1 monitor interface ge-0/0/3
set chassis high-availability services-redundancy-group 1 monitor interface ge-0/0/4
set chassis high-availability services-redundancy-group 1 active-signal-route 10.39.1.1
set chassis high-availability services-redundancy-group 1 backup-signal-route 10.39.1.2
set chassis high-availability services-redundancy-group 1 activeness-priority 1
set security pki ca-profile Root-CA ca-identity Root-CA
set security pki ca-profile Root-CA enrollment url http://10.157.69.204/certsrv/mscep/mscep.dll
set security pki ca-profile Root-CA revocation-check disable
set security ike proposal MNHA_IKE_PROP description mnha_link_encr_tunnel
set security ike proposal MNHA_IKE_PROP authentication-method pre-shared-keys
set security ike proposal MNHA_IKE_PROP dh-group group14
set security ike proposal MNHA_IKE_PROP authentication-algorithm sha-256
set security ike proposal MNHA_IKE_PROP encryption-algorithm aes-256-cbc
set security ike proposal MNHA_IKE_PROP lifetime-seconds 3600
set security ike policy MNHA_IKE_POL description mnha_link_encr_tunnel
set security ike policy MNHA_IKE_POL proposals MNHA_IKE_PROP
set security ike policy MNHA_IKE_POL pre-shared-key ascii-text "$ABC123"
set security ike gateway MNHA_IKE_GW ike-policy MNHA_IKE_POL
set security ike gateway MNHA_IKE_GW version v2-only
set security ipsec proposal MNHA_IPSEC_PROP description mnha_link_encr_tunnel
set security ipsec proposal MNHA_IPSEC_PROP protocol esp
set security ipsec proposal MNHA_IPSEC_PROP encryption-algorithm aes-256-gcm
set security ipsec proposal MNHA_IPSEC_PROP lifetime-seconds 3600
set security ipsec policy MNHA_IPSEC_POL description mnha_link_encr_tunnel
set security ipsec policy MNHA_IPSEC_POL proposals MNHA_IPSEC_PROP
set security ipsec vpn IPSEC_VPN_ICL ha-link-encryption
set security ipsec vpn IPSEC_VPN_ICL ike gateway MNHA_IKE_GW
set security ipsec vpn IPSEC_VPN_ICL ike ipsec-policy MNHA_IPSEC_POL
set security policies default-policy permit-all
set security zones security-zone untrust host-inbound-traffic system-services ike
set security zones security-zone untrust host-inbound-traffic system-services ping
set security zones security-zone untrust host-inbound-traffic protocols bfd
set security zones security-zone untrust host-inbound-traffic protocols bgp
set security zones security-zone untrust interfaces ge-0/0/4.0
set security zones security-zone untrust interfaces lo0.0
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 ge-0/0/3.0
set security zones security-zone halink host-inbound-traffic system-services ike
set security zones security-zone halink host-inbound-traffic system-services ping
set security zones security-zone halink host-inbound-traffic system-services high-availability

```

```

set security zones security-zone halink host-inbound-traffic system-services ssh
set security zones security-zone halink host-inbound-traffic protocols bfd
set security zones security-zone halink host-inbound-traffic protocols bgp
set security zones security-zone halink interfaces ge-0/0/2.0
set interfaces ge-0/0/2 description ha_link
set interfaces ge-0/0/2 unit 0 family inet address 10.22.0.2/24
set interfaces ge-0/0/3 description trust
set interfaces ge-0/0/3 unit 0 family inet address 10.1.0.2/16
set interfaces ge-0/0/4 description untrust
set interfaces ge-0/0/4 unit 0 family inet address 10.3.0.1/16
set interfaces lo0 description untrust
set interfaces lo0 unit 0 family inet address 10.11.0.1/32
set interfaces lo0 unit 0 family inet address 10.11.0.2/32
set interfaces lo0 unit 0 family inet address 10.11.0.3/32
set policy-options route-filter-list loopback 10.11.0.0/24 orlonger
set policy-options route-filter-list ipsec 10.4.0.0/16 orlonger
set policy-options policy-statement mnha-route-policy term 1 from protocol static
set policy-options policy-statement mnha-route-policy term 1 from protocol direct
set policy-options policy-statement mnha-route-policy term 1 from condition active_route_exists
set policy-options policy-statement mnha-route-policy term 1 then metric 10
set policy-options policy-statement mnha-route-policy term 1 then accept
set policy-options policy-statement mnha-route-policy term 2 from protocol static
set policy-options policy-statement mnha-route-policy term 2 from protocol direct
set policy-options policy-statement mnha-route-policy term 2 from condition backup_route_exists
set policy-options policy-statement mnha-route-policy term 2 then metric 20
set policy-options policy-statement mnha-route-policy term 2 then accept
set policy-options policy-statement mnha-route-policy term 3 from protocol static
set policy-options policy-statement mnha-route-policy term 3 from protocol direct
set policy-options policy-statement mnha-route-policy term 3 then metric 30
set policy-options policy-statement mnha-route-policy term 3 then accept
set policy-options policy-statement mnha-route-policy term default then reject
set policy-options condition active_route_exists if-route-exists address-family inet 10.39.1.1/32
set policy-options condition active_route_exists if-route-exists address-family inet table inet.0
set policy-options condition backup_route_exists if-route-exists address-family inet 10.39.1.2/32
set policy-options condition backup_route_exists if-route-exists address-family inet table inet.0
set protocols bgp group untrust type internal
set protocols bgp group untrust local-address 10.3.0.1
set protocols bgp group untrust export mnha-route-policy
set protocols bgp group untrust local-as 100
set protocols bgp group untrust bfd-liveness-detection minimum-interval 500
set protocols bgp group untrust bfd-liveness-detection minimum-receive-interval 500
set protocols bgp group untrust bfd-liveness-detection multiplier 3
set protocols bgp group untrust neighbor 10.3.0.2

```

```

set routing-options autonomous-system 100
set routing-options static route 10.4.0.0/16 next-hop 10.3.0.2
set routing-options static route 10.111.0.2/32 next-hop 10.3.0.2

```

The following sections show configuration snippets on the router and switch required for setting up Multinode High Availability setup in the network.

### On the Router (MX960)

```

set interfaces ge-0/0/0 description HA
set interfaces ge-0/0/0 unit 0 family inet address 10.2.0.2/16
set interfaces ge-0/0/1 description HA
set interfaces ge-0/0/1 unit 0 family inet address 10.3.0.2/16
set interfaces ge-0/0/2 description trust
set interfaces ge-0/0/2 unit 0 family inet address 10.4.0.1/16
set interfaces lo0 description loopback
set interfaces lo0 unit 0 family inet address 10.111.0.2/32 primary
set interfaces lo0 unit 0 family inet address 10.111.0.2/32 preferred
set routing-options autonomous-system 100
set protocols bgp group mnha_r0 type internal
set protocols bgp group mnha_r0 local-address 10.2.0.2
set protocols bgp group mnha_r0 local-as 100
set protocols bgp group mnha_r0 bfd-liveness-detection minimum-interval 500
set protocols bgp group mnha_r0 bfd-liveness-detection minimum-receive-interval 500
set protocols bgp group mnha_r0 bfd-liveness-detection multiplier 3
set protocols bgp group mnha_r0 neighbor 10.2.0.1
set protocols bgp group mnha_r0_b type internal
set protocols bgp group mnha_r0_b local-address 10.3.0.2
set protocols bgp group mnha_r0_b local-as 100
set protocols bgp group mnha_r0_b bfd-liveness-detection minimum-interval 500
set protocols bgp group mnha_r0_b bfd-liveness-detection minimum-receive-interval 500
set protocols bgp group mnha_r0_b bfd-liveness-detection multiplier 3
set protocols bgp group mnha_r0_b neighbor 10.3.0.1

```

### On the Switch (EX9214)

```

set interfaces ge-0/0/0 description lan
set interfaces ge-0/0/0 mtu 9192
set interfaces ge-0/0/0 unit 0 family ethernet-switching interface-mode access
set interfaces ge-0/0/0 unit 0 family ethernet-switching vlan members lan
set interfaces ge-0/0/1 description lan
set interfaces ge-0/0/1 mtu 9192

```

```

set interfaces ge-0/0/1 unit 0 family ethernet-switching interface-mode access
set interfaces ge-0/0/1 unit 0 family ethernet-switching vlan members lan
set interfaces ge-0/0/2 description lan
set interfaces ge-0/0/2 mtu 9192
set interfaces ge-0/0/2 unit 0 family ethernet-switching interface-mode access
set interfaces ge-0/0/2 unit 0 family ethernet-switching vlan members lan
set vlans lan vlan-id 1001

```

## Configuration

### Step-by-Step Procedure

We're showing the configuration of SRX-01 in the step-by-step procedure.

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see [Using the CLI Editor in Configuration Mode](#) in the [CLI User Guide](#).

#### 1. Configure Interfaces.

```

[edit]
user@host# set interfaces ge-0/0/3 description "trust" unit 0 family inet address
10.1.0.1/16
user@host# set interfaces ge-0/0/4 description "untrust" unit 0 family inet address
10.2.0.1/16
user@host# set interfaces ge-0/0/2 description "ha_link" unit 0 family inet address
10.22.0.1/24

```

The interfaces ge-0/0/3 connects to the switch, ge-0/0/4 connects the router and the ge-0/0/2 interface is used for the ICL.

#### 2. Configure the loopback interfaces.

```

[edit]
user@host# set interfaces lo0 description "untrust" unit 0 family inet address 10.11.0.1/32
user@host# set interfaces lo0 description "untrust" unit 0 family inet address 10.11.0.2/32
user@host# set interfaces lo0 description "untrust" unit 0 family inet address 10.11.0.3/32

```

Assign the IP address (10.11.0.1) to the loopback interface. This IP address acts as the floating IP address.

Using the loopback interface ensures that at any given point, traffic from the adjacent routers will be steered toward the floating IP address (that is, toward the active node).

### 3. Configure the security policies.

```
[edit]
user@host# set security policies default-policy permit-all
user@host# set security policies global policy All match source-address any
user@host# set security policies global policy All match destination-address any
user@host# set security policies global policy All match application any
user@host# set security policies global policy All then permit
```

Ensure you have configured security policies as per your network requirements. In this example, you'll configure a policy to permit all traffic.

### 4. Configure security zones, assign interfaces to the zones, and specify the allowed system services for the security zones.

```
[edit]
user@host# set security zones security-zone untrust host-inbound-traffic system-services ike
user@host# set security zones security-zone untrust host-inbound-traffic system-services ping
user@host# set security zones security-zone untrust host-inbound-traffic protocols bfd
user@host# set security zones security-zone untrust host-inbound-traffic protocols bgp
user@host# set security zones security-zone untrust interfaces ge-0/0/4
user@host# set security zones security-zone untrust interfaces lo0.0
user@host# set security zones security-zone trust host-inbound-traffic system-services all
user@host# set security zones security-zone trust host-inbound-traffic protocols all
user@host# set security zones security-zone trust interfaces ge-0/0/3
user@host# set security zones security-zone halink host-inbound-traffic system-services ike
user@host# set security zones security-zone halink host-inbound-traffic system-services ping
user@host# set security zones security-zone halink host-inbound-traffic system-services high-availability
user@host# set security zones security-zone halink host-inbound-traffic system-services ssh
user@host# set security zones security-zone halink host-inbound-traffic protocols bfd
user@host# set security zones security-zone halink host-inbound-traffic protocols bgp
user@host# set security zones security-zone halink interfaces ge-0/0/2
```

Assign the interfaces ge-0/0/3 and ge-0/0/4 to the trust and untrust zones respectively. Assign the lo0.0 interface to the untrust zone to connect over the public IP network. Assign the interface ge-0/0/2 to the halink zone. You use this zone to set up the ICL.

5. Configure routing options.

```
[edit]
user@host# set routing-options autonomous-system 100
user@host# set routing-options static route 10.4.0.0/16 next-hop 10.2.0.2
user@host# set routing-options static route 10.111.0.2 next-hop 10.2.0.2
```

6. Configure both local node and peer node details such as node ID, IP addresses of the local node and peer node, and the interface for the peer node.

```
[edit]
user@host# set chassis high-availability local-id 1
user@host# set chassis high-availability local-id local-ip 10.22.0.1
user@host# set chassis high-availability peer-id 2 peer-ip 10.22.0.2
user@host# set chassis high-availability peer-id 2 interface ge-0/0/2.0
```

You'll use the ge-0/0/2 interface for communicating with the peer node using the ICL.

7. Attach the IPsec VPN profile IPSEC\_VPN\_ICL to the peer node.

```
[edit]
user@host# set chassis high-availability peer-id 2 vpn-profile IPSEC_VPN_ICL
```

You'll need this configuration to establish a secure ICL link between the nodes.

8. Configure Bidirectional Forwarding Detection (BFD) protocol options for the peer node.

```
[edit]
user@host# set chassis high-availability peer-id 2 liveness-detection minimum-interval 400
user@host# set chassis high-availability peer-id 2 liveness-detection multiplier 5
```

9. Associate the peer node ID 2 to the services redundancy group 0 (SRG0).

```
[edit]
user@host# set chassis high-availability services-redundancy-group 0 peer-id 2
```

## 10. Configure the services redundancy group 1 (SRG1).

```
[edit]
user@host# set chassis high-availability services-redundancy-group 1 deployment-type hybrid
user@host# set chassis high-availability services-redundancy-group 1 peer-id 2
user@host# set chassis high-availability services-redundancy-group 1 virtual-ip 1 ip
10.1.0.200/16
user@host# set chassis high-availability services-redundancy-group 1 virtual-ip 1 interface
ge-0/0/3.0
user@host# set chassis high-availability services-redundancy-group 1 virtual-ip 1 use-
virtual-mac
```

In this step, you specify the deployment type as hybrid, because you are setting up Multinode High Availability in a Layer 3 and Layer 2 network.

Assign a virtual IP (VIP) address and an interface for SRG1.

## 11. Configure IP and BFD monitoring parameters for SRG1 to check the reachability of an IP address and to detect failures in network.

```
[edit]
user@host# set chassis high-availability services-redundancy-group 1 monitor interface
ge-0/0/3
user@host# set chassis high-availability services-redundancy-group 1 monitor interface
ge-0/0/4
user@host# set chassis high-availability services-redundancy-group 1 monitor bfd-liveliness
10.2.0.1 src-ip 10.2.0.2
user@host# set chassis high-availability services-redundancy-group 1 monitor bfd-liveliness
10.2.0.1 session-type singlehop
user@host# set chassis high-availability services-redundancy-group 1 monitor bfd-liveliness
10.2.0.1 interface ge-0/0/4.0
```

You can configure BFD liveliness by specifying source and destination IP addresses and the interface connecting to the peer device.

For IP monitoring, specify the interfaces used for connecting the neighboring router and switch.

## 12. Configure an active signal route required for activeness enforcement.

```
[edit]
user@host# set chassis high-availability services-redundancy-group 1 active-signal-route
10.39.1.1
user@host# set chassis high-availability services-redundancy-group 1 backup-signal-route
```



```
10.39.1.2
user@host# set chassis high-availability services-redundancy-group 1 preemption
user@host# set chassis high-availability services-redundancy-group 1 activeness-priority 200
```

The active signal route IP address you assign is used for route preference advertisement. You must specify the active signal route along with the route-exists policy in the policy-options statement.

**13. Configure CA certificates as per your requirements.**

```
[edit]
user@host# set security pki ca-profile Root-CA ca-identity Root-CA
user@host# set security pki ca-profile Root-CA enrollment url http://10.157.69.204/certsrv/
mscep/mscep.dll
user@host# set security pki ca-profile Root-CA revocation-check disable
```

**14. Define Internet Key Exchange (IKE) configuration for Multinode High Availability. An IKE configuration defines the algorithms and keys used to establish a secure connection.**

```
[edit]
user@host# set security ike proposal MNHA_IKE_PROP description mnha_link_encr_tunnel
user@host# set security ike proposal MNHA_IKE_PROP authentication-method pre-shared-keys
user@host# set security ike proposal MNHA_IKE_PROP dh-group group14
user@host# set security ike proposal MNHA_IKE_PROP authentication-algorithm sha-256
user@host# set security ike proposal MNHA_IKE_PROP encryption-algorithm aes-256-cbc
user@host# set security ike proposal MNHA_IKE_PROP lifetime-seconds 3600
user@host# set security ike policy MNHA_IKE_POL description mnha_link_encr_tunnel
user@host# set security ike policy MNHA_IKE_POL proposals MNHA_IKE_PROP
user@host# set security ike policy MNHA_IKE_POL pre-shared-key ascii-text "$ABC123"
user@host# set security ike gateway MNHA_IKE_GW ike-policy MNHA_IKE_POL
user@host# set security ike gateway MNHA_IKE_GW version v2-only
```

For the Multinode High availability feature, you must configure the IKE version as v2-only.

**15. Specify the IPsec proposal protocol and encryption algorithm. Specify IPsec options to create a IPsec tunnel between two participant devices to secure VPN communication.**

```
[edit]
user@host# set security ipsec proposal MNHA_IPSEC_PROP description mnha_link_encr_tunnel
user@host# set security ipsec proposal MNHA_IPSEC_PROP protocol esp
user@host# set security ipsec proposal MNHA_IPSEC_PROP encryption-algorithm aes-256-gcm
user@host# set security ipsec proposal MNHA_IPSEC_PROP lifetime-seconds 3600
```

```

user@host# set security ipsec policy MNHA_IPSEC_POL description mnha_link_encr_tunnel
user@host# set security ipsec policy MNHA_IPSEC_POL proposals MNHA_IPSEC_PROP
user@host# set security ipsec vpn IPSEC_VPN_ICL ha-link-encryption
user@host# set security ipsec vpn IPSEC_VPN_ICL ike gateway MNHA_IKE_GW
user@host# set security ipsec vpn IPSEC_VPN_ICL ike ipsec-policy MNHA_IPSEC_POL

```

The same VPN name IPSEC\_VPN\_ICL must be mentioned for *vpn\_profile* in chassis high availability configuration. Specifying the ha-link-encryption option encrypts the ICL to secure high availability traffic flow between the nodes.

## 16. Configure policy options.

```

[edit]
user@host# set policy-options condition active_route_exists if-route-exists address-family
inet 10.39.1.1 table inet.0
user@host# set policy-options condition backup_route_exists if-route-exists address-family
inet 10.39.1.2 table inet.0
user@host# set policy-options policy-statement mnha-route-policy term 1 from protocol static
user@host# set policy-options policy-statement mnha-route-policy term 1 from protocol direct
user@host# set policy-options policy-statement mnha-route-policy term 1 from condition
active_route_exists
user@host# set policy-options policy-statement mnha-route-policy term 1 then accept metric
10
user@host# set policy-options policy-statement mnha-route-policy term 2 from protocol static
user@host# set policy-options policy-statement mnha-route-policy term 2 from protocol direct
user@host# set policy-options policy-statement mnha-route-policy term 2 from condition
backup_route_exists
user@host# set policy-options policy-statement mnha-route-policy term 2 then accept metric
20
user@host# set policy-options policy-statement mnha-route-policy term 3 from protocol static
user@host# set policy-options policy-statement mnha-route-policy term 3 from protocol direct
user@host# set policy-options policy-statement mnha-route-policy term 3 then accept metric
30
user@host# set policy-options policy-statement mnha-route-policy term default then reject

```

Configure the active signal route 10.39.1.1 with the route match condition (if-route-exists). The Multinode High Availability module adds this route to the routing table when the node moves to the active role. The node also starts advertising the higher preference. Also configure the backup signal route (10.39.1.2) to advertise the backup node with a medium priority. In case of any failures, the high availability link goes down and the current active node releases its primary role and removes the active-signal-route. Now the backup node detects the condition through its probes

and transitions to the active role. The route preference is swapped to drive all the traffic to the new active node.

#### 17. Configure BFD peering sessions options and specify liveness detection timers.

```
[edit]
user@host# set protocols bgp group untrust type internal
user@host# set protocols bgp group untrust local-address 10.2.0.1
user@host# set protocols bgp group untrust export mnha-route-policy
user@host# set protocols bgp group untrust neighbor 10.2.0.2
user@host# set protocols bgp group untrust bfd-liveness-detection minimum-interval 500
user@host# set protocols bgp group untrust bfd-liveness-detection minimum-receive-interval
500
user@host# set protocols bgp group untrust bfd-liveness-detection multiplier 3
user@host# set protocols bgp group untrust local-as 100
```

### Configuration Options for Software Upgrades

In Multinode High Availability, during software upgrade, you can divert the traffic by closing down interfaces on the node. Here, traffic cannot pass through the nodes. Check ["Software Upgrade in Multinode High Availability" on page 885](#) for details.

#### 1. Configure all traffic interfaces under “shutdown-on-failure” option.

```
user@srx-02# set chassis high-availability services-redundancy-group 0 shutdown-on-failure
<interface-name>
```

Example:

```
[edit]
user@srx-02# set chassis high-availability services-redundancy-group 0 shutdown-on-failure
ge-0/0/3
user@srx-02# set chassis high-availability services-redundancy-group 0 shutdown-on-failure
ge-0/0/4
```



**CAUTION:** Do not use interfaces assigned for the interchassis link (ICL).

## Results (SRX-1)

From configuration mode, confirm your configuration by entering the following commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show chassis high-availability
local-id 1 local-ip 10.22.0.1;
peer-id 2 {
    peer-ip 10.22.0.2;
    interface ge-0/0/2.0;
    vpn-profile IPSEC_VPN_ICL;
    liveness-detection {
        minimum-interval 400;
        multiplier 5;
    }
}
services-redundancy-group 0 {
    peer-id {
        2;
    }
}
services-redundancy-group 1 {
    deployment-type hybrid;
    peer-id {
        2;
    }
    virtual-ip 1 {
        ip 10.1.0.200/16;
        interface ge-0/0/3.0;
    }
    monitor {
        bfd-liveliness 10.2.0.1 {
            src-ip 10.2.0.2;
            session-type singlehop;
            interface ge-0/0/4.0;
        }
        interface {
            ge-0/0/3;
            ge-0/0/4;
        }
    }
}
```

```

    }
    active-signal-route {
        10.39.1.1;
    }
    backup-signal-route {
        10.39.1.2;
    }
    preemption;
    activeness-priority 200;
}

```

```

[edit]
user@host# show security ike
proposal MNHA_IKE_PROP {
    description mnha_link_encr_tunnel;
    authentication-method pre-shared-keys;
    dh-group group14;
    authentication-algorithm sha-256;
    encryption-algorithm aes-256-cbc;
    lifetime-seconds 3600;
}
policy MNHA_IKE_POL {
    description mnha_link_encr_tunnel;
    proposals MNHA_IKE_PROP ;
    pre-shared-key ascii-text "$ABC123"; ## SECRET-DATA
}
gateway MNHA_IKE_GW {
    ike-policy MNHA_IKE_POL ;
    version v2-only;
}

```

```

[edit]
user@host# show security ipsec
proposal MNHA_IPSEC_PROP {
    description mnha_link_encr_tunnel;
    protocol esp;
    encryption-algorithm aes-256-gcm;
    lifetime-seconds 3600;
}
policy MNHA_IPSEC_POL {

```

```

    description mnha_link_encr_tunnel;
    proposals MNHA_IPSEC_PROP;
}
vpn IPSEC_VPN_ICL {
    ha-link-encryption;
    ike {
        gateway MNHA_IKE_GW;
        ipsec-policy MNHA_IPSEC_POL;
    }
}

```

```

[edit]
user@host# show policy-options
policy-statement mnha-route-policy {
    term 1 {
        from {
            protocol [ static direct ];
            condition active_route_exists;
        }
        then {
            metric 10;
            accept;
        }
    }
    term 2 {
        from {
            protocol [ static direct ];
            condition backup_route_exists;
        }
        then {
            metric 20;
            accept;
        }
    }
    term 3 {
        from protocol [ static direct ];
        then {
            metric 30;
            accept;
        }
    }
}

```

```

    term default {
        then reject;
    }
}
condition active_route_exists {
    if-route-exists {
        address-family {
            inet {
                10.39.1.1/32;
                table inet.0;
            }
        }
    }
}
condition backup_route_exists {
    if-route-exists {
        address-family {
            inet {
                10.39.1.2/32;
                table inet.0;
            }
        }
    }
}
}

```

```

user@host# show routing-options
autonomous-system 100;
static {
    route 10.4.0.0/16 next-hop 10.2.0.2;
    route 10.111.0.2/32 next-hop 10.2.0.2;
}

```

```

[edit]
user@host# show security zones
security-zone untrust {
    host-inbound-traffic {
        system-services {
            ike;
            ping;
        }
    }
}

```

```

        protocols {
            bfd;
            bgp;
        }
    }
    interfaces {
        ge-0/0/4.0;
        lo0.0;
    }
}
security-zone trust {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            all;
        }
    }
    interfaces {
        ge-0/0/3.0;
    }
}
security-zone halink {
    host-inbound-traffic {
        system-services {
            ike;
            ping;
            high-availability;
            ssh;
        }
        protocols {
            bfd;
            bgp;
        }
    }
    interfaces {
        ge-0/0/2.0;
    }
}

```



```

    }
}

```

```

[edit]
user@host# show interfaces
ge-0/0/2 {
    description ha_link;
    unit 0 {
        family inet {
            address 10.22.0.1/24;
        }
    }
}
ge-0/0/3 {
    description trust;
    unit 0 {
        family inet {
            address 10.1.0.1/16;
        }
    }
}
ge-0/0/4 {
    description untrust;
    unit 0 {
        family inet {
            address 10.2.0.1/16;
        }
    }
}
lo0 {
    description untrust;
    unit 0 {
        family inet {
            address 10.11.0.1/32;
            address 10.11.0.2/32;
            address 10.11.0.3/32;
        }
    }
}
}

```

If you are done configuring the device, enter `commit` from configuration mode.

## Results (SRX-2)

From configuration mode, confirm your configuration by entering the following commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show chassis high-availability
local-id 2 local-ip 10.22.0.2;
peer-id 1 {
    peer-ip 10.22.0.1;
    interface ge-0/0/2.0;
    vpn-profile IPSEC_VPN_ICL;
    liveness-detection {
        minimum-interval 400;
        multiplier 5;
    }
}
services-redundancy-group 0 {
    peer-id {
        1;
    }
}
services-redundancy-group 1 {
    deployment-type hybrid;
    peer-id {
        1;
    }
    virtual-ip 1 {
        ip 10.1.0.200/16;
        interface ge-0/0/3.0;
        use-virtual-mac;
    }
}
monitor {
    bfd-liveliness 10.3.0.1 {
        src-ip 10.3.0.2;
        session-type singlehop;
        interface ge-0/0/4.0;
    }
    interface {
        ge-0/0/3;
        ge-0/0/4;
    }
}
```

```

    }
}
active-signal-route {
    10.39.1.1;
}
backup-signal-route {
    10.39.1.2;
}
activeness-priority 1;
}

```

```

[edit]
user@host# show security ike
proposal MNHA_IKE_PROP {
    description mnha_link_encr_tunnel;
    authentication-method pre-shared-keys;
    dh-group group14;
    authentication-algorithm sha-256;
    encryption-algorithm aes-256-cbc;
    lifetime-seconds 3600;
}
policy MNHA_IKE_POL {
    description mnha_link_encr_tunnel;
    proposals MNHA_IKE_PROP ;
    pre-shared-key ascii-text "$ABC123"; ## SECRET-DATA
}
gateway MNHA_IKE_GW {
    ike-policy MNHA_IKE_POL ;
    version v2-only;
}

```

```

[edit]
user@host# show security ipsec
proposal MNHA_IPSEC_PROP {
    description mnha_link_encr_tunnel;
    protocol esp;
    encryption-algorithm aes-256-gcm;
    lifetime-seconds 3600;
}
policy MNHA_IPSEC_POL {

```

```

    description mnha_link_encr_tunnel;
    proposals MNHA_IPSEC_PROP;
}
vpn IPSEC_VPN_ICL {
    ha-link-encryption;
    ike {
        gateway MNHA_IKE_GW;
        ipsec-policy MNHA_IPSEC_POL;
    }
}

```

```

[edit]
user@host# show policy-options
route-filter-list loopback {
    10.11.0.0/24 orlonger;
}
route-filter-list ipsec {
    10.4.0.0/16 orlonger;
}
policy-statement mnha-route-policy {
    term 1 {
        from {
            protocol [ static direct ];
            condition active_route_exists;
        }
        then {
            metric 10;
            accept;
        }
    }
    term 2 {
        from {
            protocol [ static direct ];
            condition backup_route_exists;
        }
        then {
            metric 20;
            accept;
        }
    }
    term 3 {

```

```

        from protocol [ static direct ];
        then {
            metric 30;
            accept;
        }
    }
    term default {
        then reject;
    }
}
condition active_route_exists {
    if-route-exists {
        address-family {
            inet {
                10.39.1.1/32;
                table inet.0;
            }
        }
    }
}
condition backup_route_exists {
    if-route-exists {
        address-family {
            inet {
                10.39.1.2/32;
                table inet.0;
            }
        }
    }
}
}

```

[edit]

user@host# **show routing-options**

autonomous-system 100;

static {

route 10.4.0.0/16 next-hop 10.3.0.2;

```

    route 10.111.0.2/32 next-hop 10.3.0.2;
}

```

```

[edit]
user@host# show security zones
  security-zone untrust {
    host-inbound-traffic {
      system-services {
        ike;
        ping;
      }
      protocols {
        bfd;
        bgp;
      }
    }
    interfaces {
      ge-0/0/4.0;
      lo0.0;
    }
  }
  security-zone trust {
    host-inbound-traffic {
      system-services {
        all;
      }
      protocols {
        all;
      }
    }
    interfaces {
      ge-0/0/3.0;
    }
  }
  security-zone halink {
    host-inbound-traffic {
      system-services {
        ike;
        ping;
        high-availability;
        ssh;

```

```

    }
    protocols {
        bfd;
        bgp;
    }
}
interfaces {
    ge-0/0/2.0;
}
}

```

```

[edit]
user@host# show interfaces
[edit]
root@10.52.45.32# show interfaces
ge-0/0/2 {
    description ha_link;
    unit 0 {
        family inet {
            address 10.22.0.2/24;
        }
    }
}
ge-0/0/3 {
    description trust;
    unit 0 {
        family inet {
            address 10.1.0.2/16;
        }
    }
}
ge-0/0/4 {
    description untrust;
    unit 0 {
        family inet {
            address 10.3.0.1/16;
        }
    }
}
lo0 {
    description untrust;
}

```

```

unit 0 {
    family inet {
        address 10.11.0.1/32;
        address 10.11.0.2/32;
        address 10.11.0.3/32;
    }
}

```

If you are done configuring the device, enter `commit` from configuration mode.

On your security devices, you'll get the following message that asks you to reboot the device:

```

user@host# commit
warning: High Availability Mode changed, please reboot the device to avoid undesirable behavior
commit complete

```

## Verification

### IN THIS SECTION

- [Check Multinode High Availability Details | 782](#)
- [Check Multinode High Availability Peer Node Status | 785](#)
- [Check Multinode High Availability Service Redundancy Groups | 787](#)
- [Verify the Multinode High Availability Status Before and After Failover | 789](#)
- [Verify Interchassis Link \(ICL\) Encryption Status | 792](#)
- [Verify Link Encryption Tunnel Statistics | 793](#)

Confirm that the configuration is working properly.

### Check Multinode High Availability Details

#### Purpose

View and verify the details of the Multinode High Availability setup configured on your security device.



## Action

From operational mode, run the following command:

On SRX-1

```

user@host> show chassis high-availability information
Node failure codes:
    HW  Hardware monitoring    LB  Loopback monitoring
    MB  Mbuf monitoring        SP  SPU monitoring
    CS  Cold Sync monitoring    SU  Software Upgrade

Node Status: ONLINE
Local-id: 1
Local-IP: 10.22.0.1
HA Peer Information:

    Peer Id: 2      IP address: 10.22.0.2    Interface: ge-0/0/2.0
    Routing Instance: default
    Encrypted: YES   Conn State: UP
    Cold Sync Status: COMPLETE

Services Redundancy Group: 0
    Current State: ONLINE
    Peer Information:
        Peer Id: 2

SRG failure event codes:
    BF  BFD monitoring
    IP  IP monitoring
    IF  Interface monitoring
    CP  Control Plane monitoring

Services Redundancy Group: 1
    Deployment Type: HYBRID
    Status: ACTIVE
    Activeness Priority: 200
    Preemption: ENABLED
    Process Packet In Backup State: NO
    Control Plane State: READY
    System Integrity Check: N/A
    Failure Events: NONE

```

```

Peer Information:
  Peer Id: 2
  Status : BACKUP
  Health Status: HEALTHY
  Failover Readiness: NOT READY

```

## On SRX-2

```

user@host> show chassis high-availability information
Node failure codes:
  HW  Hardware monitoring    LB  Loopback monitoring
  MB  Mbuf monitoring        SP  SPU monitoring
  CS  Cold Sync monitoring   SU  Software Upgrade

Node Status: ONLINE
Local-id: 2
Local-IP: 10.22.0.2
HA Peer Information:

  Peer Id: 1      IP address: 10.22.0.1    Interface: ge-0/0/2.0
  Routing Instance: default
  Encrypted: YES   Conn State: UP
  Cold Sync Status: COMPLETE

Services Redundancy Group: 0
  Current State: ONLINE
  Peer Information:
    Peer Id: 1

SRG failure event codes:
  BF  BFD monitoring
  IP  IP monitoring
  IF  Interface monitoring
  CP  Control Plane monitoring

Services Redundancy Group: 1
  Deployment Type: HYBRID
  Status: BACKUP
  Activeness Priority: 1
  Preemption: DISABLED

```

```

Process Packet In Backup State: NO
Control Plane State: READY
System Integrity Check: COMPLETE
Failure Events: NONE
Peer Information:
  Peer Id: 1
  Status : ACTIVE
  Health Status: HEALTHY
  Failover Readiness: N/A

```

## Meaning

Verify these details from the command output:

- Local node and peer node details such as IP address and ID.
- The field Encrypted: YES indicates that the traffic is protected.
- The field Deployment Type: HYBRID indicates a hybrid mode configuration—that is, the network has a router on one side and a switch on the other.
- The field Services Redundancy Group: 1 indicates the status of the SRG1 (ACTIVE or BACKUP) on that node.

## Check Multinode High Availability Peer Node Status

### Purpose

View and verify the peer node details.

### Action

From operational mode, run the following command:

SRX-1

```

user@host> user@host> show chassis high-availability peer-info
HA Peer Information:

Peer-ID: 2      IP address: 10.22.0.2      Interface: ge-0/0/2.0
Routing Instance: default
Encrypted: YES  Conn State: UP

```

```

Cold Sync Status: COMPLETE
Internal Interface: st0.16000
Internal Local-IP: 180.100.1.1
Internal Peer-IP: 180.100.1.2
Internal Routing-instance: __juniper_private1__

```

Packet Statistics:

```

Receive Error : 0      Send Error : 0

```

Packet-type	Sent	Received
SRG Status Msg	3	2
SRG Status Ack	2	3
Attribute Msg	4	2
Attribute Ack	2	1

## SRX-2

```

user@host> show chassis high-availability peer-info

```

HA Peer Information:

```

Peer-ID: 1      IP address: 10.22.0.1      Interface: ge-0/0/2.0
Routing Instance: default
Encrypted: YES  Conn State: UP
Cold Sync Status: COMPLETE
Internal Interface: st0.16000
Internal Local-IP: 180.100.1.2
Internal Peer-IP: 180.100.1.1
Internal Routing-instance: __juniper_private1__

```

Packet Statistics:

```

Receive Error : 0      Send Error : 0

```

Packet-type	Sent	Received
SRG Status Msg	2	3
SRG Status Ack	3	2

Attribute Msg	3	1
Attribute Ack	1	2

## Meaning

Verify these details from the command output:

- Peer node details such as interface used, IP address, and ID
- Encryption status, connection status, and cold synchronization status
- Packet statistics across the node.

## Check Multinode High Availability Service Redundancy Groups

### Purpose

Verify that the SRGs are configured and working correctly.

### Action

From operational mode, run the following command:

For SRG0:

```
user@host> show chassis high-availability services-redundancy-group 0
Services Redundancy Group: 0
  Current State: ONLINE
  Peer Information:
    Peer Id: 2
```

For SRG1:

```
user@host> show chassis high-availability services-redundancy-group 1 >
SRG failure event codes:
  BF  BFD monitoring
  IP  IP monitoring
  IF  Interface monitoring
  CP  Control Plane monitoring
```

**Services Redundancy Group: 1**

Deployment Type: HYBRID

Status: ACTIVE

Activeness Priority: 200

Preemption: ENABLED

Process Packet In Backup State: NO

Control Plane State: READY

System Integrity Check: N/A

Failure Events: NONE

**Peer Information:**

Peer Id: 2

Status : BACKUP

Health Status: HEALTHY

Failover Readiness: NOT READY

**Signal Route Info:****Active Signal Route:**

IP: 10.39.1.1

Routing Instance: default

Status: INSTALLED

**Backup Signal Route:**

IP: 10.39.1.2

Routing Instance: default

Status: NOT INSTALLED

**Virtual IP Info:**

Index: 1

IP: 10.1.0.200/16

VMAC: N/A

Interface: ge-0/0/3.0

Status: INSTALLED

**Split-brain Prevention Probe Info:**

DST-IP: 10.1.0.200

Routing Instance: default

Status: NOT RUNNING

Result: N/A

Reason: N/A

**BFD Monitoring:**

Status: UNKNOWN

```

SRC-IP: 10.2.0.2      DST-IP: 10.2.0.1
Routing Instance: default
Type: SINGLE-HOP
    IFL Name: ge-0/0/4.0
State: INSTALLED

```

```

Interface Monitoring:
Status: UP

```

```

IF Name: ge-0/0/4      State: Up

```

```

IF Name: ge-0/0/3      State: Up

```

## Meaning

Verify these details from the command output:

- Peer node details such as deployment type, status, and active and back up signal routes.
- Virtual IP Information such as IP address and virtual MAC address.
- IP monitoring and BFD monitoring status.

## Verify the Multinode High Availability Status Before and After Failover

## Purpose

Check the change in node status before and after failover in a Multinode High Availability setup.

## Action

To check the Multinode High Availability status on the backup node (SRX-2), run the following command from operational mode:

```

user@host> show chassis high-availability information
Node failure codes:
    HW  Hardware monitoring    LB  Loopback monitoring
    MB  Mbuf monitoring        SP  SPU monitoring

```

CS Cold Sync monitoring SU Software Upgrade

Node Status: ONLINE

Local-id: 2

Local-IP: 10.22.0.2

HA Peer Information:

Peer Id: 1 IP address: 10.22.0.1 Interface: ge-0/0/2.0  
 Routing Instance: default  
 Encrypted: YES Conn State: UP  
 Cold Sync Status: COMPLETE

Services Redundancy Group: 0

Current State: ONLINE

Peer Information:

Peer Id: 1

SRG failure event codes:

BF BFD monitoring  
 IP IP monitoring  
 IF Interface monitoring  
 CP Control Plane monitoring

Services Redundancy Group: 1

Deployment Type: HYBRID

Status: BACKUP

Activeness Priority: 1

Preemption: DISABLED

Process Packet In Backup State: NO

Control Plane State: READY

System Integrity Check: COMPLETE

Failure Events: NONE

Peer Information:

Peer Id: 1

Status : ACTIVE

Health Status: HEALTHY

Failover Readiness: N/A

Under the Services Redundancy Group: 1 section, you can see the Status: BACKUP field. This field value indicates that the status of SRG 1 is backup.



Initiate the failover on the active node (SRX-1 device) and again run the command on the backup node (SRX-2).

```

user@host> show chassis high-availability information
Node failure codes:
    HW  Hardware monitoring    LB  Loopback monitoring
    MB  Mbuf monitoring        SP  SPU monitoring
    CS  Cold Sync monitoring    SU  Software Upgrade

Node Status: ONLINE
Local-id: 2
Local-IP: 10.22.0.2
HA Peer Information:

    Peer Id: 1      IP address: 10.22.0.1    Interface: ge-0/0/2.0
    Routing Instance: default
    Encrypted: YES   Conn State: DOWN
    Cold Sync Status: IN PROGRESS

Services Redundancy Group: 0
    Current State: ONLINE
    Peer Information:
        Peer Id: 1

SRG failure event codes:
    BF  BFD monitoring
    IP  IP monitoring
    IF  Interface monitoring
    CP  Control Plane monitoring

Services Redundancy Group: 1
    Deployment Type: HYBRID
    Status: ACTIVE
    Activeness Priority: 1
    Preemption: DISABLED
    Process Packet In Backup State: NO
    Control Plane State: READY
    System Integrity Check: N/A
    Failure Events: NONE
    Peer Information:
        Peer Id: 1
        Status : BACKUP

```

```
Health Status: HEALTHY
Failover Readiness: READY
```

Note that under the Services Redundancy Group: 1 section, the status of SRG1 has changed from **BACKUP** to **ACTIVE**.

You can also see peer node details under the Peer Information section. The output shows the status of peer as **BACKUP**.

## Verify Interchassis Link (ICL) Encryption Status

### Purpose

Verify the interchassis link (ICL) status.

### Action

From operational mode, run the following command:

```
user@host> show security ipsec security-associations ha-link-encryption detail
ID: 495003 Virtual-system: root, VPN Name: IPSEC_VPN_ICL
  Local Gateway: 10.22.0.1, Remote Gateway: 10.22.0.2
  Traffic Selector Name: __IPSEC_VPN_ICL__multi_node__
  Local Identity: ipv4(180.100.1.1-180.100.1.1)
  Remote Identity: ipv4(180.100.1.2-180.100.1.2)
  TS Type: traffic-selector
  Version: IKEv2
  PFS group: N/A
  DF-bit: clear, Copy-Outer-DSCP Disabled, Bind-interface: st0.16000, Tunnel MTU: 0, Policy-
name: MNHA_IPSEC_POL
  Port: 500, Nego#: 0, Fail#: 0, Def-Del#: 0 Flag: 0
  Multi-sa, Configured SAs# 0, Negotiated SAs#: 0
  HA Link Encryption Mode: Multi-Node
  Location: FPC -, PIC -, KMD-Instance -
  Anchorship: Thread -
  Distribution-Profile: default-profile
  Direction: inbound, SPI: 0x00022d84, AUX-SPI: 0
                    , VPN Monitoring: -
  Hard lifetime: Expires in 3395 seconds
  Lifesize Remaining: Unlimited
  Soft lifetime: Expires in 2794 seconds
  Mode: Tunnel(0 0), Type: dynamic, State: installed
```

```

Protocol: ESP, Authentication: aes256-gcm, Encryption: aes-gcm (256 bits)
Anti-replay service: counter-based enabled, Replay window size: 64
Extended-Sequence-Number: Disabled
tunnel-establishment: establish-tunnels-immediately
Location: FPC 0, PIC 0, KMD-Instance 0
Anchorship: Thread 0
IKE SA Index: 4294966277
Direction: outbound, SPI: 0x00028296, AUX-SPI: 0
                , VPN Monitoring: -
Hard lifetime: Expires in 3395 seconds
Lifesize Remaining: Unlimited
Soft lifetime: Expires in 2794 seconds
Mode: Tunnel(0 0), Type: dynamic, State: installed
Protocol: ESP, Authentication: aes256-gcm, Encryption: aes-gcm (256 bits)
Anti-replay service: counter-based enabled, Replay window size: 64
Extended-Sequence-Number: Disabled
tunnel-establishment: establish-tunnels-immediately
Location: FPC 0, PIC 0, KMD-Instance 0
Anchorship: Thread 0
IKE SA Index: 4294966277

```

## Meaning

The command output provides the following information:

- The local gateway and remote gateway details.
- The IPsec SA pair for each threads in PIC.
- HA link encryption mode (as shown in the following line):

```
HA Link Encryption Mode: Multi-Node
```

- Authentication and encryption algorithms used

## Verify Link Encryption Tunnel Statistics

### Purpose

Verify link encryption tunnel statistics on both active and backup nodes.

## Action

From operational mode, run the following command:

```
user@host> show security ipsec statistics ha-link-encryption
ESP Statistics:
  Encrypted bytes:      984248
  Decrypted bytes:      462519
  Encrypted packets:    9067
  Decrypted packets:    8797
AH Statistics:
  Input bytes:          0
  Output bytes:         0
  Input packets:        0
  Output packets:       0
Errors:
  AH authentication failures: 0, Replay errors: 0
  ESP authentication failures: 0, ESP decryption failures: 0
  Bad headers: 0, Bad trailers: 0
  Invalid SPI: 0, TS check fail: 0
  Exceeds tunnel MTU: 0
  Discarded: 0
```

## Meaning

If you see packet loss issues across a VPN, you can run the `show security ipsec statistics ha-link-encryption` command several times to verify that the encrypted and decrypted packet counters are incrementing. You should also check whether the other error counters are incrementing.

Use the `show security ike active-peer ha-link-encryption` command to display details of ICL on the active peer node.

Use the `clear security ipsec statistics ha-link-encryption` command to clear all IPsec statistics.

## SEE ALSO

[Multinode High Availability | 613](#)

[Multinode High Availability Services | 658](#)

[Prepare Your Environment for Multinode High Availability Deployment | 654](#)

[Software Upgrade in Multinode High Availability | 885](#)

[Example: Configure Multinode High Availability in a Default Gateway Deployment | 717](#)[Example: Configure Multinode High Availability in a Layer 3 Network | 672](#)

## Example: Configure IPsec VPN in Active-Active Multinode High Availability in a Layer 3 Network

### SUMMARY

This example shows how to configure and verify IPsec VPN for active-active Multinode High Availability setup.

### IN THIS SECTION

- [Overview | 795](#)
- [Requirements | 796](#)
- [Topology | 796](#)
- [Configuration | 801](#)
- [Verification | 857](#)

### Overview

In Multi-Node High Availability, participating SRX Series devices operate as independent nodes in a Layer 3 network. The nodes are connected to adjacent infrastructure belonging to different networks. An encrypted logical interchassis link (ICL) connects the nodes over a routed network. Participating nodes backup each other to ensure a fast synchronized failover in case of system or hardware failure.

You can operate Multinode High Availability in active-active mode with support of multiple services redundancy groups (SRGs). In this mode, some SRGs remain active on one node and some SRGs remain active on another node.

Multinode High Availability supports IPsec VPN in active-active mode with multiple SRGs (SRG1+). In this mode, you can establish multiple active tunnels from both the nodes, based on SRG activeness. Multinode High Availability establishes IPsec tunnel and performs key exchanges by associating termination IP address (which also identifies the tunnels ending on it) to the SRG. Since different SRG1+ can be in active state or in backup state on each of the devices, Multinode High Availability steers the matching traffic effectively to the corresponding active SRG1. Since different SRGs can be active on different nodes, tunnels belonging to these SRGs come up on both nodes independently.

**NOTE:** We support a two-node configuration in the Multinode High Availability solution.

## Requirements

### IN THIS SECTION

- [Before You Begin | 796](#)

This example uses the following hardware and software components:

- Two SRX Series devices (Supported devices are SRX5400, SRX5600, and SRX5800 with SPC3, IOC3, SCB3, SCB4, and RE3)
- Junos OS Release 22.4R1

We've used two Juniper Networks MX Series Routing Platform as upstream/downstream routers in this example.

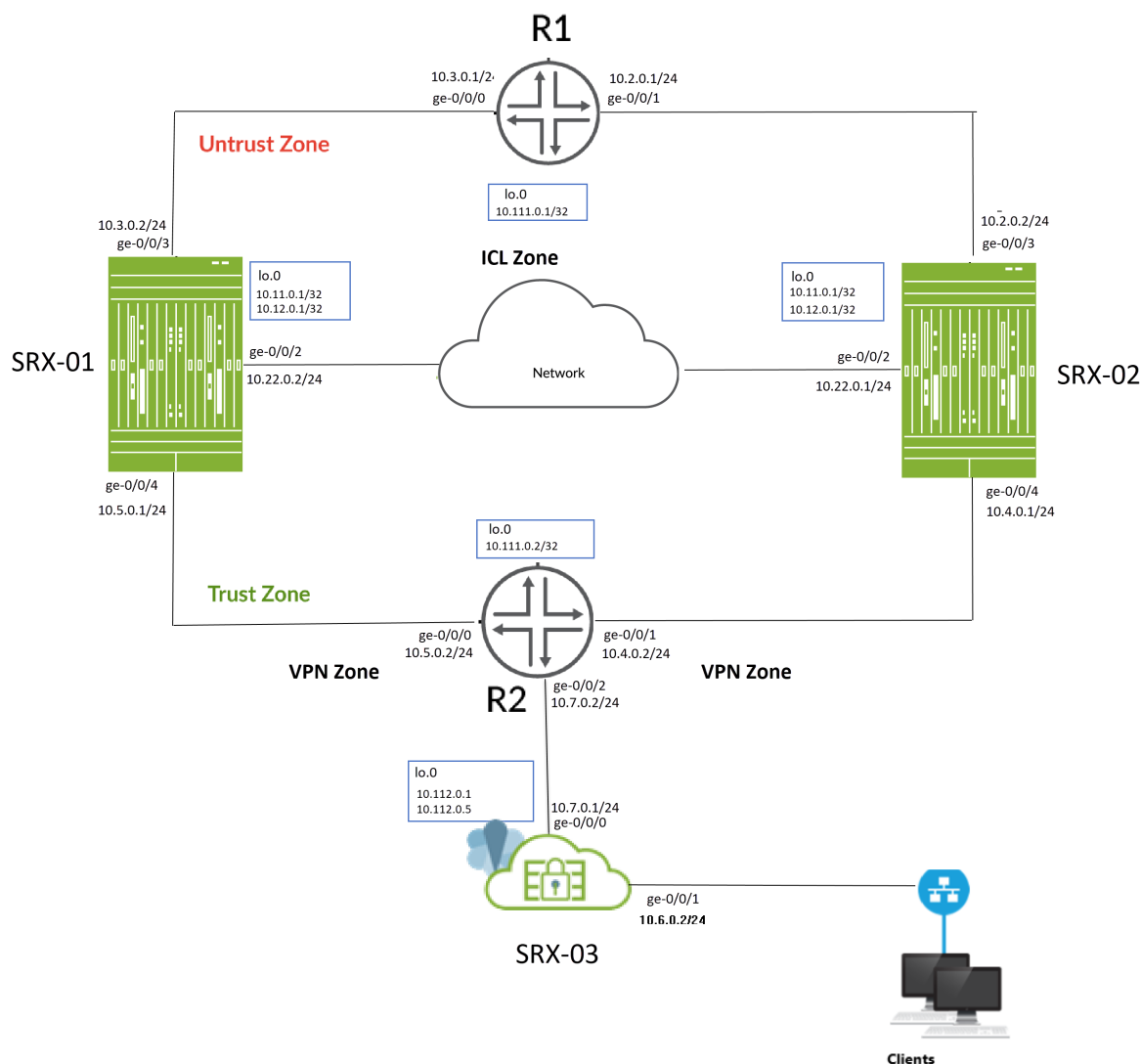
### Before You Begin

- Configure stateless firewall filtering and quality of service (QoS) as per your network requirements and have appropriate security policies to manage traffic in your network.
- In a typical high availability deployment, you have multiple routers and switches on the northbound and southbound sides of the network. For this example, we are using two routers on both sides of SRX Series devices. Ensure that you've configured upstream and downstream routers as per your network requirements.
- Install the Junos IKE package on your SRX Series devices using the `request system software add optional:///junos-ike.tgz` command. The `junos-ike` package is included in your Junos software packages (Junos OS Release 20.4R1 onwards).

### Topology

[Figure 59 on page 797](#) shows the topology used in this example.

Figure 59: Multinode High Availability in Layer 3 Network



As shown in the topology, two SRX Series devices (SRX-1 and SRX-2) are connected to adjacent routers on trust and untrust side forming a BGP neighborhood. An encrypted logical interchassis link (ICL) connects the nodes over a routed network. The nodes communicate with each other using a routable IP address (floating IP address) over the network.

The SRX-03 device acts as a peer device to the Multinode High Availability setup and it establishes IPsec VPN tunnels with SRX-01 and SRX-02 devices.

You'll perform the following tasks to build a Multinode High Availability setup:

- Configure a pair of SRX Series devices as local and peer nodes by assigning IDs.
- Configure services redundancy groups (SRG1 and SRG2).

- Configure a loopback interface (lo0.0) to host the floating IP address and to reach the peer gateway. Using the loopback interface ensures that at any given point, traffic from the adjacent routers will be steered toward the floating IP address (that is, toward the active node).
- Configure IP probes for the activeness determination and enforcement
- Configure a signal route required for activeness enforcement and use it along with the route exists policy.
- Configure a VPN profile for the high availability (ICL) traffic using IKEv2.
- Configure BFD monitoring options
- Configure a routing policy and routing options
- Configure interfaces and zones according to your network requirement. You must allow services such as IKE for link encryption and SSH for configuration synchronization as host-inbound system services on the security zone that is associated with the ICL.
- Create a group configuration for IPsec VPN on SRX-01 and SRX-02 devices to set up a tunnel with VPN peer device (SRX-03). Configuration groups enable you to apply common elements that are reused within the same configuration.
- Configure IPsec VPN options to establish tunnels with SRX-03 device and enable IPsec VPN configuration synchronization on both the devices (SRX-01 and SRX-02) by using [groups] option.
- Configure VPN peer device with IPsec VPN options.

For interchassis link (ICL), we recommend the following configuration:

- In general, you can use Aggregated Ethernet (AE) or a revenue Ethernet port on the SRX Series devices to setup an ICL connection. In this example, we've used GE ports for the ICL. We've also configured a routing instance for the ICL path to ensure maximum segmentation.
- Do not to use the dedicated HA ports (control and fabric ports) if available on your SRX Series device).
- Set MTU of 1514
- Allow the following services on the security zone associated with interfaces used for ICL
  - IKE, high-availability, SSH
  - Protocols depending on the routing protocol you need.
  - BFD to monitor the neighboring routes.

[Table 46 on page 799](#) shows the details on interfaces configuration used in this example.



Table 46: Interfaces and IP Address Configuration on Security Devices

Device	Interface	Zone	IP Address	Configured For
SRX-01	lo0	Untrust	10.11.0.1/32	Floating IP address IKE Gateway address
			10.12.0.1/32	IKE Gateway address
	ge-0/0/2	ICL	10.22.0.2/24	Connecting ICL
	ge-0/0/4	Trust	10.5.0.1/24	Connects to R2 router
	ge-0/0/3	Untrust	10.3.0.2/24	Connects to R1 router
SRX-02	lo0	Untrust	10.12.0.1/32	Floating IP address IKE Gateway address
			10.11.0.1/32	IKE Gateway address
	ge-0/0/2	ICL	10.22.0.1/24	Connecting ICL
	ge-0/0/3	Untrust	10.2.0.2/24	Connects to R1 router
	ge-0/0/4	Trust	10.4.0.1/24	Connects to R2 router
SRX-03	lo0	Untrust	10.112.0.1/32	IKE Gateway address

Table 46: Interfaces and IP Address Configuration on Security Devices *(Continued)*

Device	Interface	Zone	IP Address	Configured For
			10.112.0.5/32	IKE Gateway address
	ge-0/0/0	Untrust	10.7.0.1/24	Connects to R2 router
	ge-0/0/2	Trust	10.6.0.2/24	Connects to client device

Table 47: Interfaces and IP Address Configuration on Routing Devices

Device	Interface	IP Address	Configured for
R2	lo0	10.111.0.2/32	Loopback interface address of R2
	ge-0/0/1	10.4.0.2/24	Connects to SRX-02
	ge-0/0/0	10.5.0.2/24	Connects to SRX-01
	ge-0/0/2	10.7.0.2/24	Connects to SRX-03 (VPN peer device)
R1	lo0	10.111.0.1/32	Loopback interface address of R1
	ge-0/0/0	10.3.0.1/24	Connects to SRX-01
	ge-0/0/1	10.2.0.1/24	Connects to SRX-02

## Configuration

### IN THIS SECTION

- [CLI Quick Configuration | 801](#)
- [Configuration | 815](#)
- [Configuration \(SRX-03\) \(VPN Peer Device\) | 826](#)
- [Results \(SRX-01\) | 829](#)
- [Results \(SRX-02\) | 841](#)
- [Results \(SRX-3\) \(VPN Peer Device\) | 852](#)

### CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the [edit] hierarchy level, and then enter `commit` from configuration mode.

These configurations are captured from a lab environment and are provided for reference only. Actual configurations may vary based on the specific requirements of your environment.

#### SRX-01 Device

```
set groups vpn_config when peers SRX-01
set groups vpn_config when peers SRX-02
set groups vpn_config security ike proposal SRG1_IKE_PROP authentication-method pre-shared-keys
set groups vpn_config security ike proposal SRG1_IKE_PROP dh-group group14
set groups vpn_config security ike proposal SRG1_IKE_PROP authentication-algorithm sha-256
set groups vpn_config security ike proposal SRG1_IKE_PROP encryption-algorithm aes-256-cbc
set groups vpn_config security ike proposal SRG1_IKE_PROP lifetime-seconds 3600
set groups vpn_config security ike proposal SRG2_IKE_PROP authentication-method pre-shared-keys
set groups vpn_config security ike proposal SRG2_IKE_PROP dh-group group14
set groups vpn_config security ike proposal SRG2_IKE_PROP authentication-algorithm sha-256
set groups vpn_config security ike proposal SRG2_IKE_PROP encryption-algorithm aes-256-cbc
set groups vpn_config security ike proposal SRG2_IKE_PROP lifetime-seconds 3600
set groups vpn_config security ike policy SRG1_IKE_POL1 proposals SRG1_IKE_PROP
set groups vpn_config security ike policy SRG1_IKE_POL1 pre-shared-key ascii-text "$ABC123"
set groups vpn_config security ike policy SRG2_IKE_POL500 proposals SRG2_IKE_PROP
set groups vpn_config security ike policy SRG2_IKE_POL500 pre-shared-key ascii-text "$ABC123"
```

```

set groups vpn_config security ike gateway SRG1_IKE_GW1 ike-policy SRG1_IKE_POL1
set groups vpn_config security ike gateway SRG1_IKE_GW1 address 10.112.0.1
set groups vpn_config security ike gateway SRG1_IKE_GW1 external-interface lo0
set groups vpn_config security ike gateway SRG1_IKE_GW1 local-address 10.11.0.1
set groups vpn_config security ike gateway SRG1_IKE_GW1 version v2-only
set groups vpn_config security ike gateway SRG2_IKE_GW500 ike-policy SRG2_IKE_POL500
set groups vpn_config security ike gateway SRG2_IKE_GW500 address 10.112.0.5
set groups vpn_config security ike gateway SRG2_IKE_GW500 external-interface lo0
set groups vpn_config security ike gateway SRG2_IKE_GW500 local-address 10.12.0.1
set groups vpn_config security ike gateway SRG2_IKE_GW500 version v2-only
set groups vpn_config security ipsec proposal SRG1_IPSEC_PROP protocol esp
set groups vpn_config security ipsec proposal SRG1_IPSEC_PROP authentication-algorithm hmac-
sha-256-128
set groups vpn_config security ipsec proposal SRG1_IPSEC_PROP encryption-algorithm aes-256-cbc
set groups vpn_config security ipsec proposal SRG1_IPSEC_PROP lifetime-seconds 1800
set groups vpn_config security ipsec proposal SRG2_IPSEC_PROP protocol esp
set groups vpn_config security ipsec proposal SRG2_IPSEC_PROP authentication-algorithm hmac-
sha-256-128
set groups vpn_config security ipsec proposal SRG2_IPSEC_PROP encryption-algorithm aes-256-cbc
set groups vpn_config security ipsec proposal SRG2_IPSEC_PROP lifetime-seconds 1800
set groups vpn_config security ipsec policy SRG1_IPSEC_POL1 proposals SRG1_IPSEC_PROP
set groups vpn_config security ipsec policy SRG2_IPSEC_POL501 proposals SRG2_IPSEC_PROP
set groups vpn_config security ipsec policy SRG2_IPSEC_POL500 proposals SRG2_IPSEC_PROP
set groups vpn_config security ipsec policy SRG2_IPSEC_POL502 proposals SRG2_IPSEC_PROP
set groups vpn_config security ipsec policy SRG2_IPSEC_POL503 proposals SRG2_IPSEC_PROP
set groups vpn_config security ipsec vpn SRG1_IPSEC_VPN1 bind-interface st0.1
set groups vpn_config security ipsec vpn SRG1_IPSEC_VPN1 ike gateway SRG1_IKE_GW1
set groups vpn_config security ipsec vpn SRG1_IPSEC_VPN1 ike ipsec-policy SRG1_IPSEC_POL1
set groups vpn_config security ipsec vpn SRG1_IPSEC_VPN1 traffic-selector ts1 local-ip
10.1.0.2/32
set groups vpn_config security ipsec vpn SRG1_IPSEC_VPN1 traffic-selector ts1 remote-ip
10.7.0.2/32
set groups vpn_config security ipsec vpn SRG1_IPSEC_VPN1 establish-tunnels on-traffic
set groups vpn_config security ipsec vpn SRG2_IPSEC_VPN500 bind-interface st0.500
set groups vpn_config security ipsec vpn SRG2_IPSEC_VPN500 ike gateway SRG2_IKE_GW500
set groups vpn_config security ipsec vpn SRG2_IPSEC_VPN500 ike ipsec-policy SRG2_IPSEC_POL500
set groups vpn_config security ipsec vpn SRG2_IPSEC_VPN500 traffic-selector ts500 local-ip
10.8.0.2/32
set groups vpn_config security ipsec vpn SRG2_IPSEC_VPN500 traffic-selector ts500 remote-ip
10.9.0.2/32
set groups vpn_config security ipsec vpn SRG2_IPSEC_VPN500 establish-tunnels on-traffic
set groups vpn_config security zones security-zone vpn host-inbound-traffic system-services ike
set groups vpn_config security zones security-zone vpn host-inbound-traffic protocols all

```

```

set groups vpn_config security zones security-zone vpn interfaces st0.1
set groups vpn_config security zones security-zone vpn interfaces st0.500
set groups vpn_config interfaces st0 unit 1 family inet
set groups vpn_config interfaces st0 unit 1 family inet6
set groups vpn_config interfaces st0 unit 500 family inet
set groups vpn_config interfaces st0 unit 500 family inet6
set apply-groups vpn_config
set chassis high-availability local-id 2
set chassis high-availability local-id local-ip 10.22.0.2
set chassis high-availability peer-id 1 peer-ip 10.22.0.1
set chassis high-availability peer-id 1 interface ge-0/0/2.0
set chassis high-availability peer-id 1 vpn-profile ICL_IPSEC_VPN
set chassis high-availability peer-id 1 liveness-detection minimum-interval 200
set chassis high-availability peer-id 1 liveness-detection multiplier 3
set chassis high-availability services-redundancy-group 1 deployment-type routing
set chassis high-availability services-redundancy-group 1 peer-id 1
set chassis high-availability services-redundancy-group 1 activeness-probe dest-ip 10.111.0.1
set chassis high-availability services-redundancy-group 1 activeness-probe dest-ip src-ip
10.11.0.1
set chassis high-availability services-redundancy-group 1 monitor bfd-liveliness 10.5.0.2 src-ip
10.5.0.1
set chassis high-availability services-redundancy-group 1 monitor bfd-liveliness 10.5.0.2
session-type singlehop
set chassis high-availability services-redundancy-group 1 monitor bfd-liveliness 10.5.0.2
interface ge-0/0/3.0
set chassis high-availability services-redundancy-group 1 monitor interface ge-0/0/3
set chassis high-availability services-redundancy-group 1 monitor interface ge-0/0/4
set chassis high-availability services-redundancy-group 1 active-signal-route 10.39.1.1
set chassis high-availability services-redundancy-group 1 backup-signal-route 10.39.1.2
set chassis high-availability services-redundancy-group 1 prefix-list SRG1_PFX
set chassis high-availability services-redundancy-group 1 managed-services ipsec
set chassis high-availability services-redundancy-group 1 preemption
set chassis high-availability services-redundancy-group 1 activeness-priority 1
set chassis high-availability services-redundancy-group 2 peer-id 1
set chassis high-availability services-redundancy-group 2 activeness-probe dest-ip 10.111.0.1
set chassis high-availability services-redundancy-group 2 activeness-probe dest-ip src-ip
10.12.0.1
set chassis high-availability services-redundancy-group 2 monitor bfd-liveliness 10.5.0.2 src-ip
10.5.0.1
set chassis high-availability services-redundancy-group 2 monitor bfd-liveliness 10.5.0.2
session-type singlehop
set chassis high-availability services-redundancy-group 2 monitor bfd-liveliness 10.5.0.2
interface ge-0/0/3.0

```

```

set chassis high-availability services-redundancy-group 2 monitor interface ge-0/0/3
set chassis high-availability services-redundancy-group 2 monitor interface ge-0/0/4
set chassis high-availability services-redundancy-group 2 active-signal-route 10.49.1.1
set chassis high-availability services-redundancy-group 2 backup-signal-route 10.49.1.2
set chassis high-availability services-redundancy-group 2 prefix-list SRG2_PFX
set chassis high-availability services-redundancy-group 2 managed-services ipsec
set chassis high-availability services-redundancy-group 2 preemption
set chassis high-availability services-redundancy-group 2 activeness-priority 200
set security ike proposal ICL_IKE_PROP description interchassis_link_encr_tunnel
set security ike proposal ICL_IKE_PROP authentication-method pre-shared-keys
set security ike proposal ICL_IKE_PROP dh-group group14
set security ike proposal ICL_IKE_PROP authentication-algorithm sha-256
set security ike proposal ICL_IKE_PROP encryption-algorithm aes-256-cbc
set security ike proposal ICL_IKE_PROP lifetime-seconds 300
set security ike policy ICL_IKE_POL description interchassis_link_encr_tunnel
set security ike policy ICL_IKE_POL proposals ICL_IKE_PROP
set security ike policy ICL_IKE_POL pre-shared-key ascii-text "$ABC123"
set security ike gateway ICL_IKE_GW ike-policy ICL_IKE_POL
set security ike gateway ICL_IKE_GW version v2-only
set security ipsec proposal ICL_IPSEC_PROP description interchassis_link_encr_tunnel
set security ipsec proposal ICL_IPSEC_PROP protocol esp
set security ipsec proposal ICL_IPSEC_PROP encryption-algorithm aes-256-gcm
set security ipsec proposal ICL_IPSEC_PROP lifetime-seconds 300
set security ipsec policy ICL_IPSEC_POL description interchassis_link_encr_tunnel
set security ipsec policy ICL_IPSEC_POL proposals ICL_IPSEC_PROP
set security ipsec vpn ICL_IPSEC_VPN ha-link-encryption
set security ipsec vpn ICL_IPSEC_VPN ike gateway ICL_IKE_GW
set security ipsec vpn ICL_IPSEC_VPN ike ipsec-policy ICL_IPSEC_POL
set security policies default-policy permit-all
set security zones security-zone vpn host-inbound-traffic system-services ike
set security zones security-zone vpn host-inbound-traffic protocols all
set security zones security-zone vpn interfaces st0.1
set security zones security-zone untrust host-inbound-traffic system-services ike
set security zones security-zone untrust host-inbound-traffic system-services ping
set security zones security-zone untrust host-inbound-traffic protocols bfd
set security zones security-zone untrust host-inbound-traffic protocols bgp
set security zones security-zone untrust interfaces lo0.0
set security zones security-zone untrust interfaces ge-0/0/3.0
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 ge-0/0/4.0
set security zones security-zone icl_zone host-inbound-traffic system-services ike
set security zones security-zone icl_zone host-inbound-traffic system-services ping

```

```

set security zones security-zone icl_zone host-inbound-traffic system-services high-availability
set security zones security-zone icl_zone host-inbound-traffic system-services ssh
set security zones security-zone icl_zone host-inbound-traffic protocols bfd
set security zones security-zone icl_zone host-inbound-traffic protocols bgp
set security zones security-zone icl_zone interfaces ge-0/0/2.0
set interfaces ge-0/0/1 unit 0 family inet
set interfaces ge-0/0/2 description inter_chassis_link
set interfaces ge-0/0/2 unit 0 family inet address 10.22.0.2/24
set interfaces ge-0/0/3 description untrust
set interfaces ge-0/0/3 unit 0 family inet address 10.3.0.2/24
set interfaces ge-0/0/4 description trust
set interfaces ge-0/0/4 unit 0 family inet address 10.5.0.1/24
set interfaces lo0 apply-groups-except global
set interfaces lo0 description untrust
set interfaces lo0 unit 0 family inet address 10.11.0.1/32
set interfaces lo0 unit 0 family inet address 10.12.0.1/32
set interfaces st0 unit 1
set policy-options prefix-list SRG1_PFX 10.11.0.0/24
set policy-options prefix-list SRG2_PFX 10.12.0.0/24
set policy-options route-filter-list srg1_rf_list 10.11.0.0/24 orlonger
set policy-options route-filter-list srg1_rf_list 10.7.0.0/16 orlonger
set policy-options route-filter-list srg1_rf_list 10.1.0.0/16 orlonger
set policy-options route-filter-list srg2_rf_list 10.12.0.0/24 orlonger
set policy-options route-filter-list srg2_rf_list 10.9.0.0/16 orlonger
set policy-options route-filter-list srg2_rf_list 10.8.0.0/16 orlonger
set policy-options policy-statement mnha-route-policy term 1 from route-filter-list srg1_rf_list
set policy-options policy-statement mnha-route-policy term 1 from condition
active_route_exists_srg1
set policy-options policy-statement mnha-route-policy term 1 then metric 10
set policy-options policy-statement mnha-route-policy term 1 then accept
set policy-options policy-statement mnha-route-policy term 2 from route-filter-list srg1_rf_list
set policy-options policy-statement mnha-route-policy term 2 from condition
backup_route_exists_srg1
set policy-options policy-statement mnha-route-policy term 2 then metric 20
set policy-options policy-statement mnha-route-policy term 2 then accept
set policy-options policy-statement mnha-route-policy term 3 from route-filter-list srg2_rf_list
set policy-options policy-statement mnha-route-policy term 3 from condition
active_route_exists_srg2
set policy-options policy-statement mnha-route-policy term 3 then metric 10
set policy-options policy-statement mnha-route-policy term 3 then accept
set policy-options policy-statement mnha-route-policy term 4 from route-filter-list srg2_rf_list
set policy-options policy-statement mnha-route-policy term 4 from condition
backup_route_exists_srg2

```

```

set policy-options policy-statement mnha-route-policy term 4 then metric 20
set policy-options policy-statement mnha-route-policy term 4 then accept
set policy-options policy-statement mnha-route-policy term default then reject
set policy-options condition active_route_exists_srg1 if-route-exists address-family inet
10.39.1.1/32
set policy-options condition active_route_exists_srg1 if-route-exists address-family inet table
inet.0
set policy-options condition active_route_exists_srg2 if-route-exists address-family inet
10.49.1.1/32
set policy-options condition active_route_exists_srg2 if-route-exists address-family inet table
inet.0
set policy-options condition backup_route_exists_srg1 if-route-exists address-family inet
10.39.1.2/32
set policy-options condition backup_route_exists_srg1 if-route-exists address-family inet table
inet.0
set policy-options condition backup_route_exists_srg2 if-route-exists address-family inet
10.49.1.2/32
set policy-options condition backup_route_exists_srg2 if-route-exists address-family inet table
inet.0
set protocols bgp group trust type internal
set protocols bgp group trust local-address 10.3.0.2
set protocols bgp group trust export mnha-route-policy
set protocols bgp group trust local-as 100
set protocols bgp group trust bfd-liveness-detection minimum-interval 500
set protocols bgp group trust bfd-liveness-detection minimum-receive-interval 500
set protocols bgp group trust bfd-liveness-detection multiplier 3
set protocols bgp group trust neighbor 10.3.0.1
set protocols bgp group untrust type internal
set protocols bgp group untrust local-address 10.5.0.1
set protocols bgp group untrust export mnha-route-policy
set protocols bgp group untrust local-as 100
set protocols bgp group untrust bfd-liveness-detection minimum-interval 500
set protocols bgp group untrust bfd-liveness-detection minimum-receive-interval 500
set protocols bgp group untrust bfd-liveness-detection multiplier 3
set protocols bgp group untrust neighbor 10.5.0.2
set routing-options autonomous-system 100
set routing-options static route 10.7.0.0/16 next-hop 10.5.0.2
set routing-options static route 10.112.0.0/24 next-hop 10.5.0.2

```



## SRX-02 Device

```

set groups vpn_config when peers SRX-01
set groups vpn_config when peers SRX-02
set groups vpn_config security ike proposal SRG1_IKE_PROP authentication-method pre-shared-keys
set groups vpn_config security ike proposal SRG1_IKE_PROP dh-group group14
set groups vpn_config security ike proposal SRG1_IKE_PROP authentication-algorithm sha-256
set groups vpn_config security ike proposal SRG1_IKE_PROP encryption-algorithm aes-256-cbc
set groups vpn_config security ike proposal SRG1_IKE_PROP lifetime-seconds 3600
set groups vpn_config security ike proposal SRG2_IKE_PROP authentication-method pre-shared-keys
set groups vpn_config security ike proposal SRG2_IKE_PROP dh-group group14
set groups vpn_config security ike proposal SRG2_IKE_PROP authentication-algorithm sha-256
set groups vpn_config security ike proposal SRG2_IKE_PROP encryption-algorithm aes-256-cbc
set groups vpn_config security ike proposal SRG2_IKE_PROP lifetime-seconds 3600
set groups vpn_config security ike policy SRG1_IKE_POL1 proposals SRG1_IKE_PROP
set groups vpn_config security ike policy SRG1_IKE_POL1 pre-shared-key ascii-text "$ABC123"
set groups vpn_config security ike policy SRG2_IKE_POL500 proposals SRG2_IKE_PROP
set groups vpn_config security ike policy SRG2_IKE_POL500 pre-shared-key ascii-text "$ABC123"
set groups vpn_config security ike gateway SRG1_IKE_GW1 ike-policy SRG1_IKE_POL1
set groups vpn_config security ike gateway SRG1_IKE_GW1 address 10.112.0.1
set groups vpn_config security ike gateway SRG1_IKE_GW1 external-interface lo0
set groups vpn_config security ike gateway SRG1_IKE_GW1 local-address 10.11.0.1
set groups vpn_config security ike gateway SRG1_IKE_GW1 version v2-only
set groups vpn_config security ike gateway SRG2_IKE_GW500 ike-policy SRG2_IKE_POL500
set groups vpn_config security ike gateway SRG2_IKE_GW500 address 10.112.0.5
set groups vpn_config security ike gateway SRG2_IKE_GW500 external-interface lo0
set groups vpn_config security ike gateway SRG2_IKE_GW500 local-address 10.12.0.1
set groups vpn_config security ike gateway SRG2_IKE_GW500 version v2-only
set groups vpn_config security ipsec proposal SRG1_IPSEC_PROP protocol esp
set groups vpn_config security ipsec proposal SRG1_IPSEC_PROP authentication-algorithm hmac-sha-256-128
set groups vpn_config security ipsec proposal SRG1_IPSEC_PROP encryption-algorithm aes-256-cbc
set groups vpn_config security ipsec proposal SRG1_IPSEC_PROP lifetime-seconds 1800
set groups vpn_config security ipsec proposal SRG2_IPSEC_PROP protocol esp
set groups vpn_config security ipsec proposal SRG2_IPSEC_PROP authentication-algorithm hmac-sha-256-128
set groups vpn_config security ipsec proposal SRG2_IPSEC_PROP encryption-algorithm aes-256-cbc
set groups vpn_config security ipsec proposal SRG2_IPSEC_PROP lifetime-seconds 1800
set groups vpn_config security ipsec policy SRG1_IPSEC_POL1 proposals SRG1_IPSEC_PROP
set groups vpn_config security ipsec policy SRG2_IPSEC_POL501 proposals SRG2_IPSEC_PROP
set groups vpn_config security ipsec policy SRG2_IPSEC_POL500 proposals SRG2_IPSEC_PROP
set groups vpn_config security ipsec policy SRG2_IPSEC_POL502 proposals SRG2_IPSEC_PROP

```

```

set groups vpn_config security ipsec policy SRG2_IPSEC_POL503 proposals SRG2_IPSEC_PROP
set groups vpn_config security ipsec vpn SRG1_IPSEC_VPN1 bind-interface st0.1
set groups vpn_config security ipsec vpn SRG1_IPSEC_VPN1 ike gateway SRG1_IKE_GW1
set groups vpn_config security ipsec vpn SRG1_IPSEC_VPN1 ike ipsec-policy SRG1_IPSEC_POL1
set groups vpn_config security ipsec vpn SRG1_IPSEC_VPN1 traffic-selector ts1 local-ip
10.1.0.2/32
set groups vpn_config security ipsec vpn SRG1_IPSEC_VPN1 traffic-selector ts1 remote-ip
10.7.0.2/32
set groups vpn_config security ipsec vpn SRG1_IPSEC_VPN1 establish-tunnels on-traffic
set groups vpn_config security ipsec vpn SRG2_IPSEC_VPN500 bind-interface st0.500
set groups vpn_config security ipsec vpn SRG2_IPSEC_VPN500 ike gateway SRG2_IKE_GW500
set groups vpn_config security ipsec vpn SRG2_IPSEC_VPN500 ike ipsec-policy SRG2_IPSEC_POL500
set groups vpn_config security ipsec vpn SRG2_IPSEC_VPN500 traffic-selector ts500 local-ip
10.8.0.2/32
set groups vpn_config security ipsec vpn SRG2_IPSEC_VPN500 traffic-selector ts500 remote-ip
10.9.0.2/32
set groups vpn_config security ipsec vpn SRG2_IPSEC_VPN500 establish-tunnels on-traffic
set groups vpn_config security zones security-zone vpn host-inbound-traffic system-services ike
set groups vpn_config security zones security-zone vpn host-inbound-traffic protocols all
set groups vpn_config security zones security-zone vpn interfaces st0.1
set groups vpn_config security zones security-zone vpn interfaces st0.500
set groups vpn_config interfaces st0 unit 1 family inet
set groups vpn_config interfaces st0 unit 1 family inet6
set groups vpn_config interfaces st0 unit 500 family inet
set groups vpn_config interfaces st0 unit 500 family inet6
set apply-groups vpn_config
set chassis high-availability local-id 1
set chassis high-availability local-id local-ip 10.22.0.1
set chassis high-availability peer-id 2 peer-ip 10.22.0.2
set chassis high-availability peer-id 2 interface ge-0/0/2.0
set chassis high-availability peer-id 2 vpn-profile ICL_IPSEC_VPN
set chassis high-availability peer-id 2 liveness-detection minimum-interval 200
set chassis high-availability peer-id 2 liveness-detection multiplier 3
set chassis high-availability services-redundancy-group 1 deployment-type routing
set chassis high-availability services-redundancy-group 1 peer-id 2
set chassis high-availability services-redundancy-group 1 activeness-probe dest-ip 10.111.0.1
set chassis high-availability services-redundancy-group 1 activeness-probe dest-ip src-ip
10.11.0.1
set chassis high-availability services-redundancy-group 1 monitor bfd-liveliness 10.4.0.2 src-ip
10.4.0.1
set chassis high-availability services-redundancy-group 1 monitor bfd-liveliness 10.4.0.2
session-type singlehop
set chassis high-availability services-redundancy-group 1 monitor bfd-liveliness 10.4.0.2

```

```

interface ge-0/0/3.0
set chassis high-availability services-redundancy-group 1 monitor interface ge-0/0/3
set chassis high-availability services-redundancy-group 1 monitor interface ge-0/0/4
set chassis high-availability services-redundancy-group 1 active-signal-route 10.39.1.1
set chassis high-availability services-redundancy-group 1 backup-signal-route 10.39.1.2
set chassis high-availability services-redundancy-group 1 prefix-list SRG1_PFX
set chassis high-availability services-redundancy-group 1 managed-services ipsec
set chassis high-availability services-redundancy-group 1 preemption
set chassis high-availability services-redundancy-group 1 activeness-priority 200
set chassis high-availability services-redundancy-group 2 peer-id 2
set chassis high-availability services-redundancy-group 2 activeness-probe dest-ip 10.111.0.1
set chassis high-availability services-redundancy-group 2 activeness-probe dest-ip src-ip
10.12.0.1
set chassis high-availability services-redundancy-group 2 monitor bfd-liveliness 10.4.0.2 src-ip
10.4.0.1
set chassis high-availability services-redundancy-group 2 monitor bfd-liveliness 10.4.0.2
session-type singlehop
set chassis high-availability services-redundancy-group 2 monitor bfd-liveliness 10.4.0.2
interface ge-0/0/3.0
set chassis high-availability services-redundancy-group 2 monitor interface ge-0/0/3
set chassis high-availability services-redundancy-group 2 monitor interface ge-0/0/4
set chassis high-availability services-redundancy-group 2 active-signal-route 10.49.1.1
set chassis high-availability services-redundancy-group 2 backup-signal-route 10.49.1.2
set chassis high-availability services-redundancy-group 2 prefix-list SRG2_PFX
set chassis high-availability services-redundancy-group 2 managed-services ipsec
set chassis high-availability services-redundancy-group 2 preemption
set chassis high-availability services-redundancy-group 2 activeness-priority 1
set security ike proposal ICL_IKE_PROP description interchassis_link_encr_tunnel
set security ike proposal ICL_IKE_PROP authentication-method pre-shared-keys
set security ike proposal ICL_IKE_PROP dh-group group14
set security ike proposal ICL_IKE_PROP authentication-algorithm sha-256
set security ike proposal ICL_IKE_PROP encryption-algorithm aes-256-cbc
set security ike proposal ICL_IKE_PROP lifetime-seconds 300
set security ike policy ICL_IKE_POL description interchassis_link_encr_tunnel
set security ike policy ICL_IKE_POL proposals ICL_IKE_PROP
set security ike policy ICL_IKE_POL pre-shared-key ascii-text "$ABC123"
set security ike gateway ICL_IKE_GW ike-policy ICL_IKE_POL
set security ike gateway ICL_IKE_GW version v2-only
set security ipsec proposal ICL_IPSEC_PROP description interchassis_link_encr_tunnel
set security ipsec proposal ICL_IPSEC_PROP protocol esp
set security ipsec proposal ICL_IPSEC_PROP encryption-algorithm aes-256-gcm
set security ipsec proposal ICL_IPSEC_PROP lifetime-seconds 300
set security ipsec policy ICL_IPSEC_POL description interchassis_link_encr_tunnel

```

```

set security ipsec policy ICL_IPSEC_POL proposals ICL_IPSEC_PROP
set security ipsec vpn ICL_IPSEC_VPN ha-link-encryption
set security ipsec vpn ICL_IPSEC_VPN ike gateway ICL_IKE_GW
set security ipsec vpn ICL_IPSEC_VPN ike ipsec-policy ICL_IPSEC_POL
set security policies default-policy permit-all
set security zones security-zone untrust host-inbound-traffic system-services ike
set security zones security-zone untrust host-inbound-traffic system-services ping
set security zones security-zone untrust host-inbound-traffic protocols bfd
set security zones security-zone untrust host-inbound-traffic protocols bgp
set security zones security-zone untrust interfaces lo0.0
set security zones security-zone untrust interfaces ge-0/0/3.0
set security zones security-zone vpn host-inbound-traffic system-services ike
set security zones security-zone vpn host-inbound-traffic protocols all
set security zones security-zone vpn interfaces st0.1
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 ge-0/0/4.0
set security zones security-zone icl_zone host-inbound-traffic system-services ike
set security zones security-zone icl_zone host-inbound-traffic system-services ping
set security zones security-zone icl_zone host-inbound-traffic system-services high-availability
set security zones security-zone icl_zone host-inbound-traffic system-services ssh
set security zones security-zone icl_zone host-inbound-traffic protocols bfd
set security zones security-zone icl_zone host-inbound-traffic protocols bgp
set security zones security-zone icl_zone interfaces ge-0/0/2.0
set interfaces ge-0/0/1 unit 0 family inet
set interfaces ge-0/0/2 description inter_chassis_link
set interfaces ge-0/0/2 unit 0 family inet address 10.22.0.1/24
set interfaces ge-0/0/3 description untrust
set interfaces ge-0/0/3 unit 0 family inet address 10.2.0.2/24
set interfaces ge-0/0/4 description trust
set interfaces ge-0/0/4 unit 0 family inet address 10.4.0.1/24
set interfaces lo0 apply-groups-except global
set interfaces lo0 description untrust
set interfaces lo0 unit 0 family inet address 10.11.0.1/32
set interfaces lo0 unit 0 family inet address 10.12.0.1/32
set interfaces st0 unit 1 family inet
set interfaces st0 unit 1 family inet6
set policy-options prefix-list SRG1_PFX 10.11.0.0/24
set policy-options prefix-list SRG2_PFX 10.12.0.0/24
set policy-options route-filter-list srg1_rf_list 10.11.0.0/24 orlonger
set policy-options route-filter-list srg1_rf_list 10.7.0.0/24 orlonger
set policy-options route-filter-list srg1_rf_list 10.1.0.0/24 orlonger
set policy-options route-filter-list srg2_rf_list 10.12.0.0/24 orlonger

```

```

set policy-options route-filter-list srg2_rf_list 10.9.0.0/24 orlonger
set policy-options route-filter-list srg2_rf_list 10.8.0.0/24 orlonger
set policy-options policy-statement mnha-route-policy term 1 from route-filter-list srg1_rf_list
set policy-options policy-statement mnha-route-policy term 1 from condition
active_route_exists_srg1
set policy-options policy-statement mnha-route-policy term 1 then metric 10
set policy-options policy-statement mnha-route-policy term 1 then accept
set policy-options policy-statement mnha-route-policy term 2 from route-filter-list srg1_rf_list
set policy-options policy-statement mnha-route-policy term 2 from condition
backup_route_exists_srg1
set policy-options policy-statement mnha-route-policy term 2 then metric 20
set policy-options policy-statement mnha-route-policy term 2 then accept
set policy-options policy-statement mnha-route-policy term 3 from route-filter-list srg2_rf_list
set policy-options policy-statement mnha-route-policy term 3 from condition
active_route_exists_srg2
set policy-options policy-statement mnha-route-policy term 3 then metric 10
set policy-options policy-statement mnha-route-policy term 3 then accept
set policy-options policy-statement mnha-route-policy term 4 from route-filter-list srg2_rf_list
set policy-options policy-statement mnha-route-policy term 4 from condition
backup_route_exists_srg2
set policy-options policy-statement mnha-route-policy term 4 then metric 20
set policy-options policy-statement mnha-route-policy term 4 then accept
set policy-options policy-statement mnha-route-policy term default then reject
set policy-options condition active_route_exists_srg1 if-route-exists address-family inet
10.39.1.1/32
set policy-options condition active_route_exists_srg1 if-route-exists address-family inet table
inet.0
set policy-options condition active_route_exists_srg2 if-route-exists address-family inet
10.49.1.1/32
set policy-options condition active_route_exists_srg2 if-route-exists address-family inet table
inet.0
set policy-options condition backup_route_exists_srg1 if-route-exists address-family inet
10.39.1.2/32
set policy-options condition backup_route_exists_srg1 if-route-exists address-family inet table
inet.0
set policy-options condition backup_route_exists_srg2 if-route-exists address-family inet
10.49.1.2/32
set policy-options condition backup_route_exists_srg2 if-route-exists address-family inet table
inet.0
set protocols bgp group trust type internal
set protocols bgp group trust local-address 10.2.0.2
set protocols bgp group trust export mnha-route-policy
set protocols bgp group trust local-as 100

```

```

set protocols bgp group trust bfd-liveness-detection minimum-interval 500
set protocols bgp group trust bfd-liveness-detection minimum-receive-interval 500
set protocols bgp group trust bfd-liveness-detection multiplier 3
set protocols bgp group trust neighbor 10.2.0.1
set protocols bgp group untrust type internal
set protocols bgp group untrust local-address 10.4.0.1
set protocols bgp group untrust export mnha-route-policy
set protocols bgp group untrust local-as 100
set protocols bgp group untrust bfd-liveness-detection minimum-interval 500
set protocols bgp group untrust bfd-liveness-detection minimum-receive-interval 500
set protocols bgp group untrust bfd-liveness-detection multiplier 3
set protocols bgp group untrust neighbor 10.4.0.2
set routing-options autonomous-system 100
set routing-options static route 10.7.0.0/24 next-hop 10.4.0.2
set routing-options static route 10.112.0.0/24 next-hop 10.4.0.2

```

### SRX-3 Device

```

set security ike proposal SRG1_IKE_PROP authentication-method pre-shared-keys
set security ike proposal SRG1_IKE_PROP dh-group group14
set security ike proposal SRG1_IKE_PROP authentication-algorithm sha-256
set security ike proposal SRG1_IKE_PROP encryption-algorithm aes-256-cbc
set security ike proposal SRG1_IKE_PROP lifetime-seconds 3600
set security ike proposal SRG2_IKE_PROP authentication-method pre-shared-keys
set security ike proposal SRG2_IKE_PROP dh-group group14
set security ike proposal SRG2_IKE_PROP authentication-algorithm sha-256
set security ike proposal SRG2_IKE_PROP encryption-algorithm aes-256-cbc
set security ike proposal SRG2_IKE_PROP lifetime-seconds 3600
set security ike policy SRG1_IKE_POL1 proposals SRG1_IKE_PROP
set security ike policy SRG1_IKE_POL1 pre-shared-key ascii-text "$ABC123"
set security ike policy SRG2_IKE_POL500 proposals SRG2_IKE_PROP
set security ike policy SRG2_IKE_POL500 pre-shared-key ascii-text "$ABC123"
set security ike gateway SRG1_IKE_GW1 ike-policy SRG1_IKE_POL1
set security ike gateway SRG1_IKE_GW1 address 10.11.0.1
set security ike gateway SRG1_IKE_GW1 external-interface lo0
set security ike gateway SRG1_IKE_GW1 local-address 10.112.0.1
set security ike gateway SRG1_IKE_GW1 version v2-only
set security ike gateway SRG2_IKE_GW500 ike-policy SRG2_IKE_POL500
set security ike gateway SRG2_IKE_GW500 address 10.12.0.1
set security ike gateway SRG2_IKE_GW500 external-interface lo0
set security ike gateway SRG2_IKE_GW500 local-address 10.112.0.5
set security ike gateway SRG2_IKE_GW500 version v2-only

```

```

set security ipsec proposal SRG1_IPSEC_PROP protocol esp
set security ipsec proposal SRG1_IPSEC_PROP authentication-algorithm hmac-sha-256-128
set security ipsec proposal SRG1_IPSEC_PROP encryption-algorithm aes-256-cbc
set security ipsec proposal SRG1_IPSEC_PROP lifetime-seconds 1800
set security ipsec proposal SRG2_IPSEC_PROP protocol esp
set security ipsec proposal SRG2_IPSEC_PROP authentication-algorithm hmac-sha-256-128
set security ipsec proposal SRG2_IPSEC_PROP encryption-algorithm aes-256-cbc
set security ipsec proposal SRG2_IPSEC_PROP lifetime-seconds 1800
set security ipsec policy SRG1_IPSEC_POL1 proposals SRG1_IPSEC_PROP
set security ipsec policy SRG2_IPSEC_POL500 proposals SRG2_IPSEC_PROP
set security ipsec vpn SRG1_IPSEC_VPN1 bind-interface st0.1
set security ipsec vpn SRG1_IPSEC_VPN1 ike gateway SRG1_IKE_GW1
set security ipsec vpn SRG1_IPSEC_VPN1 ike ipsec-policy SRG1_IPSEC_POL1
set security ipsec vpn SRG1_IPSEC_VPN1 traffic-selector ts1 local-ip 10.7.0.2/32
set security ipsec vpn SRG1_IPSEC_VPN1 traffic-selector ts1 remote-ip 10.1.0.2/32
set security ipsec vpn SRG1_IPSEC_VPN1 establish-tunnels immediately
set security ipsec vpn SRG2_IPSEC_VPN500 bind-interface st0.500
set security ipsec vpn SRG2_IPSEC_VPN500 ike gateway SRG2_IKE_GW500
set security ipsec vpn SRG2_IPSEC_VPN500 ike ipsec-policy SRG2_IPSEC_POL500
set security ipsec vpn SRG2_IPSEC_VPN500 traffic-selector ts1 local-ip 10.9.0.2/32
set security ipsec vpn SRG2_IPSEC_VPN500 traffic-selector ts1 remote-ip 10.8.0.2/32
set security ipsec vpn SRG2_IPSEC_VPN500 establish-tunnels immediately
set security policies default-policy permit-all
set security zones security-zone untrust host-inbound-traffic system-services ike
set security zones security-zone untrust host-inbound-traffic protocols all
set security zones security-zone untrust interfaces st0.1
set security zones security-zone untrust interfaces lo0.0
set security zones security-zone untrust interfaces st0.500
set security zones security-zone untrust interfaces ge-0/0/1.0
set security zones security-zone untrust interfaces ge-0/0/0.0
set security zones security-zone trust host-inbound-traffic system-services ike
set security zones security-zone trust host-inbound-traffic protocols all
set security zones security-zone trust interfaces ge-0/0/2.0
set interfaces ge-0/0/0 description trust
set interfaces ge-0/0/0 unit 0 family inet address 10.7.0.1/24
set interfaces ge-0/0/1 description untrust
set interfaces ge-0/0/1 unit 0 family inet address 10.6.0.2/24
set interfaces ge-0/0/2 description trust
set interfaces ge-0/0/2 unit 0 family inet address 10.9.0.1/24
set interfaces lo0 description untrust
set interfaces lo0 unit 0 family inet address 10.112.0.1/32
set interfaces lo0 unit 0 family inet address 10.112.0.5/32
set interfaces st0 unit 1 family inet

```

```

set interfaces st0 unit 500 family inet
set routing-options autonomous-system 100
set routing-options static route 10.4.0.0/24 next-hop 10.7.0.2
set routing-options static route 10.5.0.0/24 next-hop 10.7.0.2
set routing-options static route 10.11.0.0/24 next-hop 10.7.0.2
set routing-options static route 10.12.0.0/24 next-hop 10.7.0.2
set routing-options static route 10.111.0.1/32 next-hop 10.7.0.2
set routing-options static route 10.111.0.2/32 next-hop 10.7.0.2

```

The following sections show configuration snippets on the routers required for setting up Multinode High Availability setup in the network.

### R1 Router

```

set interfaces ge-0/0/0 description srx_1
set interfaces ge-0/0/0 unit 0 family inet address 10.3.0.1/24
set interfaces ge-0/0/1 description srx_2
set interfaces ge-0/0/1 unit 0 family inet address 10.2.0.1/24
set interfaces lo0 description loopback
set interfaces lo0 unit 0 family inet address 10.111.0.1/32 primary
set interfaces lo0 unit 0 family inet address 10.111.0.1/32 preferred
set routing-options autonomous-system 100
set protocols bgp group srx2_group type internal
set protocols bgp group srx2_group local-address 10.2.0.1
set protocols bgp group srx2_group local-as 100
set protocols bgp group srx2_group bfd-liveness-detection minimum-interval 500
set protocols bgp group srx2_group bfd-liveness-detection minimum-receive-interval 500
set protocols bgp group srx2_group bfd-liveness-detection multiplier 3
set protocols bgp group srx2_group neighbor 10.2.0.2
set protocols bgp group srx1_group type internal
set protocols bgp group srx1_group local-address 10.3.0.1
set protocols bgp group srx1_group local-as 100
set protocols bgp group srx1_group bfd-liveness-detection minimum-interval 500
set protocols bgp group srx1_group bfd-liveness-detection minimum-receive-interval 500
set protocols bgp group srx1_group bfd-liveness-detection multiplier 3
set protocols bgp group srx1_group neighbor 10.3.0.2

```

### R2 Router

```

set interfaces ge-0/0/0 description srx_1
set interfaces ge-0/0/0 unit 0 family inet address 10.5.0.2/24
set interfaces ge-0/0/1 description srx_2

```



```

set interfaces ge-0/0/1 unit 0 family inet address 10.4.0.2/24
set interfaces ge-0/0/2 description srx-3
set interfaces ge-0/0/2 unit 0 family inet address 10.7.0.2/24
set interfaces lo0 description loopback
set interfaces lo0 unit 0 family inet address 10.111.0.2/32 primary
set interfaces lo0 unit 0 family inet address 10.111.0.2/32 preferred
set routing-options autonomous-system 100
set routing-options static route 10.112.0.0/24 next-hop 10.7.0.1
set protocols bgp group srx2_group type internal
set protocols bgp group srx2_group local-address 10.4.0.2
set protocols bgp group srx2_group local-as 100
set protocols bgp group srx2_group bfd-liveness-detection minimum-interval 500
set protocols bgp group srx2_group bfd-liveness-detection minimum-receive-interval 500
set protocols bgp group srx2_group bfd-liveness-detection multiplier 3
set protocols bgp group srx2_group neighbor 10.4.0.1
set protocols bgp group srx1_group type internal
set protocols bgp group srx1_group local-address 10.5.0.2
set protocols bgp group srx1_group local-as 100
set protocols bgp group srx1_group bfd-liveness-detection minimum-interval 500
set protocols bgp group srx1_group bfd-liveness-detection minimum-receive-interval 500
set protocols bgp group srx1_group bfd-liveness-detection multiplier 3
set protocols bgp group srx1_group neighbor 10.5.0.1

```

## Configuration

### Step-by-Step Procedure

We're showing the configuration of SRX-01 in the step-by-step procedure.

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see [Using the CLI Editor in Configuration Mode](#) in the [CLI User Guide](#).

#### 1. Configure Interfaces.

```

[edit]
user@srx-1# set interfaces ge-0/0/2 description inter_chassis_link
user@srx-1# set interfaces ge-0/0/2 unit 0 family inet address 10.22.0.2/24
user@srx-1# set interfaces ge-0/0/3 description untrust
user@srx-1# set interfaces ge-0/0/3 unit 0 family inet address 10.3.0.2/24
user@srx-1# set interfaces ge-0/0/4 description trust

```

```
user@srx-1# set interfaces ge-0/0/4 unit 0 family inet address 10.5.0.1/24
```

Use ge-0/0/3 and ge-0/0/4 interfaces to connect to the upstream and downstream routers and use ge-0/0/2 interface to set up the ICL.

## 2. Configure the loopback interfaces.

```
[edit]
user@srx-1# set interfaces lo0 apply-groups-except global
user@srx-1# set interfaces lo0 description untrust
user@srx-1# set interfaces lo0 unit 0 family inet address 10.11.0.1/32
user@srx-1# set interfaces lo0 unit 0 family inet address 10.12.0.1/32
user@srx-1# set interfaces st0 unit 1
```

Assign IP address 10.11.0.1 and 10.12.0.1 to the loopback interface. We'll use 10.11.0.1 as the floating IP address and 10.12.0.1 as IKE gateway address.

## 3. Configure security zones, assign interfaces to the zones, and specify the allowed system services for the security zones.

```
[edit]
user@srx-1# set security zones security-zone vpn host-inbound-traffic system-services ike
user@srx-1# set security zones security-zone vpn host-inbound-traffic protocols all
user@srx-1# set security zones security-zone vpn interfaces st0.1
user@srx-1# set security zones security-zone untrust host-inbound-traffic system-services
ike
user@srx-1# set security zones security-zone untrust host-inbound-traffic system-services
ping
user@srx-1# set security zones security-zone untrust host-inbound-traffic protocols bfd
user@srx-1# set security zones security-zone untrust host-inbound-traffic protocols bgp
user@srx-1# set security zones security-zone untrust interfaces lo0.0
user@srx-1# set security zones security-zone untrust interfaces ge-0/0/3.0
user@srx-1# set security zones security-zone trust host-inbound-traffic system-services all
user@srx-1# set security zones security-zone trust host-inbound-traffic protocols all
user@srx-1# set security zones security-zone trust interfaces ge-0/0/4.0
user@srx-1# set security zones security-zone icl_zone host-inbound-traffic system-services
ike
user@srx-1# set security zones security-zone icl_zone host-inbound-traffic system-services
ping
user@srx-1# set security zones security-zone icl_zone host-inbound-traffic system-services
high-availability
```

```

user@srx-1# set security zones security-zone icl_zone host-inbound-traffic system-services
ssh
user@srx-1# set security zones security-zone icl_zone host-inbound-traffic protocols bfd
user@srx-1# set security zones security-zone icl_zone host-inbound-traffic protocols bgp
user@srx-1# set security zones security-zone icl_zone interfaces ge-0/0/2.0

```

Assign the interfaces ge-0/0/3 and ge-0/0/4 the trust and untrust zones respectively. Assign the lo0.0 interface to the untrust zone to connect over the IP network. Assign the interface ge-0/0/2 to the ICL zone. You use this zone to set up the ICL. Assign the secure tunnel interface to the VPN security zone.

4. Configure both local node and peer node details such as node ID, IP addresses of local node and peer node, and the interface for the peer node.

```

[edit]
user@srx-1# set chassis high-availability local-id 2
user@srx-1# set chassis high-availability local-id local-ip 10.22.0.2
user@srx-1# set chassis high-availability peer-id 1 peer-ip 10.22.0.1
user@srx-1# set chassis high-availability peer-id 1 interface ge-0/0/2.0

```

You'll use the ge-0/0/2 interface for communicating with the peer node using the ICL.

5. Attach the IPsec VPN profile IPSEC\_VPN\_ICL to the peer node.

```

[edit]
user@srx-1# set chassis high-availability peer-id 1 vpn-profile ICL_IPSEC_VPN

```

You'll need this configuration to establish a secure ICL link between the nodes.

6. Configure Bidirectional Forwarding Detection (BFD) protocol options for the peer node.

```

[edit]
user@srx-1# set chassis high-availability peer-id 1 liveness-detection minimum-interval 200
user@srx-1# set chassis high-availability peer-id 1 liveness-detection multiplier 3

```

7. Configure the services redundancy groups SRG1 and SRG2.

```

[edit]
user@srx-1# set chassis high-availability services-redundancy-group 1 deployment-type
routing
user@srx-1# set chassis high-availability services-redundancy-group 1 peer-id 1

```

```
user@srx-1# set chassis high-availability services-redundancy-group 2 peer-id 1
```

In this step, you are specifying deployment type as routing because you are setting up Multinode High Availability in a Layer 3 network.

8. Setup activeness determination parameters both SRG1 and SRG2.

### SRG1

```
[edit]
user@srx-1# set chassis high-availability services-redundancy-group 1 activeness-probe dest-
ip 10.111.0.1
user@srx-1# set chassis high-availability services-redundancy-group 1 activeness-probe dest-
ip src-ip 10.11.0.1
```

### SRG2

```
[edit]
user@srx-1# set chassis high-availability services-redundancy-group 1 activeness-probe dest-
ip 10.111.0.1
user@srx-1# set chassis high-availability services-redundancy-group 1 activeness-probe dest-
ip src-ip 10.11.0.1
```

Use the floating IP address as source IP address (10.11.0.1 for SRG1 and 10.12.0.1 for SRG2) and IP addresses of the upstream routers as the destination IP address (10.111.0.1) for the activeness determination probe.

You can configure up to 64 IP addresses for IP monitoring and activeness probing. The total 64 IP addresses is sum of the number of IPv4 and IPv6 addresses)

9. Configure BFD monitoring parameters for the SRG1 and SRG2 to detect failures in network.

### SRG1

```
[edit]
user@srx-1# set chassis high-availability services-redundancy-group 1 monitor bfd-
liveliness 10.5.0.2 src-ip 10.5.0.1
user@srx-1# set chassis high-availability services-redundancy-group 1 monitor bfd-
liveliness 10.5.0.2 session-type singlehop
```

```

user@srx-1# set chassis high-availability services-redundancy-group 1 monitor bfd-
liveliness 10.5.0.2 interface ge-0/0/3.0
user@srx-1# set chassis high-availability services-redundancy-group 1 monitor interface
ge-0/0/3
user@srx-1# set chassis high-availability services-redundancy-group 1 monitor interface
ge-0/0/4

```

## SRG2

```

[edit]
user@srx-1# set chassis high-availability services-redundancy-group 2 monitor bfd-
liveliness 10.5.0.2 src-ip 10.5.0.1
user@srx-1# set chassis high-availability services-redundancy-group 2 monitor bfd-
liveliness 10.5.0.2 session-type singlehop
user@srx-1# set chassis high-availability services-redundancy-group 2 monitor bfd-
liveliness 10.5.0.2 interface ge-0/0/3.0
user@srx-1# set chassis high-availability services-redundancy-group 2 monitor interface
ge-0/0/3
user@srx-1# set chassis high-availability services-redundancy-group 2 monitor interface
ge-0/0/4

```

10. Configure an active signal route required for activeness enforcement.

## SRG1

```

[edit]
user@srx-1# set chassis high-availability services-redundancy-group 1 active-signal-route
10.39.1.1
user@srx-1# set chassis high-availability services-redundancy-group 1 backup-signal-route
10.39.1.2
user@srx-1# set chassis high-availability services-redundancy-group 1 preemption
user@srx-1# set chassis high-availability services-redundancy-group 1 activeness-priority 1

```

## SRG2

```

[edit]
user@srx-1# set chassis high-availability services-redundancy-group 2 active-signal-route
10.49.1.1
user@srx-1# set chassis high-availability services-redundancy-group 2 backup-signal-route

```

```
10.49.1.2
user@srx-1# set chassis high-availability services-redundancy-group 2 preemption
user@srx-1# set chassis high-availability services-redundancy-group 2 activeness-priority
200
```

The active signal route IP address you assign is used for route preference advertisement. You must specify the active signal route along with the route-exists policy in the policy-options statement.

11. Create an IP prefix list by including the local address of IKE gateway and associate the IP prefix list to SRG1 and SRG2:

### SRG1

```
[edit]
user@srx-1# set policy-options prefix-list SRG1_PFX 10.11.0.0/24
user@srx-1# set policy-options prefix-list SRG2_PFX 10.12.0.0/24
```

### SRG2

```
[edit]
user@srx-1# set chassis high-availability services-redundancy-group 1 prefix-list SRG1_PFX
user@srx-1# set chassis high-availability services-redundancy-group 2 prefix-list SRG2_PFX
```

This configuration anchors a certain IPsec VPN tunnel to a particular security device.

12. Enable IPsec VPN service on both SRG1 and SRG2.

```
[edit]
user@srx-1# set chassis high-availability services-redundancy-group 1 managed-services ipsec
user@srx-1# set chassis high-availability services-redundancy-group 2 managed-services ipsec
```

13. Configure IPSec VPN options for the ICL.

- a. Define Internet Key Exchange (IKE) configuration. An IKE configuration defines the algorithms and keys used to establish a secure connection.

```
[edit]
user@srx-1# set security ike proposal ICL_IKE_PROP description
interchassis_link_encr_tunnel
```

```

user@srx-1# set security ike proposal ICL_IKE_PROP authentication-method pre-shared-keys
user@srx-1# set security ike proposal ICL_IKE_PROP dh-group group14
user@srx-1# set security ike proposal ICL_IKE_PROP authentication-algorithm sha-256
user@srx-1# set security ike proposal ICL_IKE_PROP encryption-algorithm aes-256-cbc
user@srx-1# set security ike proposal ICL_IKE_PROP lifetime-seconds 300
user@srx-1# set security ike policy ICL_IKE_POL description
interchassis_link_encr_tunnel
user@srx-1# set security ike policy ICL_IKE_POL proposals ICL_IKE_PROP
user@srx-1# set security ike policy ICL_IKE_POL pre-shared-key ascii-text "$ABC123"
user@srx-1# set security ike gateway ICL_IKE_GW ike-policy ICL_IKE_POL
user@srx-1# set security ike gateway ICL_IKE_GW version v2-only

```

For the Multinode High availability feature, you must configure the IKE version as v2-only

- b. Specify the IPsec proposal protocol and encryption algorithm. Specify IPsec options to create an IPsec tunnel between two participant devices to secure VPN communication.

```

[edit]
user@srx-1# set security ipsec proposal ICL_IPSEC_PROP description
interchassis_link_encr_tunnel
user@srx-1# set security ipsec proposal ICL_IPSEC_PROP protocol esp
user@srx-1# set security ipsec proposal ICL_IPSEC_PROP encryption-algorithm aes-256-gcm
user@srx-1# set security ipsec proposal ICL_IPSEC_PROP lifetime-seconds 300
user@srx-1# set security ipsec policy ICL_IPSEC_POL description
interchassis_link_encr_tunnel
user@srx-1# set security ipsec policy ICL_IPSEC_POL proposals ICL_IPSEC_PROP
user@srx-1# set security ipsec vpn ICL_IPSEC_VPN ha-link-encryption
user@srx-1# set security ipsec vpn ICL_IPSEC_VPN ike gateway ICL_IKE_GW
user@srx-1# set security ipsec vpn ICL_IPSEC_VPN ike ipsec-policy ICL_IPSEC_POL

```

Specifying the ha-link-encryption option encrypts the ICL to secure high availability traffic flow between the nodes.

The same VPN name ICL\_IPSEC\_VPN must be mentioned for *vpn\_profile* in the set chassis high-availability peer-id <id> vpn-profile *vpn\_profile* configuration.

#### 14. Configure the security policy.

```

[edit]
user@srx-1# set security policies default-policy permit-all

```

For this example, we've configured a policy to permit all traffic. We strongly recommend you to create security policies as per your network requirements to permit traffic that is allowed by your

organizational policy and deny all other traffic. We've used the default policy for the demo purpose only in this example.

## 15. Configure routing options.

```
[edit]
user@srx-1# set routing-options autonomous-system 100
user@srx-1# set routing-options static route 10.7.0.0/16 next-hop 10.5.0.2
user@srx-1# set routing-options static route 10.112.0.0/24 next-hop 10.5.0.2
```

## 16. Configure policy options.

```
[edit]
user@srx-1# set policy-options route-filter-list srg1_rf_list 10.11.0.0/24 orlonger
user@srx-1# set policy-options route-filter-list srg1_rf_list 10.7.0.0/16 orlonger
user@srx-1# set policy-options route-filter-list srg1_rf_list 10.1.0.0/16 orlonger
user@srx-1# set policy-options route-filter-list srg2_rf_list 10.12.0.0/24 orlonger
user@srx-1# set policy-options route-filter-list srg2_rf_list 10.9.0.0/16 orlonger
user@srx-1# set policy-options route-filter-list srg2_rf_list 10.8.0.0/16 orlonger
user@srx-1# set policy-options policy-statement mnha-route-policy term 1 from route-filter-
list srg1_rf_list
user@srx-1# set policy-options policy-statement mnha-route-policy term 1 from condition
active_route_exists_srg1
user@srx-1# set policy-options policy-statement mnha-route-policy term 1 then metric 10
user@srx-1# set policy-options policy-statement mnha-route-policy term 1 then accept
user@srx-1# set policy-options policy-statement mnha-route-policy term 2 from route-filter-
list srg1_rf_list
user@srx-1# set policy-options policy-statement mnha-route-policy term 2 from condition
backup_route_exists_srg1
user@srx-1# set policy-options policy-statement mnha-route-policy term 2 then metric 20
user@srx-1# set policy-options policy-statement mnha-route-policy term 2 then accept
user@srx-1# set policy-options policy-statement mnha-route-policy term 3 from route-filter-
list srg2_rf_list
user@srx-1# set policy-options policy-statement mnha-route-policy term 3 from condition
active_route_exists_srg2
user@srx-1# set policy-options policy-statement mnha-route-policy term 3 then metric 10
user@srx-1# set policy-options policy-statement mnha-route-policy term 3 then accept
user@srx-1# set policy-options policy-statement mnha-route-policy term 4 from route-filter-
list srg2_rf_list
user@srx-1# set policy-options policy-statement mnha-route-policy term 4 from condition
backup_route_exists_srg2
```



```

user@srx-1# set policy-options policy-statement mnha-route-policy term 4 then metric 20
user@srx-1# set policy-options policy-statement mnha-route-policy term 4 then accept
user@srx-1# set policy-options policy-statement mnha-route-policy term default then reject
user@srx-1# set policy-options condition active_route_exists_srg1 if-route-exists address-
family inet 10.39.1.1/32
user@srx-1# set policy-options condition active_route_exists_srg1 if-route-exists address-
family inet table inet.0
user@srx-1# set policy-options condition active_route_exists_srg2 if-route-exists address-
family inet 10.49.1.1/32
user@srx-1# set policy-options condition active_route_exists_srg2 if-route-exists address-
family inet table inet.0
user@srx-1# set policy-options condition backup_route_exists_srg1 if-route-exists address-
family inet 10.39.1.2/32
user@srx-1# set policy-options condition backup_route_exists_srg1 if-route-exists address-
family inet table inet.0
user@srx-1# set policy-options condition backup_route_exists_srg2 if-route-exists address-
family inet 10.49.1.2/32
user@srx-1# set policy-options condition backup_route_exists_srg2 if-route-exists address-
family inet table inet.0

```

Configure the active signal route 10.39.1.1 (SRG1) and 10.49.1.1 (SRG2) with the route match condition (if-route-exists). The Multinode High Availability adds this route to the routing table when the node moves to the active role. The node also starts advertising the higher preference route. Configure the backup signal route (10.39.1.2 and 10.49.1.2) to advertise the backup node with a medium priority. In case of any failures, the high availability link goes down and the current active node releases its primary role and removes the active-signal-route. Now the backup node detects the condition through its probes and transitions to the active role. The route preference is swapped to drive all the traffic to the new active node

#### 17. Configure BFD peering sessions options and specify liveness detection timers.

```

[edit]
user@srx-1# set protocols bgp group trust type internal
user@srx-1# set protocols bgp group trust local-address 10.3.0.2
user@srx-1# set protocols bgp group trust export mnha-route-policy
user@srx-1# set protocols bgp group trust local-as 100
user@srx-1# set protocols bgp group trust bfd-liveness-detection minimum-interval 500
user@srx-1# set protocols bgp group trust bfd-liveness-detection minimum-receive-interval
500
user@srx-1# set protocols bgp group trust bfd-liveness-detection multiplier 3
user@srx-1# set protocols bgp group trust neighbor 10.3.0.1
user@srx-1# set protocols bgp group untrust type internal

```

```

user@srx-1# set protocols bgp group untrust local-address 10.5.0.1
user@srx-1# set protocols bgp group untrust export mnha-route-policy
user@srx-1# set protocols bgp group untrust local-as 100
user@srx-1# set protocols bgp group untrust bfd-liveness-detection minimum-interval 500
user@srx-1# set protocols bgp group untrust bfd-liveness-detection minimum-receive-
interval 500
user@srx-1# set protocols bgp group untrust bfd-liveness-detection multiplier 3
user@srx-1# set protocols bgp group untrust neighbor 10.5.0.2

```

## IPsec VPN Configuration (SRX-1 and SRX-2)

Use the following steps to setup IPsec VPN connection with the peer SRX Series firewall. In this example, you'll be placing all of your IPsec VPN configuration statements inside a JUNOS configuration group named `vpn_config`.

1. Create a configuration group `vpn_config` at the top of the configuration and configure IPsec VPN specific details.

```

[edit]
set groups vpn_config when peers SRX-01
set groups vpn_config when peers SRX-02
set groups vpn_config security ike proposal SRG1_IKE_PROP authentication-method pre-shared-
keys
set groups vpn_config security ike proposal SRG1_IKE_PROP dh-group group14
set groups vpn_config security ike proposal SRG1_IKE_PROP authentication-algorithm sha-256
set groups vpn_config security ike proposal SRG1_IKE_PROP encryption-algorithm aes-256-cbc
set groups vpn_config security ike proposal SRG1_IKE_PROP lifetime-seconds 3600
set groups vpn_config security ike proposal SRG2_IKE_PROP authentication-method pre-shared-
keys
set groups vpn_config security ike proposal SRG2_IKE_PROP dh-group group14
set groups vpn_config security ike proposal SRG2_IKE_PROP authentication-algorithm sha-256
set groups vpn_config security ike proposal SRG2_IKE_PROP encryption-algorithm aes-256-cbc
set groups vpn_config security ike proposal SRG2_IKE_PROP lifetime-seconds 3600
set groups vpn_config security ike policy SRG1_IKE_POL1 proposals SRG1_IKE_PROP
set groups vpn_config security ike policy SRG1_IKE_POL1 pre-shared-key ascii-text "$ABC123"
set groups vpn_config security ike policy SRG2_IKE_POL500 proposals SRG2_IKE_PROP
set groups vpn_config security ike policy SRG2_IKE_POL500 pre-shared-key ascii-text "$ABC123"
set groups vpn_config security ike gateway SRG1_IKE_GW1 ike-policy SRG1_IKE_POL1
set groups vpn_config security ike gateway SRG1_IKE_GW1 address 10.112.0.1
set groups vpn_config security ike gateway SRG1_IKE_GW1 external-interface lo0
set groups vpn_config security ike gateway SRG1_IKE_GW1 local-address 10.11.0.1
set groups vpn_config security ike gateway SRG1_IKE_GW1 version v2-only

```

```

set groups vpn_config security ike gateway SRG2_IKE_GW500 ike-policy SRG2_IKE_POL500
set groups vpn_config security ike gateway SRG2_IKE_GW500 address 10.112.0.5
set groups vpn_config security ike gateway SRG2_IKE_GW500 external-interface lo0
set groups vpn_config security ike gateway SRG2_IKE_GW500 local-address 10.12.0.1
set groups vpn_config security ike gateway SRG2_IKE_GW500 version v2-only
set groups vpn_config security ipsec proposal SRG1_IPSEC_PROP protocol esp
set groups vpn_config security ipsec proposal SRG1_IPSEC_PROP authentication-algorithm hmac-sha-256-128
set groups vpn_config security ipsec proposal SRG1_IPSEC_PROP encryption-algorithm aes-256-cbc
set groups vpn_config security ipsec proposal SRG1_IPSEC_PROP lifetime-seconds 1800
set groups vpn_config security ipsec proposal SRG2_IPSEC_PROP protocol esp
set groups vpn_config security ipsec proposal SRG2_IPSEC_PROP authentication-algorithm hmac-sha-256-128
set groups vpn_config security ipsec proposal SRG2_IPSEC_PROP encryption-algorithm aes-256-cbc
set groups vpn_config security ipsec proposal SRG2_IPSEC_PROP lifetime-seconds 1800
set groups vpn_config security ipsec policy SRG1_IPSEC_POL1 proposals SRG1_IPSEC_PROP
set groups vpn_config security ipsec policy SRG2_IPSEC_POL501 proposals SRG2_IPSEC_PROP
set groups vpn_config security ipsec policy SRG2_IPSEC_POL500 proposals SRG2_IPSEC_PROP
set groups vpn_config security ipsec policy SRG2_IPSEC_POL502 proposals SRG2_IPSEC_PROP
set groups vpn_config security ipsec policy SRG2_IPSEC_POL503 proposals SRG2_IPSEC_PROP
set groups vpn_config security ipsec vpn SRG1_IPSEC_VPN1 bind-interface st0.1
set groups vpn_config security ipsec vpn SRG1_IPSEC_VPN1 ike gateway SRG1_IKE_GW1
set groups vpn_config security ipsec vpn SRG1_IPSEC_VPN1 ike ipsec-policy SRG1_IPSEC_POL1
set groups vpn_config security ipsec vpn SRG1_IPSEC_VPN1 traffic-selector ts1 local-ip 10.1.0.2/32
set groups vpn_config security ipsec vpn SRG1_IPSEC_VPN1 traffic-selector ts1 remote-ip 10.7.0.2/32
set groups vpn_config security ipsec vpn SRG1_IPSEC_VPN1 establish-tunnels on-traffic
set groups vpn_config security ipsec vpn SRG2_IPSEC_VPN500 bind-interface st0.500
set groups vpn_config security ipsec vpn SRG2_IPSEC_VPN500 ike gateway SRG2_IKE_GW500
set groups vpn_config security ipsec vpn SRG2_IPSEC_VPN500 ike ipsec-policy SRG2_IPSEC_POL500
set groups vpn_config security ipsec vpn SRG2_IPSEC_VPN500 traffic-selector ts500 local-ip 10.8.0.2/32
set groups vpn_config security ipsec vpn SRG2_IPSEC_VPN500 traffic-selector ts500 remote-ip 10.9.0.2/32
set groups vpn_config security ipsec vpn SRG2_IPSEC_VPN500 establish-tunnels on-traffic
set groups vpn_config security zones security-zone vpn host-inbound-traffic system-services ike
set groups vpn_config security zones security-zone vpn host-inbound-traffic protocols all
set groups vpn_config security zones security-zone vpn interfaces st0.1
set groups vpn_config security zones security-zone vpn interfaces st0.500

```

```
set groups vpn_config interfaces st0 unit 1 family inet
set groups vpn_config interfaces st0 unit 500 family inet
```

2. Include the `apply-groups` statement in the configuration to inherit the statements from the `vpn_config` configuration group,

```
[edit]
user@srx-1# set apply-groups vpn_config
```

## Configuration (SRX-03) (VPN Peer Device)

### Step-By-Step Procedure

1. Create the IKE proposal.

```
[edit]
user@srx-3# set security ike proposal SRG1_IKE_PROP authentication-method pre-shared-keys
user@srx-3# set security ike proposal SRG1_IKE_PROP dh-group group14
user@srx-3# set security ike proposal SRG1_IKE_PROP authentication-algorithm sha-256
user@srx-3# set security ike proposal SRG1_IKE_PROP encryption-algorithm aes-256-cbc
user@srx-3# set security ike proposal SRG1_IKE_PROP lifetime-seconds 3600
user@srx-3# set security ike proposal SRG2_IKE_PROP authentication-method pre-shared-keys
user@srx-3# set security ike proposal SRG2_IKE_PROP dh-group group14
user@srx-3# set security ike proposal SRG2_IKE_PROP authentication-algorithm sha-256
user@srx-3# set security ike proposal SRG2_IKE_PROP encryption-algorithm aes-256-cbc
user@srx-3# set security ike proposal SRG2_IKE_PROP lifetime-seconds 3600
```

2. Define IKE policies.

```
[edit]
user@srx-3# set security ike policy SRG1_IKE_POL1 proposals SRG1_IKE_PROP
user@srx-3# set security ike policy SRG1_IKE_POL1 pre-shared-key ascii-text "$ABC123"
user@srx-3# set security ike policy SRG2_IKE_POL500 proposals SRG2_IKE_PROP
user@srx-3# set security ike policy SRG2_IKE_POL500 pre-shared-key ascii-text "$ABC123"
```

### 3. Create an IKE gateway, define address, specify external interfaces and version.

```
[edit]
user@srx-3# set security ike gateway SRG1_IKE_GW1 ike-policy SRG1_IKE_POL1
user@srx-3# set security ike gateway SRG1_IKE_GW1 address 10.11.0.1
user@srx-3# set security ike gateway SRG1_IKE_GW1 external-interface lo0
user@srx-3# set security ike gateway SRG1_IKE_GW1 local-address 10.112.0.1
user@srx-3# set security ike gateway SRG1_IKE_GW1 version v2-only
user@srx-3# set security ike gateway SRG2_IKE_GW500 ike-policy SRG2_IKE_POL500
user@srx-3# set security ike gateway SRG2_IKE_GW500 address 10.12.0.1
user@srx-3# set security ike gateway SRG2_IKE_GW500 external-interface lo0
user@srx-3# set security ike gateway SRG2_IKE_GW500 local-address 10.112.0.5
user@srx-3# set security ike gateway SRG2_IKE_GW500 version v2-only
```

### 4. Create IPsec proposals.

```
[edit]
user@srx-3# set security ipsec proposal SRG1_IPSEC_PROP protocol esp
user@srx-3# set security ipsec proposal SRG1_IPSEC_PROP authentication-algorithm hmac-sha-256-128
user@srx-3# set security ipsec proposal SRG1_IPSEC_PROP encryption-algorithm aes-256-cbc
user@srx-3# set security ipsec proposal SRG1_IPSEC_PROP lifetime-seconds 1800
user@srx-3# set security ipsec proposal SRG2_IPSEC_PROP protocol esp
user@srx-3# set security ipsec proposal SRG2_IPSEC_PROP authentication-algorithm hmac-sha-256-128
user@srx-3# set security ipsec proposal SRG2_IPSEC_PROP encryption-algorithm aes-256-cbc
user@srx-3# set security ipsec proposal SRG2_IPSEC_PROP lifetime-seconds 1800
```

### 5. Create IPsec policies.

```
[edit]
user@srx-3# set security ipsec policy SRG1_IPSEC_POL1 proposals SRG1_IPSEC_PROP
user@srx-3# set security ipsec policy SRG2_IPSEC_POL500 proposals SRG2_IPSEC_PROP
```

### 6. Specify the IPsec proposal references (IKE gateway, IPsec policy, interface to bind, and traffic selectors).

```
[edit]
user@srx-3# set security ipsec vpn SRG1_IPSEC_VPN1 bind-interface st0.1
```

```

user@srx-3# set security ipsec vpn SRG1_IPSEC_VPN1 ike gateway SRG1_IKE_GW1
user@srx-3# set security ipsec vpn SRG1_IPSEC_VPN1 ike ipsec-policy SRG1_IPSEC_POL1
user@srx-3# set security ipsec vpn SRG1_IPSEC_VPN1 traffic-selector ts1 local-ip 10.7.0.2/32
user@srx-3# set security ipsec vpn SRG1_IPSEC_VPN1 traffic-selector ts1 remote-ip
10.1.0.2/32
user@srx-3# set security ipsec vpn SRG1_IPSEC_VPN1 establish-tunnels immediately
user@srx-3# set security ipsec vpn SRG2_IPSEC_VPN500 bind-interface st0.500
user@srx-3# set security ipsec vpn SRG2_IPSEC_VPN500 ike gateway SRG2_IKE_GW500
user@srx-3# set security ipsec vpn SRG2_IPSEC_VPN500 ike ipsec-policy SRG2_IPSEC_POL500
user@srx-3# set security ipsec vpn SRG2_IPSEC_VPN500 traffic-selector ts1 local-ip
10.9.0.2/32
user@srx-3# set security ipsec vpn SRG2_IPSEC_VPN500 traffic-selector ts1 remote-ip
10.8.0.2/32
user@srx-3# set security ipsec vpn SRG2_IPSEC_VPN500 establish-tunnels immediately

```

## 7. Create a security policy.

```

[edit]
user@srx-3# set security policies default-policy permit-all

```

For this example, we've configured a policy to permit all traffic. We strongly recommend you to create security policies as per your network requirements to permit traffic that is allowed by your organizational policy and deny all other traffic. We've used the default policy for the demo purpose only in this example.

## 8. Configure the interfaces.

```

[edit]
user@srx-3# set interfaces ge-0/0/0 description trust
user@srx-3# set interfaces ge-0/0/0 unit 0 family inet address 10.7.0.1/24
user@srx-3# set interfaces ge-0/0/1 description untrust
user@srx-3# set interfaces ge-0/0/1 unit 0 family inet address 10.6.0.2/24
user@srx-3# set interfaces ge-0/0/2 description trust
user@srx-3# set interfaces ge-0/0/2 unit 0 family inet address 10.9.0.1/24
user@srx-3# set interfaces lo0 description untrust
user@srx-3# set interfaces lo0 unit 0 family inet address 10.112.0.1/32
user@srx-3# set interfaces lo0 unit 0 family inet address 10.112.0.5/32
user@srx-3# set interfaces st0 unit 1 family inet
user@srx-3# set interfaces st0 unit 500 family inet

```

## 9. Define security zones and add interfaces.

```
[edit]
user@srx-3# set security zones security-zone untrust host-inbound-traffic system-services
all
user@srx-3# set security zones security-zone untrust host-inbound-traffic protocols all
user@srx-3# set security zones security-zone untrust interfaces st0.1
user@srx-3# set security zones security-zone untrust interfaces lo0.0
user@srx-3# set security zones security-zone untrust interfaces st0.500
user@srx-3# set security zones security-zone untrust interfaces ge-0/0/1.0
user@srx-3# set security zones security-zone untrust interfaces ge-0/0/0.0
user@srx-3# set security zones security-zone trust host-inbound-traffic system-services all
user@srx-3# set security zones security-zone trust host-inbound-traffic protocols all
user@srx-3# set security zones security-zone trust interfaces ge-0/0/2.0
```

## 10. Configure the static routes.

```
[edit]
user@srx-3# set routing-options autonomous-system 100
user@srx-3# set routing-options static route 10.4.0.0/16 next-hop 10.7.0.2
user@srx-3# set routing-options static route 10.5.0.0/16 next-hop 10.7.0.2
user@srx-3# set routing-options static route 10.11.0.0/24 next-hop 10.7.0.2
user@srx-3# set routing-options static route 10.12.0.0/24 next-hop 10.7.0.2
user@srx-3# set routing-options static route 10.111.0.1/32 next-hop 10.7.0.2
user@srx-3# set routing-options static route 10.111.0.2/32 next-hop 10.7.0.2
```

## Results (SRX-01)

From configuration mode, confirm your configuration by entering the following commands.

If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@srx-1# show groups vpn_config

when {
    peers [ SRX-01 SRX-02 ];
}
security {
```

```

ike {
    proposal SRG1_IKE_PROP {
        authentication-method pre-shared-keys;
        dh-group group14;
        authentication-algorithm sha-256;
        encryption-algorithm aes-256-cbc;
        lifetime-seconds 3600;
    }
    proposal SRG2_IKE_PROP {
        authentication-method pre-shared-keys;
        dh-group group14;
        authentication-algorithm sha-256;
        encryption-algorithm aes-256-cbc;
        lifetime-seconds 3600;
    }
    policy SRG1_IKE_POL1 {
        proposals SRG1_IKE_PROP;
        pre-shared-key ascii-text "$ABC123"; ## SECRET-DATA
    }
    policy SRG2_IKE_POL500 {
        proposals SRG2_IKE_PROP;
        pre-shared-key ascii-text "$ABC123"; ## SECRET-DATA
    }
    gateway SRG1_IKE_GW1 {
        ike-policy SRG1_IKE_POL1;
        address 10.112.0.1;
        external-interface lo0;
        local-address 10.11.0.1;
        version v2-only;
    }
    gateway SRG2_IKE_GW500 {
        ike-policy SRG2_IKE_POL500;
        address 10.112.0.5;
        external-interface lo0;
        local-address 10.12.0.1;
        version v2-only;
    }
}

ipsec {
    proposal SRG1_IPSEC_PROP {
        protocol esp;
        authentication-algorithm hmac-sha-256-128;
        encryption-algorithm aes-256-cbc;
    }
}

```



```

        lifetime-seconds 1800;
    }
    proposal SRG2_IPSEC_PROP {
        protocol esp;
        authentication-algorithm hmac-sha-256-128;
        encryption-algorithm aes-256-cbc;
        lifetime-seconds 1800;
    }
    policy SRG1_IPSEC_POL1 {
        proposals SRG1_IPSEC_PROP;
    }
    policy SRG2_IPSEC_POL501 {
        proposals SRG2_IPSEC_PROP;
    }
    policy SRG2_IPSEC_POL500 {
        proposals SRG2_IPSEC_PROP;
    }
    policy SRG2_IPSEC_POL502 {
        proposals SRG2_IPSEC_PROP;
    }
    policy SRG2_IPSEC_POL503 {
        proposals SRG2_IPSEC_PROP;
    }
    vpn SRG1_IPSEC_VPN1 {
        bind-interface st0.1;
        ike {
            gateway SRG1_IKE_GW1;
            ipsec-policy SRG1_IPSEC_POL1;
        }
        traffic-selector ts1 {
            local-ip 10.1.0.2/32;
            remote-ip 10.7.0.2/32;
        }
        establish-tunnels on-traffic;
    }
    vpn SRG2_IPSEC_VPN500 {
        bind-interface st0.500;
        ike {
            gateway SRG2_IKE_GW500;
            ipsec-policy SRG2_IPSEC_POL500;
        }
        traffic-selector ts500 {
            local-ip 10.8.0.2/32;

```

```

        remote-ip 10.9.0.2/32;
    }
    establish-tunnels on-traffic;
}
zones {
    security-zone vpn {
        host-inbound-traffic {
            system-services {
                ike;
            }
            protocols {
                all;
            }
        }
        interfaces {
            st0.1;
            st0.500;
        }
    }
}
}
interfaces {
    st0 {
        unit 1 {
            family inet;
            family inet6;
        }
        unit 500 {
            family inet;
            family inet6;
        }
    }
}
}

```

```

[edit]
user@srx-1# show chassis high-availability
local-id 2 local-ip 10.22.0.2;
peer-id 1 {
    peer-ip 10.22.0.1;
    interface ge-0/0/2.0;
}

```

```

    vpn-profile ICL_IPSEC_VPN;
    liveness-detection {
        minimum-interval 200;
        multiplier 3;
    }
}
services-redundancy-group 1 {
    deployment-type routing;
    peer-id {
        1;
    }
    activeness-probe {
        dest-ip {
            10.111.0.1;
            src-ip 10.11.0.1;
        }
    }
    monitor {
        bfd-liveliness 10.5.0.2 {
            src-ip 10.5.0.1;
            session-type singlehop;
            interface ge-0/0/3.0;
        }
        interface {
            ge-0/0/3;
            ge-0/0/4;
        }
    }
    active-signal-route {
        10.39.1.1;
    }
    backup-signal-route {
        10.39.1.2;
    }
    prefix-list SRG1_PFX;
    managed-services ipsec;
    preemption;
    activeness-priority 1;
}
services-redundancy-group 2 {
    peer-id {
        1;
    }
}

```

```

activeness-probe {
    dest-ip {
        10.111.0.1;
        src-ip 10.12.0.1;
    }
}
monitor {
    bfd-liveliness 10.5.0.2 {
        src-ip 10.5.0.1;
        session-type singlehop;
        interface ge-0/0/3.0;
    }
    interface {
        ge-0/0/3;
        ge-0/0/4;
    }
}
active-signal-route {
    10.49.1.1;
}
backup-signal-route {
    10.49.1.2;
}
prefix-list SRG2_PFX;
managed-services ipsec;
preemption;
activeness-priority 200;
}

```

```

[edit]
user@srx-1# show security ike
proposal ICL_IKE_PROP {
    description interchassis_link_encr_tunnel;
    authentication-method pre-shared-keys;
    dh-group group14;
    authentication-algorithm sha-256;
    encryption-algorithm aes-256-cbc;
    lifetime-seconds 300;
}
policy ICL_IKE_POL {
    description interchassis_link_encr_tunnel;

```

```

    proposals ICL_IKE_PROP;
    pre-shared-key ascii-text "$ABC123"; ## SECRET-DATA
}
gateway ICL_IKE_GW {
    ike-policy ICL_IKE_POL;
    version v2-only;
}

```

```

[edit]
user@srx-1# show security ipsec
proposal ICL_IPSEC_PROP {
    description interchassis_link_encr_tunnel;
    protocol esp;
    encryption-algorithm aes-256-gcm;
    lifetime-seconds 300;
}
policy ICL_IPSEC_POL {
    description interchassis_link_encr_tunnel;
    proposals ICL_IPSEC_PROP;
}
vpn ICL_IPSEC_VPN {
    ha-link-encryption;
    ike {
        gateway ICL_IKE_GW;
        ipsec-policy ICL_IPSEC_POL;
    }
}

```

```

[edit]
user@srx-1# show policy-options

prefix-list SRG1_PFX {
    10.11.0.0/24;
}
prefix-list SRG2_PFX {
    10.12.0.0/24;
}
route-filter-list srg1_rf_list {
    10.11.0.0/24 orlonger;
    10.7.0.0/16 orlonger;
}

```

```

    10.1.0.0/16 orlonger;
}
route-filter-list srg2_rf_list {
    10.12.0.0/24 orlonger;
    10.9.0.0/16 orlonger;
    10.8.0.0/16 orlonger;
}
policy-statement mnha-route-policy {
    term 1 {
        from {
            route-filter-list srg1_rf_list;
            condition active_route_exists_srg1;
        }
        then {
            metric 10;
            accept;
        }
    }
    term 2 {
        from {
            route-filter-list srg1_rf_list;
            condition backup_route_exists_srg1;
        }
        then {
            metric 20;
            accept;
        }
    }
    term 3 {
        from {
            route-filter-list srg2_rf_list;
            condition active_route_exists_srg2;
        }
        then {
            metric 10;
            accept;
        }
    }
    term 4 {
        from {
            route-filter-list srg2_rf_list;
            condition backup_route_exists_srg2;
        }
    }
}

```

```

        then {
            metric 20;
            accept;
        }
    }
    term default {
        then reject;
    }
}
condition active_route_exists_srg1 {
    if-route-exists {
        address-family {
            inet {
                10.39.1.1/32;
                table inet.0;
            }
        }
    }
}
condition active_route_exists_srg2 {
    if-route-exists {
        address-family {
            inet {
                10.49.1.1/32;
                table inet.0;
            }
        }
    }
}
condition backup_route_exists_srg1 {
    if-route-exists {
        address-family {
            inet {
                10.39.1.2/32;
                table inet.0;
            }
        }
    }
}
condition backup_route_exists_srg2 {
    if-route-exists {
        address-family {
            inet {

```

```

        10.49.1.2/32;
        table inet.0;
    }
}
}
}
}

```

```

[edit]
user@srx-1# show routing-options
autonomous-system 100;
static {
    route 10.7.0.0/16 next-hop 10.5.0.2;
    route 10.112.0.0/24 next-hop 10.5.0.2;
}

```

```

[edit]
user@srx-1# show security zones
security-zone vpn {
    host-inbound-traffic {
        system-services {
            ike;
        }
        protocols {
            all;
        }
    }
    interfaces {
        st0.1;
    }
}
security-zone untrust {
    host-inbound-traffic {
        system-services {
            ike;
            ping;
        }
        protocols {
            bfd;
            bgp;

```



```

    }
}
interfaces {
    lo0.0;
    ge-0/0/3.0;
}
}
security-zone trust {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            all;
        }
    }
    interfaces {
        ge-0/0/4.0;
    }
}
security-zone icl_zone {
    host-inbound-traffic {
        system-services {
            ike;
            ping;
            high-availability;
            ssh;
        }
        protocols {
            bfd;
            bgp;
        }
    }
    interfaces {
        ge-0/0/2.0;
    }
}
}

```

```
[edit]
user@srx-1# show interfaces
ge-0/0/1 {
    unit 0 {
        family inet;
    }
}
ge-0/0/2 {
    description inter_chassis_link;
    unit 0 {
        family inet {
            address 10.22.0.2/24;
        }
    }
}
ge-0/0/3 {
    description untrust;
    unit 0 {
        family inet {
            address 10.3.0.2/24;
        }
    }
}
ge-0/0/4 {
    description trust;
    unit 0 {
        family inet {
            address 10.5.0.1/24;
        }
    }
}
lo0 {
    apply-groups-except global;
    description untrust;
    unit 0 {
        family inet {
            address 10.11.0.1/32;
            address 10.12.0.1/32;
```

```

    }
  }
}
st0 {
  unit 1;
}

```

If you are done configuring the device, enter `commit` from configuration mode.

## Results (SRX-02)

From configuration mode, confirm your configuration by entering the following commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```

[edit]
user@srx-2# show groups vpn_config
when {
  peers [ SRX-01 SRX-02 ];
}
security {
  ike {
    proposal SRG1_IKE_PROP {
      authentication-method pre-shared-keys;
      dh-group group14;
      authentication-algorithm sha-256;
      encryption-algorithm aes-256-cbc;
      lifetime-seconds 3600;
    }
    proposal SRG2_IKE_PROP {
      authentication-method pre-shared-keys;
      dh-group group14;
      authentication-algorithm sha-256;
      encryption-algorithm aes-256-cbc;
      lifetime-seconds 3600;
    }
    policy SRG1_IKE_POL1 {
      proposals SRG1_IKE_PROP;
      pre-shared-key ascii-text "$ABC123"; ## SECRET-DATA
    }
    policy SRG2_IKE_POL500 {
      proposals SRG2_IKE_PROP;
    }
  }
}

```

```

        pre-shared-key ascii-text "$ABC123"; ## SECRET-DATA
    }
    gateway SRG1_IKE_GW1 {
        ike-policy SRG1_IKE_POL1;
        address 10.112.0.1;
        external-interface lo0;
        local-address 10.11.0.1;
        version v2-only;
    }
    gateway SRG2_IKE_GW500 {
        ike-policy SRG2_IKE_POL500;
        address 10.112.0.5;
        external-interface lo0;
        local-address 10.12.0.1;
        version v2-only;
    }
}
ipsec {
    proposal SRG1_IPSEC_PROP {
        protocol esp;
        authentication-algorithm hmac-sha-256-128;
        encryption-algorithm aes-256-cbc;
        lifetime-seconds 1800;
    }
    proposal SRG2_IPSEC_PROP {
        protocol esp;
        authentication-algorithm hmac-sha-256-128;
        encryption-algorithm aes-256-cbc;
        lifetime-seconds 1800;
    }
    policy SRG1_IPSEC_POL1 {
        proposals SRG1_IPSEC_PROP;
    }
    policy SRG2_IPSEC_POL501 {
        proposals SRG2_IPSEC_PROP;
    }
    policy SRG2_IPSEC_POL500 {
        proposals SRG2_IPSEC_PROP;
    }
    policy SRG2_IPSEC_POL502 {
        proposals SRG2_IPSEC_PROP;
    }
    policy SRG2_IPSEC_POL503 {

```

```

        proposals SRG2_IPSEC_PROP;
    }
    vpn SRG1_IPSEC_VPN1 {
        bind-interface st0.1;
        ike {
            gateway SRG1_IKE_GW1;
            ipsec-policy SRG1_IPSEC_POL1;
        }
        traffic-selector ts1 {
            local-ip 10.1.0.2/32;
            remote-ip 10.7.0.2/32;
        }
        establish-tunnels on-traffic;
    }
    vpn SRG2_IPSEC_VPN500 {
        bind-interface st0.500;
        ike {
            gateway SRG2_IKE_GW500;
            ipsec-policy SRG2_IPSEC_POL500;
        }
        traffic-selector ts500 {
            local-ip 10.8.0.2/32;
            remote-ip 10.9.0.2/32;
        }
        establish-tunnels on-traffic;
    }
}
zones {
    security-zone vpn {
        host-inbound-traffic {
            system-services {
                ike;
            }
            protocols {
                all;
            }
        }
        interfaces {
            st0.1;
            st0.500;
        }
    }
}
}

```

```

}
interfaces {
    st0 {
        unit 1 {
            family inet;
            family inet6;
        }
        unit 500 {
            family inet;
            family inet6;
        }
    }
}
}

```

```

[edit]
user@srx-2# show chassis high-availability
local-id 1 local-ip 10.22.0.1;
peer-id 2 {
    peer-ip 10.22.0.2;
    interface ge-0/0/2.0;
    vpn-profile ICL_IPSEC_VPN;
    liveness-detection {
        minimum-interval 200;
        multiplier 3;
    }
}
services-redundancy-group 1 {
    deployment-type routing;
    peer-id {
        2;
    }
    activeness-probe {
        dest-ip {
            10.111.0.1;
            src-ip 10.11.0.1;
        }
    }
    monitor {
        bfd-liveliness 10.4.0.2 {
            src-ip 10.4.0.1;
            session-type singlehop;

```

```

        interface ge-0/0/3.0;
    }
    interface {
        ge-0/0/3;
        ge-0/0/4;
    }
}
active-signal-route {
    10.39.1.1;
}
backup-signal-route {
    10.39.1.2;
}
prefix-list SRG1_PFX;
managed-services ipsec;
preemption;
activeness-priority 200;
}
services-redundancy-group 2 {
    peer-id {
        2;
    }
    activeness-probe {
        dest-ip {
            10.111.0.1;
            src-ip 10.12.0.1;
        }
    }
}
monitor {
    bfd-liveliness 10.4.0.2 {
        src-ip 10.4.0.1;
        session-type singlehop;
        interface ge-0/0/3.0;
    }
    interface {
        ge-0/0/3;
        ge-0/0/4;
    }
}
active-signal-route {
    10.49.1.1;
}
backup-signal-route {

```

```

        10.49.1.2;
    }
    prefix-list SRG2_PFX;
    managed-services ipsec;
    preemption;
    activeness-priority 1;
}

```

```

[edit]
user@srx-2# show security ike
proposal ICL_IKE_PROP {
    description interchassis_link_encr_tunnel;
    authentication-method pre-shared-keys;
    dh-group group14;
    authentication-algorithm sha-256;
    encryption-algorithm aes-256-cbc;
    lifetime-seconds 300;
}
policy ICL_IKE_POL {
    description interchassis_link_encr_tunnel;
    proposals ICL_IKE_PROP;
    pre-shared-key ascii-text "$ABC123"; ## SECRET-DATA
}
gateway ICL_IKE_GW {
    ike-policy ICL_IKE_POL;
    version v2-only;
}

```

```

[edit]
user@srx-2# show security ipsec
proposal ICL_IPSEC_PROP {
    description interchassis_link_encr_tunnel;
    protocol esp;
    encryption-algorithm aes-256-gcm;
    lifetime-seconds 300;
}
policy ICL_IPSEC_POL {
    description interchassis_link_encr_tunnel;
    proposals ICL_IPSEC_PROP;
}

```



```

vpn ICL_IPSEC_VPN {
    ha-link-encryption;
    ike {
        gateway ICL_IKE_GW;
        ipsec-policy ICL_IPSEC_POL;
    }
}

```

```

[edit]
user@srx-2# show policy-options
prefix-list SRG1_PFX {
    10.11.0.0/24;
}
prefix-list SRG2_PFX {
    10.12.0.0/24;
}
route-filter-list srg1_rf_list {
    10.11.0.0/24 orlonger;
    10.7.0.0/24 orlonger;
    10.1.0.0/24 orlonger;
}
route-filter-list srg2_rf_list {
    10.12.0.0/24 orlonger;
    10.9.0.0/24 orlonger;
    10.8.0.0/24 orlonger;
}
policy-statement mnha-route-policy {
    term 1 {
        from {
            route-filter-list srg1_rf_list;
            condition active_route_exists_srg1;
        }
        then {
            metric 10;
            accept;
        }
    }
    term 2 {
        from {
            route-filter-list srg1_rf_list;
            condition backup_route_exists_srg1;

```

```

    }
    then {
        metric 20;
        accept;
    }
}
term 3 {
    from {
        route-filter-list srg2_rf_list;
        condition active_route_exists_srg2;
    }
    then {
        metric 10;
        accept;
    }
}
term 4 {
    from {
        route-filter-list srg2_rf_list;
        condition backup_route_exists_srg2;
    }
    then {
        metric 20;
        accept;
    }
}
term default {
    then reject;
}
}
condition active_route_exists_srg1 {
    if-route-exists {
        address-family {
            inet {
                10.39.1.1/32;
                table inet.0;
            }
        }
    }
}
condition active_route_exists_srg2 {
    if-route-exists {
        address-family {

```

```

        inet {
            10.49.1.1/32;
            table inet.0;
        }
    }
}
condition backup_route_exists_srg1 {
    if-route-exists {
        address-family {
            inet {
                10.39.1.2/32;
                table inet.0;
            }
        }
    }
}
condition backup_route_exists_srg2 {
    if-route-exists {
        address-family {
            inet {
                10.49.1.2/32;
                table inet.0;
            }
        }
    }
}
}

```

```

[edit]
user@srx-2# show routing-options
autonomous-system 100;
static {
    route 10.7.0.0/24 next-hop 10.4.0.2;
    route 10.112.0.0/24 next-hop 10.4.0.2;
}

```

```

[edit]
user@srx-2# show security zones
    security-zone untrust {
        host-inbound-traffic {

```

```

        system-services {
            ike;
            ping;
        }
        protocols {
            bfd;
            bgp;
        }
    }
    interfaces {
        lo0.0;
        ge-0/0/3.0;
    }
}
security-zone vpn {
    host-inbound-traffic {
        system-services {
            ike;
        }
        protocols {
            all;
        }
    }
    interfaces {
        st0.1;
    }
}
security-zone trust {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            all;
        }
    }
    interfaces {
        ge-0/0/4.0;
    }
}
security-zone icl_zone {
    host-inbound-traffic {
        system-services {

```

```

        ike;
        ping;
        high-availability;
        ssh;
    }
    protocols {
        bfd;
        bgp;
    }
}
interfaces {
    ge-0/0/2.0;
}
}

```

```

[edit]
user@srx-2# show interfaces
ge-0/0/1 {
    unit 0 {
        family inet;
    }
}
ge-0/0/2 {
    description inter_chassis_link;
    unit 0 {
        family inet {
            address 10.22.0.1/24;
        }
    }
}
ge-0/0/3 {
    description untrust;
    unit 0 {
        family inet {
            address 10.2.0.2/24;
        }
    }
}
ge-0/0/4 {
    description trust;
    unit 0 {

```

```

        family inet {
            address 10.4.0.1/24;
        }
    }
}
lo0 {
    apply-groups-except global;
    description untrust;
    unit 0 {
        family inet {
            address 10.11.0.1/32;
            address 10.12.0.1/32;
        }
    }
}
st0 {
    unit 1 {
        family inet;
    }
}
}

```

If you are done configuring the device, enter `commit` from configuration mode.

On your security devices, you'll get the following message that asks you to reboot the device:

```

user@host# commit
warning: High Availability Mode changed, please reboot the device to avoid undesirable behavior
commit complete

```

### Results (SRX-3) (VPN Peer Device)

From configuration mode, confirm your configuration by entering the following commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```

[edit]
user@srx-3# show security ike
proposal SRG1_IKE_PROP {
    authentication-method pre-shared-keys;

```

```

    dh-group group14;
    authentication-algorithm sha-256;
    encryption-algorithm aes-256-cbc;
    lifetime-seconds 3600;
}
proposal SRG2_IKE_PROP {
    authentication-method pre-shared-keys;
    dh-group group14;
    authentication-algorithm sha-256;
    encryption-algorithm aes-256-cbc;
    lifetime-seconds 3600;
}
policy SRG1_IKE_POL1 {
    proposals SRG1_IKE_PROP;
    pre-shared-key ascii-text "$ABC123"; ## SECRET-DATA
}
policy SRG2_IKE_POL500 {
    proposals SRG2_IKE_PROP;
    pre-shared-key ascii-text "$ABC123"; ## SECRET-DATA
}
gateway SRG1_IKE_GW1 {
    ike-policy SRG1_IKE_POL1;
    address 10.11.0.1;
    external-interface lo0;
    local-address 10.112.0.1;
    version v2-only;
}
gateway SRG2_IKE_GW500 {
    ike-policy SRG2_IKE_POL500;
    address 10.12.0.1;
    external-interface lo0;
    local-address 10.112.0.5;
    version v2-only;
}

```

[edit]

user@srx-3# **show security ipsec**

```

proposal SRG1_IPSEC_PROP {
    protocol esp;
    authentication-algorithm hmac-sha-256-128;
    encryption-algorithm aes-256-cbc;
}

```

```

        lifetime-seconds 1800;
    }
    proposal SRG2_IPSEC_PROP {
        protocol esp;
        authentication-algorithm hmac-sha-256-128;
        encryption-algorithm aes-256-cbc;
        lifetime-seconds 1800;
    }
    policy SRG1_IPSEC_POL1 {
        proposals SRG1_IPSEC_PROP;
    }
    policy SRG2_IPSEC_POL500 {
        proposals SRG2_IPSEC_PROP;
    }
    vpn SRG1_IPSEC_VPN1 {
        bind-interface st0.1;
        ike {
            gateway SRG1_IKE_GW1;
            ipsec-policy SRG1_IPSEC_POL1;
        }
        traffic-selector ts1 {
            local-ip 10.7.0.2/32;
            remote-ip 10.1.0.2/32;
        }
        establish-tunnels immediately;
    }
    vpn SRG2_IPSEC_VPN500 {
        bind-interface st0.500;
        ike {
            gateway SRG2_IKE_GW500;
            ipsec-policy SRG2_IPSEC_POL500;
        }
        traffic-selector ts1 {
            local-ip 10.9.0.2/32;
            remote-ip 10.8.0.2/32;
        }
        establish-tunnels immediately;
    }
}

```

[edit]

user@srx-3# **show routing-options**



```

autonomous-system 100;
static {
    route 10.4.0.0/24 next-hop 10.7.0.2;
    route 10.5.0.0/24 next-hop 10.7.0.2;
    route 10.11.0.0/24 next-hop 10.7.0.2;
    route 10.12.0.0/24 next-hop 10.7.0.2;
    route 10.111.0.1/32 next-hop 10.7.0.2;
    route 10.111.0.2/32 next-hop 10.7.0.2;
}

```

```

[edit]
user@srx-3# show security zones
    security-zone untrust {
        host-inbound-traffic {
            system-services {
                ike;
            }
            protocols {
                all;
            }
        }
        interfaces {
            st0.1;
            lo0.0;
            st0.500;
            ge-0/0/1.0;
            ge-0/0/0.0;
        }
    }
    security-zone trust {
        host-inbound-traffic {
            system-services {
                ike;
            }
            protocols {
                all;
            }
        }
        interfaces {
            ge-0/0/2.0;
        }
    }

```

```
}
```

```
[edit]
```

```
user@srx-3# show interfaces
```

```
ge-0/0/0 {
```

```
    description trust;
```

```
    unit 0 {
```

```
        family inet {
```

```
            address 10.7.0.1/24;
```

```
        }
```

```
    }
```

```
}
```

```
ge-0/0/1 {
```

```
    description untrust;
```

```
    unit 0 {
```

```
        family inet {
```

```
            address 10.6.0.2/24;
```

```
        }
```

```
    }
```

```
}
```

```
ge-0/0/2 {
```

```
    description trust;
```

```
    unit 0 {
```

```
        family inet {
```

```
            address 10.9.0.1/24;
```

```
        }
```

```
    }
```

```
}
```

```
lo0 {
```

```
    description untrust;
```

```
    unit 0 {
```

```
        family inet {
```

```
            address 10.112.0.1/32;
```

```
            address 10.112.0.5/32;
```

```
        }
```

```
    }
```

```
}
```

```
st0 {
```

```
    unit 1 {
```

```

        family inet;
    }
    unit 500 {
        family inet;
    }
}

```

If you are done configuring the device, enter `commit` from configuration mode.

## Verification

### IN THIS SECTION

- [Check Multinode High Availability Details | 857](#)
- [Check Multinode High Availability Details | 861](#)
- [Check Multinode High Availability Peer Node Status | 866](#)
- [Check Multinode High Availability Service Redundancy Groups | 868](#)
- [Verify Interchassis Link \(ICL\) Encryption Status | 874](#)
- [Verify Link Encryption Tunnel Statistics | 876](#)
- [Verify Interchassis Link Active Peers | 877](#)
- [Confirm VPN Status | 878](#)
- [Display IPsec Security Association Details | 879](#)
- [Display Active Peers Per SRG | 881](#)
- [Display IP Prefix to SRG Mapping | 882](#)
- [Display BGP Session Information. | 883](#)

Confirm that the configuration is working properly.

### Check Multinode High Availability Details

#### Purpose

View and verify the details of the Multinode High Availability setup configured on your security device.

## Action

From operational mode, run the following command:

On SRX-1

```

user@srx-01> show chassis high-availability information
Node failure codes:
    HW  Hardware monitoring    LB  Loopback monitoring
    MB  Mbuf monitoring        SP  SPU monitoring
    CS  Cold Sync monitoring    SU  Software Upgrade

Node Status: ONLINE
Local-id: 2
Local-IP: 10.22.0.2
HA Peer Information:

    Peer Id: 1      IP address: 10.22.0.1    Interface: ge-0/0/2.0
    Routing Instance: default
    Encrypted: YES   Conn State: UP
    Cold Sync Status: COMPLETE

SRG failure event codes:
    BF  BFD monitoring
    IP  IP monitoring
    IF  Interface monitoring
    CP  Control Plane monitoring

Services Redundancy Group: 1
    Deployment Type: ROUTING
    Status: BACKUP
    Activeness Priority: 1
    Preemption: ENABLED
    Process Packet In Backup State: NO
    Control Plane State: READY
    System Integrity Check: COMPLETE
    Failure Events: NONE
    Peer Information:
        Peer Id: 1
        Status : ACTIVE
        Health Status: HEALTHY
        Failover Readiness: N/A

```

```

Services Redundancy Group: 2
  Deployment Type: ROUTING
  Status: ACTIVE
  Activeness Priority: 200
  Preemption: ENABLED
  Process Packet In Backup State: NO
  Control Plane State: READY
  System Integrity Check: N/A
  Failure Events: NONE
  Peer Information:
    Peer Id: 1
    Status : BACKUP
    Health Status: HEALTHY
    Failover Readiness: NOT READY

```

## On SRX-2

```

user@srx-02> show chassis high-availability information
Node failure codes:
  HW  Hardware monitoring    LB  Loopback monitoring
  MB  Mbuf monitoring        SP  SPU monitoring
  CS  Cold Sync monitoring    SU  Software Upgrade

Node Status: ONLINE
Local-id: 1
Local-IP: 10.22.0.1
HA Peer Information:

  Peer Id: 2      IP address: 10.22.0.2    Interface: ge-0/0/2.0
  Routing Instance: default
  Encrypted: YES   Conn State: UP
  Cold Sync Status: COMPLETE

SRG failure event codes:
  BF  BFD monitoring
  IP  IP monitoring
  IF  Interface monitoring
  CP  Control Plane monitoring

Services Redundancy Group: 1

```

```

Deployment Type: ROUTING
Status: ACTIVE
Activeness Priority: 200
Preemption: ENABLED
Process Packet In Backup State: NO
Control Plane State: READY
System Integrity Check: N/A
Failure Events: NONE
Peer Information:
  Peer Id: 2
  Status : BACKUP
  Health Status: HEALTHY
  Failover Readiness: NOT READY

```

```

Services Redundancy Group: 2
  Deployment Type: ROUTING
  Status: BACKUP
  Activeness Priority: 1
  Preemption: ENABLED
  Process Packet In Backup State: NO
  Control Plane State: READY
  System Integrity Check: COMPLETE
  Failure Events: NONE
  Peer Information:
    Peer Id: 2
    Status : ACTIVE
    Health Status: HEALTHY
    Failover Readiness: N/A

```

## Meaning

Verify these details from the command output:

- Local node and peer node details such as IP address and ID.
- The field Encrypted: YES indicates that the traffic is protected.
- The field Deployment Type: ROUTING indicates a Layer 3 mode configuration—that is, the network has routers on both sides.
- The field Services Redundancy Group: 1 and Services Redundancy Group: 2 indicate the status of the SRG1 and SRG2 (active or backup) on that node.

## Check Multinode High Availability Details

### Purpose

View and verify the details of the Multinode High Availability setup configured on your security device.

### Action

From operational mode, run the following command:

On SRX-01

```
user@srx-01> show chassis high-availability information detail
Node level Information:
    Node Status: ONLINE
    Local-id: 2
    Local-IP: 10.22.0.2
HA Peer Information:

    Peer-ID: 1      IP address: 10.22.0.1      Interface: ge-0/0/2.0
    Routing Instance: default
    Encrypted: YES   Conn State: UP
    Cold Sync Status: COMPLETE
    Internal Interface: st0.16000
    Internal Local-IP: 180.100.1.2
    Internal Peer-IP: 180.100.1.1
    Internal Routing-instance: __juniper_private1__
Packet Statistics:
    Receive Error : 0      Send Error : 0

    Packet-type      Sent      Received
    SRG Status Msg   4         6
    SRG Status Ack    4         4
    Attribute Msg     1         1
    Attribute Ack     1         1

HA Peer Conn events:
    Jan 31 00:55:19.249 : HA Peer 180.100.1.1 BFD conn came up

Cold Synchronization:
    Status:
        Cold synchronization completed for: N/A
```

Cold synchronization failed for: N/A  
 Cold synchronization not known for: N/A  
 Current Monitoring Weight: 0

Progress:

CS Prereq	1 of 1 SPU's completed
1. if_state sync	1 SPU's completed
2. ha peer conn	1 SPU's completed
3. policy data sync	1 SPU's completed
4. cp ready	1 SPU's completed
5. VPN data sync	1 SPU's completed
6. IPID data sync	1 SPU's completed
7. All SPU ready	1 SPU's completed
8. AppID ready	1 SPU's completed
9. Tunnel Sess ready	1 SPU's completed
CS RTO sync	1 of 1 SPU's completed
CS Postreq	1 of 1 SPU's completed

Statistics:

Number of cold synchronization completed: 0  
 Number of cold synchronization failed: 0

Events:

Jan 31 00:55:24.616 : Cold sync for PFE is Post-req check in process  
 Jan 31 00:55:25.615 : Cold sync for PFE is Completed

SPU monitoring:

Status: Enabled

Current monitoring weight: 0

Statistics:

SPU up count: 1  
 NPC up count: 0  
 SPU down count: 0  
 NPC down count: 0  
 Chassis info processing error count: 0

Loopback Information:

PIC Name	Loopback	Nexthop	Mbuf
-----			
	Success	Success	Success



## Hardware monitoring:

## Status:

Activation status: Enabled

Ctrl Plane Hardware errors: 0

Data Plane Hardware errors: 0

## SRGS Information:

## Services Redundancy Group: 1

Deployment Type: ROUTING

Status: BACKUP

Activeness Priority: 1

Hold Timer: 1

Services: [ IPSEC ]

Process Packet In Backup State: NO

Control Plane State: READY

System Integrity Check: COMPLETE

## Peer Information:

Failure Events: NONE

Peer Id: 1

Last Advertised HA Status: ACTIVE

Last Advertised Health Status: HEALTHY

Failover Readiness: N/A

## Signal Route Info:

Active Signal Route:

IP: 10.39.1.1

Routing Instance: default

Status: NOT INSTALLED

Backup Signal Route:

IP: 10.39.1.2

Routing Instance: default

Status: INSTALLED

## Split-brain Prevention Probe Info:

DST-IP: 10.111.0.1

SRC-IP: 10.11.0.1

Routing Instance: default

Status: NOT RUNNING

Result: N/A

Reason: N/A

## SRG State Change Events:

Jan 31 00:52:14.347 : SRG[1] state UNKNOWN -> HOLD, Reason: State machine start  
 Jan 31 00:56:33.046 : SRG[1] state HOLD -> BACKUP, Reason: Peer state Active received

## BFD Monitoring:

Status: UNKNOWN

SRC-IP: 10.5.0.1      DST-IP: 10.5.0.2

Routing Instance: default

Type: SINGLE-HOP

IFL Name: ge-0/0/3.0

State: INSTALLED

## Interface Monitoring:

Status: UP

IF Name: ge-0/0/4      State: Up

IF Name: ge-0/0/3      State: Up

## Probe status events:

Jan 31 00:54:12.695 : SRG[1] HA probe dst 10.111.0.1 became unreachable, Reason: UNKNOWN

## SRGS Information:

## Services Redundancy Group: 2

Deployment Type: ROUTING

Status: ACTIVE

Activeness Priority: 200

Hold Timer: 1

**Services: [ IPSEC ]**

Process Packet In Backup State: NO

Control Plane State: READY

System Integrity Check: N/A

Peer Information:

Failure Events: NONE

Peer Id: 1

Last Advertised HA Status: BACKUP

Last Advertised Health Status: HEALTHY

Failover Readiness: NOT READY

## Signal Route Info:

Active Signal Route:

IP: 10.49.1.1

Routing Instance: default

Status: INSTALLED

Backup Signal Route:

IP: 10.49.1.2

Routing Instance: default

Status: NOT INSTALLED

## Split-brain Prevention Probe Info:

DST-IP: 10.111.0.1

SRC-IP: 10.12.0.1

Routing Instance: default

Status: NOT RUNNING

Result: N/A

Reason: N/A

## SRG State Change Events:

Jan 31 00:52:14.439 : SRG[2] state UNKNOWN -&gt; HOLD, Reason: State machine start

Jan 31 00:55:24.263 : SRG[2] state HOLD -&gt; ACTIVE, Reason: Local Priority Higher

## BFD Monitoring:

Status: UNKNOWN

SRC-IP: 10.5.0.1      DST-IP: 10.5.0.2

Routing Instance: default

Type: SINGLE-HOP

IFL Name: ge-0/0/3.0

State: INSTALLED

## Interface Monitoring:

Status: UP

IF Name: ge-0/0/4      State: Up

IF Name: ge-0/0/3      State: Up

Probe status events:

```
Jan 31 00:54:13.698 : SRG[2] HA probe dst 10.111.0.1 became unreachable, Reason: UNKNOWN
```

## Meaning

Verify these details from the command output:

- The field Services: [ IPSEC ] indicates the associated IPSec VPN for each SRG.
- The fields BFD Monitoring, Interface Monitoring, Split-brain Prevention Probe Info display monitoring details.
- The fields Cold Synchronization, SRG State Change Events provide details on current status and recent changes.
- The field Services Redundancy Group: 1 and Services Redundancy Group: 2 indicate the status of the SRG1 and SRG2 (active or backup) on that node.

In the command output, the IP addresses such as IP 180.100.1.2 are generated internally by Junos OS and these addresses do not interfere with routing tables.

## Check Multinode High Availability Peer Node Status

### Purpose

View and verify the peer node details.

### Action

From operational mode, run the following command on SRX-01 and SRX-02:

#### SRX-01

```
user@srx-01> show chassis high-availability peer-info
```

HA Peer Information:

```
Peer-ID: 1      IP address: 10.22.0.1      Interface: ge-0/0/2.0
Routing Instance: default
Encrypted: YES  Conn State: UP
Cold Sync Status: COMPLETE
Internal Interface: st0.16000
Internal Local-IP: 180.100.1.2
Internal Peer-IP: 180.100.1.1
Internal Routing-instance: __juniper_private1__
```

#### Packet Statistics:

Receive Error : 0

Send Error : 0

Packet-type	Sent	Received
SRG Status Msg	4	6
SRG Status Ack	4	4
Attribute Msg	1	1
Attribute Ack	1	1

## SRX-02

```
user@srx-02> show chassis high-availability peer-info
```

HA Peer Information:

Peer-ID: 2      IP address: 10.22.0.2      Interface: ge-0/0/2.0

Routing Instance: default

Encrypted: YES      Conn State: UP

Cold Sync Status: COMPLETE

Internal Interface: st0.16000

Internal Local-IP: 180.100.1.1

Internal Peer-IP: 180.100.1.2

Internal Routing-instance: \_\_juniper\_private1\_\_

#### Packet Statistics:

Receive Error : 0

Send Error : 0

Packet-type	Sent	Received
SRG Status Msg	6	4
SRG Status Ack	4	4
Attribute Msg	2	1
Attribute Ack	1	1

## Meaning

Verify these details from the command output:

- Peer node details such as interface used, IP address, and ID
- Encryption status, connection status, and cold synchronization status
- Packet statistics across the node.

## Check Multinode High Availability Service Redundancy Groups

### Purpose

Verify that the SRGs are configured and working correctly.

### Action

From operational mode, run the following command on both security devices:

#### SRG1 on SRX-02

```
user@srx-02> show chassis high-availability services-redundancy-group 1
```

```
SRG failure event codes:
```

```
BF  BFD monitoring
IP  IP monitoring
IF  Interface monitoring
CP  Control Plane monitoring
```

```
Services Redundancy Group: 1
```

```
Deployment Type: ROUTING
Status: ACTIVE
Activeness Priority: 200
Preemption: ENABLED
Process Packet In Backup State: NO
Control Plane State: READY
System Integrity Check: N/A
Failure Events: NONE
Peer Information:
  Peer Id: 2
  Status : BACKUP
  Health Status: HEALTHY
  Failover Readiness: NOT READY
```

```
Signal Route Info:
```

```
Active Signal Route:
IP: 10.39.1.1
Routing Instance: default
Status: INSTALLED
```

```
Backup Signal Route:
IP: 10.39.1.2
```

Routing Instance: default  
Status: NOT INSTALLED

Split-brain Prevention Probe Info:

DST-IP: 10.111.0.1  
SRC-IP: 10.11.0.1  
Routing Instance: default  
Status: NOT RUNNING  
Result: N/A                      Reason: N/A

BFD Monitoring:

Status: UNKNOWN

SRC-IP: 10.4.0.1      DST-IP: 10.4.0.2  
Routing Instance: default  
Type: SINGLE-HOP  
IFL Name: ge-0/0/3.0  
State: INSTALLED

Interface Monitoring:

Status: UP

IF Name: ge-0/0/4      State: Up

IF Name: ge-0/0/3      State: Up

IP SRGID Table:

SRGID	IP Prefix	Routing Table
1	10.11.0.0/24	default

## SRG2 on SRX-02

```
user@srx-02> show chassis high-availability services-redundancy-group 2
```

SRG failure event codes:

BF BFD monitoring  
IP IP monitoring  
IF Interface monitoring  
CP Control Plane monitoring

## Services Redundancy Group: 2

Deployment Type: ROUTING

Status: BACKUP

Activeness Priority: 1

Preemption: ENABLED

Process Packet In Backup State: NO

Control Plane State: READY

System Integrity Check: COMPLETE

Failure Events: NONE

## Peer Information:

Peer Id: 2

Status : ACTIVE

Health Status: HEALTHY

Failover Readiness: N/A

## Signal Route Info:

Active Signal Route:

IP: 10.49.1.1

Routing Instance: default

Status: NOT INSTALLED

Backup Signal Route:

IP: 10.49.1.2

Routing Instance: default

Status: INSTALLED

## Split-brain Prevention Probe Info:

DST-IP: 10.111.0.1

SRC-IP: 10.12.0.1

Routing Instance: default

Status: NOT RUNNING

Result: N/A

Reason: N/A

## BFD Monitoring:

Status: UNKNOWN

SRC-IP: 10.4.0.1      DST-IP: 10.4.0.2

Routing Instance: default

Type: SINGLE-HOP

IFL Name: ge-0/0/3.0

State: INSTALLED



## Interface Monitoring:

Status: UP

IF Name: ge-0/0/4      State: Up

IF Name: ge-0/0/3      State: Up

## IP SRGID Table:

SRGID	IP Prefix	Routing Table
2	10.12.0.0/24	default

**SRG1 on SRX-01**user@srx-01> **show chassis high-availability services-redundancy-group 1**

## SRG failure event codes:

BF BFD monitoring  
 IP IP monitoring  
 IF Interface monitoring  
 CP Control Plane monitoring

## Services Redundancy Group: 1

Deployment Type: ROUTING  
 Status: BACKUP  
 Activeness Priority: 1  
 Preemption: ENABLED  
 Process Packet In Backup State: NO  
 Control Plane State: READY  
 System Integrity Check: COMPLETE  
 Failure Events: NONE  
 Peer Information:  
   Peer Id: 1  
   Status : ACTIVE  
   Health Status: HEALTHY  
   Failover Readiness: N/A

## Signal Route Info:

Active Signal Route:  
 IP: 10.39.1.1  
 Routing Instance: default  
 Status: NOT INSTALLED

Backup Signal Route:  
 IP: 10.39.1.2  
 Routing Instance: default  
 Status: INSTALLED

Split-brain Prevention Probe Info:  
 DST-IP: 10.111.0.1  
 SRC-IP: 10.11.0.1  
 Routing Instance: default  
 Status: NOT RUNNING  
 Result: N/A                      Reason: N/A

BFD Monitoring:  
 Status: UNKNOWN

SRC-IP: 10.5.0.1      DST-IP: 10.5.0.2  
 Routing Instance: default  
 Type: SINGLE-HOP  
     IFL Name: ge-0/0/3.0  
 State: INSTALLED

Interface Monitoring:  
 Status: UP

IF Name: ge-0/0/4      State: Up

IF Name: ge-0/0/3      State: Up

IP SRGID Table:

SRGID	IP Prefix	Routing Table
1	10.11.0.0/24	default

## SRG2 on SRX-01

```
user@srx-01> show chassis high-availability services-redundancy-group 2
SRG failure event codes:
  BF  BFD monitoring
  IP  IP monitoring
```

IF Interface monitoring  
 CP Control Plane monitoring

#### Services Redundancy Group: 2

Deployment Type: ROUTING  
 Status: ACTIVE  
 Activeness Priority: 200  
 Preemption: ENABLED  
 Process Packet In Backup State: NO  
 Control Plane State: READY  
 System Integrity Check: N/A  
 Failure Events: NONE  
 Peer Information:  
   Peer Id: 1  
   Status : BACKUP  
   Health Status: HEALTHY  
   Failover Readiness: NOT READY

#### Signal Route Info:

Active Signal Route:  
 IP: 10.49.1.1  
 Routing Instance: default  
 Status: INSTALLED

Backup Signal Route:  
 IP: 10.49.1.2  
 Routing Instance: default  
 Status: NOT INSTALLED

#### Split-brain Prevention Probe Info:

DST-IP: 10.111.0.1  
 SRC-IP: 10.12.0.1  
 Routing Instance: default  
 Status: NOT RUNNING  
 Result: N/A                      Reason: N/A

#### BFD Monitoring:

Status: UNKNOWN

SRC-IP: 10.5.0.1      DST-IP: 10.5.0.2  
 Routing Instance: default  
 Type: SINGLE-HOP

```
IFL Name: ge-0/0/3.0
State: INSTALLED
```

```
Interface Monitoring:
Status: UP
```

```
IF Name: ge-0/0/4      State: Up
```

```
IF Name: ge-0/0/3      State: Up
```

```
IP SRGID Table:
```

SRGID	IP Prefix	Routing Table
2	10.12.0.0/24	default

## Meaning

Verify these details from the command output:

- Peer node details such as deployment type, status, active and back up signal routes.
- Split-brain prevention probe, IP monitoring and BFD monitoring status.
- Associated IP prefix table.

## Verify Interchassis Link (ICL) Encryption Status

### Purpose

Verify the interchassis link (ICL) status.

### Action

Run the following command on SRX-01:

```
user@srx-01> show security ipsec security-associations ha-link-encryption
Total active tunnels: 1      Total IPsec sas: 1
ID      Algorithm      SPI      Life:sec/kb  Mon   lsys   Port   Gateway
```

```
<495002 ESP:aes-gcm-256/aes256-gcm 0x0008d9c7 236/ unlim - root 500 10.22.0.1
>495002 ESP:aes-gcm-256/aes256-gcm 0x0001a573 236/ unlim - root 500 10.22.0.1
```

```
user@srx-01> show security ike security-associations ha-link-encryption
```

Index	State	Initiator cookie	Responder cookie	Mode	Remote Address
16776938	UP	9f8fe46ce3be92f8	44e6b3fd74cc9294	IKEv2	10.22.0.1

```
user@srx-01> show security ipsec security-associations ha-link-encryption detail
```

```
ID: 495002 Virtual-system: root, VPN Name: ICL_IPSEC_VPN
```

```
Local Gateway: 10.22.0.2, Remote Gateway: 10.22.0.1
```

```
Traffic Selector Name: __ICL_IPSEC_VPN__multi_node__
```

```
Local Identity: ipv4(180.100.1.2-180.100.1.2)
```

```
Remote Identity: ipv4(180.100.1.1-180.100.1.1)
```

```
TS Type: traffic-selector
```

```
Version: IKEv2
```

```
Quantum Secured: No
```

```
PFS group: N/A
```

```
SRG ID: 0
```

```
DF-bit: clear, Copy-Outer-DSCP Disabled, Bind-interface: st0.16000, Policy-name: ICL_IPSEC_POL
```

```
Port: 500, Nego#: 0, Fail#: 0, Def-Del#: 0 Flag: 0
```

```
Multi-sa, Configured SAs# 0, Negotiated SAs#: 0
```

```
HA Link Encryption Mode: Multi-Node
```

```
Location: FPC -, PIC -, KMD-Instance -
```

```
Anchorship: Thread -
```

```
Distribution-Profile: default-profile
```

```
Direction: inbound, SPI: 0x0008d9c7, AUX-SPI: 0
```

```
, VPN Monitoring: -
```

```
Hard lifetime: Expires in 200 seconds
```

```
Lifesize Remaining: Unlimited
```

```
Soft lifetime: Expires in 115 seconds
```

```
Mode: Tunnel(0 0), Type: dynamic, State: installed
```

```
Protocol: ESP, Authentication: aes256-gcm, Encryption: aes-gcm (256 bits)
```

```
Anti-replay service: counter-based enabled, Replay window size: 64
```

```
Extended-Sequence-Number: Disabled
```

```
tunnel-establishment: establish-tunnels-immediately
```

```
Location: FPC 0, PIC 0, KMD-Instance 0
```

```
Anchorship: Thread 0
```

```
IKE SA Index: 16776938
```

```
Direction: outbound, SPI: 0x0001a573, AUX-SPI: 0
```

```

, VPN Monitoring: -
Hard lifetime: Expires in 200 seconds
Lifesize Remaining: Unlimited
Soft lifetime: Expires in 115 seconds
Mode: Tunnel(0 0), Type: dynamic, State: installed
Protocol: ESP, Authentication: aes256-gcm, Encryption: aes-gcm (256 bits)
Anti-replay service: counter-based enabled, Replay window size: 64
Extended-Sequence-Number: Disabled
tunnel-establishment: establish-tunnels-immediately
Location: FPC 0, PIC 0, KMD-Instance 0
Anchorship: Thread 0
IKE SA Index: 16776938

```

## Meaning

The command output provides the following information:

- The local gateway and remote gateway details.
- The IPsec SA pair for each threads in PIC.
- HA link encryption mode (as shown in the following line):

```
HA Link Encryption Mode: Multi-Node
```

- Authentication and encryption algorithms used

## Verify Link Encryption Tunnel Statistics

### Purpose

Verify link encryption tunnel statistics on both active and backup nodes.

### Action

Run the following command on SRX-01:

```

user@srx-01> show security ipsec statistics ha-link-encryption
ESP Statistics:
  Encrypted bytes:      106294156
  Decrypted bytes:      51961287

```

```

Encrypted packets:      979531
Decrypted packets:      989651
AH Statistics:
Input bytes:            0
Output bytes:           0
Input packets:          0
Output packets:         0
Errors:
AH authentication failures: 0, Replay errors: 0
ESP authentication failures: 0, ESP decryption failures: 0
Bad headers: 0, Bad trailers: 0
Invalid SPI: 0, TS check fail: 0
Exceeds tunnel MTU: 0
Discarded: 0

```

## Meaning

If you see packet loss issues across a VPN, you can run the `show security ipsec statistics ha-link-encryption` command several times to verify that the encrypted and decrypted packet counters are incrementing. You should also check whether the other error counters are incrementing.

Use the `clear security ipsec security-associations ha-link-encryption` command to clear all IPsec statistics.

## Verify Interchassis Link Active Peers

### Purpose

View only ICL active peers, but not regular IKE active peers.

### Action

Run the following commands on SRX-01 and SRX-02 devices:

SRX-1

```

user@srx-01> show security ike active-peer ha-link-encryption
Remote Address  Port    Peer IKE-ID  AAA username  Assigned IP
10.22.0.1       500     10.22.0.1   not available  0.0.0.0

```

## SRX-2

```
user@srx-02> show security ike active-peer ha-link-encryption
```

Remote Address	Port	Peer IKE-ID	AAA username	Assigned IP
10.22.0.2	500	10.22.0.2	not available	0.0.0.0

**Meaning**

Command output displays only the active peer of the ICL with details such as the peer addresses and ports the active peer is using.

**Confirm VPN Status****Purpose**

Confirm VPN status by checking the status of any IKE security associations at SRG level.

**Action**

Run the following commands on SRX-1, SRX-2, and SRX-3 (VPN peer device):

## SRX-01

```
user@srx-01> show security ike security-associations srg-id 1
```

Index	State	Initiator cookie	Responder cookie	Mode	Remote Address
16777319	UP	19e7cd4e503eeb2e	0800a7ceaafda740	IKEv2	10.112.0.1

```
user@srx-01> show security ike security-associations srg-id 2
```

Index	State	Initiator cookie	Responder cookie	Mode	Remote Address
33554536	UP	9944aaf1ab914b42	15cef0da496bdd92	IKEv2	10.112.0.5



## SRX-02

```
user@srx-02> show security ike security-associations srg-id 1
```

Index	State	Initiator cookie	Responder cookie	Mode	Remote Address
16777319	UP	19e7cd4e503eeb2e	0800a7ceafda740	IKEv2	10.112.0.1

```
user@srx-02> show security ike security-associations srg-id 2
```

Index	State	Initiator cookie	Responder cookie	Mode	Remote Address
33554534	UP	366d174d847f8c71	2f654c6f1c463d80	IKEv2	10.112.0.5

## SRX-3 (VPN Peer Device)

```
user@srx-03> show security ike security-associations
```

Index	State	Initiator cookie	Responder cookie	Mode	Remote Address
5929032	UP	366d174d847f8c71	2f654c6f1c463d80	IKEv2	10.12.0.1
5929033	UP	19e7cd4e503eeb2e	0800a7ceafda740	IKEv2	10.11.0.1

## Meaning

The output indicates that:

- IP addresses of the remote peers.
- The state showing UP for both remote peers indicates the successful association of Phase 1 establishment.
- The remote peer IP address, IKE policy, and external interfaces are all correct.

## Display IPsec Security Association Details

## Purpose

Display the individual IPsec SA details identified by SRG IDs.

## Action

Run the following command on the SRX Series devices:

## SRX-1

```
user@srx-01> show security ipsec security-associations srg-id 1
```

```
Total active tunnels: 1      Total IPsec sas: 1
```

ID	Algorithm	SPI	Life:sec/kb	Mon	lsys	Port	Gateway
<17277223	ESP:aes-cbc-256/sha256	0xc50520d4	1210/ unlim	-	root	500	10.112.0.1
>17277223	ESP:aes-cbc-256/sha256	0x6d1e9c89	1210/ unlim	-	root	500	10.112.0.1

```
user@srx-01> show security ipsec security-associations srg-id 2
```

```
Total active tunnels: 1      Total IPsec sas: 1
```

ID	Algorithm	SPI	Life:sec/kb	Mon	lsys	Port	Gateway
<34054437	ESP:aes-cbc-256/sha256	0x9feb290c	1382/ unlim	-	root	500	10.112.0.5
>34054437	ESP:aes-cbc-256/sha256	0xf41d091c	1382/ unlim	-	root	500	10.112.0.5

## SRX-02

```
user@srx-02> show security ipsec security-associations srg-id 1
```

```
Total active tunnels: 1      Total IPsec sas: 1
```

ID	Algorithm	SPI	Life:sec/kb	Mon	lsys	Port	Gateway
<17277223	ESP:aes-cbc-256/sha256	0xc50520d4	1286/ unlim	-	root	500	10.112.0.1
>17277223	ESP:aes-cbc-256/sha256	0x6d1e9c89	1286/ unlim	-	root	500	10.112.0.1

```
user@srx-02> show security ipsec security-associations srg-id 2
```

```
Total active tunnels: 1      Total IPsec sas: 1
```

ID	Algorithm	SPI	Life:sec/kb	Mon	lsys	Port	Gateway
<34054437	ESP:aes-cbc-256/sha256	0x9feb290c	1461/ unlim	-	root	500	10.112.0.5
>34054437	ESP:aes-cbc-256/sha256	0xf41d091c	1461/ unlim	-	root	500	10.112.0.5

## SRX-03

```
user@srx-03> show security ipsec security-associations
```

```
Total active tunnels: 2      Total IPsec sas: 2
```

ID	Algorithm	SPI	Life:sec/kb	Mon	lsys	Port	Gateway
<67108865	ESP:aes-cbc-256/sha256	6d1e9c89	1392/ unlim	-	root	500	10.11.0.1
>67108865	ESP:aes-cbc-256/sha256	c50520d4	1392/ unlim	-	root	500	10.11.0.1

```
<67108866 ESP:aes-cbc-256/sha256 f41d091c 1570/ unlim - root 500 10.12.0.1
>67108866 ESP:aes-cbc-256/sha256 9feb290c 1570/ unlim - root 500 10.12.0.1
```

## Meaning

The output displays the state of the VPN.

## Display Active Peers Per SRG

## Purpose

Display the list of connected active peers with peer addresses and ports they are using.

## Action

Run the following commands on the SRX Series devices:

SRX-01

```
user@srx-01> show security ike active-peer srg-id 1
```

Remote Address	Port	Peer IKE-ID	AAA username	Assigned IP
10.112.0.1	500	10.112.0.1	not available	0.0.0.0

```
user@srx-01> show security ike active-peer srg-id 2
```

Remote Address	Port	Peer IKE-ID	AAA username	Assigned IP
10.112.0.5	500	10.112.0.5	not available	0.0.0.0

## SRX-02

```
user@srx-02> show security ike active-peer srg-id 1
```

Remote Address	Port	Peer IKE-ID	AAA username	Assigned IP
10.112.0.1	500	10.112.0.1	not available	0.0.0.0

```
user@srx-02> show security ike active-peer srg-id 2
```

Remote Address	Port	Peer IKE-ID	AAA username	Assigned IP
10.112.0.5	500	10.112.0.5	not available	0.0.0.0

**Meaning**

The output displays the list of connected devices with details about the peer addresses and ports used.

**Display IP Prefix to SRG Mapping****Purpose**

Display IP prefix to SRG mapping information.

**Action**

Run the following command on SRX-01 device.

```
user@srx-01> show chassis high-availability prefix-srgid-table
```

IP SRGID Table:		
SRGID	IP Prefix	Routing Table
1	10.11.0.0/24	default
2	10.12.0.0/24	default

**Meaning**

Output shows IP address prefixes mapped to SRGs in the setup.

Display BGP Session Information.

Purpose

Display summary information about BGP and its neighbors to determine if routes are received from peers.

Action

Run the following commands on the SRX Series devices:

SRX-1 Device

```
user@srx-01> show bgp summary
Threading mode: BGP I/O
Default eBGP mode: advertise - accept, receive - accept
Groups: 2 Peers: 2 Down peers: 0
Table          Tot Paths  Act Paths Suppressed    History Damp State    Pending
inet.0
                0         0         0         0         0         0         0
Peer           AS      InPkt    OutPkt    OutQ   Flaps Last Up/Dwn State|#Active/
Received/Accepted/Damped...
10.3.0.1       100      37       40        0       0      15:43 Establ
  inet.0: 0/0/0/0
10.5.0.2       100      37       40        0       0      15:42 Establ
  inet.0: 0/0/0/0
```

SRX-2 Device

```
user@srx-02> show bgp summary
Threading mode: BGP I/O
Default eBGP mode: advertise - accept, receive - accept
Groups: 2 Peers: 2 Down peers: 0
Table          Tot Paths  Act Paths Suppressed    History Damp State    Pending
inet.0
                0         0         0         0         0         0         0
Peer           AS      InPkt    OutPkt    OutQ   Flaps Last Up/Dwn
St                                     ate|#Active/
Received/Accepted/Damped...
10.2.0.1       100     842     846        0       0     6:18:40
Es                                     tabl
```

```
inet.0: 0/0/0/0
10.4.0.2      100      842      846      0      0      6:18:42
Es
inet.0: 0/0/0/0
```

Meaning

The output shows that the BGP session is established and the peers are exchanging update messages.

SEE ALSO

<a href="#">Multinode High Availability   613</a>
<a href="#">IPsec VPN Support in Multinode High Availability   664</a>
<a href="#">Prepare Your Environment for Multinode High Availability Deployment   654</a>

# Hardware and Software Upgrades

IN THIS CHAPTER

- [Software Upgrade in Multinode High Availability | 885](#)
- [Insert Additional SRX5K-SPC3 in a Multinode High Availability Setup | 904](#)

## Software Upgrade in Multinode High Availability

IN THIS SECTION

- [Overview | 885](#)
- [Preinstallation Steps | 887](#)
- [Upgrade Software using install-on-failure-route | 889](#)
- [Upgrade Software using shutdown-on-failure interface | 896](#)

### Overview

In a Multinode High Availability setup, you can upgrade your SRX Series devices between two different Junos OS releases with minimal disruption of traffic.

We support a software upgrade method using the CLI as in Junos OS Release 22.3R1.

From Junos OS Release	To Junos OS Release	Use Software Upgrade Method
20.4	Any release post 20.4	No
22.3	Next version of Junos OS Release	Yes

For information about upgrade and downgrade support for Junos OS releases, see *Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases* in Release Notes.



**CAUTION:** When you are upgrading an SRX Series device from Junos OS Release 22.3 to the next version of the Junos OS release, you may experience some disruption in traffic.

You must install the same version of Junos OS on both the SRX Series devices in a Multinode High Availability setup. Therefore, when you upgrade Junos OS on one device, ensure that you upgrade the other device also to the same version.

We support following upgrade methods in Multinode High Availability setup:

- **For Layer 3 deployments:** The install-on-failure-route configuration (recommended). In this method, you can divert the traffic by changing the route. Here, traffic can still go through the node and interface remains up. Go to ["Upgrade Software using install-on-failure-route" on page 889](#) for details. You can also use the shutdown-on-failure interfaces method for Layer 3 deployments.
- **For Hybrid deployment and Default gateway (Layer 2/switching) deployments:** The shutdown-on-failure interfaces method. In this method, you can divert the traffic by closing down interfaces on the node. Here, traffic cannot pass through the nodes. Go to ["Upgrade Software using shutdown-on-failure interface" on page 896](#) for details..

In the following procedure, we'll show you how to upgrade two SRX Series devices (SRX-01 and SRX-02) from Junos OS Release 22.3R1.1 to Junos OS Release 22.3R1.3 using CLI. To avoid downtime when upgrading SRX Series devices in Multinode High Availability setup, we'll update one device at a time.

## Best Practices for Upgrading Junos OS

Consider the following best practices when you plan your software upgrade:

- Ensure both nodes are online and have the same version of Junos OS.
- Prepare your SRX Series devices for an upgrade using the checklist available in [Preparing for Software Installation and Upgrade \(Junos OS\)](#).
- Check whether both nodes have sufficient storage in the `/var` file system by using the `show system storage` command.
- Check the status of all the cards on both the devices by using the `show chassis fpc pic-status` command.
- Verify that there are no major alarms on the devices by using the `show chassis alarms` command.
- Ensure that there are no uncommitted changes.
- Back up the active configuration and license keys.



We recommend that you perform software upgrades during a maintenance window.

## Preinstallation Steps

Complete the following tasks before you start the software upgrade.

- Check the current Junos OS software version on your device.

```
user@host> show version
Hostname: srx-01
Model: vSRX
Junos: 22.3R1.1
```

- Download the Junos OS image from the [Juniper Networks Support](#) page on both SRX Series devices and save it in the `/var/tmp` location.
- Use the `show chassis high-availability information` command to verify that your Multinode High Availability setup is healthy, functional, and that the interchassis link (ICL) is up.

### On SRX-01 Device

```
user@srx-01> show chassis high-availability information
Node failure codes:
  HW  Hardware monitoring    LB  Loopback monitoring
  MB  Mbuf monitoring        SP  SPU monitoring
  CS  Cold Sync monitoring    SU  Software Upgrade

Node Status: ONLINE
Local-id: 1
Local-IP: 10.22.0.1
HA Peer Information:

  Peer Id: 2      IP address: 10.22.0.2    Interface: ge-0/0/2.0
  Routing Instance: default
  Encrypted: YES   Conn State: UP
  Cold Sync Status: COMPLETE

Services Redundancy Group: 0
  Current State: ONLINE
  Peer Information:
    Peer Id: 2
```

SRG failure event codes:

BF BFD monitoring  
 IP IP monitoring  
 IF Interface monitoring  
 CP Control Plane monitoring

Services Redundancy Group: 1

Deployment Type: ROUTING  
 Status: ACTIVE  
 Activeness Priority: 200  
 Preemption: ENABLED  
 Process Packet In Backup State: NO  
 Control Plane State: READY  
 System Integrity Check: N/A  
 Failure Events: NONE  
 Peer Information:  
 Peer Id: 2  
 Status : BACKUP  
 Health Status: HEALTHY  
 Failover Readiness: READY

## On SRX-02 Device

```
user@srx-02> show chassis high-availability information
```

Node failure codes:

HW	Hardware monitoring	LB	Loopback monitoring
MB	Mbuf monitoring	SP	SPU monitoring
CS	Cold Sync monitoring	SU	Software Upgrade

Node Status: ONLINE

Local-id: 2

Local-IP: 10.22.0.2

HA Peer Information:

Peer Id: 1	IP address: 10.22.0.1	Interface: ge-0/0/2.0
Routing Instance: default		
Encrypted: YES	Conn State: UP	
Cold Sync Status: COMPLETE		

Services Redundancy Group: 0

Current State: ONLINE

Peer Information:

```

Peer Id: 1

SRG failure event codes:
  BF  BFD monitoring
  IP  IP monitoring
  IF  Interface monitoring
  CP  Control Plane monitoring

Services Redundancy Group: 1
  Deployment Type: ROUTING
  Status: BACKUP
  Activeness Priority: 1
  Preemption: DISABLED
  Process Packet In Backup State: NO
  Control Plane State: READY
  System Integrity Check: COMPLETE
  Failure Events: NONE
  Peer Information:
    Peer Id: 1
    Status : ACTIVE
    Health Status: HEALTHY
    Failover Readiness: N/A

```

These output samples confirm that the two SRX Series devices in the Multinode High Availability setup are in a healthy state and are operating normally.

You are now ready to proceed with software upgrade.

## Upgrade Software using install-on-failure-route

### Prerequisite for Diverting Transit Traffic

Check whether your device has the configuration required to divert transit traffic by changing the route as mentioned in ["Configuring Multinode High Availability In a Layer 3 Network" on page 672](#). If you haven't configured:

1. Create a dedicated custom virtual router for the route used for diverting traffic during the upgrade.

```

user@host# set routing-instances MNHA-signal-routes instance-type virtual-router

```

2. Configure the `install-on-failure-route` statement for SRG0. Here, you have configured the route with IP address 10.39.1.3 as the route to install when the node fails.

```
user@host# set routing-instances MNHA-signal-routes instance-type virtual-router
user@host# set chassis high-availability services-redundancy-group 0 install-on-failure-route
10.39.1.3 routing-instance MNHA-signal-routes
user@host# set chassis high-availability services-redundancy-group 1 active-signal-route
10.39.1.1 routing-instance MNHA-signal-routes
user@host# set chassis high-availability services-redundancy-group 1 backup-signal-route
10.39.1.2 routing-instance MNHA-signal-routes
```

The routing table installs the route mentioned in the statement when the node fails.

3. Configure a matching routing policy and define a policy condition based on the existence of routes. Here you include the route 10.39.1.3 as the route match condition for the `if-route-exists`.

```
user@host# set policy-options condition active_route_exists if-route-exists address-family
inet 10.39.1.1/32
user@host# set policy-options condition active_route_exists if-route-exists address-family
inet table MNHA-signal-routes.inet.0
user@host# set policy-options condition backup_route_exists if-route-exists address-family
inet 10.39.1.2/32
user@host# set policy-options condition backup_route_exists if-route-exists address-family
inet table MNHA-signal-routes.inet.0
user@host# set policy-options condition failure_route_exists if-route-exists address-family
inet 10.39.1.3/32
user@host# set policy-options condition failure_route_exists if-route-exists address-family
inet table MNHA-signal-routes.inet.0
```

Create the policy statement to refer the condition as one of the matching term.

```
user@host# set policy-options policy-statement mnha-route-policy term 4 from protocol static
user@host# set policy-options policy-statement mnha-route-policy term 4 from protocol direct
user@host# set policy-options policy-statement mnha-route-policy term 4 from condition
failure_route_exists
user@host# set policy-options policy-statement mnha-route-policy term 4 then metric 100
user@host# set policy-options policy-statement mnha-route-policy term 4 then accept
```

## Upgrade Multinode High Availability Software

Let's upgrade the device that is acting as the backup node (SRX-02).

1. Initiate the software upgrade process and commit the configuration.

```
user@srx-02# set chassis high-availability software-upgrade
```

This command initiates local failure for SRG0 and transitions SRG1 (if configured) to the INELIGIBLE state on the local device. The peer device now transitions to or stays in active state for SRG1. On the local node, the active and backup signal routes of SRG1 are removed. If you've configured the install-on-failure-route statement, the signal route associated with the install-on-failure-route configuration is installed. With the appropriate routing policies, the local device can advertise higher route metrics and divert the traffic away from the local device and steer the traffic toward the peer device,

2. Verify the status of Multinode High Availability.

```
user@srx-02> show chassis high-availability information
Node failure codes:
  HW  Hardware monitoring   LB  Loopback monitoring
  MB  Mbuf monitoring       SP  SPU monitoring
  CS  Cold Sync monitoring  SU  Software Upgrade

Node Status: OFFLINE [ SU ]
Local-id: 1
Local-IP: 10.22.0.1
HA Peer Information:

  Peer Id: 2      IP address: 10.22.0.2      Interface: ge-0/0/2.0
  Routing Instance: default
  Encrypted: YES   Conn State: UP
  Cold Sync Status: COMPLETE

Services Redundancy Group: 0
  Current State: ONLINE
  Peer Information:
    Peer Id: 2

SRG failure event codes:
  BF  BFD monitoring
  IP  IP monitoring
```

```
IF Interface monitoring
CP Control Plane monitoring
```

```
Services Redundancy Group: 1
  Deployment Type: ROUTING
  Status: INELIGIBLE
  Activeness Priority: 200
  Preemption: ENABLED
  Process Packet In Backup State: NO
  Control Plane State: N/A
  System Integrity Check: IN PROGRESS
  Failure Events: NONE
  Peer Information:
    Peer Id: 2
    Status : ACTIVE
    Health Status: HEALTHY
    Failover Readiness: N/A
```

The output shows Node Status: OFFLINE [ SU ], which indicates that the node is ready for the software upgrade. You can see that the status of the SRG1 has changed to INELIGIBLE.

3. Confirm that the other device (SRX-01) is in the active role and is functioning normally.

```
user@srx-01> show chassis high-availability informationNode failure codes:
```

```
HW Hardware monitoring  LB Loopback monitoring
MB Mbuf monitoring      SP SPU monitoring
CS Cold Sync monitoring  SU Software Upgrade
```

```
Node Status: ONLINE
```

```
Local-id: 2
```

```
Local-IP: 10.22.0.2
```

```
HA Peer Information:
```

```
Peer Id: 1      IP address: 10.22.0.1      Interface: ge-0/0/2.0
Routing Instance: default
Encrypted: YES   Conn State: UP
Cold Sync Status: COMPLETE
```

```
Services Redundancy Group: 0
```

```
Current State: ONLINE
```

```
Peer Information:
```

```
Peer Id: 1
```

```

SRG failure event codes:
  BF  BFD monitoring
  IP  IP monitoring
  IF  Interface monitoring
  CP  Control Plane monitoring

Services Redundancy Group: 1
  Deployment Type: ROUTING
  Status: ACTIVE
  Activeness Priority: 1
  Preemption: DISABLED
  Process Packet In Backup State: NO
  Control Plane State: READY
  System Integrity Check: N/A
  Failure Events: NONE
  Peer Information:
    Peer Id: 1
    Status : INELIGIBLE
    Health Status: UNHEALTHY
    Failover Readiness: NOT READY

```

The command output shows that the status of SRG1 is **ACTIVE**.

Also note that under the Peer Information section of the SRG1, the status is INELIGIBLE which indicates that the other node is in ineligible state.

4. Install the Junos OS software on the SRX-02 device.

```

user@srx-02> request system software add /var/tmp/junos-install-vsrx3-x86-64-22.3R1.3.tgz
no-copy

```

5. After a successful installation, reboot the device using the `request system reboot` command.
6. After the reboot, check the Junos OS version using the `show version` command.

```

user@srx-02> show version
Hostname: srx-02
Model: vSRX
Junos: 22.3R1.3

```

The output confirms that the device is upgraded to the correct Junos OS version.

## 7. Check status of the Multinode High Availability on the device.

```
user@srx-02> show chassis high-availability information
```

Node failure codes:

HW	Hardware monitoring	LB	Loopback monitoring
MB	Mbuf monitoring	SP	SPU monitoring
CS	Cold Sync monitoring	SU	Software Upgrade

Node Status: OFFLINE [ SU ]

Local-id: 1

Local-IP: 10.22.0.1

HA Peer Information:

Peer Id: 2	IP address: 10.22.0.2	Interface: ge-0/0/2.0
Routing Instance: default		
Encrypted: YES	Conn State: UP	
Cold Sync Status: COMPLETE		

Services Redundancy Group: 0

Current State: ONLINE

Peer Information:

Peer Id: 2

SRG failure event codes:

BF	BFD monitoring
IP	IP monitoring
IF	Interface monitoring
CP	Control Plane monitoring

Services Redundancy Group: 1

Deployment Type: ROUTING

Status: INELIGIBLE

Activeness Priority: 200

Preemption: ENABLED

Process Packet In Backup State: NO

Control Plane State: N/A

System Integrity Check: COMPLETE

Failure Events: NONE

Peer Information:

Peer Id: 2

Status : ACTIVE



```
Health Status: HEALTHY
Failover Readiness: N/A
```

The output continues to display the node status as OFFLINE [ SU ] and SRG1 status as INELIGIBLE.

8. Remove the software-upgrade statement and commit the configuration.

```
user@srx-02# delete chassis high-availability software-upgrade
```

When you remove software-upgrade statement, the local failure state and installed routes are removed.

9. Check the Multinode High Availability status again to confirm that the device is online and the overall status is healthy and functioning.

```
user@srx02> show chassis high-availability information
Node failure codes:
  HW  Hardware monitoring   LB  Loopback monitoring
  MB  Mbuf monitoring       SP  SPU monitoring
  CS  Cold Sync monitoring  SU  Software Upgrade

Node Status: ONLINE
Local-id: 1
Local-IP: 10.22.0.1
HA Peer Information:

  Peer Id: 2      IP address: 10.22.0.2      Interface: ge-0/0/2.0
  Routing Instance: default
  Encrypted: YES   Conn State: UP
  Cold Sync Status: COMPLETE

Services Redundancy Group: 0
  Current State: ONLINE
  Peer Information:
    Peer Id: 2

SRG failure event codes:
  BF  BFD monitoring
  IP  IP monitoring
  IF  Interface monitoring
  CP  Control Plane monitoring
```

```

Services Redundancy Group: 1
  Deployment Type: ROUTING
  Status: BACKUP
  Activeness Priority: 200
  Preemption: ENABLED
  Process Packet In Backup State: NO
  Control Plane State: READY
  System Integrity Check: IN PROGRESS
  Failure Events: NONE
  Peer Information:
    Peer Id: 2
    Status : ACTIVE
    Health Status: HEALTHY
    Failover Readiness: N/A

```

The output shows Node Status: ONLINE and SRG1 status as BACKUP, which indicates that the node is back online and is functioning normally in backup role.

10. Check interfaces, routing protocols, routes advertised and so on to confirm that your setup is operating normally.

Now you can proceed to upgrade the other device (SRX-01) using the same procedure.

**NOTE:** In case if you face any issues and are not able to complete the upgrade, you can roll back the software on the device, and then reboot the system. Use the `request system software rollback` command to restore the previously installed software version.

## Upgrade Software using shutdown-on-failure interface

### Prerequisite to Divert Transit Traffic

Check whether your SRX Series includes the configuration required to isolate traffic by shutting down interfaces as mentioned in ["Configuring Multinode High Availability In a Default Gateway Deployment" on page 717](#). if the feature is not configured:

1. Configure all traffic interfaces under the shutdown-on-failure option.

```

user@srx-02# set chassis high-availability services-redundancy-group 0 shutdown-on-failure
interface-name

```

Example:

```
[edit]
user@srx-02# set chassis high-availability services-redundancy-group 0 shutdown-on-failure
ge-0/0/0
user@srx-02# set chassis high-availability services-redundancy-group 0 shutdown-on-failure
ge-0/0/1
user@srx-02# set chassis high-availability services-redundancy-group 0 shutdown-on-failure
ge-0/0/3
user@srx-02# set chassis high-availability services-redundancy-group 0 shutdown-on-failure
ge-0/0/4
```



**CAUTION:** Donot use interfaces assigned for the interchassis link (ICL).

## Upgrade Multinode High Availability Software

Let's upgrade the device that is acting as backup node (SRX-02).

1. Initiate the software upgrade and commit the configuration.

```
user@srx-02# set chassis high-availability software-upgrade
```

This command marks interfaces offline and transitions status to ineligible state.

2. Check the Multinode High Availability status.

```
user@srx-02> show chassis high-availability information
Node failure codes:
  HW  Hardware monitoring   LB  Loopback monitoring
  MB  Mbuf monitoring       SP  SPU monitoring
  CS  Cold Sync monitoring  SU  Software Upgrade

Node Status: OFFLINE [ SU ]
Local-id: 2
Local-IP: 10.22.0.2
HA Peer Information:

  Peer Id: 1      IP address: 10.22.0.1      Interface: ge-0/0/2.0
  Routing Instance: default
```

```

Encrypted: YES    Conn State: UP
Cold Sync Status: COMPLETE

```

```

Services Redundancy Group: 0
    Current State: ISOLATED [ Node Failure ]
    Peer Information:
        Peer Id: 1

    Shut-on-failures interfaces:
        ge-0/0/4

        ge-0/0/3

        ge-0/0/1

        ge-0/0/0

```

```

SRG failure event codes:
    BF  BFD monitoring
    IP  IP monitoring
    IF  Interface monitoring
    CP  Control Plane monitoring

```

```

Services Redundancy Group: 1
    Deployment Type: ROUTING
    Status: INELIGIBLE
    Activeness Priority: 1
    Preemption: DISABLED
    Process Packet In Backup State: NO
    Control Plane State: N/A
    System Integrity Check: COMPLETE
    Failure Events: NONE
    Peer Information:
        Peer Id: 1
        Status : ACTIVE
        Health Status: HEALTHY
        Failover Readiness: N/A

```

The output shows Node Status: OFFLINE [ SU ], which indicates that the node is ready for the software upgrade. You can also see SRG0 status as ISOLATED [ Node Failure ] and SRG1 status as INELIGIBLE.

3. Check the status of the interfaces.

```
user@host> show interfaces terse
```

Interface	Admin	Link	Proto	Local	Remote
ge-0/0/0	down	down			
ge-0/0/1	down	down			
ge-0/0/2	up	up			
ge-0/0/2.0	up	up	inet	10.22.0.2/24	
ge-0/0/3	down	down			
ge-0/0/3.0	up	down	inet	10.3.0.2/16	
ge-0/0/4	down	down			
ge-0/0/4.0	up	down	inet	10.5.0.1/16	

The output shows that interfaces marked for shutdown-on-failure are down.

4. Confirm that the other device (SRX-01) is in the active role and is functioning normally.

```
user@srx-01> show chassis high-availability information
```

Node failure codes:

```

Node failure codes:
  HW  Hardware monitoring   LB  Loopback monitoring
  MB  Mbuf monitoring       SP  SPU monitoring
  CS  Cold Sync monitoring  SU  Software Upgrade

```

Node Status: ONLINE

Local-id: 1

Local-IP: 10.22.0.1

HA Peer Information:

```

Peer Id: 2      IP address: 10.22.0.2      Interface: ge-0/0/2.0
Routing Instance: default
Encrypted: YES   Conn State: UP
Cold Sync Status: COMPLETE

```

Services Redundancy Group: 0

```

Current State: ONLINE
Peer Information:
Peer Id: 2

```

SRG failure event codes:

```

BF  BFD monitoring
IP  IP monitoring

```

```
IF Interface monitoring
CP Control Plane monitoring
```

```
Services Redundancy Group: 1
  Deployment Type: ROUTING
  Status: ACTIVE
  Activeness Priority: 200
  Preemption: ENABLED
  Process Packet In Backup State: NO
  Control Plane State: READY
  System Integrity Check: N/A
  Failure Events: NONE
  Peer Information:
    Peer Id: 2
    Status : INELIGIBLE
    Health Status: UNHEALTHY
    Failover Readiness: NOT READY
```

The output shows that the status of SRG1 is ACTIVE.

Also note that under the Peer Information section of the SRG1, the status is INELIGIBLE which indicates that the other node is in ineligible state.

5. Install the Junos OS image on SRX-02.

```
user@srx-02> request system software add /var/tmp/junos-install-vsrx3-x86-64-22.3R1.3.tgz
no-copy
```

6. After the successful upgrade, reboot the device using the `request system reboot` command.
7. Check the Junos OS version.

```
user@srx-02> show version
Hostname: srx-02
Model: vSRX
Junos: 22.3R1.3
```

The output confirms that the device is upgraded to the correct Junos OS version.

## 8. Check the status of Multinode High Availability on the device.

```
user@srx-02> show chassis high-availability information
```

Node failure codes:

HW	Hardware monitoring	LB	Loopback monitoring
MB	Mbuf monitoring	SP	SPU monitoring
CS	Cold Sync monitoring	SU	Software Upgrade

Node Status: OFFLINE [ SU ]

Local-id: 2

Local-IP: 10.22.0.2

HA Peer Information:

Peer Id: 1	IP address: 10.22.0.1	Interface: ge-0/0/2.0
Routing Instance: default		
Encrypted: YES	Conn State: UP	
Cold Sync Status: COMPLETE		

Services Redundancy Group: 0

Current State: ISOLATED [ Node Failure ]

Peer Information:

Peer Id: 1

Shut-on-failures interfaces:

ge-0/0/4

ge-0/0/3

ge-0/0/1

ge-0/0/0

SRG failure event codes:

BF	BFD monitoring
IP	IP monitoring
IF	Interface monitoring
CP	Control Plane monitoring

Services Redundancy Group: 1

Deployment Type: ROUTING

Status: INELIGIBLE

```

Activeness Priority: 1
Preemption: DISABLED
Process Packet In Backup State: NO
Control Plane State: N/A
System Integrity Check: COMPLETE
Failure Events: NONE
Peer Information:
  Peer Id: 1
  Status : ACTIVE
  Health Status: HEALTHY
  Failover Readiness: N/A

```

The command output continues to display the node status as OFFLINE [ SU ] and SRG0 status as ISOLATED [ Node Failure ].

9. Remove the software-upgrade statement and commit the configuration.

```
user@srx-02# delete chassis high-availability software-upgrade
```

10. Check the Multinode High Availability status again on the device and confirm that the device is online and that the overall status is healthy.

```

user@srx-02> show chassis high-availability information
Node failure codes:
  HW Hardware monitoring   LB Loopback monitoring
  MB Mbuf monitoring       SP SPU monitoring
  CS Cold Sync monitoring  SU Software Upgrade

Node Status: ONLINE
Local-id: 2
Local-IP: 10.22.0.2
HA Peer Information:

  Peer Id: 1      IP address: 10.22.0.1    Interface: ge-0/0/2.0
  Routing Instance: default
  Encrypted: YES   Conn State: UP
  Cold Sync Status: COMPLETE

Services Redundancy Group: 0
  Current State: ONLINE
  Peer Information:

```



```

Peer Id: 1

Shut-on-failures interfaces:
ge-0/0/4

ge-0/0/3

ge-0/0/1

ge-0/0/0

SRG failure event codes:
BF  BFD monitoring
IP  IP monitoring
IF  Interface monitoring
CP  Control Plane monitoring

Services Redundancy Group: 1
Deployment Type: ROUTING
Status: BACKUP
Activeness Priority: 1
Preemption: DISABLED
Process Packet In Backup State: NO
Control Plane State: READY
System Integrity Check: COMPLETE
Failure Events: NONE
Peer Information:
Peer Id: 1
Status : ACTIVE
Health Status: HEALTHY
Failover Readiness: N/A

```

The output shows Node Status: ONLINE, and SRGO ONLINE, which indicates that the node is back online and is functioning normally.

#### 11. Verify the status of interfaces.

```

user@srx-02> show interfaces terse

```

Interface	Admin	Link	Proto	Local	Remote
ge-0/0/0	up	up			
gr-0/0/0	up	up			
ge-0/0/1	up	up			

ge-0/0/2	up	up		
ge-0/0/2.0	up	up	inet	10.22.0.2/24
ge-0/0/3	up	up		
ge-0/0/3.0	up	up	inet	10.3.0.2/16
ge-0/0/4	up	up		
ge-0/0/4.0	up	up	inet	10.5.0.1/16
.....				

The output shows that interfaces that were previously down are up now.

12. Check interfaces, routing protocols, routes advertised, and so on to confirm that your setup is operating normally.

Now you can proceed to upgrade the other device (SRX-01) using the same procedure.

RELATED DOCUMENTATION

<a href="#">Multinode High Availability   613</a>
<a href="#">Prepare Your Environment for Multinode High Availability Deployment   654</a>
<a href="#">Insert Additional SRX5K-SPC3 in a Multinode High Availability Setup   904</a>
<a href="#">Example: Configure Multinode High Availability in a Default Gateway Deployment   717</a>
<a href="#">Example: Configure Multinode High Availability in a Layer 3 Network   672</a>
<a href="#">Example: Configure Multinode High Availability in a Hybrid Deployment   752</a>

Insert Additional SRX5K-SPC3 in a Multinode High Availability Setup

IN THIS SECTION

- [Insert SRX5K-SPC3 in a Multinode High Availability Setup | 905](#)

## Insert SRX5K-SPC3 in a Multinode High Availability Setup

Starting in Junos OS Release 22.2R1, you can insert additional Service Processing Cards (SPC3) cards in a SRX5000-Line devices in Multinode High Availability setup without interrupting the existing traffic flow or without incurring downtime on your network.

We strongly recommend that you install the additional SPC3 card during a maintenance window, or during times of low-traffic as the backup node is not available for some time.

### Requirements

Note the following requirements before you install additional SPC3 cards in a SRX5000-line device in a Multinode High Availability setup:

- Each security device must have at least one SPC3 card installed.
- When you are inserting a new SPC3 card, you must install it in a slot that has a higher number than the slots in which other SPCs are already installed. For example, if both nodes have an SPC3 card on slot 2, then you must insert the new SPC3 card in slot 3 or in a higher-numbered slot. You must not install the card in slot 0 or slot 1.
- Use the following table to know whether you can insert an additional SPC3 card on an SRX5000 chassis without interrupting the traffic based on the count of already installed SPC3 cards.

Existing Count of SPC3 Cards	Count After Inserting Additional SPC3 Cards	Installation Without Traffic Interruption
1	2	Yes
1	3 or more	No
2	3 or more	No
3 or more	4 or more	Yes

### Install Additional SPC3 Cards

Consider a Multinode High Availability setup with two SRX5000 line devices. You've two nodes—node 1 acting as the active node and node 2 as the backup node. You want to install SPC3 cards on both the nodes.

Familiarize yourself with the SPC3 installation procedure for your security device. See [Installing an SRX5400 Services Gateway SPC](#), or [Installing an SRX5600 Services Gateway SPC](#), or [Installing an SRX5800 Services Gateway SPC](#).

The following procedures guide you how to install an additional SPC3 card in a Multinode High Availability system.

#### Case 1: Nonencrypted ICL

1. Power off node 2 (backup node) using the `request system power off` command from operational mode.
2. Insert an SPC3 card or cards on node 2.
3. Boot up node 2.
4. Run the `show chassis high-availability information` command. If the device displays an error with the SPU Slot Mismatch message, you must halt the installation procedure and redo the procedure. If there are no error messages, continue with the next step.
5. When node 2 is back online and ready to failover on all SRGs, initiate a failover for all traffic and SRGs to node 2. You can use the `request chassis high-availability failover services-redundancy-group` command from the operational mode. When you run the command, the node 2 transitions to the active role.
6. Power off node 1.
7. Insert an SPC3 card or cards on node 1.
8. Boot up node 1 after you complete the installation.

#### Case-2: Encrypted ICL

1. Configure the `set chassis high-availability hardware-upgrade` statement and commit the configuration on both nodes.
2. Power off node 2 (backup node) using the `request system power off` command from operational mode.
3. Insert an SPC3 card or cards on node 2.
4. Run the `show chassis high-availability information` command. If the device displays an error with the SPU Slot Mismatch message, you must halt the upgrade procedure to not cause any disruption to the traffic. If there are no error messages, continue with the next step.
5. Boot up node 2.
6. When node 2 is back online and ready to fail over on all SRGs, initiate a failover for all traffic and SRGs to node 2 using the `request chassis high-availability failover services-redundancy-group` command from the operational mode. When you run the command, the node 2 transitions to the active role.
7. Power off node 1.
8. Insert an SPC3 card or cards on node 1.

9. Boot up node 1 after you complete the installation.
10. After node 1 is back online, configure the `delete chassis high-availability hardware-upgrade statement` on both the nodes and commit the configuration.

## How to Address SPC3 Slot Mismatch

If you face any issues while installing an additional SPC3 card, use the following steps to address the issue:

1. Run the `show chassis high-availability information` command.

If the device displays an error with the `Peer Hardware Incompatible: SPU Slot Mismatch` message, you must halt the upgrade procedure to not cause any disruption to the traffic.

2. Run the `show chassis fpc pic-status` command to check mismatched chassis slots between the two nodes.
3. Remove the wrongly placed card, and reinsert it into a correct slot, and perform the upgrade procedure once again.

## SEE ALSO

---

[Multinode High Availability | 613](#)

---

[Prepare Your Environment for Multinode High Availability Deployment | 654](#)

---

[Software Upgrade in Multinode High Availability | 885](#)

---

[Example: Configure Multinode High Availability in a Default Gateway Deployment | 717](#)

---

[Example: Configure Multinode High Availability in a Layer 3 Network | 672](#)

---

[Example: Configure Multinode High Availability in a Hybrid Deployment | 752](#)

# Multinode High Availability Support for vSRX

## IN THIS CHAPTER

- [Multinode High Availability Support for vSRX Instances in Public Cloud Deployments | 908](#)

## Multinode High Availability Support for vSRX Instances in Public Cloud Deployments

### SUMMARY

Read this topic to understand Multinode High Availability support for vSRX instances in Amazon Web Services (AWS) deployments.

### IN THIS SECTION

- [Overview | 908](#)
- [Multinode High Availability in AWS | 909](#)
- [Example: Configure Multinode High Availability in AWS Deployment | 912](#)

## Overview

Multinode High Availability addresses high availability requirements for private and public cloud deployments by offering interchassis resiliency.

Starting in Junos OS Release 22.3R1, we support Multinode High Availability on Juniper Networks vSRX Virtual Firewalls for the private (Kernel-based virtual machine [KVM] and VMware ESXi) and public cloud (AWS) deployments.

## Multinode High Availability in AWS

IN THIS SECTION

- Terminology | 909
- Architecture | 910

You can configure Multinode High Availability on the vSRX firewalls deployed on AWS. Participating nodes run both active control and data planes at the same time and the nodes backup each other to ensure a fast synchronized failover in case of system or hardware failure. The interchassis link (ICL) connection between the two devices synchronizes and maintains the state information and handles device failover scenarios.

Let's begin by getting familiar with the Multinode High Availability terms specific to the AWS deployment.

Terminology

Term	Description
Elastic IP address	Public IPv4 address that is routable from a specified network or from the Internet. Elastic IP addresses are dynamically bound to an interface of any node in a Multinode High Availability setup. At any given time, these addresses are bound to only one interface and are also bound to the same node. The Multinode High Availability setup uses Elastic IP addresses to control the traffic in AWS deployments. Elastic IP address acts similar to floating IP address in the Layer 3 deployment or a virtual IP address as in the default gateway deployment. The node with an active SRG1 owns the Elastic IP address and draws the traffic toward it.

*(Continued)*

Term	Description
Interchassis link (ICL)	IP-based link (logical link) that connects nodes over a routed network in a Multinode High Availability system. The security device uses the ICL to synchronize and maintain the state information and to handle device failover scenarios. You can use only the ge-0/0/0 interface to configure an ICL. The ICL uses the MAC address assigned by AWS (not the virtual MAC created by vSRX). When you configure the ICL, ensure that the IP address is a subnet of of the virtual private cloud (VPC). Note that Multibode High Availability does not support cross-VPC deployment
Juniper Services Redundancy Protocol (jsrpd) process	Process that manages activeness determination and enforcement, and provide split-brain protection.

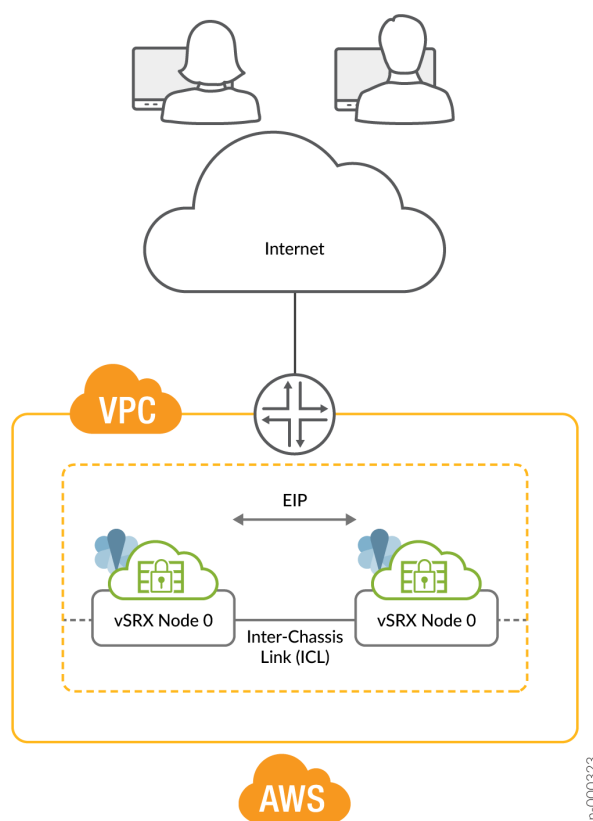
We don't support IPsec VPN for Multinode High Availability in AWS deployments.

**Architecture**

Figure 60 on page 911 shows two vSRX instances form an HA pair in the Multinode High Availability deployment in AWS. One vSRX instance acts as the active node and the other as the backup node.



Figure 60: Public Cloud Deployment



In a Multinode High Availability setup, an ICL connects the two nodes (vSRX instances) and helps synchronize the control-plane and data-plane states.

In Multinode High Availability setup, two vSRX instances are operating in active/backup mode. Both nodes connect to each other using an ICL for synchronizing control and data plane states. The vSRX instance on which the SRG1 is active hosts the Elastic IP address. The active node steers traffic toward it using the Elastic IP address. The backup node remains in standby mode and takes over on failover.

The Juniper Services Redundancy Protocol (jsrpd) process communicates with the AWS infrastructure to perform activeness determination and enforcement and provides split-brain protection.

During a failover, the Elastic IP address moves from the old active node to the new active node by triggering the AWS SDK API and draws traffic toward the new active node. AWS updates the route tables to divert the traffic to the new active node. This mechanism enables clients to communicate with the nodes using a single IP address. You configure the Elastic IP address on the interface that connects to participating networks/segments.

### Split-Brain Protection

When the ICL between two nodes goes down, each node starts pinging to the peer node's interface IP address using the probes. If the peer node is healthy, it responds to the probes. Otherwise, the jsrpd process communicates with the AWS infrastructure to enforce the active role for the healthy node.

## Example: Configure Multinode High Availability in AWS Deployment

### IN THIS SECTION

- [Requirements | 912](#)
- [Topology | 912](#)
- [Configuration | 915](#)
- [Results | 919](#)
- [Verification | 926](#)

In this example, we'll show you how to configure Multinode High Availability on two vSRX instances in the Amazon Virtual Private Cloud (Amazon VPC).

### Requirements

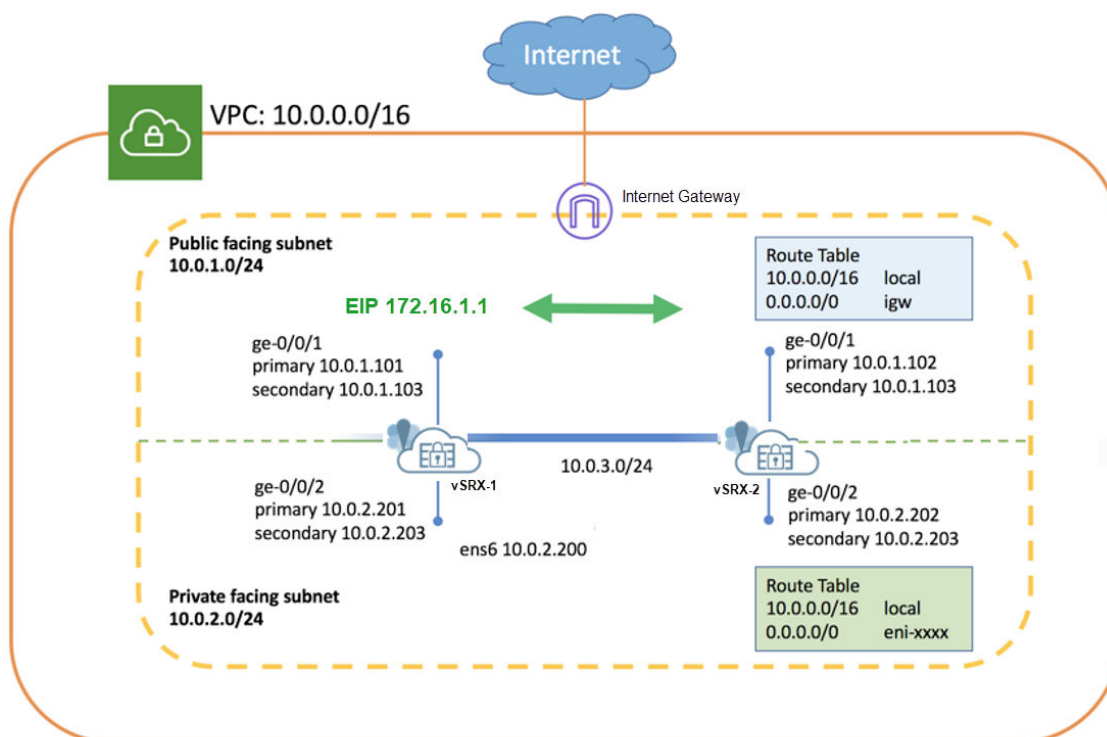
This example uses the following components:

- Two vSRX instances
- Junos OS Release 22.3R1
- An Amazon Web Services (AWS) account and an identity and access management (IAM) role, with all required permissions to access, create, modify, and delete Amazon Elastic Compute Cloud (Amazon EC2), Amazon Simple Storage Service (S3), and Amazon Virtual Private Cloud (Amazon VPC) objects. See [Configure an Amazon Virtual Private Cloud for vSRX](#) for details.
- An Amazon VPC configured with its associated Internet gateway, subnets, route table, and security groups. See [Configure an Amazon Virtual Private Cloud for vSRX](#).
- A vSRX instance launched and configured in Amazon VPC. See [Launch a vSRX Instance on an Amazon Virtual Private Cloud](#).

### Topology

[Figure 61 on page 913](#) shows the topology used in this example.

Figure 61: Multinode High Availability in AWS Deployment



As shown in the topology, two vSRX instances (vSRX-1 and vSRX-2) are deployed in the Amazon VPC. The nodes communicate with each other using a routable IP address (Elastic IP address). The untrust side connects to a public network while the trust side connects to the protected resources.

Complete the following configurations before configuring Multinode High Availability on the vSRX instances:

- Use instance tag in AWS to identify the two vSRX instances as Multinode High Availability peers. For example, you can use **vsrx-node-1** as the name of one peer (**Name** option) and **vsrx-node-2** as the HA peer (**ha-peer** option).
- Deploy both vSRX instances in the same Amazon VPC and availability zone.
- Assign IAM role for both the vSRX instances and launch vSRX instances as a Amazon Elastic Compute Cloud (EC2) instance with full permissions.
- Enable communication to the Internet by placing vSRX instances in the public subnet. In the Amazon VPC, public subnets have access to the Internet gateway.
- Configure a VPC with multiple subnets to host the high availability pair. The subnets are used to connect the two vSRX nodes using a logical connection (similar to the physical cable connecting ports). In this example, we have defined CIDR for VPC as 10.0.0.0/16, and created a total of four

subnets to host the vSRX traffic. You need a minimum of four interfaces for both vSRX instances. [Table 48 on page 914](#) provides the subnet and interface details.

**Table 48: Subnets Configurations**

Function	Port Number	Interface	Connection	Traffic Type	Subnet
Management	0	fxp0	Management interface	Management traffic	10.0.254.0/24
ICL	1	ge-0/0/0	ICL to peer node	RTO, sync, and probes-related traffic	10.0.253.0/24
Public	2	ge-0/0/1	Connect to public network. (Revenue interface)	External traffic	10.0.1.0/24
Private	3	ge-0/0/2	Connect to private network. (Revenue interface)	Internal traffic	10.0.2.0/24

Note that the interface mapping with functionality mentioned in the table is for default configuration. We recommend to use the same mapping in the configuration.

- Configure interfaces with primary and secondary IP addresses. You can assign Elastic IP address as secondary IP addresses for an interface. You need the primary IP address while launching the instance. The secondary IP address is transferable from one vSRX node to another during a failover. [Table 49 on page 914](#) shows interface and IP address mappings used in this example.

**Table 49: Interface and IP Address Mappings**

Instance	Interface	Primary IP Address	Secondary IP Address (Elastic IP Address)
vSRX-1	ge-0/0/1	10.0.1.101	10.0.1.103
	ge-0/0/2	10.0.2.201	10.0.2.203
vSRX-2	ge-0/0/1	10.0.1.102	10.0.1.103

Table 49: Interface and IP Address Mappings *(Continued)*

Instance	Interface	Primary IP Address	Secondary IP Address (Elastic IP Address)
	ge-0/0/2	10.0.2.202	10.0.2.203

- Configure neighboring routers to include vSRX in the data path and mark vSRX as the next hop for the traffic. You can use an Elastic IP address to configure the route. For example, use the command `sudo ip route x.x.x.x/x dev ens6 via 10.0.2.203`, where the 10.0.2.203 address is an Elastic IP address.

## Configuration

### CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the [edit] hierarchy level, and then enter `commit` from configuration mode.

These configurations are captured from a lab environment, and are provided for reference only. Actual configurations may vary based on the specific requirements of your environment.

#### On vSRX-1

```

set chassis high-availability local-id 1
set chassis high-availability local-id local-ip 10.0.3.10
set chassis high-availability peer-id 2 peer-ip 10.0.3.11
set chassis high-availability peer-id 2 interface ge-0/0/0.0
set chassis high-availability peer-id 2 liveness-detection minimum-interval 400
set chassis high-availability peer-id 2 liveness-detection multiplier 5
set chassis high-availability services-redundancy-group 1 deployment-type cloud
set chassis high-availability services-redundancy-group 1 peer-id 2
set chassis high-availability services-redundancy-group 1 preemption
set chassis high-availability services-redundancy-group 1 activeness-priority 200
set security policies default-policy permit-all
set security zones security-zone fab host-inbound-traffic system-services all
set security zones security-zone fab host-inbound-traffic protocols all
set security zones security-zone fab interfaces ge-0/0/0.0
set security zones security-zone untrust host-inbound-traffic system-services all
set security zones security-zone untrust host-inbound-traffic protocols all
set security zones security-zone untrust interfaces ge-0/0/1.0
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 ge-0/0/2.0
set security cloud high-availability aws eip-based
set security cloud high-availability aws peer-liveliness probe-ip 10.0.1.102
set security cloud high-availability aws peer-liveliness probe-ip routing-instance s1-router
set interfaces ge-0/0/0 mtu 9192
set interfaces ge-0/0/0 unit 0 family inet address 10.0.3.10/24
set interfaces ge-0/0/1 mtu 9192
set interfaces ge-0/0/1 unit 0 family inet address 10.0.1.101/24 primary
set interfaces ge-0/0/1 unit 0 family inet address 10.0.1.103/24
set interfaces ge-0/0/2 mtu 9192
set interfaces ge-0/0/2 unit 0 family inet address 10.0.2.201/24 primary
set interfaces ge-0/0/2 unit 0 family inet address 10.0.2.203/24
set routing-instances s1-router instance-type virtual-router
set routing-instances s1-router routing-options static route 0.0.0.0/0 next-hop 10.0.1.1
set routing-instances s1-router interface ge-0/0/1.0
set routing-instances s1-router interface ge-0/0/2.0

```

## On vSRX-2

```

set chassis high-availability local-id 2
set chassis high-availability local-id local-ip 10.0.3.11
set chassis high-availability peer-id 1 peer-ip 10.0.3.10
set chassis high-availability peer-id 1 interface ge-0/0/0.0
set chassis high-availability peer-id 1 liveness-detection minimum-interval 400
set chassis high-availability peer-id 1 liveness-detection multiplier 5
set chassis high-availability services-redundancy-group 1 deployment-type cloud
set chassis high-availability services-redundancy-group 1 peer-id 1
set chassis high-availability services-redundancy-group 1 preemption
set chassis high-availability services-redundancy-group 1 activeness-priority 100
set security policies default-policy permit-all
set security zones security-zone fab host-inbound-traffic system-services all
set security zones security-zone fab host-inbound-traffic protocols all
set security zones security-zone fab interfaces ge-0/0/0.0
set security zones security-zone untrust host-inbound-traffic system-services all
set security zones security-zone untrust host-inbound-traffic protocols all
set security zones security-zone untrust interfaces ge-0/0/1.0
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 ge-0/0/2.0
set security cloud high-availability aws eip-based
set security cloud high-availability aws peer-liveliness probe-ip 10.0.1.101

```

```

set security cloud high-availability aws peer-liveliness probe-ip routing-instance s1-router
set interfaces ge-0/0/0 mtu 9192
set interfaces ge-0/0/0 unit 0 family inet address 10.0.3.11/24
set interfaces ge-0/0/1 mtu 9192
set interfaces ge-0/0/1 unit 0 family inet address 10.0.1.102/24 primary
set interfaces ge-0/0/1 unit 0 family inet address 10.0.1.103/24
set interfaces ge-0/0/2 mtu 9192
set interfaces ge-0/0/2 unit 0 family inet address 10.0.2.202/24 primary
set interfaces ge-0/0/2 unit 0 family inet address 10.0.2.203/24
set routing-instances s1-router instance-type virtual-router
set routing-instances s1-router routing-options static route 0.0.0.0/0 next-hop 10.0.1.1
set routing-instances s1-router interface ge-0/0/1.0
set routing-instances s1-router interface ge-0/0/2.0

```

## Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see [Using the CLI Editor in Configuration Mode](#) in the [CLI User Guide](#).

### 1. Configure ge-0/0/0 as the interface for the ICL

```

[edit]
user@host# set interfaces ge-0/0/0 mtu 9192
user@host# set interfaces ge-0/0/0 unit 0 family inet address 10.0.3.11/24

```

### 2. Configure interfaces for internal and external traffic.

```

[edit]
user@host# set interfaces ge-0/0/1 mtu 9192
user@host# set interfaces ge-0/0/1 unit 0 family inet address 10.0.1.102/24 primary
user@host# set interfaces ge-0/0/1 unit 0 family inet address 10.0.1.103/24
user@host# set interfaces ge-0/0/2 mtu 9192
user@host# set interfaces ge-0/0/2 unit 0 family inet address 10.0.2.202/24 primary
user@host# set interfaces ge-0/0/2 unit 0 family inet address 10.0.2.203/24

```

We'll use the secondary IP address assigned to ge-0/0/1 and ge-0/0/2 as Elastic IP address.

3. Configure security zones, assign interfaces to the zones, and specify allowed system services for the security zones .

```
[edit]
user@host# set security zones security-zone fab host-inbound-traffic system-services all
user@host# set security zones security-zone fab host-inbound-traffic protocols all
user@host# set security zones security-zone fab interfaces ge-0/0/0.0
user@host# set security zones security-zone untrust host-inbound-traffic system-services all
user@host# set security zones security-zone untrust host-inbound-traffic protocols all
user@host# set security zones security-zone untrust interfaces ge-0/0/1.0
user@host# set security zones security-zone trust host-inbound-traffic system-services all
user@host# set security zones security-zone trust host-inbound-traffic protocols all
user@host# set security zones security-zone trust interfaces ge-0/0/2.0
```

4. Configure routing options.

```
[edit]
user@host# set routing-instances s1-router instance-type virtual-router
user@host# set routing-instances s1-router routing-options static route 0.0.0.0/0 next-hop
10.0.1.1
user@host# set routing-instances s1-router interface ge-0/0/1.0
user@host# set routing-instances s1-router interface ge-0/0/2.0
```

Here, you'll require a separate routing instance type virtual router to separate management traffic and revenue traffic.

5. Configure local node and peer node details.

```
[edit]
user@host# set chassis high-availability local-id 1
user@host# set chassis high-availability local-id local-ip 10.0.3.10
user@host# set chassis high-availability peer-id 2 peer-ip 10.0.3.11
```

6. Associate the interface to the peer node for interface monitoring, and configure the liveness detection details.

```
[edit]
user@host# set chassis high-availability peer-id 2 interface ge-0/0/0.0
```



```
user@host# set chassis high-availability peer-id 2 liveness-detection minimum-interval 400
user@host# set chassis high-availability peer-id 2 liveness-detection multiplier 5
```

7. Configure SRG1 with deployment type as cloud, assign an ID, and set preemption and activeness priority.

```
[edit]
user@host# set chassis high-availability services-redundancy-group 1 deployment-type cloud
user@host# set chassis high-availability services-redundancy-group 1 peer-id 2
user@host# set chassis high-availability services-redundancy-group 1 preemption
user@host# set chassis high-availability services-redundancy-group 1 activeness-priority 200
```

8. Configure AWS deployment-related options. For example, specify eip-based as the service type and also, configure monitoring options such as AWS peer liveness.

```
[edit]
user@host# set security cloud high-availability aws eip-based
user@host# set security cloud high-availability aws peer-liveliness probe-ip 10.0.1.101
user@host# set security cloud high-availability aws peer-liveliness probe-ip routing-instance
s1-router
```

**NOTE:** In Multinode High Availability for vSRX instances in VMWare ESXi environment with VMXNET3 vNIC, configuration of virtual MAC address is not supported in the following statement:

```
[set chassis high-availability services-redundancy-group <number> virtual-ip <id> use-virtual-
mac
```

## Results

### vSRX-1

From configuration mode, confirm your configuration by entering the following commands.

If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show chassis high-availability
local-id 1 local-ip 10.0.3.10;
peer-id 2 {
    peer-ip 10.0.3.11;
    interface ge-0/0/0.0;
    liveness-detection {
        minimum-interval 400;
        multiplier 5;
    }
}
services-redundancy-group 1 {
    deployment-type cloud;
    peer-id {
        2;
    }
    preemption;
    activeness-priority 200;
}
```

```
[edit]
user@host# show routing-instances
s1-router {
    instance-type virtual-router;
    routing-options {
        static {
            route 0.0.0.0/0 next-hop 10.0.1.1;
        }
    }
    interface ge-0/0/1.0;
    interface ge-0/0/2.0;
}
```

```
[edit]
user@host# show security zones security-zone
security-zone fab {
```

```
host-inbound-traffic {
    system-services {
        all;
    }
    protocols {
        all;
    }
}
interfaces {
    ge-0/0/0.0;
}
}
security-zone untrust {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            all;
        }
    }
    interfaces {
        ge-0/0/1.0;
    }
}
security-zone trust {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            all;
        }
    }
    interfaces {
        ge-0/0/2.0;
    }
}
}
```

```

[edit]
user@host# show interfaces
ge-0/0/0 {
    mtu 9192;
    unit 0 {
        family inet {
            address 10.0.3.10/24;
        }
    }
}
ge-0/0/1 {
    mtu 9192;
    unit 0 {
        family inet {
            address 10.0.1.101/24 {
                primary;
            }
            address 10.0.1.103/24;
        }
    }
}
ge-0/0/2 {
    mtu 9192;
    unit 0 {
        family inet {
            address 10.0.2.201/24 {
                primary;
            }
            address 10.0.2.203/24;
        }
    }
}

```

If you are done configuring the device, enter `commit` from configuration mode.

## vSRX-2

From configuration mode, confirm your configuration by entering the following commands.

If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show chassis high-availability
local-id 2 local-ip 10.0.3.11;
peer-id 1 {
    peer-ip 10.0.3.10;
    interface ge-0/0/0.0;
    liveness-detection {
        minimum-interval 400;
        multiplier 5;
    }
}
services-redundancy-group 1 {
    deployment-type cloud;
    peer-id {
        1;
    }
    preemption;
    activeness-priority 100;
}
```

```
[edit]
user@host# show routing-instances
s1-router {
    instance-type virtual-router;
    routing-options {
        static {
            route 0.0.0.0/0 next-hop 10.0.1.1;
        }
    }
    interface ge-0/0/1.0;
    interface ge-0/0/2.0;
}
```

```
[edit]
user@host# show security zones
security-zone fab {
  host-inbound-traffic {
    system-services {
      all;
    }
    protocols {
      all;
    }
  }
  interfaces {
    ge-0/0/0.0;
  }
}
security-zone untrust {
  host-inbound-traffic {
    system-services {
      all;
    }
    protocols {
      all;
    }
  }
  interfaces {
    ge-0/0/1.0;
  }
}
security-zone trust {
  host-inbound-traffic {
    system-services {
      all;
    }
    protocols {
      all;
    }
  }
  interfaces {
```

```

        ge-0/0/2.0;
    }
}

```

```

[edit]
user@host# show interfaces
ge-0/0/0 {
    mtu 9192;
    unit 0 {
        family inet {
            address 10.0.3.11/24;
        }
    }
}
ge-0/0/1 {
    mtu 9192;
    unit 0 {
        family inet {
            address 10.0.1.102/24 {
                primary;
            }
            address 10.0.1.103/24;
        }
    }
}
ge-0/0/2 {
    mtu 9192;
    unit 0 {
        family inet {
            address 10.0.2.202/24 {
                primary;
            }
            address 10.0.2.203/24;
        }
    }
}

```

If you are done configuring the device, enter `commit` from configuration mode.

## Verification

### Check Multinode High Availability Details

#### Purpose

View and verify the details of the Multinode High Availability setup configured on your vSRX instance.

#### Action

From operational mode, run the following command:

vSRX-1

```
user@host> show chassis high-availability information
Node failure codes:
  HW  Hardware monitoring   LB  Loopback monitoring
  MB  Mbuf monitoring       SP  SPU monitoring
  CS  Cold Sync monitoring  SU  Software Upgrade

Node Status: ONLINE
Local-id: 1
Local-IP: 10.0.3.10
HA Peer Information:

  Peer Id: 2      IP address: 10.0.3.11    Interface: ge-0/0/0.0
  Routing Instance: default
  Encrypted: NO   Conn State: UP
  Cold Sync Status: COMPLETE

SRG failure event codes:
  BF  BFD monitoring
  IP  IP monitoring
  IF  Interface monitoring
  CP  Control Plane monitoring

Services Redundancy Group: 1
  Deployment Type: CLOUD
  Status: ACTIVE
  Activeness Priority: 200
  Preemption: ENABLED
  Process Packet In Backup State: NO
  Control Plane State: READY
```



```

System Integrity Check: N/A
Failure Events: NONE
Peer Information:
  Peer Id: 2
  Status : BACKUP
  Health Status: HEALTHY
  Failover Readiness: NOT READY

```

## vSRX-2

```

user@host> show chassis high-availability information
Node failure codes:
  HW  Hardware monitoring    LB  Loopback monitoring
  MB  Mbuf monitoring        SP  SPU monitoring
  CS  Cold Sync monitoring    SU  Software Upgrade

Node Status: ONLINE
Local-id: 2
Local-IP: 10.0.3.11
HA Peer Information:

  Peer Id: 1      IP address: 10.0.3.10    Interface: ge-0/0/0.0
  Routing Instance: default
  Encrypted: NO   Conn State: UP
  Cold Sync Status: COMPLETE

SRG failure event codes:
  BF  BFD monitoring
  IP  IP monitoring
  IF  Interface monitoring
  CP  Control Plane monitoring

Services Redundancy Group: 1
  Deployment Type: CLOUD
  Status: BACKUP
  Activeness Priority: 100
  Preemption: ENABLED
  Process Packet In Backup State: NO
  Control Plane State: NOT READY
  System Integrity Check: COMPLETE
  Failure Events: NONE
  Peer Information:

```

```

Peer Id: 1
Status : ACTIVE
Health Status: HEALTHY
Failover Readiness: N/A

```

### Meaning

Verify these details from the command output:

- Local node and peer node details such as IP address and ID.
- The field `Deployment Type: CLOUD` indicates that configuration is for the cloud deployment.
- The field `Services Redundancy Group: 1` indicates the status of the SRG1 (ACTIVE or BACKUP) on that node.

## Check Multinode High Availability Information on AWS

### Purpose

Check whether Multinode High Availability is deployed in AWS cloud.

### Action

From operational mode, run the following command:

```

user@host> show security cloud high-availability information
Cloud HA Information:

Cloud Type      Cloud Service Type  Cloud Service Status
AWS             EIP                 Bind to Local Node

```

### Meaning

Verify these details from the command output:

- The field `Cloud Type: AWS` indicates the deployment is for AWS.
- The field `Cloud Service Type: EIP` indicates that the the AWS deployment uses the EIP service type (for Elastic IP address) to control traffic.
- The field `Cloud Service Status: Bind to Local Node` indicates the binding of the Elastic IP address to the local node. For the backup node, this field displays `Bind to Peer Node`.

## Check Multinode High Availability Peer Node Status

### Purpose

Check the Multinode High Availability peer node status.

### Action

From operational mode, run the following command:

vSRX-1

```
user@host> show chassis high-availability peer-info
  HA Peer Information:

  Peer-ID: 2      IP address: 10.0.3.11      Interface: ge-0/0/0.0
  Routing Instance: default
  Encrypted: NO    Conn State: UP
  Cold Sync Status: COMPLETE
  Internal Interface: N/A
  Internal Local-IP: N/A
  Internal Peer-IP: N/A
  Internal Routing-instance: N/A
Packet Statistics:
  Receive Error : 0      Send Error : 0

  Packet-type      Sent      Received

  SRG Status Msg   7         6
  SRG Status Ack   6         7
  Attribute Msg     2         1
  Attribute Ack     1         1
```

vSRX-2

```
user@host> show chassis high-availability peer-info
  HA Peer Information:
```

```

Peer-ID: 1      IP address: 10.0.3.10    Interface: ge-0/0/0.0
Routing Instance: default
Encrypted: NO    Conn State: UP
Cold Sync Status: COMPLETE
Internal Interface: N/A
Internal Local-IP: N/A
Internal Peer-IP: N/A
Internal Routing-instance: N/A
Packet Statistics:

```

```

    Receive Error : 0      Send Error : 0

    Packet-type      Sent      Received

    SRG Status Msg   9        9

    SRG Status Ack   9        9

    Attribute Msg     3        2

    Attribute Ack     2        2

```

### Meaning

Verify these details from the command output:

- Peer node details including ID, IP address, interface.
- Packet statistics across the node.

## Check Multinode High Availability SRG

### Purpose

View and verify SRG details in Multinode High Availability.

### Action

From operational mode, run the following command:

```

user@host> show chassis high-availability services-redundancy-group 1
      SRG failure event codes:
      BF  BFD monitoring
      IP  IP monitoring

```

```

IF Interface monitoring
CP Control Plane monitoring

```

```

Services Redundancy Group: 1
  Deployment Type: CLOUD
  Status: ACTIVE
  Activeness Priority: 200
  Preemption: ENABLED
  Process Packet In Backup State: NO
  Control Plane State: READY
  System Integrity Check: N/A
  Failure Events: NONE
  Peer Information:
    Peer Id: 2
    Status : BACKUP
    Health Status: HEALTHY
    Failover Readiness: READY

  Split-brain Prevention Probe Info:
    DST-IP: 10.0.1.102
    SRC-IP: 0.0.0.0
    Routing Instance: s1-router
    Status: NOT RUNNING
    Result: N/A          Reason: N/A

```

### Meaning

Verify these details from the command output:

- SRG details such deployment type. The field Status: ACTIVE indicates that the particular SRG1 is in active role. You can also view activeness priority and preemption state in the output.
- Peer node details.
- Split-brain prevention probe details.

### Verify the Multinode High Availability Status Before and After Failover

#### Purpose

Check the change in node status before and after a failover in a Multinode High Availability setup.

#### Action

Check the Multinode High Availability status on the backup node (SRX-2).

From operational mode, run the following command:

```

user@host> show chassis high-availability information

Node failure codes:
  HW  Hardware monitoring   LB  Loopback monitoring
  MB  Mbuf monitoring       SP  SPU monitoring
  CS  Cold Sync monitoring  SU  Software Upgrade

Node Status: ONLINE
Local-id: 2
Local-IP: 10.0.3.11
HA Peer Information:

  Peer Id: 1      IP address: 10.0.3.10   Interface: ge-0/0/0.0
  Routing Instance: default
  Encrypted: NO   Conn State: UP
  Cold Sync Status: COMPLETE

SRG failure event codes:
  BF  BFD monitoring
  IP  IP monitoring
  IF  Interface monitoring
  CP  Control Plane monitoring

Services Redundancy Group: 1
  Deployment Type: CLOUD
  Status: BACKUP
  Activeness Priority: 100
  Preemption: ENABLED
  Process Packet In Backup State: NO
  Control Plane State: NOT READY
  System Integrity Check: COMPLETE
  Failure Events: NONE
  Peer Information:
    Peer Id: 1
    Status : ACTIVE
    Health Status: HEALTHY
    Failover Readiness: N/A

```

## Meaning

In Services Redundancy Group: 1 section, you can see the Status: BACKUP. This field indicates that the SRG-1 is in the backup mode.

### Action

Initiate the failover on the active node (vSRX-1) and again run the command on the backup node (vSRX-2).

```
user@host> show chassis high-availability information
Node failure codes:
  HW  Hardware monitoring   LB  Loopback monitoring
  MB  Mbuf monitoring       SP  SPU monitoring
  CS  Cold Sync monitoring  SU  Software Upgrade

Node Status: ONLINE
Local-id: 2
Local-IP: 10.0.3.11
HA Peer Information:

  Peer Id: 1      IP address: 10.0.3.10   Interface: ge-0/0/0.0
  Routing Instance: default
  Encrypted: NO   Conn State: UP
  Cold Sync Status: COMPLETE

SRG failure event codes:
  BF  BFD monitoring
  IP  IP monitoring
  IF  Interface monitoring
  CP  Control Plane monitoring

Services Redundancy Group: 1
  Deployment Type: CLOUD
  Status: ACTIVE
  Activeness Priority: 100
  Preemption: ENABLED
  Process Packet In Backup State: NO
  Control Plane State: READY
  System Integrity Check: N/A
  Failure Events: NONE
  Peer Information:
    Peer Id: 1
    Status : BACKUP
```

Health Status: HEALTHY  
Failover Readiness: NOT READY

Meaning

In the Services Redundancy Group: 1 section, the status of SRG1 changes from BACKUP to ACTIVE. The change in the field value indicates that the node has transitioned into the active role and the other node (previously active) has transitioned to the backup role. You can see the other node's status in the Peer Information option, which shows BACKUP.

SEE ALSO

- [Multinode High Availability | 613](#)
- [Multinode High Availability Services | 658](#)
- [Prepare Your Environment for Multinode High Availability Deployment | 654](#)
- [Example: Configure Multinode High Availability in a Default Gateway Deployment | 717](#)
- [Example: Configure Multinode High Availability in a Layer 3 Network | 672](#)
- [Example: Configure Multinode High Availability in a Hybrid Deployment | 752](#)



# 16

PART

## Configuration Statements and Operational Commands

---

Configuration Statements: Adaptive Load Balancing | 937

Configuration Statements: Bidirectional Forwarding Detection | 940

Ethernet Automatic Protection Switching | 955

Configuration Statements: Ethernet Ring Protection Switching | 961

Configuration Statements: Graceful Routing Engine Switchover | 993

Configuration Statements: Graceful Restart | 998

Configuration Statements: Multinode High Availability | 1035

Configuration Statements: Nonstop Active Routing | 1064

Configuration Statements: Nonstop Bridging | 1074

Configuration Statements: NSSU | 1077

Configuration Statements: Power Management | 1085

Configuration Statements: Redundant Power System | 1091

Configuration Statements: Routing Engine and Switching Control Board  
Redundancy | 1096

Configuration Statements: Unified ISSU | 1129

Configuration Statements: VRRP | 1134

Administration | 1198

Verification Tasks | 1220

Operational Commands | 1224

Troubleshooting | 1562

Knowledge Base | 1571

---

# Configuration Statements: Adaptive Load Balancing

## IN THIS CHAPTER

- [adaptive | 937](#)

## adaptive

## IN THIS SECTION

- [Syntax | 937](#)
- [Hierarchy Level | 938](#)
- [Description | 938](#)
- [Options | 938](#)
- [Required Privilege Level | 939](#)
- [Release Information | 939](#)

## Syntax

```
adaptive {  
    pps;  
    scan-interval multiple;  
    tolerance tolerance-percentage;  
}
```

# Hierarchy Level

```
[edit dynamic-profiles name interfaces name aggregated-ether-options load-balance],
[edit dynamic-profiles name interfaces name logical-tunnel-options load-balance],
[edit dynamic-profiles name interfaces interface-range name aggregated-ether-options load-
balance],
[edit dynamic-profiles name interfaces interface-range name logical-tunnel-options load-balance],
[edit dynamic-profiles name logical-systems name interfaces name aggregated-ether-options load-
balance],
[edit dynamic-profiles name logical-systems name interfaces name logical-tunnel-options load-
balance],
[edit dynamic-profiles name logical-systems name interfaces interface-range name aggregated-
ether-options load-balance],
[edit dynamic-profiles name logical-systems name interfaces interface-range name logical-tunnel-
options load-balance],
[edit interfaces name aggregated-ether-options load-balance],
[edit interfaces name logical-tunnel-options load-balance],
[edit interfaces interface-range name aggregated-ether-options load-balance],
[edit interfaces interface-range name logical-tunnel-options load-balance]
```

# Description

Correct a genuine traffic imbalance by using a feedback mechanism to distribute the traffic across the links of an aggregated Ethernet bundle.

# Options

<b>pps</b>	(PTX Series only) The type of traffic rate among the members of the AE bundle is measured packets per second. The default rate type is bytes per second.
<b>scan-interval multiple</b>	(PTX Series only) Scan interval, as a multiple of a 30-second interval. <ul style="list-style-type: none"> <li>• <b>Range:</b> 1 through 5</li> <li>• <b>Default:</b> 1</li> </ul>
<b>tolerance tolerance- percentage</b>	(MX Series and PTX Series) Limit to the variance in the packet traffic flow to the aggregated Ethernet links in a percentage. <ul style="list-style-type: none"> <li>• <b>Range:</b> 1 through 100 percent</li> <li>• <b>Default:</b> 20 percent</li> </ul>

## Required Privilege Level

interface - To view this statement in the configuration.

interface-control - To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 13.2R3.

## RELATED DOCUMENTATION

[Understanding Aggregated Ethernet Load Balancing | 144](#)

[Example: Configuring Aggregated Ethernet Load Balancing | 165](#)

# Configuration Statements: Bidirectional Forwarding Detection

## IN THIS CHAPTER

- [dedicated-ukern-cpu \(BFD\) | 940](#)
- [realtime-ukern-thread \(BFD\) | 941](#)
- [authentication \(LAG\) | 943](#)
- [bfd-liveness-detection \(LAG\) | 945](#)
- [detection-time \(LAG\) | 948](#)
- [traceoptions \(Protocols BFD\) | 949](#)
- [transmit-interval \(LAG\) | 952](#)

## dedicated-ukern-cpu (BFD)

### IN THIS SECTION

- [Syntax | 940](#)
- [Hierarchy Level | 941](#)
- [Description | 941](#)
- [Required Privilege Level | 941](#)
- [Release Information | 941](#)

### Syntax

```
dedicated-ukern-cpu;
```

# Hierarchy Level

[edit chassis]

## Description

Enable the dedicated Bidirectional Forwarding Detection (BFD) protocol. One dedicated CPU core is allocated for the flowd ukernel thread to handle the dedicated BFD. This ensures that the BFD packet processing does not compete with the Routing Engine daemons.

## Required Privilege Level

- interface—To view this statement in the configuration.
- interface-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 15.1X49-D100.

## RELATED DOCUMENTATION

Enabling Dedicated and Real-Time BFD on SRX Devices
<a href="#">show chassis dedicated-ukern-cpu</a>   <a href="#">1388</a>
<a href="#">bfd-liveness-detection (LAG)</a>   <a href="#">945</a>
<a href="#">authentication (LAG)</a>   <a href="#">943</a>
<a href="#">detection-time (LAG)</a>   <a href="#">948</a>
<a href="#">transmit-interval (LAG)</a>   <a href="#">952</a>

## realtime-ukern-thread (BFD)

### IN THIS SECTION

- [Syntax](#) | [942](#)

- [Hierarchy Level | 942](#)
- [Description | 942](#)
- [Required Privilege Level | 942](#)
- [Release Information | 942](#)

## Syntax

```
realtime-ukern-thread;
```

## Hierarchy Level

```
[edit chassis]
```

## Description

Enable the real-time Bidirectional Forwarding Detection (BFD) protocol. After real-time BFD is enabled, the priority of the flowd ukernel thread is changed to the highest level and, therefore, the flowd ukernel thread gets more CPU cycles for processing the BFD packets.

## Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

## Release Information

Command introduced in Junos OS Release 15.1X49-D100.

## RELATED DOCUMENTATION

Enabling Dedicated and Real-Time BFD on SRX Devices

[show chassis realtime-ukern-thread | 1395](#)



[bfd-liveness-detection \(LAG\) | 945](#)

[authentication \(LAG\) | 943](#)

[detection-time \(LAG\) | 948](#)

[transmit-interval \(LAG\) | 952](#)

## authentication (LAG)

### IN THIS SECTION

- [Syntax | 943](#)
- [Hierarchy Level | 943](#)
- [Description | 943](#)
- [Options | 944](#)
- [Required Privilege Level | 944](#)
- [Release Information | 944](#)

### Syntax

```
authentication {  
    algorithm algorithm-name;  
    key-chain key-chain-name;  
    loose-check;  
}
```

### Hierarchy Level

```
[edit interfaces aex aggregated-ether-options bfd-liveness-detection]
```

### Description

Configure the authentication criteria of the BFD session for aggregated Ethernet interfaces.

## Options

<b>algorithm</b> <i>algorithm-name</i>	Specify the algorithm to be used to authenticate the BFD session. You can use one of the following algorithms for authentication: <ul style="list-style-type: none"> <li>• keyed-md5</li> <li>• keyed-sha-1</li> <li>• meticulous-keyed-md5</li> <li>• meticulous-keyed-sha-1</li> <li>• simple-password</li> </ul>
<b>key-chain</b> <i>key-chain-name</i>	Specify the name that is associated with the security key for the BFD session. The name you specify must match one of the keychains configured in the authentication-key-chains key-chain statement at the [edit security] hierarchy level.
<b>loose-check</b>	(Optional) Configure loose authentication checking on the BFD session. Use only for transitional periods when authentication might not be configured at both ends of the BFD session.

## Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 13.3.

## RELATED DOCUMENTATION

[bfd-liveness-detection \(LAG\) | 945](#)

[detection-time \(LAG\) | 948](#)

[transmit-interval \(LAG\) | 952](#)

[Configuring Micro BFD Sessions for LAG](#)

[Example: Configuring Independent Micro BFD Sessions for LAG](#)

[Understanding Independent Micro BFD Sessions for LAG](#)

## bfd-liveness-detection (LAG)

### IN THIS SECTION

- [Syntax | 945](#)
- [Hierarchy Level | 946](#)
- [Description | 946](#)
- [Options | 946](#)
- [Required Privilege Level | 947](#)
- [Release Information | 947](#)

### Syntax

```
bfd-liveness-detection {  
    authentication {  
        algorithm algorithm-name;  
        key-chain key-chain-name;  
        loose-check;  
    }  
    detection-time {  
        threshold milliseconds;  
    }  
    holddown-interval milliseconds;  
    local-address bfd-local-address;  
    minimum-interval milliseconds;  
    minimum-receive-interval milliseconds;  
    multiplier number;  
    neighbor bfd-neighbor-address;  
    no-adaptation;  
    transmit-interval {  
        minimum-interval milliseconds;  
        threshold milliseconds;  
    }  
    version (1 | automatic);  
}
```

## Hierarchy Level

```
[edit interfaces aex aggregated-ether-options]
```

## Description

Configure Bidirectional Forwarding Detection (BFD) timers and authentication for aggregated Ethernet interfaces.

For an aggregated ethernet interface, you cannot configure all three configuration options, `bfd-liveness-detection`, `minimum-links`, and `sync-reset` at the same time.

## Options

**holddown-interval**  
*milliseconds*

Specify a time limit, in milliseconds, indicating the time that a BFD session remains up before a state change notification is sent. If the BFD session goes down and then comes back up during the hold-down interval, the timer is restarted.

- **Range:** 0 through 255,000
- **Default:** 0

**local-address**  
*bfd-local-address*

Specify the loopback address or the AE interface address of the source of the BFD session.

**NOTE:** Beginning with Release 16.1R2, Junos OS checks and validates the configured micro BFD `local-address` against the interface or loopback IP address before the configuration commit. Junos OS performs this check on both IPv4 and IPv6 micro BFD address configurations, and if they do not match, the commit fails. The configured micro-BFD `local-address` should match with the micro-BFD `neighbour-address` configured on the peer router.

**minimum-interval**  
*milliseconds*

Specify a minimum time interval after which the local routing device transmits a BFD packet and then expects to receive a reply from the BFD neighbor. Optionally, instead of using this statement, you can configure the minimum transmit and receive intervals separately using the `transmit-interval` `minimum-interval` statement.

- **Range:** 1 through 255,000

<b>minimum-receive-interval</b> <i>milliseconds</i>	Specify the minimum time interval after which the routing device expects to receive a reply from the BFD neighbor. <ul style="list-style-type: none"> <li>• <b>Range:</b> 1 through 255,000</li> </ul>
<b>multiplier</b> <i>number</i>	Specify the number of BFD packets that were not received by the BFD neighbor before the originating interface is declared down. <ul style="list-style-type: none"> <li>• <b>Range:</b> 1 through 255</li> </ul>
<b>neighbor bfd-neighbor-address</b>	Specify the loopback address or the AE interface address of a remote destination to send BFD packets.
<b>no-adaptation</b>	Disable the BFD adaptation. Include this statement if you do not want the BFD sessions to adapt to changing network conditions. We recommend that you do not disable BFD adaptation unless it is preferable not to have BFD adaptation enabled in your network.
<b>version</b>	Configure the BFD version to detect (BFD version 1) or autodetect (the BFD version). <div data-bbox="435 919 1432 1125" style="background-color: #e6f2ff; padding: 10px; margin-top: 10px;"> <p><b>NOTE:</b> The <code>version</code> option is not supported on the QFX Series. Starting in Junos OS Release 17.2R1, a warning will appear if you attempt to use this command.</p> </div> <ul style="list-style-type: none"> <li>• <b>Default:</b> automatic</li> </ul>

The remaining statements are explained separately. See [CLI Explorer](#).

## Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 13.3.

## RELATED DOCUMENTATION

[authentication](#)

[detection-time](#)[transmit-interval](#)[\*Configuring Micro BFD Sessions for LAG\*](#)[Example: Configuring Independent Micro BFD Sessions for LAG](#)[Understanding Independent Micro BFD Sessions for LAG](#)

## detection-time (LAG)

### IN THIS SECTION

- [Syntax | 948](#)
- [Hierarchy Level | 948](#)
- [Description | 948](#)
- [Options | 949](#)
- [Required Privilege Level | 949](#)
- [Release Information | 949](#)

### Syntax

```
detection-time {  
    threshold milliseconds;  
}
```

### Hierarchy Level

```
[edit interfaces aex aggregated-ether-options bfd-liveness-detection]
```

### Description

Configure BFD timers for aggregated Ethernet interfaces.

# Options

**threshold**  
*milliseconds* Specify the maximum time interval for detecting a BFD neighbor. If the transmit interval is greater than this value, the device triggers a trap.

## Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 13.3.

## RELATED DOCUMENTATION

[authentication \(LAG\) | 943](#)

[bfd-liveness-detection \(LAG\) | 945](#)

[transmit-interval \(LAG\) | 952](#)

[Configuring Micro BFD Sessions for LAG](#)

[Example: Configuring Independent Micro BFD Sessions for LAG](#)

[Understanding Independent Micro BFD Sessions for LAG](#)

## traceoptions (Protocols BFD)

### IN THIS SECTION

- [Syntax | 950](#)
- [Hierarchy Level | 950](#)
- [Description | 950](#)
- [Default | 950](#)
- [Options | 950](#)
- [Required Privilege Level | 952](#)

## Syntax

```
traceoptions {  
    file name <size size> <files number> <world-readable | no-world-readable>;  
    flag flag <flag-modifier> <disable>;  
}
```

## Hierarchy Level

```
[edit protocols bfd]
```

## Description

Define tracing operations that track unified in-service software upgrade (ISSU) functionality in the router.

To specify more than one tracing operation, include multiple `flag` statements.

## Default

If you do not include this statement, no global tracing operations are performed.

## Options

**disable**—(Optional) Disable the tracing operation. You can use this option to disable a single operation when you have defined a broad group of tracing operations, such as **all**.

**file *name***—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory **/var/log**. We recommend that you place global routing protocol tracing output in the file **routing-log**.

**files *number***—(Optional) Maximum number of trace files. When a trace file named ***trace-file*** reaches its maximum size, it is renamed ***trace-file.0***, then ***trace-file.1***, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.



- **Range:** 2 through 1000 files
- **Default:** 2 files

If you specify a maximum number of files, you also must specify a maximum file size with the **size** option.

**flag *flag***—Tracing operation to perform. The tracing options are as follows:

- **adjacency**—Trace adjacency messages.
- **all**—Trace everything.
- **error**—Trace all errors.
- **events**—Trace all events.
- **issu**—Trace ISSU packet activity.
- **nsr-packet**—Trace packet activity of NSR.
- **nsr-synchronization**—Trace NSR synchronization events.
- **packet**—Trace all packets.
- **pipe**—Trace pipe messages.
- **pipe-detail**—Trace pipe messages in detail.
- **ppm-packet**—Trace packet activity by periodic packet management.
- **state**—Trace state transitions.
- **timer**—Trace timer processing.

**no-world-readable**—Restrict users from reading the log file.

**size *size***—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named ***trace-file*** reaches this size, it is renamed ***trace-file.0***. When the ***trace-file*** again reaches its maximum size, ***trace-file.0*** is renamed ***trace-file.1*** and ***trace-file*** is renamed ***trace-file.0***. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

- **Syntax:** ***xk*** to specify KB, ***xm*** to specify MB, or ***xg*** to specify GB
- **Range:** 10 KB through the maximum file size supported on your system
- **Default:** 128 KB

If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option.

**world-readable**—Allow users to read the log file.

### Required Privilege Level

routing and trace—To view this statement in the configuration.

routing-control and trace-control—To add this statement to the configuration.

### Release Information

Statement introduced before Junos OS Release 7.4.

**issu** flag for BFD added in Junos OS Release 9.1.

### RELATED DOCUMENTATION

| Managing and Tracing BFD Sessions During Unified ISSU Procedures

## transmit-interval (LAG)

#### IN THIS SECTION

- [Syntax | 953](#)
- [Hierarchy Level | 953](#)
- [Description | 953](#)
- [Options | 953](#)
- [Required Privilege Level | 953](#)
- [Release Information | 953](#)

## Syntax

```
transmit-interval {
  minimum-interval milliseconds;
  threshold milliseconds;
}
```

## Hierarchy Level

```
[edit interfaces aex aggregated-ether-options bfd-liveness-detection]
```

## Description

Configure the minimum interval and the threshold for transmission of BFD packets for aggregated Ethernet interfaces.

## Options

<b>minimum-interval</b> <i>milliseconds</i>	Specify the minimum time interval between two transmissions of packets. <ul style="list-style-type: none"> <li>• <b>Range:</b> 1 through 255,000</li> </ul>
<b>threshold</b> <i>milliseconds</i>	Specify the maximum interval between transmission of packets. If the transmit interval is greater than this value, the device triggers a trap.

## Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 13.3.

## RELATED DOCUMENTATION

[authentication \(LAG\)](#) | 943

[bfd-liveness-detection \(LAG\) | 945](#)

---

[detection-time \(LAG\) | 948](#)

---

[Configuring Micro BFD Sessions for LAG](#)

---

[Example: Configuring Independent Micro BFD Sessions for LAG](#)

---

[Understanding Independent Micro BFD Sessions for LAG](#)

# Ethernet Automatic Protection Switching

## IN THIS CHAPTER

- [clear](#) | 955
- [exercise](#) | 956
- [force switch](#) | 957
- [lockout](#) | 958
- [manual switch](#) | 959

## clear

## IN THIS SECTION

- [Syntax](#) | 955
- [Hierarchy Level](#) | 955
- [Description](#) | 956
- [Required Privilege Level](#) | 956

## Syntax

```
request protection-group ethernet-aps clear md <md> ma <ma>
```

## Hierarchy Level

```
[edit protocols protection-group ethernet-aps]
```

## Description

Clears the lockout, force switch, manual switch, exercise, and wait-to-restore (WTR) states.

## Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

## RELATED DOCUMENTATION

Ethernet Automatic Protection Switching Overview

## exercise

### IN THIS SECTION

- Syntax | 956
- Hierarchy Level | 956
- Description | 957
- Required Privilege Level | 957

## Syntax

```
request protection-group ethernet-aps exercise md <md> ma <ma>
```

## Hierarchy Level

```
[edit protocols protection-group ethernet-aps]
```

## Description

This configuration statement is used to test if APS is operating correctly, it does not interrupt regular APS operations.

## Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

## RELATED DOCUMENTATION

Ethernet Automatic Protection Switching Overview

## force switch

### IN THIS SECTION

- [Syntax | 957](#)
- [Hierarchy Level | 957](#)
- [Description | 958](#)
- [Required Privilege Level | 958](#)

## Syntax

```
request protection-group ethernet-aps force-switch md <md> ma <ma>
```

## Hierarchy Level

```
[edit protocols protection-group ethernet-aps]
```

## Description

Forces traffic to switch from the active path to the alternate path. If the working path is the active path, traffic will be switched to the protection path. If the protection path is the active path, traffic will be switched to the protection path.

## Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

## RELATED DOCUMENTATION

Ethernet Automatic Protection Switching Overview

## lockout

### IN THIS SECTION

- [Syntax | 958](#)
- [Hierarchy Level | 958](#)
- [Description | 959](#)
- [Required Privilege Level | 959](#)

## Syntax

```
request protection-group ethernet-aps lockout md <md> ma <ma>
```

## Hierarchy Level

```
[edit protocols protection-group ethernet-aps]
```



## Description

Configure a lockout of the protection path, forcing the use of the working path and locking out the protect path regardless of anything else.

## Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

## RELATED DOCUMENTATION

| [Ethernet Automatic Protection Switching Overview](#)

## manual switch

### IN THIS SECTION

- [Syntax | 959](#)
- [Hierarchy Level | 959](#)
- [Description | 960](#)
- [Required Privilege Level | 960](#)

## Syntax

```
request protection-group ethernet-aps manual-switch md <md> ma <ma>
```

## Hierarchy Level

```
[edit protocols protection-group ethernet-aps]
```

## Description

Forces traffic to switch from the active path to the alternate path, even in the absence of a failure on the working path. If the working path is the active path, traffic will be switched to the protection path. If the protection path is the active path, traffic will be switched to the protection path.

## Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

## RELATED DOCUMENTATION

Ethernet Automatic Protection Switching Overview

# Configuration Statements: Ethernet Ring Protection Switching

## IN THIS CHAPTER

- `compatibility-version` | 962
- `control-channel` | 963
- `data-channel` | 965
- `dot1p-priority` | 966
- `east-interface` | 968
- `ethernet-ring` | 970
- `guard-interval` | 972
- `hold-interval (Protection Group)` | 973
- `major-ring-name` | 975
- `non-revertive` | 976
- `non-vc-mode` | 977
- `node-id` | 978
- `propagate-tc` | 979
- `protection-group` | 981
- `restore-interval` | 984
- `ring-id` | 985
- `ring-protection-link-end` | 987
- `ring-protection-link-owner` | 988
- `wait-to-block-interval` | 989
- `west-interface` | 990

## compatibility-version

### IN THIS SECTION

- [Syntax | 962](#)
- [Hierarchy Level | 962](#)
- [Description | 962](#)
- [Options | 962](#)
- [Required Privilege Level | 963](#)
- [Release Information | 963](#)

### Syntax

```
compatibility-version;
```

### Hierarchy Level

```
[edit protocols protection-group ethernet-ring ring-name]
```

### Description

Specify the compatible version mode to be used. When compatibility-version is set to value 1, the node operates in ITU-T Recommendation G.8032/Y.1344 version 1 compatible mode. In this mode all the supported external commands are blocked, ring-id is forced to be 1 and mode of operation is set to revertive mode.

### Options

- 1—Use ITU-T Recommendation G.8032/Y.1344 compatible mode version 1.
- 2—Use ITU-T Recommendation G.8032/Y.1344 compatible mode version 2.

## Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 14.2.

## RELATED DOCUMENTATION

Ethernet Ring Protection Switching Overview

[Configuring Ethernet Ring Protection Switching on Switches \(CLI Procedure\)](#)

## control-channel

### IN THIS SECTION

- [Syntax | 963](#)
- [Hierarchy Level | 964](#)
- [Description | 964](#)
- [Options | 964](#)
- [Required Privilege Level | 964](#)
- [Release Information | 964](#)

## Syntax

```
control-channel channel-name {  
    vlan vlan-id;  
    interface name interface-name  
}
```

## Hierarchy Level

```
[edit protocols protection-group ethernet-ring name (east-interface | west-interface)]
```

## Description

Configure the Ethernet RPS control channel logical interface to carry the RAPS PDU. The related physical interface is the physical ring port.

## Options

`vlan vlan-id`—If the control channel logical interface is a trunk port, then a dedicated `vlan vlan-id` defines the dedicated VLAN channel to carry the RAPS traffic. Only configure the `vlan-id` when the control channel logical interface is the trunk port.

`interface name interface-name`—Interface name of the control channel.

## Required Privilege Level

`interface`—To view this statement in the configuration.

`interface-control`—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 9.4.

Statement introduced in Junos OS Release 12.1 for EX Series switches.

Statement introduced in Junos OS Release 14.153-D10 for QFX Series switches.

## RELATED DOCUMENTATION

Ethernet Ring Protection Switching Overview

*Example: Configuring Ethernet Ring Protection Switching on EX Series Switches*

*Example: Configuring Ethernet Ring Protection Switching on QFX Series and EX Series Switches Supporting ELS*

[Configuring Ethernet Ring Protection Switching on Switches \(CLI Procedure\)](#)

## data-channel

### IN THIS SECTION

- [Syntax | 965](#)
- [Hierarchy Level | 965](#)
- [Description | 965](#)
- [Options | 965](#)
- [Required Privilege Level | 966](#)
- [Release Information | 966](#)

### Syntax

```
data-channel {  
    vlan number;  
}
```

### Hierarchy Level

```
[edit protocols protection-group ethernet-ring ring-name]
```

### Description

For Ethernet ring protection, configure a data channel to define a set of VLAN IDs that belong to a ring instance.

VLANs specified in the data channel use the same topology used by the ERPS PDU in the control channel. Therefore, if a ring interface is blocked in the control channel, all traffic in the data channel is also blocked on that interface.

### Options

*vlan number*—Specify (by VLAN ID) one or more VLANs that belong to a ring instance.

## Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 10.2.

Statement introduced in Junos OS Release 12.1 for EX Series switches.

Statement introduced in Junos OS Release 14.153-D10 for QFX Series switches.

## RELATED DOCUMENTATION

[Ethernet Ring Protection Using Ring Instances for Load Balancing](#)

[Example: Configuring Load Balancing Within Ethernet Ring Protection for MX Series Routers](#)

*Example: Configuring Ethernet Ring Protection Switching on QFX Series and EX Series Switches Supporting ELS*

[Configuring Ethernet Ring Protection Switching on Switches \(CLI Procedure\)](#)

## dot1p-priority

### IN THIS SECTION

- [Syntax | 967](#)
- [Hierarchy Level | 967](#)
- [Description | 967](#)
- [Options | 967](#)
- [Required Privilege Level | 967](#)
- [Release Information | 967](#)



## Syntax

```
dot1p-priority number;
```

## Hierarchy Level

```
[edit protocols protection-group ethernet-ring ring-name]
```

## Description

Specify the IEEE 802.1p priority to be used in the transmitted RAPS protocol data units.

## Options

*number*—802.1p priority number.

- **Range:** 0 through 7
- **Default:** 0

## Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 14.2.

## RELATED DOCUMENTATION

Ethernet Ring Protection Switching Overview

[Configuring Ethernet Ring Protection Switching on Switches \(CLI Procedure\)](#)

## east-interface

### IN THIS SECTION

- [Syntax | 968](#)
- [Hierarchy Level | 968](#)
- [Description | 968](#)
- [Required Privilege Level | 969](#)
- [Release Information | 969](#)

### Syntax

```
east-interface {
    node-id mac-address;
    control-channel channel-name {
        vlan number;
        interface name interface-name
    }
    interface-none
    ring-protection-link-end;
}
```

### Hierarchy Level

```
[edit protocols protection-group ethernet-ring ring-name]
```

### Description

Define one of the two interface ports for Ethernet ring protection, the other being defined by the `west-interface` statement at the same hierarchy level. The interface must use the control channel's logical interface name. The control channel is a dedicated VLAN channel for the ring port.

EX Series switches do not use the `node-id` statement--the node ID is automatically configured on the switches using the MAC address.

**NOTE:** Always configure this port first, before configuring the `west-interface` statement.

**NOTE:** The Node ID is not configurable on EX Series switches. The node ID is automatically configured using the MAC address.

The remaining statements are explained separately. See [CLI Explorer](#).

## Required Privilege Level

`interface`—To view this statement in the configuration.

`interface-control`—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 9.4.

Statement introduced in Junos OS Release 12.1 for EX Series switches.

Statement introduced in Junos OS Release 14.153-D10 for QFX Series switches.

## RELATED DOCUMENTATION

Ethernet Ring Protection Switching Overview

[Ethernet Ring Protection Using Ring Instances for Load Balancing](#)

*west-interface*

*ethernet-ring*

*Example: Configuring Ethernet Ring Protection Switching on EX Series Switches*

*Example: Configuring Ethernet Ring Protection Switching on QFX Series and EX Series Switches Supporting ELS*

[Configuring Ethernet Ring Protection Switching on Switches \(CLI Procedure\)](#)

## ethernet-ring

### IN THIS SECTION

- [Syntax | 970](#)
- [Hierarchy Level | 971](#)
- [Description | 971](#)
- [Options | 971](#)
- [Required Privilege Level | 971](#)
- [Release Information | 971](#)

### Syntax

```
ethernet-ring ring-name {  
    control-vlan (vlan-id | vlan-name);  
    data-channel {  
        vlan number  
    }  
    east-interface {  
        control-channel channel-name {  
            vlan number;  
            interface name interface-name  
        }  
    }  
    guard-interval number;  
    node-id mac-address;  
    restore-interval number;  
    ring-protection-link-owner;  
    west-interface {  
        control-channel channel-name {  
            vlan number;  
        }  
    }  
}
```

## Hierarchy Level

```
[edit protocols protection-group]
```

## Description

For Ethernet PICs on MX Series routers or for EX Series switches, , specify the Ethernet ring in an Ethernet ring protection switching configuration.

## Options

*ring-name*—Name of the Ethernet protection ring.

The remaining statements are explained separately. See [CLI Explorer](#).

## Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 9.4.

Statement introduced in Junos OS Release 12.1 for EX Series switches.

Statement introduced in Junos OS Release 14.153-D10 for QFX Series switches.

## RELATED DOCUMENTATION

Ethernet Ring Protection Switching Overview

*Example: Configuring Ethernet Ring Protection Switching on EX Series Switches*

*Example: Configuring Ethernet Ring Protection Switching on QFX Series and EX Series Switches Supporting ELS*

[Configuring Ethernet Ring Protection Switching on Switches \(CLI Procedure\)](#)

## guard-interval

### IN THIS SECTION

- [Syntax | 972](#)
- [Hierarchy Level | 972](#)
- [Description | 972](#)
- [Options | 972](#)
- [Required Privilege Level | 973](#)
- [Release Information | 973](#)

### Syntax

```
guard-interval number;
```

### Hierarchy Level

```
[edit protocols protection-group ethernet-ring ring-name]
```

### Description

When a link goes down, the ring protection link (RPL) activates. When the downed link comes back up, the RPL link receives notification, restores the link, and waits for the restore interval before issuing another block on the same link. This configuration is a global configuration and applies to all Ethernet rings if the Ethernet ring does not have a more specific configuration for this value. If no parameter is configured at the protection group level, the global configuration of this parameter uses the default value.

### Options

*number*—Guard timer interval, in milliseconds.

- **Range:** 10 through 2000 ms

- **Default:** 500 ms

## Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 9.4.

Statement introduced in Junos OS Release 12.1 for EX Series switches.

Statement introduced in Junos OS Release 14.153-D10 for QFX Series switches.

## RELATED DOCUMENTATION

Ethernet Ring Protection Switching Overview

*Example: Configuring Ethernet Ring Protection Switching on EX Series Switches*

*Example: Configuring Ethernet Ring Protection Switching on QFX Series and EX Series Switches Supporting ELS*

[Configuring Ethernet Ring Protection Switching on Switches \(CLI Procedure\)](#)

## hold-interval (Protection Group)

### IN THIS SECTION

- [Syntax | 974](#)
- [Hierarchy Level | 974](#)
- [Description | 974](#)
- [Options | 974](#)
- [Required Privilege Level | 974](#)
- [Release Information | 974](#)

## Syntax

```
hold-interval number;
```

## Hierarchy Level

```
[edit protocols protection-group ethernet-ring name]
```

## Description

Specify the hold-off timer interval *for all rings* in 100 millisecond (ms) increments.

## Options

*number*—Hold-timer interval, in milliseconds.

- **Range:** 0 through 10,000 ms
- **Default:** 100 ms

## Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 9.4.

## RELATED DOCUMENTATION

Ethernet Ring Protection Switching Overview

*Example: Configuring Ethernet Ring Protection Switching on QFX Series and EX Series Switches Supporting ELS*



## major-ring-name

### IN THIS SECTION

- [Syntax | 975](#)
- [Hierarchy Level | 975](#)
- [Description | 975](#)
- [Required Privilege Level | 975](#)
- [Release Information | 975](#)

### Syntax

```
major-ring-name name;
```

### Hierarchy Level

```
[edit protocols protection-group ethernet-ring ring-name]
```

### Description

Specify the name of major ring to which the sub-ring node is interconnected.

### Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

### Release Information

Statement introduced in Junos OS Release 14.2.

## RELATED DOCUMENTATION

Ethernet Ring Protection Switching Overview

[Configuring Ethernet Ring Protection Switching on Switches \(CLI Procedure\)](#)

## non-revertive

### IN THIS SECTION

- [Syntax | 976](#)
- [Hierarchy Level | 976](#)
- [Description | 976](#)
- [Required Privilege Level | 976](#)
- [Release Information | 977](#)

### Syntax

```
non-revertive;
```

### Hierarchy Level

```
[edit protocols protection-group ethernet-ring ring-name]
```

### Description

Enable nonrevertive operation where traffic is allowed to use the RPL if it has not failed, even after a switch condition has cleared. The default mode of operation is revertive.

### Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 14.2.

## RELATED DOCUMENTATION

Ethernet Ring Protection Switching Overview

[Configuring Ethernet Ring Protection Switching on Switches \(CLI Procedure\)](#)

## non-vc-mode

### IN THIS SECTION

- [Syntax | 977](#)
- [Hierarchy Level | 977](#)
- [Description | 977](#)
- [Required Privilege Level | 978](#)
- [Release Information | 978](#)

## Syntax

```
non-vc-mode;
```

## Hierarchy Level

```
[edit protocols protection-group ethernet-ring ring-name]
```

## Description

Configure a node on the sub-ring to operate in non-virtual channel mode. If this option is enabled then all the nodes in the sub-ring are configured with this option. Also, the `non-vc-mode` option should be used

with care and only for open rings. Using this option for closed rings creates loops for RAPS control messages.

## Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 14.2.

## RELATED DOCUMENTATION

Ethernet Ring Protection Switching Overview

[Configuring Ethernet Ring Protection Switching on Switches \(CLI Procedure\)](#)

## node-id

### IN THIS SECTION

- [Syntax | 978](#)
- [Hierarchy Level | 979](#)
- [Description | 979](#)
- [Required Privilege Level | 979](#)
- [Release Information | 979](#)

## Syntax

```
node-id mac-address;
```

## Hierarchy Level

```
[edit protocols protection-group ethernet-ring ring-name]
```

## Description

For EX Series switches and QFX Series switches, node-id is not configurable.

For MX Series routers, optionally specify the MAC address of a node in the protection group. If this statement is not included, the router assigns the node's MAC address.

## Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 9.4.

## RELATED DOCUMENTATION

Ethernet Ring Protection Switching Overview

*Example: Configuring Ethernet Ring Protection Switching on EX Series Switches*

*Example: Configuring Ethernet Ring Protection Switching on QFX Series and EX Series Switches Supporting ELS*

## propagate-tc

### IN THIS SECTION

- [Syntax | 980](#)
- [Hierarchy Level | 980](#)
- [Description | 980](#)

- Required Privilege Level | 980
- Release Information | 980

## Syntax

```
propagate-tc;
```

## Hierarchy Level

```
[edit protocols protection-group ethernet-ring ring-name]
```

## Description

Enable topology change propagation from a sub-ring to an interconnected major-ring. By default, topology change propagation is disabled.

## Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 14.2.

## RELATED DOCUMENTATION

Ethernet Ring Protection Switching Overview

[Configuring Ethernet Ring Protection Switching on Switches \(CLI Procedure\)](#)

## protection-group

### IN THIS SECTION

- Syntax | 981
- Hierarchy Level | 983
- Description | 983
- Required Privilege Level | 983
- Release Information | 983

### Syntax

```

protection-group {
    ethernet-ring ring-name {
        data-channel {
            vlan number
        }
        east-interface {
            control-channel channel-name {
                vlan number;
                interface name interface-name
            }
        }
    }
    guard-interval number;
    node-id mac-address;
    restore-interval number;
    ring-protection-link-owner;
    non-revertive;
    wait-to-block-interval number;
    major-ring-name name;
    propagate-tc;
    compatibility-version (1|2);
    ring-id number;
    non-vc-mode;
    dot1p-priority number;
    west-interface {
        control-channel channel-name {

```

```

        vlan number;
        interface name interface-name
    }
    virtual-control-channel {
        west-interface name;
        east-interface name;
    }
}
}
control-vlan (vlan-id | vlan-name);
    east-interface {
        node-id mac-address;
        control-channel channel-name {
            vlan number;
            interface name interface-name
        }
        interface-none
        ring-protection-link-end;
    }
}
    control-channel channel-name {
        vlan number;
        interface name interface-name
    }
}
data-channel {
    vlan number
}
guard-interval number;
node-id mac-address;
restore-interval number;
ring-protection-link-owner;
    west-interface {
        node-id mac-address;
        control-channel channel-name {
            vlan number;
            interface name interface-name
        }
        interface-none
        ring-protection-link-end;
    }
    control-channel channel-name {
        vlan number;

```



```

        interface name interface-name
        }
    }
}
guard-interval number;
restore-interval number;
traceoptions {
    file filename <no-stamp> <world-readable | no-world-readable> <replace> <size size>;
    flag flag;
}
}

```

## Hierarchy Level

[edit protocols]

## Description

Configure Ethernet ring protection switching.

The statements are explained separately. All statements apply to MX Series routers. EX Series switches do not assign `node-id` and use `control-vlan` instead of `control-channel`.

## Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 9.4.

## RELATED DOCUMENTATION

Ethernet Ring Protection Switching Overview

[Ethernet Ring Protection Using Ring Instances for Load Balancing](#)

[Example: Configuring Load Balancing Within Ethernet Ring Protection for MX Series Routers](#)

## Configuring Ethernet Ring Protection Switching on Switches (CLI Procedure)

*Example: Configuring Ethernet Ring Protection Switching on EX Series Switches*

*Example: Configuring Ethernet Ring Protection Switching on QFX Series and EX Series Switches Supporting ELS*

## restore-interval

### IN THIS SECTION

- [Syntax | 984](#)
- [Hierarchy Level | 984](#)
- [Description | 984](#)
- [Options | 985](#)
- [Required Privilege Level | 985](#)
- [Release Information | 985](#)

### Syntax

```
restore-interval number;
```

### Hierarchy Level

```
[edit protocols protection-group ethernet-ring ring-name]
```

### Description

Configures the number of minutes that the node does not process any Ethernet ring protection (ERP) protocol data units (PDUs).. This configuration is a global configuration and applies to all Ethernet rings if the Ethernet ring does not have a more specific configuration for this value. If no parameter is configured at the protection group level, the global configuration of this parameter uses the default value.

## Options

*number*—Specify the restore interval.

- **Range:** 1 through 12 minutes

## Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 9.4.

Statement introduced in Junos OS Release 12.1 for EX Series switches.

Statement introduced in Junos OS Release 14.153-D10 for QFX Series switches.

## RELATED DOCUMENTATION

[Ethernet Ring Protection Switching Overview](#)

[Example: Configuring Ethernet Ring Protection Switching on EX Series Switches](#)

[Example: Configuring Ethernet Ring Protection Switching on QFX Series and EX Series Switches Supporting ELS](#)

[Configuring Ethernet Ring Protection Switching on Switches \(CLI Procedure\)](#)

## ring-id

### IN THIS SECTION

- [Syntax | 986](#)
- [Hierarchy Level | 986](#)
- [Description | 986](#)
- [Options | 986](#)
- [Required Privilege Level | 986](#)
- [Release Information | 986](#)

## Syntax

```
ring-id number;
```

## Hierarchy Level

```
[edit protocols protection-group ethernet-ring ring-name]
```

## Description

Specify the ring ID.

## Options

*number*—Ring ID number.

- **Range:** 1 through 239
- **Default:** 1

## Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 14.2.

## RELATED DOCUMENTATION

Ethernet Ring Protection Switching Overview

[Configuring Ethernet Ring Protection Switching on Switches \(CLI Procedure\)](#)

## ring-protection-link-end

### IN THIS SECTION

- [Syntax | 987](#)
- [Hierarchy Level | 987](#)
- [Description | 987](#)
- [Required Privilege Level | 987](#)
- [Release Information | 987](#)

### Syntax

```
ring-protection-link-end;
```

### Hierarchy Level

```
[edit protocols protection-group ethernet-ring ring-name (east-interface | west-interface)]
```

### Description

Specify that the port is one side of a ring protection link (RPL) by setting the RPL end flag.

### Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

### Release Information

Statement introduced in Junos OS Release 9.4.

## RELATED DOCUMENTATION

Ethernet Ring Protection Switching Overview

*Example: Configuring Ethernet Ring Protection Switching on EX Series Switches*

*Example: Configuring Ethernet Ring Protection Switching on QFX Series and EX Series Switches Supporting ELS*

[Configuring Ethernet Ring Protection Switching on Switches \(CLI Procedure\)](#)

## ring-protection-link-owner

### IN THIS SECTION

- [Syntax | 988](#)
- [Hierarchy Level | 988](#)
- [Description | 988](#)
- [Required Privilege Level | 989](#)
- [Release Information | 989](#)

### Syntax

```
ring-protection-link-owner;
```

### Hierarchy Level

```
[edit protocols protection-group ethernet-ring ring-name]
```

### Description

Specify the ring protection link (RPL) owner flag in the Ethernet protection ring. Include this statement only once for each ring (only one node can function as the RPL owner).

## Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 9.4.

## RELATED DOCUMENTATION

Ethernet Ring Protection Switching Overview

*Example: Configuring Ethernet Ring Protection Switching on EX Series Switches*

*Example: Configuring Ethernet Ring Protection Switching on QFX Series and EX Series Switches Supporting ELS*

## wait-to-block-interval

### IN THIS SECTION

- [Syntax | 989](#)
- [Hierarchy Level | 990](#)
- [Description | 990](#)
- [Options | 990](#)
- [Required Privilege Level | 990](#)
- [Release Information | 990](#)

## Syntax

```
wait-to-block-interval number;
```

## Hierarchy Level

```
[edit protocols protection-group ethernet-ring ring-name]
```

## Description

Enable the Wait to Block (WTB) timer interval when clearing force switch and manual switch commands.

## Options

*number*—Wait-to-block interval, in seconds.

- **Range:** 5 through 10 s
- **Default:** 5 s

## Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 14.2.

## RELATED DOCUMENTATION

Ethernet Ring Protection Switching Overview

[Configuring Ethernet Ring Protection Switching on Switches \(CLI Procedure\)](#)

## west-interface

### IN THIS SECTION

● [Syntax](#) | 991



- Hierarchy Level | 991
- Description | 991
- Required Privilege Level | 992
- Release Information | 992

## Syntax

```
west-interface {
    node-id mac-address;
    control-channel channel-name {
        vlan number;
        interface name interface-name
    }
    interface-none
    ring-protection-link-end;
    virtual-control-channel {
        west-interface name;
        east-interface name;
    }
}
```

## Hierarchy Level

```
[edit protocols protection-group ethernet-ring ring-name]
```

## Description

Define one of the two interface ports for Ethernet ring protection, the other being defined by the east-interface statement at the same hierarchy level. The interface must use the control channel's logical interface name. The control channel is a dedicated VLAN channel for the ring port.

**NOTE:** Always configure this port second, after configuring the east-interface statement.

The remaining statements are explained separately. See [CLI Explorer](#).

## Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 9.5.

## RELATED DOCUMENTATION

Ethernet Ring Protection Switching Overview

[Ethernet Ring Protection Using Ring Instances for Load Balancing](#)

*east-interface*

*ethernet-ring*

*Example: Configuring Ethernet Ring Protection Switching on EX Series Switches*

*Example: Configuring Ethernet Ring Protection Switching on QFX Series and EX Series Switches Supporting ELS*

[Configuring Ethernet Ring Protection Switching on Switches \(CLI Procedure\)](#)

# Configuration Statements: Graceful Routing Engine Switchover

## IN THIS CHAPTER

- [graceful-switchover](#) | 993
- [graceful-switchover](#) | 994
- [redundancy \(Graceful Switchover\)](#) | 996

## graceful-switchover

## IN THIS SECTION

- [Syntax](#) | 993
- [Hierarchy Level](#) | 994
- [Description](#) | 994
- [Required Privilege Level](#) | 994
- [Release Information](#) | 994

## Syntax

```
graceful-switchover;
```

## Hierarchy Level

```
[edit chassis redundancy]
```

## Description

For routing platforms with two Routing Engines, configure a primary Routing Engine to switch over gracefully to a backup Routing Engine without interruption to packet forwarding.

**NOTE:** The graceful-switchover statement at the [edit chassis redundancy] hierarchy level is not supported for Junos OS Evolved. Graceful switchover is enabled on the Junos OS Evolved system by default.

## Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

## Release Information

Statement introduced before Junos OS Release 7.4.

## RELATED DOCUMENTATION

[Configuring Graceful Routing Engine Switchover](#) | 200

## graceful-switchover

### IN THIS SECTION

- [Syntax](#) | 995
- [Hierarchy Level](#) | 995

- [Description | 995](#)
- [Default | 995](#)
- [Required Privilege Level | 995](#)
- [Release Information | 995](#)

## Syntax

```
graceful-switchover;
```

## Hierarchy Level

```
[edit chassis (EX Series) redundancy]
```

## Description

For switches with more than one Routing Engine, including those in a Virtual Chassis or a Virtual Chassis Fabric, configure the primary Routing Engine to switch over gracefully to a backup Routing Engine without interruption to packet forwarding.

## Default

Graceful Routing Engine switchover (GRES) is disabled.

## Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 9.2.

## RELATED DOCUMENTATION

[Example: Configuring Nonstop Active Routing on Switches](#)

[Configuring Graceful Routing Engine Switchover](#)

[Configuring Graceful Routing Engine Switchover in a Virtual Chassis](#)

[Configuring Nonstop Active Routing on Switches](#)

[Installing Software on an EX Series Switch with Redundant Routing Engines \(CLI Procedure\)](#)

## redundancy (Graceful Switchover)

### IN THIS SECTION

- [Syntax | 996](#)
- [Hierarchy Level | 996](#)
- [Description | 997](#)
- [Default | 997](#)
- [Required Privilege Level | 997](#)
- [Release Information | 997](#)

### Syntax

```
redundancy {  
    failover {  
        on-disk-failure;  
        on-loss-of-keepalives;  
    }  
    graceful-switchover;  
}
```

### Hierarchy Level

[edit chassis (EX Series)]

## Description

Enable redundant Routing Engines on a Virtual Chassis with two or more member switches or on a Virtual Chassis Fabric, on a standalone EX6200 or EX8200 switch with more than one Routing Engine.

The remaining statements are explained separately. See [CLI Explorer](#).

## Default

Redundancy is enabled for the Routing Engines.

## Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 9.2.

## RELATED DOCUMENTATION

[graceful-switchover](#) | [994](#)

---

[Configuring Graceful Routing Engine Switchover in a Virtual Chassis](#)

---

[Configuring Graceful Routing Engine Switchover](#)

---

[Installing Software on an EX Series Switch with Redundant Routing Engines \(CLI Procedure\)](#)

---

[High Availability Features for EX Series Switches Overview](#)

## Configuration Statements: Graceful Restart

### IN THIS CHAPTER

- [disable](#) | 999
- [disable \(BGP Graceful Restart\)](#) | 1000
- [dont-help-shared-fate-bfd-down](#) | 1002
- [graceful-restart \(Enabling Globally\)](#) | 1003
- [graceful-restart \(Multicast Snooping\)](#) | 1006
- [graceful-restart \(Protocols BGP\)](#) | 1007
- [graceful-restart \(Protocols OSPF\)](#) | 1009
- [helper-disable \(Multiple Protocols\)](#) | 1012
- [kernel-replication](#) | 1013
- [maximum-helper-recovery-time](#) | 1015
- [maximum-helper-restart-time \(RSVP\)](#) | 1016
- [maximum-neighbor-reconnect-time](#) | 1018
- [maximum-neighbor-recovery-time](#) | 1019
- [not-on-disk-underperform](#) | 1021
- [reconnect-time](#) | 1022
- [recovery-time](#) | 1023
- [restart-duration](#) | 1025
- [restart-time \(BGP Graceful Restart\)](#) | 1027
- [stale-routes-time](#) | 1029
- [traceoptions \(Protocols\)](#) | 1030
- [warm-standby](#) | 1033



## disable

### IN THIS SECTION

- [Syntax | 999](#)
- [Hierarchy Level | 999](#)
- [Description | 999](#)
- [Required Privilege Level | 1000](#)
- [Release Information | 1000](#)

### Syntax

```
disable;
```

### Hierarchy Level

```
[edit logical-systems logical-system-name protocols (bgp | isis | ldp | ospf | ospf3 | pim | rip  
| ripng | rsvp) graceful-restart],  
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols (bgp  
| ldp | ospf | ospf3 | pim) graceful-restart],  
[edit protocols (bgp | esis | isis | ospf | ospf3 | ldp | pim | rip | ripng | rsvp) graceful-  
restart],  
[edit protocols bgp group group-name graceful-restart],  
[edit protocols bgp group group-name neighbor ip-address graceful-restart],  
[edit routing-instances routing-instance-name protocols (bgp | ldp | ospf | ospf3 | pim) graceful-  
restart],  
[edit routing-instances routing-instance-name routing-options graceful-restart],  
[edit routing-options graceful-restart]
```

### Description

Disable graceful restart.

Required Privilege Level

routing—To view this statement in the configuration.

routing-control—To add this statement to the configuration.

Release Information

Statement introduced before Junos OS Release 7.4.

RELATED DOCUMENTATION

Enabling Graceful Restart
<a href="#">Configuring Graceful Restart for Routing Protocols   359</a>
Configuring Graceful Restart for MPLS-Related Protocols
Configuring VPN Graceful Restart
Configuring Logical System Graceful Restart
<a href="#">Graceful Restart Configuration Statements</a>
Configuring Graceful Restart for QFabric Systems

disable (BGP Graceful Restart)

IN THIS SECTION

- [Syntax | 1001](#)
- [Hierarchy Level | 1001](#)
- [Description | 1001](#)
- [Required Privilege Level | 1001](#)
- [Release Information | 1001](#)

## Syntax

```
disable;
```

## Hierarchy Level

```
[edit logical-systems logical-system-name protocols bgp graceful-restart],
[edit logical-systems logical-system-name protocols bgp group group-name graceful-restart],
[edit logical-systems logical-system-name protocols bgp group group-name neighbor address
 graceful-restart],
[edit protocols bgp graceful-restart],
[edit protocols bgp group group-name graceful-restart],
[edit protocols bgp group group-name neighbor address graceful-restart]
```

## Description

Disable graceful restart for BGP. Graceful restart allows a routing device undergoing a restart to inform its adjacent neighbors and peers of its condition.

**NOTE:** When you disable graceful restart at one level in the configuration statement hierarchy, it is also disabled at lower levels in the same hierarchy. For example, if you disable graceful restart at the `[edit protocols bgp group group-name]` hierarchy level, it is disabled for all the peers in the group. Therefore, if you want to enable graceful restart for some peers in a group and disable it for others, enable graceful restart at the `[edit protocols bgp group group-name]` hierarchy level and disable graceful restart for each peer at the `[edit protocols bgp group group-name neighbor address]` hierarchy level.

## Required Privilege Level

routing—To view this statement in the configuration.

routing-control—To add this statement to the configuration.

## Release Information

Statement introduced before Junos OS Release 7.4.

## RELATED DOCUMENTATION

[Configuring Graceful Restart Options for BGP | 361](#)

*graceful-restart*

*restart-time*

*stale-routes-time*

## dont-help-shared-fate-bfd-down

### IN THIS SECTION

- [Syntax | 1002](#)
- [Hierarchy Level | 1002](#)
- [Description | 1002](#)
- [Default | 1003](#)
- [Required Privilege Level | 1003](#)
- [Release Information | 1003](#)

### Syntax

```
dont-help-shared-fate-bfd-down
```

### Hierarchy Level

```
[edit protocols bgp graceful-restart]
```

### Description

When BFD is control plane dependent and the device detects a BFD down event and is not already entering the graceful restart helper mode, this is treated as a regular BFD down event and the device enters the graceful restart helper mode. This behavior makes the control plane dependent BFD unusable in conjunction with graceful restart.

Include the `dont-help-shared-fate-bfd-down` statement at the `[edit protocols bgp graceful-restart]` hierarchy to ensure that the device does not enter the graceful restart helper mode and data traffic continues to be forwarded to an alternate path even if there is an interface failure (without a control plane restart on the BGP neighbor).

## Default

By default, this option is not enabled.

## Required Privilege Level

routing—To view this statement in the configuration.

routing-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 18.3R1.

## RELATED DOCUMENTATION

[Using Control Plane Dependent BFD along with Graceful Restart Helper Mode | 362](#)

*Understanding External BGP Peering Sessions*

## graceful-restart (Enabling Globally)

### IN THIS SECTION

- [Syntax | 1004](#)
- [Hierarchy Level | 1004](#)
- [Description | 1004](#)
- [Default | 1005](#)
- [Options | 1005](#)
- [Required Privilege Level | 1005](#)
- [Release Information | 1005](#)

## Syntax

```
graceful-restart {  
    disable;  
    helper-disable;  
    maximum-helper-recovery-time seconds;  
    maximum-helper-restart-time seconds;  
    notify-duration seconds;  
    recovery-time seconds;  
    restart-duration seconds;  
    stale-routes-time seconds;  
}
```

## Hierarchy Level

```
[edit logical-systems logical-system-name routing-options],  
[edit logical-systems logical-system-name routing-instances routing-instance-name routing-  
options],  
[edit routing-options],  
[edit routing-instances routing-instance-name routing-options]
```

## Description

You configure the graceful restart routing option globally to enable the feature, but not to enable graceful restart for all routing protocols in a routing instance. To enable graceful restart globally, include the graceful-restart statement under the [edit routing options] hierarchy level. This enables graceful restart globally for all routing protocols. You can, optionally, modify the global settings at the individual protocol level.

### NOTE:

- For VPNs, the graceful-restart statement allows a router whose VPN control plane is undergoing a restart to continue to forward traffic while recovering its state from neighboring routers.
- For BGP, if you configure graceful restart after a BGP session has been established, the BGP session restarts and the peers negotiate graceful restart capabilities.

- LDP sessions flap when graceful-restart configurations change.

## Default

Graceful restart is disabled by default.

## Options

The remaining statements are explained separately. See [CLI Explorer](#).

## Required Privilege Level

routing—To view this statement in the configuration.

routing-control—To add this statement to the configuration.

## Release Information

Statement introduced before Junos OS Release 7.4.

## RELATED DOCUMENTATION

---

[Enabling Graceful Restart](#)

---

[Configuring Routing Protocols Graceful Restart](#)

---

[Configuring Graceful Restart for MPLS-Related Protocols](#)

---

[Configuring VPN Graceful Restart](#)

---

[Configuring Logical System Graceful Restart](#)

---

[Configuring Graceful Restart for QFabric Systems](#)

## graceful-restart (Multicast Snooping)

### IN THIS SECTION

- [Syntax | 1006](#)
- [Hierarchy Level | 1006](#)
- [Description | 1006](#)
- [Default | 1006](#)
- [Required Privilege Level | 1007](#)
- [Release Information | 1007](#)

### Syntax

```
graceful-restart {  
    disable;  
    restart-duration seconds;  
}
```

### Hierarchy Level

```
[edit multicast-snooping-options]
```

### Description

Establish the graceful restart duration for multicast snooping. You can set this value between 0 and 300 seconds. If you set the duration to 0, graceful restart is effectively disabled. Set this value slightly larger than the IGMP query response interval.

### Default

180 seconds



## Required Privilege Level

routing—To view this statement in the configuration.

routing-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 9.2.

## RELATED DOCUMENTATION

*Example: Configuring Multicast Snooping  
query-response-interval (Bridge Domains)*

## graceful-restart (Protocols BGP)

### IN THIS SECTION

- [Syntax | 1007](#)
- [Hierarchy Level | 1008](#)
- [Description | 1008](#)
- [Required Privilege Level | 1009](#)
- [Release Information | 1009](#)

## Syntax

```
graceful-restart {  
  disable;  
  restart-time seconds;  
  stale-routes-time seconds;  
}
```

## Hierarchy Level

```
[edit logical-systems logical-system-name protocols bgp],
[edit logical-systems logical-system-name protocols bgp group group-name],
[edit logical-systems logical-system-name protocols bgp group group-name neighbor address],
[edit protocols bgp],
[edit protocols bgp group group-name],
[edit protocols bgp group group-name neighbor address]
```

## Description

Configure graceful restart for BGP. Graceful restart allows a routing device undergoing a restart to inform its adjacent neighbors and peers of its condition. Graceful restart is disabled by default. However, helper mode, the ability to assist a neighboring router attempting a graceful restart, is enabled by default.

To configure the duration of the BGP graceful restart period, include the `restart-time` statement at the `[edit protocols bgp graceful-restart]` hierarchy level. To set the length of time the router waits to receive messages from restarting neighbors before declaring them down, include the `stale-routes-time` statement at the `[edit protocols bgp graceful-restart]` hierarchy level.

**NOTE:** If you configure graceful restart after a BGP session has been established, the BGP session restarts and the peers negotiate graceful restart capabilities.

Enable graceful restart mode for BGP (and other protocols) by configuring `graceful-restart` at the routing-options level. Note that you cannot enable graceful restart for specific protocols unless graceful restart is also enabled globally.

For example, this configuration is required to enable graceful restart:

```
routing-options {
  graceful-restart
}
```

If you want to disable graceful restart for some protocols, you can do this at the protocol's graceful-restart command. The following configuration along with the configuration above will keep graceful restart for all protocols but BGP.

```
protocols{
  bgp{
    graceful-restart; {
      disable;
    }
  }
}
```

The remaining statements are explained separately. See [CLI Explorer](#).

## Required Privilege Level

routing—To view this statement in the configuration.

routing-control—To add this statement to the configuration.

## Release Information

Statement introduced before Junos OS Release 7.4.

## RELATED DOCUMENTATION

[Configuring Graceful Restart Options for BGP](#)

[Configuring Graceful Restart for QFabric Systems](#)

[Junos OS High Availability User Guide](#)

## graceful-restart (Protocols OSPF)

### IN THIS SECTION

- [Syntax](#) | 1010
- [Hierarchy Level](#) | 1010
- [Description](#) | 1010

- Options | 1010
- Required Privilege Level | 1011
- Release Information | 1011

## Syntax

```
graceful-restart {
    disable;
    helper-disable (standard | restart-signaling | both);
    no-strict-lsa-checking;
    notify-duration seconds;
    restart-duration seconds;
}
```

## Hierarchy Level

```
[edit logical-systems logical-system-name protocols (ospf | ospf3)],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols
(ospf | ospf3)],
[edit protocols (ospf | ospf3)],
[edit routing-instances routing-instance-name protocols ospf]
```

## Description

Configure graceful restart for OSPF.

Graceful restart allows a routing device to restart with minimal effects to the network, and is enabled for all routing protocols at the [edit routing-options] hierarchy level.

## Options

<b>disable</b>	Disable graceful restart for OSPF.
<b>helper-disable</b> ( <b>standard</b>   <b>restart-</b>	Disable helper mode for graceful restart. When helper mode is disabled, a device cannot help a neighboring device that is attempting to restart. Beginning with Junos OS

**signaling|  
both)**

Release 11.4, you can configure restart signaling-based helper mode for OSPFv2 graceful restart configurations. The last committed statement takes precedence over the previously configured statement.

- `standard` disables helper mode for standard graceful restart (based on RFC 3623).
- `restart-signaling` disables helper mode for restart signaling-based graceful restart (based on RFC 4811, RFC 4812, and RFC 4813).
- `both` disables helper mode for both standard and restart signaling-based graceful restart.

Helper mode is enabled by default. For OSPFv2, both standard and restart-signaling based helper modes are enabled by default.

**no-strict-lsa-  
checking**

Disable strict OSPF link-state advertisement (LSA) checking to prevent the termination of graceful restart by a helping router. LSA checking is enabled by default.

**NOTE:** The `helper-disable` statement and the `no-strict-lsa-checking` statement cannot be configured at the same time. If you attempt to configure both statements at the same time, the routing device displays a warning message when you enter the `show protocols (ospf | ospf3)` command.

**notify-  
duration  
*seconds***

Estimated time needed to send out purged grace LSAs over all the interfaces. Range is 1 through 3600 seconds, and the default is 30 seconds.

**restart-  
duration  
*seconds***

Estimated time needed to reacquire a full OSPF neighbor from each area. Range is 1 through 3600 seconds, and the default is 180 seconds.

**Required Privilege Level**

routing—To view this statement in the configuration.

routing-control—To add this statement to the configuration.

**Release Information**

Statement introduced before Junos OS Release 7.4.

Support for the `no-strict-lsa-checking` statement introduced in Junos OS Release 8.5.

Support for the helper mode `standard`, `restart-signaling`, and `both` options introduced in Junos OS Release 11.4.

## RELATED DOCUMENTATION

*Example: Configuring Graceful Restart for OSPF*

*Example: Configuring the Helper Capability Mode for OSPFv2 Graceful Restart*

*Example: Configuring the Helper Capability Mode for OSPFv3 Graceful Restart*

*Example: Disabling Strict LSA Checking for OSPF Graceful Restart*

## helper-disable (Multiple Protocols)

### IN THIS SECTION

- [Syntax | 1012](#)
- [Hierarchy Level | 1012](#)
- [Description | 1013](#)
- [Default | 1013](#)
- [Required Privilege Level | 1013](#)
- [Release Information | 1013](#)

### Syntax

```
helper-disable;
```

### Hierarchy Level

```
[edit logical-systems logical-system-name protocols (isis | ldp | ospf | ospf3 | rsvp) graceful-  
restart],  
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols (ldp  
| ospf | ospf3) graceful-restart],  
[edit protocols (isis | ldp | ospf | ospf3 | rsvp) graceful-restart],  
[edit routing-instances routing-instance-name protocols (ldp | ospf | ospf3) graceful-restart]
```

## Description

Disable helper mode for graceful restart. When helper mode is disabled, a router or switch cannot help a neighboring router that is attempting to restart.

## Default

Helper mode is enabled by default for these supported protocols: IS-IS, LDP, OSPF/OSPFv3, and RSVP.

## Required Privilege Level

routing—To view this statement in the configuration.

routing-control—To add this statement to the configuration.

## Release Information

Statement introduced before Junos OS Release 7.4.

## RELATED DOCUMENTATION

[Configuring Graceful Restart for Routing Protocols | 359](#)

[Configuring Graceful Restart for MPLS-Related Protocols](#)

## kernel-replication

### IN THIS SECTION

- [Syntax | 1014](#)
- [Hierarchy Level | 1014](#)
- [Description | 1014](#)
- [Options | 1014](#)
- [Required Privilege Level | 1014](#)
- [Release Information | 1014](#)

## Syntax

```
kernel-replication {
  no-multithreading;
  system-reboot recovery-failure;
}
```

## Hierarchy Level

```
[edit system]
```

## Description

Configure kernel replication. Use this configuration statement to debug the kernel synchronization process (ksyncd) and configure automatic recovery from ksyncd initialization errors.

## Options

<b>no-multithreading</b>	-(Optional) Run ksyncd in single thread mode for debugging purposes.
<b>system-reboot recovery-failure</b>	-(Optional) Configure the backup RE to automatically reboot if a ksyncd initialization error is detected.

## Required Privilege Level

system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 17.2R1.

## RELATED DOCUMENTATION

Understanding Graceful Routing Engine Switchover

[show system switchover](#) | 1526



## maximum-helper-recovery-time

### IN THIS SECTION

- [Syntax | 1015](#)
- [Hierarchy Level | 1015](#)
- [Description | 1015](#)
- [Options | 1015](#)
- [Required Privilege Level | 1016](#)
- [Release Information | 1016](#)

### Syntax

```
maximum-helper-recovery-time seconds;
```

### Hierarchy Level

```
[edit protocols rsvp graceful-restart],  
[edit logical-systems logical-system-name protocols rsvp graceful-restart]
```

### Description

Specify the length of time the router or switch retains the state of its Resource Reservation Protocol (RSVP) neighbors while they undergo a graceful restart.

### Options

***seconds***—Length of time that the router retains the state of its Resource Reservation Protocol (RSVP) neighbors while they undergo a graceful restart.

- **Range:** 1 through 3600
- **Default:** 180

## Required Privilege Level

routing—To view this statement in the configuration.

routing-control—To add this statement to the configuration.

## Release Information

Statement introduced before Junos OS Release 7.4.

## RELATED DOCUMENTATION

Configuring Graceful Restart Options for RSVP, CCC, and TCC

*maximum-helper-restart-time (RSVP)*

## maximum-helper-restart-time (RSVP)

### IN THIS SECTION

- [Syntax | 1016](#)
- [Hierarchy Level | 1017](#)
- [Description | 1017](#)
- [Options | 1017](#)
- [Required Privilege Level | 1017](#)
- [Release Information | 1017](#)

## Syntax

```
maximum-helper-restart-time seconds;
```

## Hierarchy Level

```
[edit protocols rsvp graceful-restart],  
[edit logical-systems logical-system-name protocols rsvp graceful-restart]
```

## Description

Specify the length of time the router or switch waits after it discovers that a neighboring router has gone down before it declares the neighbor down. This value is applied to all RSVP neighbor routers and should be based on the time that the slowest RSVP neighbor requires for restart.

## Options

***seconds***—The time the router or switch waits after it discovers that a neighboring router has gone down before it declares the neighbor down.

- **Range:** 1 through 1800
- **Default:** 60

## Required Privilege Level

routing—To view this statement in the configuration.

routing-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 8.3.

## RELATED DOCUMENTATION

Configuring Graceful Restart Options for RSVP, CCC, and TCC

*maximum-helper-recovery-time*

## maximum-neighbor-reconnect-time

### IN THIS SECTION

- [Syntax | 1018](#)
- [Hierarchy Level | 1018](#)
- [Description | 1018](#)
- [Options | 1018](#)
- [Required Privilege Level | 1018](#)
- [Release Information | 1019](#)

### Syntax

```
maximum-neighbor-reconnect-time seconds;
```

### Hierarchy Level

```
[edit protocols ldp graceful-restart],  
[edit logical-systems logical-system-name protocols ldp graceful-restart],  
[edit routing-instances routing-instance-name protocols ldp graceful-restart]
```

### Description

Specify the maximum length of time allowed to reestablish connection from a restarting neighbor.

### Options

*seconds*—Maximum time allowed for reconnection.

- **Range:** 30 through 300

### Required Privilege Level

routing—To view this statement in the configuration.

routing-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 9.1.

## RELATED DOCUMENTATION

Configuring Graceful Restart Options for LDP

## maximum-neighbor-recovery-time

### IN THIS SECTION

- [Syntax | 1019](#)
- [Hierarchy Level | 1019](#)
- [Description | 1020](#)
- [Options | 1020](#)
- [Required Privilege Level | 1020](#)
- [Release Information | 1020](#)

## Syntax

```
maximum-neighbor-recovery-time seconds;
```

## Hierarchy Level

```
[edit logical-systems logical-system-name protocols ldp graceful-restart],  
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols  
  ldp graceful-restart],
```

```
[edit protocols ldp graceful-restart],  
[edit routing-instances routing-instance-name protocols ldp graceful-restart]
```

## Description

Specify the maximum amount of time to wait before giving up an attempt to gracefully restart.

## Options

*seconds*—Configure the maximum recovery time, in seconds.

- **Range:** 120 through 1800 seconds
- **Default:** 140 seconds

## Required Privilege Level

routing—To view this statement in the configuration.

routing-control—To add this statement to the configuration.

## Release Information

Statement introduced before Junos OS Release 7.4. Statement changed from *maximum-recovery-time* to *maximum-neighbor-recovery-time* in Junos OS Release 9.1.

## RELATED DOCUMENTATION

---

*Configuring Recovery Time and Maximum Recovery Time*

---

Configuring Graceful Restart Options for LDP

---

[recovery-time](#) | **1023**

## not-on-disk-underperform

### IN THIS SECTION

- [Syntax | 1021](#)
- [Hierarchy Level | 1021](#)
- [Description | 1021](#)
- [Required Privilege Level | 1021](#)
- [Release Information | 1022](#)

### Syntax

```
not-on-disk-underperform;
```

### Hierarchy Level

```
[edit chassis redundancy failover]
```

### Description

Prevent gstatd from causing failovers in dual Routing Engines set for graceful Routing Engine switchover (GRES). The gstatd log message is still generated. This is an optional configuration.

**NOTE:** Configure the disk-write-threshold and disk-read-threshold statements to customize the gstatd timeout threshold.

### Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 13.3R6.

## RELATED DOCUMENTATION

Preventing Graceful Routing Engine Switchover in the Case of Slow Disks

## reconnect-time

### IN THIS SECTION

- [Syntax | 1022](#)
- [Hierarchy Level | 1022](#)
- [Description | 1023](#)
- [Options | 1023](#)
- [Required Privilege Level | 1023](#)
- [Release Information | 1023](#)

## Syntax

```
reconnect-time seconds;
```

## Hierarchy Level

```
[edit logical-systems logical-system-name protocols ldp graceful-restart],  
[edit protocols ldp graceful-restart],  
[edit routing-instances routing-instance-name protocols ldp graceful-restart]
```



## Description

Specify the length of time required to reestablish a Label Distribution Protocol (LDP) session after graceful restart.

## Options

*seconds*—Time required for reconnection.

- **Range:** 30 through 300
- **Default:** 60 seconds

## Required Privilege Level

routing—To view this statement in the configuration.

routing-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 9.1.

## RELATED DOCUMENTATION

*Configuring LDP Graceful Restart*

[MPLS Applications User Guide](#)

Configuring Graceful Restart Options for LDP

## recovery-time

### IN THIS SECTION

- [Syntax | 1024](#)
- [Hierarchy Level | 1024](#)
- [Description | 1024](#)

- Options | 1024
- Required Privilege Level | 1024
- Release Information | 1025

## Syntax

```
recovery-time seconds;
```

## Hierarchy Level

```
[edit logical-systems logical-system-name protocols ldp graceful-restart],  
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols ldp  
graceful-restart],  
[edit protocols ldp graceful-restart],  
[edit routing-instances routing-instance-name protocols ldp graceful-restart]
```

## Description

Specify the length of time a router or switch waits for Label Distribution Protocol (LDP) neighbors to assist it with a graceful restart.

## Options

***seconds***—Time the router waits for LDP to restart gracefully.

- **Range:** 120 through 1800
- **Default:** 160

## Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

## Release Information

Statement introduced before Junos OS Release 7.4.

## RELATED DOCUMENTATION

Configuring Graceful Restart Options for LDP

*maximum-neighbor-recovery-time*

## restart-duration

### IN THIS SECTION

- [Syntax | 1025](#)
- [Hierarchy Level | 1025](#)
- [Description | 1026](#)
- [Options | 1026](#)
- [Required Privilege Level | 1027](#)
- [Release Information | 1027](#)

## Syntax

```
restart-duration seconds;
```

## Hierarchy Level

```
[edit logical-systems logical-system-name protocols (isis | ospf | ospf3 | pim) graceful-restart],  
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols  
(ospf | ospf3 | pim) graceful-restart],  
[edit protocols (esis | isis | ospf | ospf3 | pim) graceful-restart],
```

```
[edit routing-instances routing-instance-name protocols (ospf | ospf3 | pim) graceful-restart],
[edit routing-options graceful-restart]
```

## Description

Configure the grace period for graceful restart globally.

Additionally, you can individually configure the duration of the graceful restart period for the End System-to-Intermediate System (ES-IS), Intermediate System-to-Intermediate System (IS-IS), Open Shortest Path First (OSPF), and OSPFv3 protocols and for Protocol Independent Multicast (PIM) sparse mode.

## Options

***seconds***—Time for the graceful restart period.

Range:

- The range of values varies according to whether the graceful restart period is being set globally or for a particular protocol:
  - [edit routing-options graceful-restart] (global setting)—120 through 900
  - ES-IS—30 through 300
  - IS-IS—30 through 300
  - OSPF/OSPFv3—1 through 3600
  - PIM—30 through 300

Default:

- The default value varies according to whether the graceful restart period is being set globally or for a particular protocol:
  - [edit routing-options graceful-restart] (global setting)—300
  - ES-IS—180
  - IS-IS—210
  - OSPF/OSPFv3—180
  - PIM—60

## Required Privilege Level

routing—To view this statement in the configuration.

routing-control—To add this statement to the configuration.

## Release Information

Statement introduced before Junos OS Release 7.4.

## RELATED DOCUMENTATION

Enabling Graceful Restart

Configuring Graceful Restart for MPLS-Related Protocols

Configuring VPN Graceful Restart

*Configuring Graceful Restart for VPNs*

Configuring Logical System Graceful Restart

## restart-time (BGP Graceful Restart)

### IN THIS SECTION

- [Syntax | 1027](#)
- [Hierarchy Level | 1028](#)
- [Description | 1028](#)
- [Options | 1028](#)
- [Required Privilege Level | 1028](#)
- [Release Information | 1028](#)

## Syntax

```
restart-time seconds;
```

## Hierarchy Level

```
[edit protocols (bgp | rip | ripng) graceful-restart],
[edit logical-systems logical-system-name protocols (bgp | rip | ripng) graceful-restart (Enabling Globally)],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp graceful-restart],
[edit routing-instances routing-instance-name protocols bgp graceful-restart]
```

## Description

Configure the duration of the BGP, RIP, or next-generation RIP (RIPng) graceful restart period.

## Options

***seconds***—Length of time for the graceful restart period.

- **Range:** Varies by protocol
  - BGP— 1 through 1800 seconds
  - RIP — 1 through 600 seconds
- **Default:** Varies by protocol:
  - BGP—120 seconds
  - RIP and RIPng—60 seconds

## Required Privilege Level

routing—To view this statement in the configuration.

routing-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 8.3.

## RELATED DOCUMENTATION

[Configuring Graceful Restart Options for BGP | 361](#)

[Configuring Graceful Restart Options for RIP and RIPng | 366](#)

[Configuring Graceful Restart for QFabric Systems](#)

*stale-routes-time*

## stale-routes-time

### IN THIS SECTION

- [Syntax | 1029](#)
- [Hierarchy Level | 1029](#)
- [Description | 1030](#)
- [Options | 1030](#)
- [Required Privilege Level | 1030](#)
- [Release Information | 1030](#)

## Syntax

```
stale-routes-time seconds;
```

## Hierarchy Level

```
[edit logical-systems logical-routing-name protocols bgp graceful-restart],  
[edit logical-systems logical-routing-name routing-instances routing-instance-name protocols bgp  
graceful-restart],  
[edit protocols bgp graceful-restart],  
[edit routing-instances routing-instance-name protocols bgp graceful-restart]
```

## Description

Specify the maximum time that stale routes are kept during a restart. The `stale-routes-time` statement allows you to set the length of time the routing device waits to receive messages from restarting neighbors before declaring them down.

## Options

***seconds***—Time the router device waits to receive messages from restarting neighbors before declaring them down.

- **Range:** 1 through 600 seconds
- **Default:** 300 seconds

## Required Privilege Level

routing—To view this statement in the configuration.

routing-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 8.3.

## RELATED DOCUMENTATION

[Configuring Graceful Restart Options for BGP | 361](#)

[Configuring Graceful Restart for QFabric Systems](#)

*restart-time (BGP Graceful Restart)*

## traceoptions (Protocols)

### IN THIS SECTION

- [Syntax | 1031](#)
- [Hierarchy Level | 1031](#)



- [Description | 1031](#)
- [Default | 1031](#)
- [Options | 1031](#)
- [Required Privilege Level | 1032](#)
- [Release Information | 1033](#)

## Syntax

```
traceoptions {
    file name <size size> <files number> <world-readable | no-world-readable>;
    flag flag <flag-modifier> <disable>;
}
```

## Hierarchy Level

```
[edit protocols isis],
[edit protocols (ospf | ospf3)]
```

## Description

Define tracing operations that graceful restart functionality in the router or switch.

To specify more than one tracing operation, include multiple `flag` statements.

## Default

If you do not include this statement, no global tracing operations are performed.

## Options

**disable**—(Optional) Disable the tracing operation. You can use this option to disable a single operation when you have defined a broad group of tracing operations, such as **all**.

**file *name***—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory **/var/log**. We recommend that you place global routing protocol tracing output in the file **routing-log**.

**files *number***—(Optional) Maximum number of trace files. When a trace file named ***trace-file*** reaches its maximum size, it is renamed ***trace-file.0***, then ***trace-file.1***, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

- **Range:** 2 through 1000 files
- **Default:** 2 files

If you specify a maximum number of files, you also must specify a maximum file size with the **size** option.

**flag *flag***—Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements. The nonstop active routing tracing option is:

- **graceful-restart**—Tracing operations for nonstop active routing

**no-world-readable**—Restrict users from reading the log file.

**size *size***—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named ***trace-file*** reaches this size, it is renamed ***trace-file.0***. When the ***trace-file*** again reaches its maximum size, ***trace-file.0*** is renamed ***trace-file.1*** and ***trace-file*** is renamed ***trace-file.0***. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

- **Syntax:** ***xk*** to specify KB, ***xm*** to specify MB, or ***xg*** to specify GB
- **Range:** 10 KB through the maximum file size supported on your system
- **Default:** 128 KB

If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option.

**world-readable**—Allow users to read the log file.

## Required Privilege Level

routing and trace—To view this statement in the configuration.

routing-control and trace-control—To add this statement to the configuration.

## Release Information

Statement introduced before Junos OS Release 7.4.

**graceful-restart** flag for IS-IS and OSPF/OSPFv3 added in Junos OS Release 8.4.

## RELATED DOCUMENTATION

| [Tracking Graceful Restart Events](#) | 367

## warm-standby

### IN THIS SECTION

- [Syntax](#) | 1033
- [Hierarchy Level](#) | 1033
- [Description](#) | 1033
- [Required Privilege Level](#) | 1034
- [Release Information](#) | 1034

## Syntax

```
warm-standby;
```

## Hierarchy Level

```
[edit routing-options]
```

## Description

Set the routing protocols process (rpd) mode to warm standby. Warm standby mode helps the backup RE stay synchronized with the primary RE, allowing for faster RE switchover during GRES.

## Required Privilege Level

routing—To view this statement in the configuration.

routing-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 17.2R1.

Statement introduced in Junos OS Evolved Release 21.2R1.

## RELATED DOCUMENTATION

| [Understanding Graceful Routing Engine Switchover](#)

# Configuration Statements: Multinode High Availability

## IN THIS CHAPTER

- [activeness-probe](#) | 1035
- [hardware-upgrade](#) | 1037
- [high-availability \(Chassis\)](#) | 1039
- [high-availability \(security cloud\)](#) | 1042
- [liveness-detection \(high availability\)](#) | 1043
- [local-id](#) | 1046
- [managed-services](#) | 1048
- [peer-id](#) | 1049
- [monitor \(Multinode High Availability\)](#) | 1051
- [services-redundancy-group](#) | 1053
- [software-upgrade](#) | 1058
- [traceoptions](#) | 1059
- [virtual-ip](#) | 1062

## activeness-probe

## IN THIS SECTION

- [Syntax](#) | 1036
- [Hierarchy Level](#) | 1036
- [Description](#) | 1036
- [Options](#) | 1036

- Required Privilege Level | 1037
- Release Information | 1037

## Syntax

```
activeness-probe {  
  dest-ip {  
    ip-address;  
    routing-instance routing-instance;  
    src-ip src-ip;  
    minimal-interval milliseconds;  
    multiplier number;  
  }  
}
```

## Hierarchy Level

```
[edit chassis high-availability services-redundancy-group]
```

## Description

Specify the probe destination IP details for activeness determination.

## Options

**activeness-probe**

- `dest-ip ip-address`—Destination IP address to send the probe requests.
- `routing-instance name`—Routing instance used by the probe requests.
- `src-ip ip-address`—Source IP address to send the probe requests.

minimal-interval *milliseconds*—(Optional) Time period between the probes sent to the destination IP address. You can configure 1000 milliseconds for minimal interval activeness probes. (supported in default gateway [switching] and hybrid deployments).

multiplier *number*—(Optional) Time period, after which the backup node transitions to the active state, if the backup node fails to receive response to the activeness-probes from the peer node. (supported in default gateway [switching] and hybrid deployments).

- **Range:** 2 through 15

## Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 22.3R1

## RELATED DOCUMENTATION

[Example: Configure Multinode High Availability in a Layer 3 Network](#) | 672

## hardware-upgrade

### IN THIS SECTION

- [Syntax](#) | 1038
- [Hierarchy Level](#) | 1038
- [Description](#) | 1038
- [Required Privilege Level](#) | 1038
- [Release Information](#) | 1038

## Syntax

```
hardware-upgrade
```

## Hierarchy Level

```
[edit chassis high-availability]
```

## Description

Install an additional SPC3 card in a Multinode High Availability statement. Use this statement when you insert an additional SPC3 on an SRX5000-line device in Multinode High Availability and has an interchassis link (ICL) in encryption mode. You must run the command on both nodes in Multinode High Availability before you start SPC3 installation.

Once you complete the installation, and both nodes are online, delete the statement on both nodes using the command `delete chassis high-availability hardware-upgrade`.

## Required Privilege Level

interface

## Release Information

Statement introduced in Junos OS Release 22.2R1.

## RELATED DOCUMENTATION

| [Hardware Upgrade for SRX5000-Line SPC3 in a Multinode High Availability Setup](#)



## high-availability (Chassis)

### IN THIS SECTION

- [Syntax | 1039](#)
- [Hierarchy Level | 1041](#)
- [Description | 1041](#)
- [Options | 1041](#)
- [Required Privilege Level | 1041](#)
- [Release Information | 1041](#)

### Syntax

```
high-availability {
  local-id id local-ip local-ip;
  peer-id name {
    desc desc;
    interface interface;
    liveness-detection {
      no-adaptation;
      detection-time {
        threshold milliseconds;
      }
      minimum-interval milliseconds;
      minimum-receive-interval milliseconds;
      multiplier multiplier;
      transmit-interval {
        minimum-interval milliseconds;
        threshold milliseconds;
      }
      version (0 | 1 | automatic);
    }
    peer-ip peer-ip;
    routing-instance routing-instance;
    vpn-profile vpn-profile;
  }
  services-redundancy-group name {
```

```

    active-signal-route {
        ip-address;
        routing-instance routing-instance;
    }
    activeness-priority activeness-priority;
    activeness-probe {
        dest-ip {
            ip-address;
            routing-instance routing-instance;
        }
    }
    backup-signal-route {
        ip-address;
        routing-instance routing-instance;
    }
    monitor {
        bfd-liveliness name {
            interface interface;
            routing-instance routing-instance;
            session-type (multihop | singlehop);
            src-ip src-ip;
        }
        ip name {
            routing-instance routing-instance;
        }
    }
    peer-id id;
    process-packet-on-backup;
    shutdown-on-failure name;
}
traceoptions {
    file <filename> <files files> <match match> <size size> <(world-readable | no-world-readable)>;
    flag name;
    level (alert | all | critical | debug | emergency | error | info | notice | warning);
    no-remote-trace;
}
}

```

Hierarchy Level

[edit chassis]

Description

Configure Multinode High Availability options on SRX Series devices.

Options

<a href="#">"local-id" on page 1046</a>	Define local node identifier.
<a href="#">"peer-id" on page 1049</a>	Define peer node related information.
<a href="#">"services-redundancy-group" on page 1053</a>	Define the services redundancy group details.
<a href="#">"traceoptions" on page 1059</a>	Define high availability traceoptions.

Required Privilege Level

interface

Release Information

Statement introduced in Junos OS Release 20.4R1.

RELATED DOCUMENTATION

<a href="#">Multinode High Availability   613</a>
<a href="#">Example: Configure Multinode High Availability in a Layer 3 Network   672</a>
<a href="#">Example: Configure Multinode High Availability in a Default Gateway Deployment   717</a>
<a href="#">Example: Configure Multinode High Availability in a Hybrid Deployment   752</a>

## high-availability (security cloud)

### IN THIS SECTION

- [Syntax | 1042](#)
- [Hierarchy Level | 1042](#)
- [Description | 1043](#)
- [Options | 1043](#)
- [Required Privilege Level | 1043](#)
- [Release Information | 1043](#)

### Syntax

```
high-availability {  
    aws {  
        eip-based;  
        peer-liveliness {  
            probe-ip {  
                destination-ip-address;  
                routing-instance instance-name;  
                source-ip source-ip-address;  
            }  
        }  
    }  
}
```

### Hierarchy Level

[edit security cloud]

## Description

Configure vSRX instances to work in Multinode High Availability mode with Amazon Web Services (AWS).

## Options

aws—Define deployment type as Amazon Web Server (AWS)

- EIP-based—Deployment type based on EIP.
- peer-liveness—Configure activeness probe options.
  - probe-ip *destination-ip*—IP address for activeness probe configuration. Specify destination IP address (of upstream router) for probing.
  - routing-instance—Routing-instance name.
  - source-ip—Source IP address to initiate probes.

## Required Privilege Level

interface

## Release Information

Statement introduced in Junos OS Release 22.3R1.

## RELATED DOCUMENTATION

[Multinode High Availability Support for vSRX Instances in Public Cloud Deployments](#) | 908

## liveness-detection (high availability)

### IN THIS SECTION

● [Syntax](#) | 1044

- [Hierarchy Level | 1044](#)
- [Description | 1044](#)
- [Options | 1045](#)
- [Required Privilege Level | 1046](#)
- [Release Information | 1046](#)

## Syntax

```
liveness-detection {  
    detection-time {  
        threshold milliseconds;  
    }  
    minimum-interval milliseconds;  
    minimum-receive-interval milliseconds;  
    multiplier multiplier;  
    transmit-interval {  
        minimum-interval milliseconds;  
        threshold milliseconds;  
    }  
    version (0 | 1 | automatic);  
}
```

## Hierarchy Level

```
[edit chassis high-availability peer-id]
```

## Description

Configure Bidirectional Forwarding Detection (BFD) options for the peer node.

## Options

<b>detection-time</b>	<p>Specify BFD failure detection time.</p> <ul style="list-style-type: none"> <li>threshold—Specify the threshold for the adaptation of the BFD session detection time. When the detection time adapts to a value equal to or greater than the threshold, a single trap and a single system log message are sent.</li> </ul> <p>Range: 1 through 255,000 milliseconds</p>
<b>minimum-interval</b>	<p>Configure the minimum interval at which the device transmits hello packets and then expects to receive a reply from a neighbor with which it has established a BFD session</p> <ul style="list-style-type: none"> <li>Range: 1 through 255,000 milliseconds</li> </ul>
<b>minimum-receive-interval</b>	<p>(Optional) Configure the minimum interval after which the local device must receive a reply from a neighbor with which it has established a BFD session.</p> <ul style="list-style-type: none"> <li>Range: 1 through 255,000 milliseconds</li> </ul>
<b>multiplier</b>	<p>(Optional) Configure the number of hello packets not received by a neighbor that causes the originating interface to be declared down.</p> <ul style="list-style-type: none"> <li>Range: 1 through 255</li> <li>Default: 3</li> </ul>
<b>transmit-interval</b>	<p>The negotiated transmit interval for a peer is the interval between the sending of BFD packets to peers. The receive interval for a peer is the minimum time that it requires between packets sent from its peer; the receive interval is not negotiated between peers.</p> <ul style="list-style-type: none"> <li>minimum-interval <i>milliseconds</i>—Configure the minimum interval at which the local routing device transmits hello packets to a neighbor with which it has established a BFD session. <ul style="list-style-type: none"> <li>Range: 1 through 255</li> </ul> </li> <li>threshold <i>milliseconds</i>—Specify the threshold for the adaptation of the BFD session transmit interval. When the transmit interval adapts to a value greater than the threshold, a single trap and a single system message are sent. <ul style="list-style-type: none"> <li>Range: 0 through 4,294,967,295 (<math>2^{32} - 1</math>)</li> </ul> </li> </ul> <p>The threshold value specified in the threshold statement must be greater than the value specified in the minimum-interval statement for the transmit-interval statement.</p>
<b>version</b>	BFD protocol version number

- 0—BFD version 0 (deprecated)
- 1—BFD version 1
- automatic—Choose BFD version automatically

The remaining statements are explained separately. See [CLI Explorer](#).

## Required Privilege Level

interface

## Release Information

Statement introduced in Junos OS Release 20.4R1.

## RELATED DOCUMENTATION

[Multinode High Availability | 613](#)

[Example: Configure Multinode High Availability in a Layer 3 Network | 672](#)

## local-id

### IN THIS SECTION

- [Syntax | 1047](#)
- [Hierarchy Level | 1047](#)
- [Description | 1047](#)
- [Options | 1047](#)
- [Required Privilege Level | 1047](#)
- [Release Information | 1047](#)



Syntax

```
local-id id-number local-ip ip-address
```

Hierarchy Level

```
[edit chassis high-availability]
```

Description

Configure the local node identifier for Multinode High Availability.

Options

- id

Local identifier number

- Range: 1 through 10
- local-ip

Local IPv4 address

Required Privilege Level

interface

Release Information

Statement introduced in Junos OS Release 20.4R1.

RELATED DOCUMENTATION

<a href="#">Multinode High Availability   613</a>
<a href="#">Example: Configure Multinode High Availability in a Layer 3 Network   672</a>

## managed-services

### IN THIS SECTION

- [Syntax | 1048](#)
- [Hierarchy Level | 1048](#)
- [Description | 1048](#)
- [Options | 1048](#)
- [Required Privilege Level | 1049](#)
- [Release Information | 1049](#)

### Syntax

```
managed-services name;
```

### Hierarchy Level

```
[edit chassis high-availability services-redundancy-group]
```

### Description

Enable set of services for the specified services redundancy group (SRG).

You can selectively and flexibly associate a service such as IPsec VPN to one of multiple SRGs configured on SRX Series firewall in a Multinode High Availability setup.

### Options

- name**
- ipsec—IPsec VPN Service

## Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 22.4R1.

## peer-id

### IN THIS SECTION

- [Syntax | 1049](#)
- [Hierarchy Level | 1050](#)
- [Description | 1050](#)
- [Options | 1050](#)
- [Required Privilege Level | 1050](#)
- [Release Information | 1051](#)

## Syntax

```
peer-id name {  
    desc desc;  
    interface interface;  
    liveness-detection {  
        no-adaptation;  
        detection-time {  
            threshold milliseconds;  
        }  
        minimum-interval milliseconds;  
        minimum-receive-interval milliseconds;  
        multiplier multiplier;  
        transmit-interval {
```

```
        minimum-interval milliseconds;  
        threshold milliseconds;  
    }  
    version (0 | 1 | automatic);  
}  
peer-ip peer-ip;  
routing-instance routing-instance;  
vpn-profile vpn-profile;  
}
```

Hierarchy Level

[edit chassis high-availability]

Description

Configure the other node related information in a Multinode High Availability setup.

Options

ID	Peer node identifier.
desc	Peer node description.
interface	Name of the interface used for communicating with the peer node using the interchassis link (ICL.
<a href="#">"liveness-detection" on page 1043</a>	Liveness detection options for the peer node.
peer-ip	IPv4 address of the peer node.
routing-instance	Routing instance to locate the peer node route.
vpn-profile	VPN profile name for ICL encryption. You must configure a VPN profile for the HA traffic and apply the profile for both the nodes.

Required Privilege Level

interface

## Release Information

Statement introduced in Junos OS Release 20.4R1.

## RELATED DOCUMENTATION

[Multinode High Availability | 613](#)

[Example: Configure Multinode High Availability in a Layer 3 Network | 672](#)

## monitor (Multinode High Availability)

### IN THIS SECTION

- [Syntax | 1051](#)
- [Hierarchy Level | 1052](#)
- [Description | 1052](#)
- [Options | 1052](#)
- [Required Privilege Level | 1052](#)
- [Release Information | 1053](#)

## Syntax

```
monitor {  
  bfd-liveliness destination-ip-address {  
    interface interface-name;  
    routing-instance routing-instance-name;  
    session-type (multihop | singlehop);  
    src-ip src-ip;  
  }  
  interface name;  
  ip destination-ip-address {  
    routing-instance routing-instance-name;
```

```
}
}
```

## Hierarchy Level

```
[edit chassis high-availability services-redundancy-group id-number]
```

## Description

Configure monitoring options for the Multinode High Availability setup.

## Options

**bfd-liveliness** Configure Bidirectional Forwarding Detection (BFD) monitoring to detect failures in a network. You can configure Multinode High Availability to monitor one or more links using BFD. This configuration triggers a failover in the event of BFD failure. Configure BFD liveliness by specifying source and destination IP and the interface where the peer device is directly connected to.

- **interface**—Name of the interface for single-hop sessions
- **routing-instance**—Routing instance to locate the route
- **session-type** —(Optional) Configure BFD session mode to be single-hop or multihop. By default, BGP uses single-hop BFD sessions if the peer is directly connected to the router's interface.
- **src-ip**—Source IPv4 or IPv6 address for activeness probe.

**interface**  
***interface-name*** Configure interface monitoring for SRG. The node which detects the interface monitoring failure transitions to ineligible state for the corresponding SRG and the other node (if healthy) takes over the active role or that SRG and the subsequent GARP ensures traffic switching and recovery.

**ip destination-**  
***ip-address*** Configure IP monitoring. You can configure IP monitoring by specifying destination IP address (of upstream router) for probing.

## Required Privilege Level

interface

## Release Information

Statement introduced in Junos OS Release 20.4R1.

## RELATED DOCUMENTATION

[Multinode High Availability Monitoring | 645](#)

[Example: Configure Multinode High Availability in a Layer 3 Network | 672](#)

## services-redundancy-group

### IN THIS SECTION

- [Syntax | 1053](#)
- [Hierarchy Level | 1055](#)
- [Description | 1055](#)
- [Options | 1055](#)
- [Required Privilege Level | 1057](#)
- [Release Information | 1057](#)

## Syntax

```
services-redundancy-group name {  
  activeness-priority activeness-priority;  
  activeness-probe {  
    dest-ip {  
      ip-address;  
      routing-instance routing-instance;  
      src-ip src-ip;  
    }  
    minimum-interval minimum-interval;  
    multiplier multiplier;
```

```

}
active-signal-route {
    ip-address;mandatory
    routing-instance routing-instance;
}
backup-signal-route {
    ip-address;mandatory
    routing-instance routing-instance;
}
deployment-type(cloud | hybrid | routing | switching);
install-on-failure-route {
    ip-address;
    routing-instance routing-instance;
}
managed-services name;

monitor {
    bfd-liveliness name {
        interface interface;
        routing-instance routing-instance;
        session-type(multihop | singlehop);
        src-ip src-ip;
    }
    interface name;

    ip name {
        routing-instance routing-instance;
    }
}
peer-id id;mandatory
preemption;
prefix-list name {
    routing-instance routing-instance;
}
process-packet-on-backup;
shutdown-on-failure name;

virtual-ip name {
    interface interface;
    ip ip;mandatory
    use-virtual-mac;

```



```
}  
}
```

Hierarchy Level

```
[edit chassis high-availability]
```

Description

Configure a service redundancy group (SRG). An SRG includes and manages a collection of resources on both nodes of a Multinode High Availability and it fails over between the two devices. You can configure upto 20 SRGs in a Multinode Highavailability setup.

Options

name	Services redundancy group identifier. <ul style="list-style-type: none"><li>• <b>Range:</b> 0 through 20</li></ul>
active-signal-route	<p>IP address used for route preference advertisement. You must specify the active signal route along with the route-exists policy in the policy-options statement.</p> <p>Signal route required for active role enforcement. When you configure the active-signal-route with if-route-exists condition, the HA module adds this route to the routing table.</p> <ul style="list-style-type: none"><li>• ip-address—IP address for active signal route</li><li>• routing-instance—Routing instance of the active signal route.</li></ul>
activeness-priority	<p>Specify priority for the SRG1 in a node to take up the active role in a case where both nodes initialize at the same time. The node where SRG1 is in active state is considered as active node.</p> <p>If you prefer a certain node to take over as the active node on boot, you can do one of the followings:</p> <ul style="list-style-type: none"><li>• Configure the upstream routers to include preferences for the path where the node is located.</li></ul>

- Configure the activeness priority for SRG1 on the SRX Series device (higher activeness priority). You can configure a priority for each node. As long as the nodes can communicate with each other through the ICL, the priority is honored.
- Allow the node with higher node ID (in case above two options not configured) to take the active role.
- **Range:** 1 through 254

"activeness-probe" on page 1035

Specify the probe destination IP address for activeness determination.

**backup-signal-route**

Specify the backup signal route to advertise a route with a medium priority. When the HA link is down or the current active node relinquishes active role after any failure, the active signal route is removed from the routing table. The backup overwrites the default routing preference toward the old active node with the medium priority.

- *ip-address*—IP address for backup signal route
- *routing-instance*—Routing instance of the backup signal route.

**deployment-type**

Deployment type of the Services Redundancy Group.

- *cloud*—Cloud deployment
- *hybrid*—Hybrid deployment
- *routing*—Routing deployment
- *switching*—Switching/default gateway deployment

**install-on-failure-route**

Divert the traffic by changing the route in a Multinode High Availability setup during a software upgrade. In this case, traffic still traverses through the node and interface remains up.

- *ip-address*—IP address of the route. Multinode High Availability installs this route to divert the traffic during the upgrade.
- *routing-instance* *routing-instance*—Routing instance. You must create a dedicated custom virtual router for the route used for diverting traffic during the upgrade.

"managed-services " on page 1048

Enable set of services for the specified SRG.

"monitor" on page 1051

Specify to configure the BFD and IP monitoring options.

<b>peer-id</b>	Allows you to choose a specific peer when multiple HA peers are configured globally to the service redundancy group.
<b>preemption</b>	Allow preemption of activeness based on priority. When you configure the activeness priority (1-254) for the SRG1 and enable the preemptive behavior on both nodes, the preempt option ensures that the node with higher activeness priority always remains active after a failover.
<b>prefix-list</b>	Define a named set of address prefixes. Associate the IP prefix list to the SRG. A prefix list is a listing of IP prefixes that include the local address of IKE gateway. A prefix list is given a name and is configured within the [edit policy-options] configuration hierarchy.
<b>process-packet-on-backup</b>	Enable packet forward engine to forward packets on backup node for the corresponding service redundancy group. When you configure the process packet on back up option, the Packet Forwarding Engine forwards packets on backup node for the corresponding SRG. This configuration processes VPN packets on the backup node even when the node is not active.
<b>services</b>	Enable IPsec VPN service on a particular SRG.
<b>shutdown-on-failure</b>	Configure one or multiple Interfaces which are required to be shut down to isolate the node in case of internal failures or during software upgrades. During software upgrades, you can divert the traffic by closing down interfaces on the node.
<a href="#">"virtual-ip" on page 1062</a>	IP address used for activeness determination and enforcement on the switching side. Required for hybrid and default gateway deployments.

The remaining statements are explained separately. See [CLI Explorer](#).

## Required Privilege Level

interface

## Release Information

Statement introduced in Junos OS Release 20.4R1.

Multi SRG1s (SRG1+) support is added in Junos OS Release 22.4R1.

install-on-failure-route option is added in Junos OS Release 22.4R2.

## RELATED DOCUMENTATION

[Example: Configure Multinode High Availability in a Layer 3 Network | 672](#)

[Example: Configure Multinode High Availability in a Default Gateway Deployment | 717](#)

[Example: Configure Multinode High Availability in a Hybrid Deployment | 752](#)

## software-upgrade

### IN THIS SECTION

- [Syntax | 1058](#)
- [Hierarchy Level | 1058](#)
- [Description | 1058](#)
- [Required Privilege Level | 1059](#)
- [Release Information | 1059](#)

### Syntax

```
software-upgrade
```

### Hierarchy Level

```
[edit chassis high-availability]
```

### Description

Enable software upgrade mode. Use this configuration option when you want to upgrade your security device in Multinode High Availability. This statement marks SRG status as offline and diverts the transit traffic to the other node.

Once you complete the software upgrade, delete the statement on both nodes using the command `delete chassis high-availability software-upgrade`.

## Required Privilege Level

interface

## Release Information

Statement introduced in Junos OS Release 22.3R1.

## RELATED DOCUMENTATION

[Software Upgrade in Multinode High Availability | 885](#)

## traceoptions

### IN THIS SECTION

- [Syntax | 1059](#)
- [Hierarchy Level | 1060](#)
- [Description | 1060](#)
- [Options | 1060](#)
- [Required Privilege Level | 1061](#)
- [Release Information | 1061](#)

## Syntax

```
traceoptions {  
    file <filename> <files files> <match match> <size size> <(world-readable | no-world-readable)>;  
    flag name;  
    level (alert | all | critical | debug | emergency | error | info | notice | warning);  
    no-remote-trace;  
}
```

## Hierarchy Level

[edit chassis high-availability]

## Description

Set Multinode High Availability traceoptions

## Options

**file *filename***—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks

**file *name***—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory `/var/log`. We recommend that you place global routing protocol tracing output in the file **routing-log**.

**files *number***—(Optional) Maximum number of trace files. When a trace file named **trace-file** reaches its maximum size, it is renamed **trace-file.0**, then **trace-file.1**, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

- **Range:** 2 through 1000 files
- **Default:** 2 files

If you specify a maximum number of files, you also must specify a maximum file size with the **size** option.

**no-world-readable**—Restrict users from reading the log file.

**size *size***—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named **trace-file** reaches this size, it is renamed **trace-file.0**. When the **trace-file** again reaches its maximum size, **trace-file.0** is renamed **trace-file.1** and **trace-file** is renamed **trace-file.0**. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

- **Syntax:** **xk** to specify KB, **xm** to specify MB, or **xg** to specify GB
- **Range:** 10 KB through the maximum file size supported on your system
- **Default:** 128 KB

If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option.

**world-readable**—Allow users to read the log file.

**level**—Set a level of tracing.

- Values:
  - alert—Match alert conditions
  - all—Match all levels
  - critical—Match critical conditions
  - debug—Match debug messages
  - emergency—Match emergency conditions
  - error—Match error conditions
  - info—Match informational messages
  - notice—Match notice level messages
  - warning—Match warning messages

**no-remote-trace**—Disable remote tracing.

## Required Privilege Level

trace

## Release Information

Statement introduced in Junos OS Release 20.4R1.

## RELATED DOCUMENTATION

[Multinode High Availability](#) | 613

## virtual-ip

### IN THIS SECTION

- [Syntax | 1062](#)
- [Hierarchy Level | 1062](#)
- [Description | 1062](#)
- [Options | 1063](#)
- [Required Privilege Level | 1063](#)
- [Release Information | 1063](#)

### Syntax

```
virtual-ip name {  
    interface interface;  
    ip ip;  
    use-virtual-mac;  
}
```

### Hierarchy Level

```
[edit chassis high-availability services-redundancy-group]
```

### Description

Specify IP address used for activeness determination and enforcement on the switching side of Multinode High Availability deployments. Required for hybrid and default gateway deployments.



Options

<b>name</b>	Virtual IP Identifier.
<b>interface</b>	Name of the interface for virtual IP.
<b>ip</b>	IPV4/IPV6 prefix, should be in the same subnet as the interface IP
<b>use-virtual-mac</b>	Use virtual MAC (vMAC) address for services redundancy group role enforcement. Virtual MAC address dynamically assigned to the interface on active node that faces the switching side.

Required Privilege Level

- interface—To view this statement in the configuration.
- interface-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 22.3R1.

RELATED DOCUMENTATION

<a href="#">Multinode High Availability   613</a>
<a href="#">Example: Configure Multinode High Availability in a Default Gateway Deployment   717</a>

# Configuration Statements: Nonstop Active Routing

## IN THIS CHAPTER

- [nonstop-routing | 1064](#)
- [switchover-on-routing-crash | 1066](#)
- [synchronize | 1067](#)
- [traceoptions | 1069](#)

## nonstop-routing

## IN THIS SECTION

- [Syntax | 1064](#)
- [Hierarchy Level | 1065](#)
- [Description | 1065](#)
- [Default | 1065](#)
- [Required Privilege Level | 1065](#)
- [Release Information | 1065](#)

## Syntax

```
nonstop-routing;
```

## Hierarchy Level

[edit routing-options]

**NOTE:** Although nonstop-routing is also a valid keyword at the logical-systems hierarchy level, it is not supported.

## Description

For routing platforms with two Routing Engines, configure a primary Routing Engine to switch over gracefully to a backup Routing Engine and to preserve routing protocol information.

## Default

disabled

## Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 8.4.

## RELATED DOCUMENTATION

[Configuring Nonstop Active Routing](#) | 281

## switchover-on-routing-crash

### IN THIS SECTION

- [Syntax | 1066](#)
- [Hierarchy Level | 1066](#)
- [Description | 1066](#)
- [Required Privilege Level | 1066](#)
- [Release Information | 1067](#)

### Syntax

```
switchover-on-routing-crash;
```

### Hierarchy Level

```
[edit system]
```

### Description

Prevent loss of traffic in the case of NSR being configured. With the `switchover-on-routing-crash` configuration statement enabled, when `rpd` on the primary Routing Engine crashes with NSR configured, the Routing Engine will switch over immediately to the backup Routing Engine to preserve protocol state and adjacencies. Prior to having this statement, if NSR was configured and `rpd` on the primary Routing Engine crashed, it would cause network impact (protocol neighbor and adjacency drops and traffic loss).

### Required Privilege Level

`admin`—To view this statement in the configuration.

`admin-control`—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 13.3.

## RELATED DOCUMENTATION

[Configuring Nonstop Active Routing](#) | 281

# synchronize

## IN THIS SECTION

- [Syntax](#) | 1067
- [Hierarchy Level](#) | 1067
- [Description](#) | 1067
- [Options](#) | 1069
- [Required Privilege Level](#) | 1069
- [Release Information](#) | 1069

## Syntax

```
synchronize;
```

## Hierarchy Level

```
[edit system commit]
```

## Description

For devices with multiple Routing Engines only. Configure the `commit` command to automatically perform a `commit synchronize` action between dual Routing Engines within the same chassis. The Routing Engine on

which you execute the `commit` command (the requesting Routing Engine) copies and loads its candidate configuration to the other (the responding) Routing Engine. Each Routing Engine then performs a syntax check on the candidate configuration file being committed. If no errors are found, the configuration is activated and becomes the current operational configuration on both Routing Engines.

**NOTE:** If you configure the `commit synchronize` statement at the `[edit system]` hierarchy level and issue a `commit` in the primary Routing Engine, the primary configuration is automatically synchronized with the backup. However, if the backup Routing Engine is down when you issue the `commit`, the Junos OS displays a warning and commits the candidate configuration in the primary Routing Engine. When the backup Routing Engine comes up, its configuration will automatically be synchronized with the primary. A newly inserted backup Routing Engine automatically synchronizes its configuration with the primary Routing Engine configuration.

**NOTE:** When you configure nonstop active routing (NSR), you must configure the `commit synchronize` statement. Otherwise, the `commit` operation fails.

**NOTE:** Starting in Junos OS Release 20.2R1, when the `commit synchronize` statement is configured and the backup Routing Engine synchronizes its configuration with the primary Routing Engine, for example, when it is newly inserted, brought back online, or during a change in primary role, it also synchronizes the ephemeral configuration database.

On the TX Matrix router, synchronization only occurs between the Routing Engines within the same chassis. When synchronization is complete, the new configuration is then distributed to the Routing Engines on the T640 routers. That is, the primary Routing Engine on the TX Matrix router distributes the configuration to the primary Routing Engine on each T640 router. Likewise, the backup Routing Engine on the TX Matrix router distributes the configuration to the backup Routing Engine on each T640 router.

On the TX Matrix Plus router, synchronization only occurs between the Routing Engines within the switch-fabric chassis and when synchronization is complete, the new configuration is then distributed to the Routing Engines on the line-card chassis (LCC). That is, the primary Routing Engine on the TX Matrix Plus router distributes the configuration to the primary Routing Engine on each LCC. Likewise, the backup Routing Engine on the TX Matrix Plus router distributes the configuration to the backup Routing Engine on each LCC.

In EX Series Virtual Chassis configurations:

- On EX4200 switches in Virtual Chassis, synchronization occurs between the switch in the primary role and the switch in the backup role.

- On EX8200 switches in a Virtual Chassis, synchronization occurs only between the primary and backup XRE200 External Routing Engines.

## Options

- and-quit** (Optional) Quit configuration mode if the commit synchronization succeeds.
- at** (Optional) Time at which to activate configuration changes.
- comment** (Optional) Write a message to the commit log.
- force** (Optional) Force a commit synchronization on the other Routing Engine (ignore warnings).
- scripts** (Optional) Push scripts to the other Routing Engine.

## Required Privilege Level

system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 7.4.

## RELATED DOCUMENTATION

[Synchronizing the Routing Engine Configuration](#)

*Configuring Multiple Routing Engines to Synchronize Committed Configurations Automatically*

## traceoptions

### IN THIS SECTION

- [Syntax | 1070](#)
- [Hierarchy Level | 1070](#)

- [Description | 1070](#)
- [Default | 1071](#)
- [Options | 1071](#)
- [Required Privilege Level | 1072](#)
- [Release Information | 1073](#)

## Syntax

```
traceoptions {
    file filename <files number> <size size> <world-readable | no-world-readable>;
    flag flag <disable>;
}
```

## Hierarchy Level

```
[edit logical-systems logical-system-name routing-instances routing-instance-name routing-
options],
[edit logical-systems logical-system-name routing-instances routing-instance-name routing-
options multicast],
[edit logical-systems logical-system-name routing-options],
[edit logical-systems logical-system-name routing-options multicast],
[edit routing-instances routing-instance-name routing-options],
[edit routing-instances routing-instance-name routing-options multicast],
[edit routing-options],
[edit routing-options flow],
[edit routing-options multicast]
```

## Description

Define tracing operations that track all routing protocol functionality in the routing device. You can also trace clock synchronization information using this command.

To specify more than one tracing operation, include multiple `flag` statements.



**NOTE:** On Junos OS Evolved, `traceoptions` is disabled for `op`, `event`, and `commit` scripts. Instead, Junos OS Evolved enables default tracking and trace messages that are logged under `/var/log/` traces.

Use the command `set protocols clock-synchronization traceoptions file <filename> size <size>` and `set protocols clock-synchronization traceoptions flag enable` to enable clock synchronization tracing. This option is only available on ACX7900 devices.

For example, use `set protocols clock-synchronization traceoptions file clksyncd size 500M` to enable clock synchronization tracing with maximum size of each trace file as 500 megabytes (500MB).

## Default

If you do not include this statement, no global tracing operations are performed.

## Options

Values:

- 

**disable**—(Optional) Disable the tracing operation. You can use this option to disable a single operation when you have defined a broad group of tracing operations, such as **all**.

**file filename**—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory `/var/log`. We recommend that you place global routing protocol tracing output in the file **routing-log**.

**files number**—(Optional) Maximum number of trace files. When a trace file named **trace-file** reaches its maximum size, it is renamed **trace-file.0**, then **trace-file.1**, and so on, until the maximum number of trace files is reached. Then, the oldest trace file is overwritten. Note that if you specify a maximum number of files, you also must specify a maximum file size with the **size** option.

- **Range:** 2 through 1000 files
- **Default:** 10 files

**flag flag**—Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements. These are the global routing protocol tracing options:

- **all**—All tracing operations
- **condition-manager**—Condition-manager events

- **config-internal**—Configuration internals
- **general**—All normal operations and routing table changes (a combination of the **normal** and **route** trace operations)
- **graceful-restart**—Graceful restart operations
- **normal**—All normal operations
- **nsr-packet**—Detailed trace information for BFD nonstop active routing only
- **nsr-synchronization**—Tracing operations for nonstop active routing
- **nsr-synchronization**—Nonstop active routing synchronization
- **parse**—Configuration parsing
- **policy**—Routing policy operations and actions
- **regex-parse**—Regular-expression parsing
- **route**—Routing table changes
- **state**—State transitions
- **task**—Interface transactions and processing
- **timer**—Timer usage

**no-world-readable**—(Optional) Prevent any user from reading the log file.

**size *size***—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named ***trace-file*** reaches this size, it is renamed ***trace-file.0***. When the ***trace-file*** again reaches its maximum size, ***trace-file.0*** is renamed ***trace-file.1*** and ***trace-file*** is renamed ***trace-file.0***. This renaming scheme continues until the maximum number of trace files is reached. Then, the oldest trace file is overwritten. Note that if you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option.

- **Syntax:** ***xk*** to specify KB, ***xm*** to specify MB, or ***xg*** to specify GB
- **Range:** 10 KB through the maximum file size supported on your system
- **Default:** 128 KB

**world-readable**—(Optional) Allow any user to read the log file.

## Required Privilege Level

routing and trace—To view this statement in the configuration.

routing-control and trace-control—To add this statement to the configuration.

## Release Information

Statement introduced before Junos OS Release 7.4.

**nsr-synchronization** flag for BGP, IS-IS, LDP, and OSPF added in Junos OS Release 8.4.

**nsr-synchronization** and **nsr-packet** flags for BFD sessions added in Junos OS Release 8.5.

**nsr-synchronization** flag for RIP and RIPng added in Junos OS Release 9.0.

**nsr-synchronization** flag for Layer 2 VPNs and VPLS added in Junos OS Release 9.1.

**nsr-synchronization** flag for PIM added in Junos OS Release 9.3.

**nsr-synchronization** flag for MPLS added in Junos OS Release 10.1.

**nsr-synchronization** flag for MSDP added in Junos OS Release 12.1.

## RELATED DOCUMENTATION

| *Example: Tracing Global Routing Protocol Operations*

# Configuration Statements: Nonstop Bridging

## IN THIS CHAPTER

- [nonstop-bridging](#) | 1074
- [nonstop-bridging \(Ethernet Switching\)](#) | 1075

## nonstop-bridging

## IN THIS SECTION

- [Syntax](#) | 1074
- [Hierarchy Level](#) | 1074
- [Description](#) | 1075
- [Required Privilege Level](#) | 1075
- [Release Information](#) | 1075

## Syntax

```
nonstop-bridging;
```

## Hierarchy Level

```
[edit protocols layer2-control]
```

## Description

For platforms with two Routing Engines, configure a primary Routing Engine to switch over gracefully to a backup Routing Engine and preserve Layer 2 Control Protocol (L2CP) information.

## Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 8.4.

## RELATED DOCUMENTATION

---

[Synchronizing the Routing Engine Configuration | 283](#)

---

[Configuring Nonstop Bridging | 254](#)

---

[Configuring Nonstop Bridging on EX Series Switches \(CLI Procedure\)](#)

---

[Configuring Nonstop Bridging on Switches \(CLI Procedure\)](#)

## nonstop-bridging (Ethernet Switching)

### IN THIS SECTION

- [Syntax | 1076](#)
- [Hierarchy Level | 1076](#)
- [Description | 1076](#)
- [Required Privilege Level | 1076](#)
- [Release Information | 1076](#)

## Syntax

```
nonstop-bridging;
```

## Hierarchy Level

```
[edit ethernet-switching-options]
```

## Description

For switches with two Routing Engines or for Virtual Chassis, configure a primary Routing Engine to switch over gracefully to a backup Routing Engine and preserve Layer 2 protocol information for the Layer 2 protocols that support nonstop bridging (NSB). For a list of the EX Series switches and Layer 2 protocols that support nonstop bridging, see [EX Series Switch Software Features Overview](#).

## Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 11.3.

## RELATED DOCUMENTATION

| [Configuring Nonstop Bridging on EX Series Switches \(CLI Procedure\)](#)

# Configuration Statements: NSSU

## IN THIS CHAPTER

- [fpcs \(NSSU Upgrade Groups\) | 1077](#)
- [member \(NSSU Upgrade Groups\) | 1079](#)
- [nssu | 1081](#)
- [upgrade-group | 1083](#)

## fpcs (NSSU Upgrade Groups)

## IN THIS SECTION

- [Syntax | 1077](#)
- [Hierarchy Level | 1078](#)
- [Description | 1078](#)
- [Options | 1078](#)
- [Required Privilege Level | 1079](#)
- [Release Information | 1079](#)

## Syntax

```
fpcs (slot-number | [list-of-slot-numbers]);
```

## Hierarchy Level

```
[edit chassis nssu upgrade-group group-name],
[edit chassis nssu upgrade-group group-name member member-id]
```

## Description

Configure switch line cards, Virtual Chassis member switches, or Virtual Chassis Fabric (VCF) member switches as part of an NSSU upgrade group.

To reduce the time an NSSU takes, you can configure line-card upgrade groups for an EX6200 or EX8200 switch with redundant Routing Engines; an EX8200 Virtual Chassis; an EX4650 Virtual Chassis with more than three member switches; QFX3500, QFX3600, and QFX5100 Virtual Chassis; or a QFX5100 Virtual Chassis Fabric (VCF). NSSU upgrades the devices in the order in which you configure the upgrade groups, so you can also use upgrade groups to control the upgrade sequence.

For switches that have separate line cards, use this statement to assign one or more line cards to an NSSU upgrade group based on their line-card slot numbers.

For Virtual Chassis or VCF member switches that do not have separate line cards, use this statement to assign one or more Virtual Chassis or VCF members to an NSSU upgrade group by specifying their member IDs.

**NOTE:** For a Virtual Chassis or VCF, you do not use this statement with the `member` option. When to use the `member` statement hierarchy is explained next.

To configure an upgrade group that includes line cards on switches that support multiple line cards and comprise a Virtual Chassis, use this statement with the `member` option to specify the Virtual Chassis member ID and the desired line card slot number or numbers on that member switch to include in the upgrade group. Use multiple statements to add line cards from different Virtual Chassis members to the upgrade group.

## Options

### *list-of-slot-numbers*

A list of slot numbers of multiple line cards or member IDs of Virtual Chassis or VCF members to be included in the upgrade group. Separate multiple slot numbers or member IDs with spaces and enclose the list in square brackets—for example: [3 4 7].

### *slot-number*

The slot number of a single line card or member ID of a Virtual Chassis or VCF member to be included in the upgrade group.



## Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 10.4.

## RELATED DOCUMENTATION

[Example: Configuring Line-Card Upgrade Groups for Nonstop Software Upgrade on EX Series Switches](#)

Configuring Line-Card Upgrade Groups for Nonstop Software Upgrade

## member (NSSU Upgrade Groups)

### IN THIS SECTION

- [Syntax | 1079](#)
- [Hierarchy Level | 1080](#)
- [Description | 1080](#)
- [Options | 1080](#)
- [Required Privilege Level | 1080](#)
- [Release Information | 1081](#)

## Syntax

```
member member-id {
  fpcs (slot-number | [list-of-slot-numbers]);
}
```

## Hierarchy Level

```
[edit chassis nssu upgrade-group group-name]
```

## Description

Specify the Virtual Chassis member whose line-card slot numbers you are assigning to an NSSU upgrade group.

**NOTE:** This statement is not applicable to Virtual Chassis or VCF member switches that do not support separate line cards. To configure Virtual Chassis or VCF member switches that do not have separate line cards into an NSSU upgrade group, use the `fpcs` statement alone, and specify the Virtual Chassis or VCF member IDs to include in the upgrade group in place of line card slot numbers.

To reduce the time an NSSU takes, you can configure NSSU line-card upgrade groups on an EX6200 or EX8200 switch with redundant Routing Engines; EX8200 Virtual Chassis; QFX3500, QFX3600, and QFX5100 Virtual Chassis; and Virtual Chassis Fabric (VCF).

To configure an upgrade group that includes line cards on different switches that support multiple line cards and comprise a Virtual Chassis, use this statement hierarchy with the `fpcs` option to first specify the Virtual Chassis member ID and then desired line card slot number or numbers on that member switch to include in the upgrade group. Use multiple statements to add line cards from different Virtual Chassis members to the upgrade group.

## Options

***member-id*** The ID of the Virtual Chassis or VCF member switch containing one or more line cards to include in an NSSU upgrade group.

The remaining statement is explained separately. See [CLI Explorer](#).

## Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 11.1.

## RELATED DOCUMENTATION

[Example: Configuring Line-Card Upgrade Groups for Nonstop Software Upgrade on EX Series Switches](#)

Configuring Line-Card Upgrade Groups for Nonstop Software Upgrade

## nssu

### IN THIS SECTION

- [Syntax | 1081](#)
- [Hierarchy Level | 1082](#)
- [Description | 1082](#)
- [Default | 1082](#)
- [Required Privilege Level | 1082](#)
- [Release Information | 1083](#)

## Syntax

```
nssu {  
  rcp-count number;  
  upgrade-group group-name {  
    fpcs (slot-number | [list-of-slot-numbers]);  
    member member-id {  
      fpcs (slot-number | [list-of-slot-numbers]);  
    }  
  }  
}
```

## Hierarchy Level

[edit [chassis](#)]

## Description

Configure parameters that affect the nonstop software upgrade (NSSU) process.

**NOTE:** You use the "[request system software nonstop-upgrade](#)" on [page 1314](#) command to initiate NSSU.

The `rcp-count` option (available only on QFX5100 switches) sets the number of parallel `rcp` sessions that NSSU uses to copy the new software to multiple Virtual Chassis or VCF member switches at a time.

The `upgrade-group` options define line-card upgrade groups for NSSU. When you initiate NSSU with at least one upgrade group configured, NSSU upgrades the line cards or Virtual Chassis or VCF members in each upgrade group to the new software version at the same time, in the order in which you configured them. Upgrade groups reduce the time required to complete an NSSU operation and control the order in which the line cards or members are upgraded.

Line-card upgrade groups are supported on some EX Series switches and EX Series Virtual Chassis that support NSSU and on a QFX5100 VCF.

These statements are all explained separately. You can also consult [CLI Explorer](#).

## Default

If you do not configure `rcp-count`, NSSU uses a default algorithm to determine the number of parallel `rcp` sessions to use based on the number of members in the Virtual Chassis or VCF.

If you do not define any line-card upgrade groups, NSSU upgrades line cards or members of a Virtual Chassis or VCF one at a time in ascending order by slot or member number.

## Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 10.4.

rcp-count statement introduced in Junos OS Release 14.1X53-D40 for QFX5100 switches only.

## RELATED DOCUMENTATION

Configuring Line-Card Upgrade Groups for Nonstop Software Upgrade

[Example: Configuring Line-Card Upgrade Groups for Nonstop Software Upgrade on EX Series Switches](#)

## upgrade-group

### IN THIS SECTION

- [Syntax | 1083](#)
- [Hierarchy Level | 1084](#)
- [Description | 1084](#)
- [Options | 1084](#)
- [Required Privilege Level | 1084](#)
- [Release Information | 1084](#)

## Syntax

```
upgrade-group group-name {
  fpcs (slot-number | [list-of-slot-numbers]);
  member member-id {
    fpcs (slot-number | [list-of-slot-numbers]);
  }
}
```

## Hierarchy Level

```
[edit chassis nssu]
```

## Description

Assign a name to a line-card upgrade group being created for nonstop software upgrade (NSSU).

To reduce the time an NSSU takes, you can configure line-card upgrade groups on an EX6200 or EX8200 switch with redundant Routing Engines; EX8200 Virtual Chassis; EX4650 Virtual Chassis; QFX3500, QFX3600, and QFX5100 Virtual Chassis; and QFX5100 Virtual Chassis Fabric (VCF).

NSSU upgrades the groups in the order that they appear in the configuration (in other words, in the order you configure them). If you do not define any line-card upgrade groups, NSSU upgrades line cards or members of a Virtual Chassis or VCF one at a time in ascending order by slot or member number.

## Options

*group-name*                      Name of the upgrade group.

The remaining statements are explained separately. See [CLI Explorer](#).

## Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 10.4.

## RELATED DOCUMENTATION

Configuring Line-Card Upgrade Groups for Nonstop Software Upgrade

[Example: Configuring Line-Card Upgrade Groups for Nonstop Software Upgrade on EX Series Switches](#)

*Upgrading Software on a Virtual Chassis Fabric Using Nonstop Software Upgrade*

# Configuration Statements: Power Management

## IN THIS CHAPTER

- [power-budget-priority](#) | 1085
- [n-plus-n \(Power Management\)](#) | 1087
- [psu](#) | 1088
- [redundancy \(Power Management\)](#) | 1089

## power-budget-priority

## IN THIS SECTION

- [Syntax](#) | 1085
- [Hierarchy Level](#) | 1086
- [Description](#) | 1086
- [Default](#) | 1086
- [Options](#) | 1086
- [Required Privilege Level](#) | 1086
- [Release Information](#) | 1086

## Syntax

```
power-budget-priority priority;
```

## Hierarchy Level

[edit chassis (EX Series)

fpc slot]

## Description

Assign a power priority to the specified line card slot on an EX6200 or EX8200 switch.

**NOTE:** On an EX6200 switch, you cannot change the power priority of a slot containing a Switch Fabric and Routing Engine (SRE) module. Although the CLI allows you to set a different power priority for the slot, your change does not go into effect, and the power priority remains 0. A message is sent to the system log to inform you that changing the power priority of the slot is unsupported.

## Default

All line card slots are initially assigned the lowest priority, with the exception of slot 4 and slot 5 on the EX6200 switch, which always are assigned a priority of 0.

## Options

***priority***—Assigned power priority for the slot, with 0 being the highest priority:

- 0 through 9 for an EX6200 switch
- 0 through 7 for an EX8208 switch
- 0 through 15 for an EX8216 switch

## Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 10.2.



## RELATED DOCUMENTATION

Configuring the Power Priority of Line Cards (CLI Procedure)

## n-plus-n (Power Management)

### IN THIS SECTION

- [Syntax | 1087](#)
- [Hierarchy Level | 1087](#)
- [Description | 1087](#)
- [Required Privilege Level | 1087](#)
- [Release Information | 1088](#)

### Syntax

```
n-plus-n;
```

### Hierarchy Level

```
[edit chassis (EX Series) psu redundancy]
```

### Description

Configure  $N+N$  power supply redundancy for power management on an EX6200 or EX8200 switch.

### Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 10.2.

## RELATED DOCUMENTATION

| [Configuring Power Supply Redundancy \(CLI Procedure\)](#)

## psu

### IN THIS SECTION

- [Syntax | 1088](#)
- [Hierarchy Level | 1088](#)
- [Description | 1089](#)
- [Required Privilege Level | 1089](#)
- [Release Information | 1089](#)

## Syntax

```
psu {  
  redundancy {  
    n-plus-n (Power Management);  
  }  
}
```

## Hierarchy Level

[edit [chassis \(EX Series\)](#)]

## Description

Configure *N+N* power supply redundancy for power management on an EX6200 or EX8200 switch or SRX380 device.

The remaining statements are explained separately. See [CLI Explorer](#).

## Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 10.2.

## RELATED DOCUMENTATION

| [Configuring Power Supply Redundancy \(CLI Procedure\)](#)

## redundancy (Power Management)

### IN THIS SECTION

- [Syntax | 1090](#)
- [Hierarchy Level | 1090](#)
- [Description | 1090](#)
- [Default | 1090](#)
- [Required Privilege Level | 1090](#)
- [Release Information | 1090](#)

## Syntax

```
redundancy {  
    n-plus-n (Power Management);  
}
```

## Hierarchy Level

```
[edit chassis (EX Series)    psu]
```

## Description

Configure  $N+M$  power supply redundancy for power management on an EX6200 or EX8200 switch.

The remaining statement is explained separately. See [CLI Explorer](#).

## Default

$N+1$  power supply redundancy is configured by default.

## Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 10.2.

## RELATED DOCUMENTATION

| [Configuring Power Supply Redundancy \(CLI Procedure\)](#)

# Configuration Statements: Redundant Power System

## IN THIS CHAPTER

- [member \(Redundant Power System\) | 1091](#)
- [priority \(Redundant Power System\) | 1093](#)
- [redundant-power-system | 1094](#)

## member (Redundant Power System)

## IN THIS SECTION

- [Syntax | 1091](#)
- [Hierarchy Level | 1092](#)
- [Description | 1092](#)
- [Options | 1092](#)
- [Required Privilege Level | 1092](#)
- [Release Information | 1092](#)

## Syntax

```
member vc-member-number {  
    priority (0|1|2|3|4|5|6);  
}
```

## Hierarchy Level

[edit [redundant-power-system](#)]

## Description

Specify the Virtual Chassis member ID of a switch connected to the Redundant Power System (RPS) for backup power supply. The member ID is required only for switches that can be configured in a Virtual Chassis. If the switch has never been configured in a Virtual Chassis, the value is always 0.

## Options

*member-number*—Member ID of a switch that has Virtual Chassis capability that is connected to the RPS.

- **Range:** 0 through maximum members in the Virtual Chassis
- **Default:** 0

The remaining statement is explained separately. See [CLI Explorer](#).

## Required Privilege Level

admin—To view this statement in the configuration.

admin-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 12.1.

## RELATED DOCUMENTATION

| [Determining and Setting Priority for Switches Connected to an EX Series RPS](#)

## priority (Redundant Power System)

### IN THIS SECTION

- [Syntax | 1093](#)
- [Hierarchy Level | 1093](#)
- [Description | 1093](#)
- [Required Privilege Level | 1094](#)
- [Release Information | 1094](#)

### Syntax

```
priority (0|1|2|3|4|5|6);
```

### Hierarchy Level

```
[edit redundant-power-system member]  
[edit redundant-power-system member member-number]
```

### Description

Configure the backup of any switch connected to the Redundant Power System (RPS) using the CLI on each switch. The determines the order in which the RPS supplies backup power to the switches connected to the RPS. 6 is the highest priority and 1 is lowest. Zero means off or no RPS backup.

If the switch is not reconfigured from the CLI, the default priority is 1. In this case, priority is determined by connector location with the rightmost connector having the highest priority.

For switches that can only be used as standalone switches, this hierarchy level is used for configuration:

```
[edit redundant-power-system]
```

For switches that can be used either as standalone switches or configured in a Virtual Chassis, this hierarchy level is used for configuration:

```
[edit redundant-power-system member vc-member-number]
```

If two or more connections are assigned the same , then the power of each connection is determined based on its switch connector port location, with the rightmost port receiving power first.

## Required Privilege Level

admin—To view this statement in the configuration.

admin-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 12.1.

# redundant-power-system

## IN THIS SECTION

- [Syntax | 1094](#)
- [Hierarchy Level | 1095](#)
- [Description | 1095](#)
- [Required Privilege Level | 1095](#)
- [Release Information | 1095](#)

## Syntax

EX2200 switch:

```
redundant-power-system {
  priority (0|1|2|3|4|5|6)
```



```
    }
}
```

EX3300 switch:

```
redundant-power-system {
  member vc-member-number {
    priority (0|1|2|3|4|5|6)
  }
}
```

## Hierarchy Level

[edit]

## Description

Configure Redundant Power System (RPS) member to ensure higher- switches always receive power backup.

The remaining statements are explained separately. See [CLI Explorer](#).

## Required Privilege Level

admin—To view this statement in the configuration.

admin-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 12.1.

## RELATED DOCUMENTATION

| Determining and Setting Priority for Switches Connected to an EX Series RPS

# Configuration Statements: Routing Engine and Switching Control Board Redundancy

## IN THIS CHAPTER

- [cfeb](#) | 1097
- [description \(Chassis Redundancy\)](#) | 1098
- [disk-failure-action](#) | 1099
- [failover \(Chassis\)](#) | 1101
- [failover \(Chassis\)](#) | 1103
- [failover \(System Process\)](#) | 1104
- [feb \(Creating a Redundancy Group\)](#) | 1105
- [feb \(Assigning a FEB to a Redundancy Group\)](#) | 1107
- [keepalive-time](#) | 1108
- [keepalive-time](#) | 1110
- [no-auto-failover](#) | 1112
- [on-disk-failure \(Chassis Redundancy Failover\)](#) | 1113
- [on-disk-failure](#) | 1114
- [on-loss-of-keepalives](#) | 1116
- [on-loss-of-keepalives](#) | 1117
- [redundancy](#) | 1119
- [redundancy-group](#) | 1121
- [routing-engine \(Chassis Redundancy\)](#) | 1122
- [sfm \(Chassis Redundancy\)](#) | 1124
- [ssb](#) | 1125
- [vcp-no-hold-time](#) | 1127

## cfeb

### IN THIS SECTION

- [Syntax | 1097](#)
- [Hierarchy Level | 1097](#)
- [Description | 1097](#)
- [Default | 1097](#)
- [Options | 1097](#)
- [Required Privilege Level | 1098](#)
- [Release Information | 1098](#)

### Syntax

```
cfeb slot-number (always | preferred);
```

### Hierarchy Level

```
[edit chassis redundancy]
```

### Description

On M10i routers only, configure which Compact Forwarding Engine Board (CFEB) is the primary and which is the backup.

### Default

By default, the CFEB in slot 0 is the primary and the CFEB in slot 1 is the backup.

### Options

***slot-number***—Specify which slot is the primary and which is the backup.

***always***—Define this CFEB as the sole device.

**preferred**—Define this CFEB as the preferred device of at least two.

### Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

### Release Information

Statement introduced before Junos OS Release 7.4.

### RELATED DOCUMENTATION

| [Configuring CFEB Redundancy on the M10i Router](#)

## description (Chassis Redundancy)

### IN THIS SECTION

- [Syntax | 1098](#)
- [Hierarchy Level | 1099](#)
- [Description | 1099](#)
- [Options | 1099](#)
- [Required Privilege Level | 1099](#)
- [Release Information | 1099](#)

### Syntax

```
description description;
```

## Hierarchy Level

```
[edit chassis redundancy feb redundancy-group group-name]
```

## Description

Provide a description of the FEB redundancy group.

## Options

*description*—Provide a description for the FEB redundancy group.

## Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

## Release Information

Statement introduced before Junos OS Release 7.4.

## RELATED DOCUMENTATION

| [Configuring FEB Redundancy on the M120 Router](#)

## disk-failure-action

### IN THIS SECTION

- [Syntax | 1100](#)
- [Hierarchy Level | 1100](#)
- [Description | 1100](#)
- [Options | 1100](#)

- Required Privilege Level | 1100
- Release Information | 1100

## Syntax

```
disk-failure-action (halt | reboot);
```

## Hierarchy Level

```
[edit chassis redundancy on-disk-failure]  
[edit chassis routing-engine on-disk-failure]
```

## Description

Configure the Routing Engine to halt or reboot when the Routing Engine hard disk fails.

## Options

**halt**—Specify the Routing Engine to halt.

**reboot**—Specify the Routing Engine to reboot.

## Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 9.2.

## RELATED DOCUMENTATION

| [graceful-switchover](#) | 994

*Enabling a Routing Engine to Reboot on Hard Disk Errors*

*Installing Software on an EX Series Switch with Redundant Routing Engines (CLI Procedure)*

[High Availability Features for EX Series Switches Overview](#) | 9

## failover (Chassis)

### IN THIS SECTION

- [Syntax](#) | 1101
- [Hierarchy Level](#) | 1101
- [Description](#) | 1101
- [Options](#) | 1102
- [Required Privilege Level](#) | 1102
- [Release Information](#) | 1102

### Syntax

```
failover {  
    on-disk-failure;  
    on-loss-of-keepalives;  
    on-re-to-fpc-stale;  
}
```

### Hierarchy Level

```
[edit chassis redundancy]
```

### Description

Specify conditions on the primary Routing Engine that cause the backup router to take primary role.

On Junos OS devices this statement enables automatic Routine Engine switchover. By default this statement is disabled on Junos OS Evolved, but it may be enabled if you are upgrading an existing configuration from Junos OS to Junos OS Evolved. To disable automatic failover on Junos OS Evolved devices, delete this statement by entering the **delete chassis redundancy failover** command.

The remaining statements are explained separately. See [CLI Explorer](#).

## Options

**on-disk-failure**—Instruct the backup router to take primary role if it detects hard disk errors on the primary Routing Engine.

**on-loss-of-keepalives**—Instruct the backup router to take primary role if it detects a loss of keepalive signal from the primary Routing Engine.

**on-re-to-fpc-stale**—Instruct the backup router to take mastership if the `em0` interface fails on the master Routing Engine.

## Required Privilege Level

**interface**—To view this statement in the configuration.

**interface-control**—To add this statement to the configuration.

## Release Information

Statement introduced before Junos OS Release 7.4.

**on-re-to-fpc-stale** option introduced in Junos OS Release 15.2 on the MX240, MX480, MX960, MX2010, and MX2020.

**on-re-to-fpc-stale** option added in Junos OS Release 22.2R1 on the MX10008, MX10016, PTX10008, PTX10016, QFX10008, and QFX10016.

## RELATED DOCUMENTATION

| [On Detection of a Hard Disk Error on the Primary Routing Engine](#) | 133



## failover (Chassis)

### IN THIS SECTION

- [Syntax | 1103](#)
- [Hierarchy Level | 1103](#)
- [Description | 1103](#)
- [Required Privilege Level | 1103](#)
- [Release Information | 1104](#)

### Syntax

```
failover {  
    on-disk-failure;  
    on-loss-of-keepalives;  
}
```

### Hierarchy Level

```
[edit chassis redundancy]
```

### Description

Specify conditions on the primary Routing Engine that cause the backup router to take primary role.

The remaining statements are explained separately. See [CLI Explorer](#).

### Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 9.2.

### RELATED DOCUMENTATION

[graceful-switchover](#) | [994](#)

[On Detection of a Hard Disk Error on the Primary Routing Engine](#) | [133](#)

*Installing Software on an EX Series Switch with Redundant Routing Engines (CLI Procedure)*

[High Availability Features for EX Series Switches Overview](#) | [9](#)

## failover (System Process)

### IN THIS SECTION

- [Syntax](#) | [1104](#)
- [Hierarchy Level](#) | [1104](#)
- [Description](#) | [1105](#)
- [Options](#) | [1105](#)
- [Required Privilege Level](#) | [1105](#)
- [Release Information](#) | [1105](#)

### Syntax

```
failover (alternate-media | other-routing-engine);
```

### Hierarchy Level

```
[edit system processes process-name]
```

## Description

Configure the router to reboot if the software process fails four times within 30 seconds, and specify the software to use during the reboot.

## Options

*process-name*—Junos OS process name. Some of the processes that support the failover statement are bootp, chassis-control, craft-control, ethernet-connectivity-fault-management, init, interface-control, neighbor-liveness, pfe, redundancy-interface-process, routing, smg-service, and vrrp.

*alternate-media*—Use the Junos OS image on alternate media during the reboot.

*other-routing-engine*—On routers with dual Routing Engines, use the Junos OS image on the other Routing Engine during the reboot. That Routing Engine assumes the primary role; in the usual configuration, the other Routing Engine is the designated backup Routing Engine.

## Required Privilege Level

*system*—To view this statement in the configuration.

*system-control*—To add this statement to the configuration.

## Release Information

Statement introduced before Junos OS Release 7.4.

## RELATED DOCUMENTATION

[When a Software Process Fails  
processes](#)

## feb (Creating a Redundancy Group)

### IN THIS SECTION

 [Syntax](#) | 1106

- [Hierarchy Level | 1106](#)
- [Description | 1106](#)
- [Options | 1106](#)
- [Required Privilege Level | 1106](#)
- [Release Information | 1107](#)

## Syntax

```
feb {
    redundancy-group group-name {
        description description;
        feb slot-number (backup | primary);
        no-auto-failover;
    }
}
```

## Hierarchy Level

```
[edit chassis redundancy]
```

## Description

On M120 routers only, configure a Forwarding Engine Board (FEB) redundancy group.

## Options

The remaining statements are described separately.

## Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 8.2.

## RELATED DOCUMENTATION

| [Configuring FEB Redundancy on the M120 Router](#)

## feb (Assigning a FEB to a Redundancy Group)

### IN THIS SECTION

- [Syntax | 1107](#)
- [Hierarchy Level | 1107](#)
- [Description | 1107](#)
- [Options | 1108](#)
- [Required Privilege Level | 1108](#)
- [Release Information | 1108](#)

## Syntax

```
feb slot-number (backup | primary);
```

## Hierarchy Level

```
[edit chassis redundancy feb redundancy-group group-name]
```

## Description

On M120 routers only, configure a Forwarding Engine Board (FEB) as part of a FEB redundancy group.

## Options

**slot-number**—Slot number of the FEB. The range of values is from **0** to **5**.

**backup**—(Optional) For each redundancy group, you must configure exactly one backup FEB.

**primary**—(Optional) For each redundancy group, you can optionally configure one primary FEB.

## Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 8.2.

## RELATED DOCUMENTATION

| [Configuring FEB Redundancy on the M120 Router](#)

## keepalive-time

### IN THIS SECTION

- [Syntax | 1109](#)
- [Hierarchy Level | 1109](#)
- [Description | 1109](#)
- [Default | 1109](#)
- [Options | 1109](#)
- [Required Privilege Level | 1109](#)
- [Release Information | 1109](#)

## Syntax

```
keepalive-time seconds;
```

## Hierarchy Level

```
[edit chassis redundancy]
```

## Description

Configure the time period that must elapse before the backup router takes primary role when it detects loss of the keepalive signal.

## Default

The on-loss-of-keepalives statement at the [edit chassis redundancy failover] hierarchy level must be included for failover to occur.

When the on-loss-of-keepalives statement is included and graceful Routing Engine switchover *is not* configured, failover occurs after 300 seconds (5 minutes).

When the on-loss-of-keepalives statement is included and graceful Routing Engine switchover *is* configured, the keepalive signal is automatically enabled and the failover time is set to 2 seconds (4 seconds on M20 routers). You cannot manually reset the keepalive time.

## Options

***seconds***—Time before the backup router takes primary role when it detects loss of the keepalive signal. The range of values is 2 through 10,000.

## Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

## Release Information

Statement introduced before Junos OS Release 7.4.

## RELATED DOCUMENTATION

[On Detection of a Loss of Keepalive Signal from the Primary Routing Engine | 133](#)

[failover \(Chassis\) | 1101](#)

[on-loss-of-keepalives | 1116](#)

## keepalive-time

### IN THIS SECTION

- [Syntax | 1110](#)
- [Hierarchy Level | 1110](#)
- [Description | 1110](#)
- [Default | 1111](#)
- [Options | 1111](#)
- [Required Privilege Level | 1111](#)
- [Release Information | 1111](#)

### Syntax

```
keepalive-time seconds;
```

### Hierarchy Level

```
[edit chassis redundancy]
```

### Description

Configure the time period that must elapse before the backup router takes primary role when it detects loss of the keepalive signal.



## Default

The `on-loss-of-keepalives` statement at the `[edit chassis redundancy failover]` hierarchy level must be included for failover to occur.

When the `on-loss-of-keepalives` statement is included and graceful Routing Engine switchover *is not* configured, failover occurs after 300 seconds (5 minutes).

When the `on-loss-of-keepalives` statement is included and graceful Routing Engine switchover *is* configured, the keepalive signal is automatically enabled and the failover time is set to 2 seconds.

## Options

***seconds***—Time before the backup router takes primary role when it detects loss of the keepalive signal. The range of values is 2 through 10,000.

## Required Privilege Level

`interface`—To view this statement in the configuration.

`interface-control`—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 9.2.

## RELATED DOCUMENTATION

---

[failover \(Chassis\) | 1103](#)

---

[graceful-switchover | 994](#)

---

[on-loss-of-keepalives | 1117](#)

---

[High Availability Features for EX Series Switches Overview | 9](#)

## no-auto-failover

### IN THIS SECTION

- [Syntax | 1112](#)
- [Hierarchy Level | 1112](#)
- [Description | 1112](#)
- [Default | 1112](#)
- [Required Privilege Level | 1112](#)
- [Release Information | 1113](#)

### Syntax

```
no-auto-failover;
```

### Hierarchy Level

```
[edit chassis redundancy feb redundancy-group group-name]
```

### Description

Disable automatic failover to a backup FEB when an active FEB in a redundancy group fails.

### Default

Automatic failover is enabled by default.

### Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

## Release Information

Statement introduced before Junos OS Release 7.4.

## RELATED DOCUMENTATION

| [Configuring FEB Redundancy on the M120 Router](#)

## on-disk-failure (Chassis Redundancy Failover)

### IN THIS SECTION

- [Syntax | 1113](#)
- [Hierarchy Level | 1113](#)
- [Description | 1113](#)
- [Required Privilege Level | 1114](#)
- [Release Information | 1114](#)

## Syntax

```
on-disk-failure;
```

## Hierarchy Level

```
[edit chassis redundancy failover]
```

## Description

Instruct the backup router to take primary role if it detects hard disk errors on the primary Routing Engine.

## Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

## Release Information

Statement introduced before Junos OS Release 7.4.

## RELATED DOCUMENTATION

| [On Detection of a Hard Disk Error on the Primary Routing Engine](#) | 133

## on-disk-failure

### IN THIS SECTION

- [Syntax](#) | 1114
- [Hierarchy Level](#) | 1115
- [Description](#) | 1115
- [Options](#) | 1115
- [Required Privilege Level](#) | 1115
- [Release Information](#) | 1115

## Syntax

```
on-disk-failure {  
    disk-failure-action (halt | reboot);  
}
```

## Hierarchy Level

```
[edit chassis redundancy]  
[edit chassis routing-engine]
```

## Description

Instruct the router to halt or reboot if it detects hard disk errors on the Routing Engine.

## Options

The remaining statement is explained separately. See [CLI Explorer](#).

## Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 9.2.

## RELATED DOCUMENTATION

[graceful-switchover](#) | 994

---

*Enabling a Routing Engine to Reboot on Hard Disk Errors*

---

*Installing Software on an EX Series Switch with Redundant Routing Engines (CLI Procedure)*

---

[High Availability Features for EX Series Switches Overview](#) | 9

## on-loss-of-keepalives

### IN THIS SECTION

- [Syntax | 1116](#)
- [Hierarchy Level | 1116](#)
- [Description | 1116](#)
- [Default | 1116](#)
- [Required Privilege Level | 1117](#)
- [Release Information | 1117](#)

### Syntax

```
on-loss-of-keepalives;
```

### Hierarchy Level

```
[edit chassis redundancy failover]
```

### Description

Instruct the backup router to take primary role if it detects a loss of keepalive signal from the primary Routing Engine.

### Default

The on-loss-of-keepalives statement must be included at the [edit chassis redundancy failover] hierarchy level for failover to occur.

When the on-loss-of-keepalives statement is included but graceful Routing Engine switchover *is not* configured, failover occurs after 300 seconds (5 minutes).

When the `on-loss-of-keepalives` statement is included and graceful Routing Engine switchover *is* configured, the keepalive signal is automatically enabled and the failover time is set to 2 seconds (4 seconds on M20 routers) . The keepalive time is not configurable.

## Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

## Release Information

Statement introduced before Junos OS Release 7.4.

## RELATED DOCUMENTATION

[On Detection of a Loss of Keepalive Signal from the Primary Routing Engine | 133](#)  
[keepalive-time | 1108](#)

## on-loss-of-keepalives

### IN THIS SECTION

- [Syntax | 1117](#)
- [Hierarchy Level | 1118](#)
- [Description | 1118](#)
- [Default | 1118](#)
- [Required Privilege Level | 1118](#)
- [Release Information | 1118](#)

## Syntax

```
on-loss-of-keepalives;
```

## Hierarchy Level

```
[edit chassis redundancy failover]
```

## Description

Instruct the backup router to take primary role if it detects a loss of keepalive signal from the primary Routing Engine.

## Default

The on-loss-of-keepalives statement must be included at the [edit chassis redundancy failover] hierarchy level for failover to occur.

When the on-loss-of-keepalives statement is included but graceful Routing Engine switchover *is not* configured, failover occurs after 300 seconds (5 minutes).

When the on-loss-of-keepalives statement is included and graceful Routing Engine switchover *is* configured, the keepalive signal is automatically enabled and the failover time is set to 2 seconds.

## Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 9.2.

## RELATED DOCUMENTATION

[graceful-switchover](#) | 994

[keepalive-time](#) | 1110

*Installing Software on an EX Series Switch with Redundant Routing Engines (CLI Procedure)*

[High Availability Features for EX Series Switches Overview](#) | 9



## redundancy

### IN THIS SECTION

- [Syntax | 1119](#)
- [Hierarchy Level | 1120](#)
- [Description | 1120](#)
- [Options | 1120](#)
- [Required Privilege Level | 1120](#)
- [Release Information | 1120](#)

### Syntax

```

redundancy {
  cfeb slot (always | preferred);
  failover {
    on-disk-failure;
    on-loss-of-keepalives;
    on-re-to-fpc-stale;
  }
  feb {
    redundancy-group group-name {
      description description;
      feb slot-number (backup | primary);
      no-auto-failover;
    }
  }
  graceful-switchover;
  keepalive-time seconds;
  routing-engine slot-number (backup | disabled | master);
  sfm slot-number (always | preferred);
  ssb slot-number (always | preferred);
}

```

## Hierarchy Level

[edit chassis]

## Description

Configure redundancy options.

## Options

The remaining statements are explained separately. See [CLI Explorer](#).

## Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

## Release Information

Statement introduced before Junos OS Release 7.4.

## RELATED DOCUMENTATION

[Configuring Routing Engine Redundancy | 131](#)

Configuring CFEB Redundancy on the M10i Router

Configuring FEB Redundancy on the M120 Router

Configuring SFM Redundancy on M40e and M160 Routers

Configuring SSB Redundancy on the M20 Router

## redundancy-group

### IN THIS SECTION

- [Syntax | 1121](#)
- [Hierarchy Level | 1121](#)
- [Description | 1121](#)
- [Options | 1121](#)
- [Required Privilege Level | 1122](#)
- [Release Information | 1122](#)

### Syntax

```
redundancy-group group-name {  
    description description;  
    feb slot-number (backup | primary);  
    no-auto-failover;  
}
```

### Hierarchy Level

```
[edit chassis redundancy feb]
```

### Description

On M120 routers only, configure a Forwarding Engine Board (FEB) redundancy group.

### Options

***group-name*** is the unique name for the redundancy group. The maximum length is 39 alphanumeric characters.

Other statements are explained separately.

## Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 8.2.

## RELATED DOCUMENTATION

Configuring FEB Redundancy on the M120 Router

## routing-engine (Chassis Redundancy)

### IN THIS SECTION

- [Syntax | 1122](#)
- [Hierarchy Level | 1123](#)
- [Description | 1123](#)
- [Default | 1123](#)
- [Options | 1123](#)
- [Required Privilege Level | 1123](#)
- [Release Information | 1123](#)

## Syntax

```
routing-engine slot-number (backup | disabled | master);
```

## Hierarchy Level

[edit chassis [redundancy](#)]

## Description

Configure Routing Engine redundancy.

## Default

By default, the Routing Engine in slot 0 is the primary Routing Engine and the Routing Engine in slot 1 is the backup Routing Engine.

## Options

*slot-number*—Specify the slot number (0 or 1).

Set the function of the Routing Engine for the specified slot:

- **master**—Routing Engine in the specified slot is the primary.
- **backup**—Routing Engine in the specified slot is the backup.
- **disabled**—Routing Engine in the specified slot is disabled.

## Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

## Release Information

Statement introduced before Junos OS Release 7.4.

## RELATED DOCUMENTATION

| [Configuring Routing Engine Redundancy](#) | 131

## sfm (Chassis Redundancy)

### IN THIS SECTION

- [Syntax | 1124](#)
- [Hierarchy Level | 1124](#)
- [Description | 1124](#)
- [Default | 1124](#)
- [Options | 1124](#)
- [Required Privilege Level | 1125](#)
- [Release Information | 1125](#)

### Syntax

```
sfm slot-number (always | preferred);
```

### Hierarchy Level

```
[edit chassis redundancy]
```

### Description

On M40e and M160 routers, configure which Switching and Forwarding Module (SFM) is the primary and which is the backup.

### Default

By default, the SFM in slot 0 is the primary and the SFM in slot 1 is the backup.

### Options

***slot-number***—Specify which slot is the primary and which is the backup. On the M40e router, ***slot-number*** can be 0 or 1. On the M160 router, ***slot-number*** can be 0 through 3.

**always**—Define this SFM as the sole device.

**preferred**—Define this SFM as the preferred device of at least two.

### Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

### Release Information

Statement introduced before Junos OS Release 7.4.

### RELATED DOCUMENTATION

| [Configuring SFM Redundancy on M40e and M160 Routers](#)

## ssb

### IN THIS SECTION

- [Syntax | 1125](#)
- [Hierarchy Level | 1126](#)
- [Description | 1126](#)
- [Default | 1126](#)
- [Options | 1126](#)
- [Required Privilege Level | 1126](#)
- [Release Information | 1126](#)

### Syntax

```
ssb slot-number (always | preferred);
```

## Hierarchy Level

[edit chassis [redundancy](#)]

## Description

On M20 routers, configure which System and Switch Board (SSB) is the primary and which is the backup.

## Default

By default, the SSB in slot 0 is the primary and the SSB in slot 1 is the backup.

## Options

***slot-number***—Specify which slot is the primary and which is the backup.

***always***—Define this SSB as the sole device.

***preferred***—Define this SSB as the preferred device of at least two.

## Required Privilege Level

**interface**—To view this statement in the configuration.

**interface-control**—To add this statement to the configuration.

## Release Information

Statement introduced before Junos OS Release 7.4.

## RELATED DOCUMENTATION

| [Configuring SSB Redundancy on the M20 Router](#)



## vcp-no-hold-time

### IN THIS SECTION

- [Syntax | 1127](#)
- [Hierarchy Level | 1127](#)
- [Description | 1127](#)
- [Default | 1128](#)
- [Required Privilege Level | 1128](#)
- [Release Information | 1128](#)

### Syntax

```
vcp-no-hold-time;
```

### Hierarchy Level

```
[edit virtual-chassis]
```

### Description

Disable the Virtual Chassis port (VCP) holddown timer for all VCPs in the Virtual Chassis or Virtual Chassis Fabric (VCF).

The VCP holddown timer is an internal mechanism that delays a Virtual Chassis reconvergence for several seconds when a VCP becomes inactive. The purpose of this delay is to provide the VCP time to return online without having to reconverge the Virtual Chassis to adjust to the inactive VCP. All traffic to the VCP is dropped while the VCP is inactive. If the VCP remains down for a time that exceeds the VCP holddown timer, a Virtual Chassis reconvergence occurs.

This statement disables the holddown timer only in an EX4300 Virtual Chassis or a mixed Virtual Chassis that contains EX4300 switches in releases in the Junos OS 13.2X50 release train. In releases after that, the `vcp-no-hold-time` option is no longer needed and has no effect because the holddown timer is replaced by a planned PFE restart for actions that affect Virtual Chassis reconvergence. Switches and releases that don't support the holddown timer might allow you to configure this statement, but the

configuration posts a warning message saying the statement has no effect. The option will be deprecated in an upcoming release and will no longer appear in the CLI.

When this statement is enabled, the VCP holddown timer is disabled and the Virtual Chassis reconvergence occurs when a VCP becomes inactive. The period of time where traffic is dropped waiting for the VCP to return online is avoided.

We recommend enabling this statement after a Virtual Chassis is operational. We recommend disabling this statement when you are adding or removing member switches from your Virtual Chassis.

The VCP holddown timer cannot be viewed and is not user-configurable. You can only control whether the VCP holddown timer is enabled or disabled by configuring this statement.

**NOTE:** In an EX4300 Virtual Chassis running a Junos OS 13.2X50 release, you should enable the `vcp-no-hold-time` statement before performing a software upgrade using NSSU. If you do not enable the `vcp-no-hold-time` statement, the Virtual Chassis may split during the upgrade. A split Virtual Chassis can cause disruptions to your network, and you may have to manually reconfigure your Virtual Chassis after the NSSU if the split and merge feature was disabled. For more information about a split Virtual Chassis, see [Understanding Split and Merge in a Virtual Chassis](#).

## Default

The VCP holddown timer is enabled by default on all devices that support this statement.

## Required Privilege Level

system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 13.2X50-D10.

## RELATED DOCUMENTATION

---

*Understanding EX Series Virtual Chassis*

---

*Understanding QFX Series Virtual Chassis*

---

*Understanding Virtual Chassis Components*

# Configuration Statements: Unified ISSU

## IN THIS CHAPTER

- [no-issu-timer-negotiation](#) | 1129
- [traceoptions \(Protocols BFD\)](#) | 1130

## no-issu-timer-negotiation

## IN THIS SECTION

- [Syntax](#) | 1129
- [Hierarchy Level](#) | 1129
- [Description](#) | 1130
- [Required Privilege Level](#) | 1130
- [Release Information](#) | 1130

## Syntax

```
no-issu-timer-negotiation;
```

## Hierarchy Level

```
[edit protocols bfd],  
[edit logical-systems logical-system-name protocols bfd],  
[edit routing-instances routing-instance-name protocols bfd]
```

## Description

Disable unified ISSU timer negotiation for Bidirectional Forwarding Detection (BFD) sessions.



**CAUTION:** The sessions might flap during unified ISSU or Routing Engine switchover, depending on the detection intervals.

## Required Privilege Level

routing—To view this statement in the configuration.

routing-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 9.1.

## RELATED DOCUMENTATION

Managing and Tracing BFD Sessions During Unified ISSU Procedures

[Junos OS Routing Protocols Library for Routing Devices](#)

## traceoptions (Protocols BFD)

### IN THIS SECTION

- [Syntax | 1131](#)
- [Hierarchy Level | 1131](#)
- [Description | 1131](#)
- [Default | 1131](#)
- [Options | 1131](#)
- [Required Privilege Level | 1133](#)
- [Release Information | 1133](#)

## Syntax

```
traceoptions {
    file name <size size> <files number> <world-readable | no-world-readable>;
    flag flag <flag-modifier> <disable>;
}
```

## Hierarchy Level

```
[edit protocols bfd]
```

## Description

Define tracing operations that track unified in-service software upgrade (ISSU) functionality in the router.

To specify more than one tracing operation, include multiple `flag` statements.

## Default

If you do not include this statement, no global tracing operations are performed.

## Options

**disable**—(Optional) Disable the tracing operation. You can use this option to disable a single operation when you have defined a broad group of tracing operations, such as **all**.

**file *name***—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory **/var/log**. We recommend that you place global routing protocol tracing output in the file **routing-log**.

**files *number***—(Optional) Maximum number of trace files. When a trace file named ***trace-file*** reaches its maximum size, it is renamed ***trace-file.0***, then ***trace-file.1***, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

- **Range:** 2 through 1000 files
- **Default:** 2 files

If you specify a maximum number of files, you also must specify a maximum file size with the **size** option.

**flag *flag***—Tracing operation to perform. The tracing options are as follows:

- **adjacency**—Trace adjacency messages.
- **all**—Trace everything.
- **error**—Trace all errors.
- **events**—Trace all events.
- **issu**—Trace ISSU packet activity.
- **nsr-packet**—Trace packet activity of NSR.
- **nsr-synchronization**—Trace NSR synchronization events.
- **packet**—Trace all packets.
- **pipe**—Trace pipe messages.
- **pipe-detail**—Trace pipe messages in detail.
- **ppm-packet**—Trace packet activity by periodic packet management.
- **state**—Trace state transitions.
- **timer**—Trace timer processing.

**no-world-readable**—Restrict users from reading the log file.

**size *size***—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named ***trace-file*** reaches this size, it is renamed ***trace-file.0***. When the ***trace-file*** again reaches its maximum size, ***trace-file.0*** is renamed ***trace-file.1*** and ***trace-file*** is renamed ***trace-file.0***. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

- **Syntax:** ***xk*** to specify KB, ***xm*** to specify MB, or ***xg*** to specify GB
- **Range:** 10 KB through the maximum file size supported on your system
- **Default:** 128 KB

If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option.

**world-readable**—Allow users to read the log file.

## Required Privilege Level

routing and trace—To view this statement in the configuration.

routing-control and trace-control—To add this statement to the configuration.

## Release Information

Statement introduced before Junos OS Release 7.4.

**issu** flag for BFD added in Junos OS Release 9.1.

## RELATED DOCUMENTATION

Managing and Tracing BFD Sessions During Unified ISSU Procedures

# Configuration Statements: VRRP

## IN THIS CHAPTER

- [accept-data | 1135](#)
- [advertise-interval | 1137](#)
- [asymmetric-hold-time | 1139](#)
- [asymmetric-hold-time | 1140](#)
- [authentication-key | 1141](#)
- [authentication-type | 1143](#)
- [bandwidth-threshold | 1145](#)
- [delegate-processing \(VRRP\) | 1147](#)
- [failover-delay | 1148](#)
- [failover-delay | 1150](#)
- [fast-interval | 1151](#)
- [global-advertisements-threshold | 1153](#)
- [hold-time \(VRRP\) | 1155](#)
- [hold-time | 1157](#)
- [inherit-advertisement-interval | 1158](#)
- [inet6-advertise-interval | 1159](#)
- [inet6-advertise-interval | 1161](#)
- [interface | 1162](#)
- [preempt \(VRRP\) | 1164](#)
- [preempt | 1165](#)
- [priority \(Protocols VRRP\) | 1167](#)
- [priority | 1169](#)
- [priority-cost \(VRRP\) | 1170](#)
- [priority-hold-time | 1172](#)
- [route \(Interfaces\) | 1174](#)
- [skew-timer-disable | 1175](#)



- [startup-silent-period | 1177](#)
- [traceoptions \(Protocols VRRP\) | 1178](#)
- [traceoptions | 1181](#)
- [track \(VRRP\) | 1184](#)
- [version-3 | 1186](#)
- [virtual-address | 1187](#)
- [virtual-inet6-address | 1189](#)
- [virtual-link-local-address | 1190](#)
- [vrrp-group | 1192](#)
- [vrrp-inet6-group | 1194](#)
- [vrrp-inherit-from | 1196](#)

## accept-data

### IN THIS SECTION

- [Syntax | 1135](#)
- [Hierarchy Level | 1136](#)
- [Description | 1136](#)
- [Default | 1136](#)
- [Required Privilege Level | 1136](#)
- [Release Information | 1137](#)

### Syntax

```
(accept-data | no-accept-data);
```

## Hierarchy Level

```
[edit interfaces interface-name unit logical-unit-number family inet address address vrrp-  
group group-id],  
[edit interfaces interface-name unit logical-unit-number family inet6 address address vrrp-inet6-  
group group-id],  
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number  
family inet address address vrrp-group group-id],  
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number  
family inet6 address address vrrp-inet6-group group-id]
```

## Description

In a Virtual Router Redundancy Protocol (VRRP) configuration, determine whether or not a router that is acting as the primary router accepts all packets destined for the virtual IP address.

- **accept-data**—Enable the primary router to accept all packets destined for the virtual IP address.
- **no-accept-data**—Prevent the primary router from accepting packets other than the ARP packets destined for the virtual IP address.

## Default

If the router acting as the primary router is the IP address owner or has its priority set to 255, the primary router, by default, responds to all packets sent to the virtual IP address. However, if the router acting as the primary router does not own the IP address or has its priority set to a value less than 255, the primary router responds only to ARP requests.

### NOTE:

- If you want to restrict the incoming IP packets to ICMP packets only, you must configure firewall filters to accept only ICMP packets.
- If you include the **accept-data** statement, your routing platform configuration does not comply with RFC 3768 (see section 6.4.3 of RFC 3768, *Virtual Router Redundancy Protocol (VRRP)*).

## Required Privilege Level

**interface**—To view this statement in the configuration.

**interface-control**—To add this statement to the configuration.

## Release Information

Statement introduced before Junos OS Release 7.4.

## RELATED DOCUMENTATION

Configuring an Interface to Accept All Packets Destined for the Virtual IP Address of a VRRP Group

## advertise-interval

### IN THIS SECTION

- [Syntax | 1137](#)
- [Hierarchy Level | 1137](#)
- [Description | 1138](#)
- [Options | 1138](#)
- [Required Privilege Level | 1138](#)
- [Release Information | 1138](#)

## Syntax

```
advertise-interval seconds;
```

## Hierarchy Level

```
[edit interfaces interface-name unit logical-unit-number family inet address address vrrp-group group-id],  
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number  
family inet address address vrrp-group group-id]
```

## Description

Configure the interval between Virtual Router Redundancy Protocol (VRRP) IPv4 advertisement packets.

All routers in the VRRP group must use the same advertisement interval.

**NOTE:** When VRRPv3 is enabled, the `advertise-interval` statement cannot be used to configure advertisement intervals. Instead, use the `fast-interval` statement to configure advertisement intervals.

## Options

*seconds*—Interval between advertisement packets.

- **Range:** 1 through 255 seconds
- **Default:** 1 second

## Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

## Release Information

Statement introduced before Junos OS Release 7.4.

## RELATED DOCUMENTATION

Configuring the Advertisement Interval for the VRRP Primary Router

[fast-interval](#) | 1151

[inet6-advertise-interval](#) | 1159

[version-3](#) | 1186

## asymmetric-hold-time

### IN THIS SECTION

- [Syntax | 1139](#)
- [Hierarchy Level | 1139](#)
- [Description | 1139](#)
- [Default | 1139](#)
- [Required Privilege Level | 1139](#)
- [Release Information | 1140](#)

### Syntax

```
asymmetric-hold-time;
```

### Hierarchy Level

```
[edit protocols vrrp]
```

### Description

Enable the VRRP primary router to switch over to the backup router immediately, without waiting for the priority hold time to expire, when a tracked route or interface goes down. When the route or interface comes back online, the original primary router that is now acting as the backup router waits for the priority hold time to expire before it reasserts primary role.

### Default

asymmetric-hold-time is disabled.

### Required Privilege Level

routing—To view this statement in the configuration.

routing-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 9.5.

## RELATED DOCUMENTATION

| [Configuring the Asymmetric Hold Time for VRRP Routers](#)

## asymmetric-hold-time

### IN THIS SECTION

- [Syntax | 1140](#)
- [Hierarchy Level | 1140](#)
- [Description | 1141](#)
- [Default | 1141](#)
- [Required Privilege Level | 1141](#)
- [Release Information | 1141](#)

## Syntax

```
asymmetric-hold-time;
```

## Hierarchy Level

```
[edit protocols vrrp]
```

## Description

Configure a VRRP primary to fail over to a backup immediately—without waiting for the priority hold time to expire—when a tracked route goes down. Otherwise, the primary waits for the hold time to expire before it initiates a failover when a tracked interface or route goes down.

When the tracked interface or route comes up again, the new backup (original primary) router waits for the priority hold time to expire before it reasserts primary role.

## Default

**asymmetric-hold-time** is disabled.

## Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS 11.3.

## RELATED DOCUMENTATION

| [Configuring VRRP Preemption and Hold Time](#)

## authentication-key

### IN THIS SECTION

- [Syntax | 1142](#)
- [Hierarchy Level | 1142](#)
- [Description | 1142](#)
- [Options | 1142](#)
- [Required Privilege Level | 1142](#)

## Syntax

```
authentication-key key;
```

## Hierarchy Level

```
[edit interfaces interface-name unit logical-unit-number family inet address address vrrp-  
group group-id],  
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number  
family inet address address vrrp-group group-id]
```

## Description

Configure a Virtual Router Redundancy Protocol (VRRP) IPv4 authentication key. You also must specify a VRRP authentication scheme by including the `authentication-type` statement.

All devices in the VRRP group must use the same authentication scheme and password.

**NOTE:** When VRRPv3 is enabled, the `authentication-type` and `authentication-key` statements cannot be configured for any VRRP groups.

## Options

**key**—Authentication password. For simple authentication, it can be 1 through 8 characters long. For Message Digest 5 (MD5) authentication, it can be 1 through 16 characters long. If you include spaces, enclose all characters in quotation marks (" ").

## Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.



## Release Information

Statement introduced before Junos OS Release 7.4.

## RELATED DOCUMENTATION

[Configuring VRRP Authentication \(IPv4 Only\)](#)

[authentication-type](#) | [1143](#)

[version-3](#)

*Understanding VRRP on SRX Series Devices*

*Example: Configuring VRRP/VRRPv3 on Chassis Cluster Redundant Ethernet Interfaces*

## authentication-type

### IN THIS SECTION

- [Syntax](#) | [1143](#)
- [Hierarchy Level](#) | [1143](#)
- [Description](#) | [1144](#)
- [Options](#) | [1144](#)
- [Required Privilege Level](#) | [1144](#)
- [Release Information](#) | [1144](#)

## Syntax

```
authentication-type (md5 | simple);
```

## Hierarchy Level

```
[edit interfaces interface-name unit logical-unit-number family inet address address vrrp-  
group group-id],
```

```
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number
family inet address address vrrp-group group-id]
```

## Description

Enable Virtual Router Redundancy Protocol (VRRP) IPv4 authentication and specify the authentication scheme for the VRRP group. If you enable authentication, you must specify a password by including the authentication-key statement. The specific type of authentication used by OSPF is encoded in this field.

All devices in the VRRP group must use the same authentication scheme and password.

**NOTE:** When VRRPv3 is enabled, the authentication-type and authentication-key statements cannot be configured for any VRRP groups.

## Options

### authentication

Authentication scheme:

- **simple** Use a simple password. The password is included in the transmitted packet, so this method of authentication is relatively insecure.
- **md5** Use the MD5 algorithm to create an encoded checksum of the packet. The encoded checksum is included in the transmitted packet. The receiving routing platform uses the authentication key to verify the packet, discarding it if the digest does not match. This algorithm provides a more secure authentication scheme.
- **Default:** none (no authentication is performed).

## Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

## Release Information

Statement introduced before Junos OS Release 7.4.

## RELATED DOCUMENTATION

[Configuring VRRP Authentication \(IPv4 Only\)](#)

[authentication-key](#) | **1141**

[version-3](#)

*Understanding VRRP on SRX Series Devices*

*Example: Configuring VRRP/VRRPv3 on Chassis Cluster Redundant Ethernet Interfaces*

## bandwidth-threshold

### IN THIS SECTION

- [Syntax](#) | **1145**
- [Hierarchy Level](#) | **1145**
- [Description](#) | **1146**
- [Options](#) | **1146**
- [Required Privilege Level](#) | **1146**
- [Release Information](#) | **1146**

### Syntax

```
bandwidth-threshold bits-per-second priority-cost priority;
```

### Hierarchy Level

```
[edit interfaces interface-name unit logical-unit-number family inet address address vrrp-group group-id track interface interface-name],
[edit interfaces interface-name unit logical-unit-number family inet6 address address vrrp-inet6-group group-id track interface interface-name],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family inet address address vrrp-group group-id track interface interface-name],
```

```
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number
family inet6 address address vrrp-inet6-group group-id track interface interface-name]
```

## Description

Specify the bandwidth threshold for Virtual Router Redundancy Protocol (VRRP) logical interface tracking.

## Options

*bits-per-second*—Bandwidth threshold for the tracked interface. When the bandwidth of the tracked interface drops below the specified value, the VRRP group uses the bandwidth threshold priority cost value. You can include up to five bandwidth threshold statements for each interface you track.

- **Range:** 1 through 10000000000000 bits per second

*priority-cost priority*—The value subtracted from the configured VRRP priority when the tracked interface or route is down to force a new primary router election. The sum of all the costs for all interfaces or routes that are tracked must be less than or equal to the configured priority of the VRRP group.

## Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 8.1.

## RELATED DOCUMENTATION

| [Configuring a Logical Interface to Be Tracked for a VRRP Group](#)

## delegate-processing (VRRP)

### IN THIS SECTION

- [Syntax | 1147](#)
- [Hierarchy Level | 1147](#)
- [Description | 1147](#)
- [Options | 1148](#)
- [Required Privilege Level | 1148](#)
- [Release Information | 1148](#)

### Syntax

```
delegate-processing {  
    ae-irb;  
}
```

### Hierarchy Level

```
[edit protocols vrrp]
```

### Description

Configure the distributed periodic packet management process (ppmd) to send Virtual Router Redundancy Protocol (VRRP) advertisements .

Using a hash logic based on iflIndex, the vrrp group ID, and the IP version, select one of the Flexible OIC Concentrators (FPCs) for distribution. The selected FPC is called the *anchor FPC*. All transmit instances and receive instances are from and to the anchor FPC. The anchor FPC is static, and VRRP is not guaranteed to get distributed to all available FPCs uniformly for all VRRP sessions.

## Options

**ae-irb** Enable distributed pppd for VRRP over aggregated Ethernet and integrated routing and bridging (IRB) interfaces.

Using the ae-irb option is only for MPC line cards. ae-irb is not supported on small MX Series routing devices with built-in MPCs such as the MX104 and below. Using the ae-irb option requires use of the enhanced-ip mode.

## Required Privilege Level

routing—To view this statement in the configuration.

routing-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 9.6.

ae-irb option introduced in Junos OS Release 15.1.

## RELATED DOCUMENTATION

Enabling the Distributed Periodic Packet Management Process for VRRP

## failover-delay

### IN THIS SECTION

- [Syntax | 1149](#)
- [Hierarchy Level | 1149](#)
- [Description | 1149](#)
- [Options | 1149](#)
- [Required Privilege Level | 1149](#)
- [Release Information | 1149](#)

## Syntax

```
failover-delay milliseconds;
```

## Hierarchy Level

```
[edit protocols vrrp]
```

## Description

If you configure multiple VRRP groups on an interface (using multiple VLANs), traffic for some of the groups might be briefly dropped if a failover occurs. This can happen because the new primary must send gratuitous ARP replies for each VRRP group to update the ARP tables in the connected devices, and there is a short delay between each gratuitous ARP reply. Traffic sent by devices that have not yet received the gratuitous ARP reply is dropped (until the device receives the reply and learns the MAC address of the new primary).

If you configure a failover delay, the new primary delays sending gratuitous ARP replies for the period that you set. This allows the new primary to send the ARP replies for all of the VRRP groups simultaneously.

## Options

*milliseconds*—Specify the failover delay time, in milliseconds.

- **Range:** 50 through 2000

## Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 11.3.

## RELATED DOCUMENTATION

Troubleshooting VRRP

[show vrrp](#)

## failover-delay

### IN THIS SECTION

- [Syntax | 1150](#)
- [Hierarchy Level | 1150](#)
- [Description | 1150](#)
- [Options | 1150](#)
- [Required Privilege Level | 1151](#)
- [Release Information | 1151](#)

### Syntax

```
failover-delay milliseconds;
```

### Hierarchy Level

```
[edit protocols vrrp]
```

### Description

Configure the failover delay for VRRP and VRRP for IPv6 operations.

### Options

*milliseconds*—Specify the failover delay time, in milliseconds.

- **Range:** 50 through 2000



## Required Privilege Level

routing—To view this statement in the configuration.

routing-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 9.4.

## RELATED DOCUMENTATION

Configuring VRRP and VRRP for IPv6

## fast-interval

### IN THIS SECTION

- [Syntax | 1151](#)
- [Hierarchy Level | 1152](#)
- [Description | 1152](#)
- [Options | 1152](#)
- [Required Privilege Level | 1153](#)
- [Release Information | 1153](#)

## Syntax

```
fast-interval milliseconds;
```

## Hierarchy Level

```
[edit interfaces interface-name unit logical-unit-number family inet address address vrrp-group group-id],
[edit interfaces interface-name unit logical-unit-number family inet6 address address vrrp-inet6-group group-id],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family inet address address vrrp-group group-id],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family inet6 address address vrrp-inet6-group group-id]
```

## Description

Configure the interval, in milliseconds, between Virtual Router Redundancy Protocol (VRRP) advertisement packets.

All routers in the VRRP group must use the same advertisement interval.

## Options

*milliseconds*—Interval between advertisement packets.

- **Range:**
  - 10 through 40,950 milliseconds for VRRPv3.
  - 100-999 milliseconds for VRRP.

**NOTE:** When configuring VRRPv2, we recommend using `advertise-interval` instead of `fast-interval`.

- **NOTE:** When configuring VRRP for IPv4, if you have chosen not to enable VRRPv3, you cannot set a value less than 100 for `fast-interval`. Commit check fails if a value less than 100 is configured.
- **Default:** 1 second

## Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

## Release Information

Statement introduced before Junos OS Release 7.4.

## RELATED DOCUMENTATION

Configuring the Advertisement Interval for the VRRP Primary Router

[advertise-interval](#) | [1137](#)

[advertise-interval](#) | [1137](#)

[inet6-advertise-interval](#) | [1159](#)

[version-3](#) | [1186](#)

## global-advertisements-threshold

### IN THIS SECTION

- [Syntax](#) | [1153](#)
- [Hierarchy Level](#) | [1154](#)
- [Description](#) | [1154](#)
- [Options](#) | [1154](#)
- [Required Privilege Level](#) | [1154](#)
- [Release Information](#) | [1155](#)

## Syntax

```
global-advertisements-threshold advertisement-value;
```

## Hierarchy Level

[edit protocols vrrp]

## Description

Configure the number of fast advertisements that can be missed by a backup router before the primary router is declared as down.

### NOTE:

- The advertisement value configured using the `global-advertisements-threshold` statement is applicable to all the Virtual Router Redundancy Protocol (VRRP) groups in the system.
- Setting the advertisement value of the **global-advertisements-threshold** configuration to **1** is not recommended for a scaled configuration with an aggressive advertisement interval. For example, if you have 1000 VRRP groups with an advertisement interval of 100 ms, then do not set the **global-advertisements-threshold** value to 1.
- Changing the advertisement value of the **global-advertisements-threshold** configuration during runtime can result in unpredictable behavior by the VRRP state machine. For example, momentary ownership change from the primary router to the backup router and vice versa. Therefore, avoid changing the advertisement value of the `global-advertisements-threshold` statement during runtime.

## Options

***advertisement-value***—Number of VRRP advertisements missed before the primary router is declared as down.

- **Range:** 1 through 15
- **Default:** 3

## Required Privilege Level

routing—To view this statement in the configuration.

routing-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 12.2.

## RELATED DOCUMENTATION

Improving the Convergence Time for VRRP

Configuring VRRP to Improve Convergence Time

## hold-time (VRRP)

### IN THIS SECTION

- [Syntax | 1155](#)
- [Hierarchy Level | 1155](#)
- [Description | 1156](#)
- [Default | 1156](#)
- [Options | 1156](#)
- [Required Privilege Level | 1156](#)
- [Release Information | 1156](#)

## Syntax

```
hold-time seconds;
```

## Hierarchy Level

```
[edit interfaces interface-name unit logical-unit-number family inet address address vrrp-group group-id preempt],  
[edit interfaces interface-name unit logical-unit-number family inet6 address address vrrp-inet6-group group-id preempt],  
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number
```

```
family inet address address vrrp-group group-id preempt],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number
family inet6 address address vrrp-inet6-group group-id preempt]
```

## Description

In a Virtual Router Redundancy Protocol (VRRP) configuration, set the hold time before a higher-priority backup router preempts the primary router.

## Default

VRRP preemption is not timed.

## Options

*seconds*—Hold-time period.

- **Range:** 0 through 3600 seconds
- **Default:** 0 seconds (VRRP preemption is not timed.)

## Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

## Release Information

Statement introduced before Junos OS Release 7.4.

## RELATED DOCUMENTATION

Configuring a Backup Router to Preempt the VRRP Primary Router

Configuring VRRP Preemption and Hold Time

## hold-time

### IN THIS SECTION

- [Syntax | 1157](#)
- [Hierarchy Level | 1157](#)
- [Description | 1157](#)
- [Options | 1157](#)
- [Required Privilege Level | 1157](#)
- [Release Information | 1158](#)

### Syntax

```
hold-time seconds;
```

### Hierarchy Level

```
[edit interfaces interface-name unit logical-unit-number family inet6 address address vrrp-inet6-  
group group-id preempt]
```

### Description

Configure the time in seconds after which a backup router with the highest priority preempts the primary router.

### Options

*seconds*—Hold-time period.

### Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 10.0.

## RELATED DOCUMENTATION

| [Configuring VRRP for IPv6 \(CLI Procedure\)](#)

## inherit-advertisement-interval

### IN THIS SECTION

- [Syntax | 1158](#)
- [Hierarchy Level | 1158](#)
- [Description | 1158](#)
- [Options | 1159](#)
- [Required Privilege Level | 1159](#)
- [Release Information | 1159](#)

## Syntax

```
inherit-advertisement-interval seconds;
```

## Hierarchy Level

```
[edit protocols vrrp]
```

## Description

Set the time interval for advertisement for inherit sessions.



## Options

### **inherit-advertisement-interval** *seconds*

Time interval for inherit sessions advertisements in seconds. The default value is the recommended value.

- **Default:** 120
- **Range:** 5 to 120

## Required Privilege Level

routing—To view this statement in the configuration.

routing-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 14.2R3.

## inet6-advertise-interval

### IN THIS SECTION

- [Syntax | 1159](#)
- [Hierarchy Level | 1160](#)
- [Description | 1160](#)
- [Options | 1160](#)
- [Required Privilege Level | 1160](#)
- [Release Information | 1160](#)

## Syntax

```
inet6-advertise-interval milliseconds;
```

## Hierarchy Level

```
[edit interfaces interface-name unit logical-unit-number family inet6 address address vrrp-inet6-group group-id],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number
family inet6 address address vrrp-inet6-group group-id]
```

## Description

Configure the interval between Virtual Router Redundancy Protocol (VRRP) IPv6 advertisement packets.

All routers in the VRRP group must use the same advertisement interval.

**NOTE:** When VRRPv3 is enabled, the `inet6-advertise-interval` statement cannot be used to configure advertisement intervals. Instead, use the `fast-interval` statement to configure advertisement intervals.

## Options

***milliseconds***—Interval, in milliseconds, between advertisement packets.

- **Range:** 100 to 40,000 milliseconds (ms)
- **Default:** 1 second

## Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 8.4R2.

## RELATED DOCUMENTATION

Configuring the Advertisement Interval for the VRRP Primary Router

[advertise-interval](#) | **1137**

[fast-interval | 1151](#)[version-3 | 1186](#)

## inet6-advertise-interval

### IN THIS SECTION

- [Syntax | 1161](#)
- [Hierarchy Level | 1161](#)
- [Description | 1161](#)
- [Options | 1161](#)
- [Required Privilege Level | 1162](#)
- [Release Information | 1162](#)

### Syntax

```
inet6-advertise-interval milliseconds;
```

### Hierarchy Level

```
[edit interfaces interface-name unit logical-unit-number family inet6 address address vrrp-inet6-group group-id]
```

### Description

Configure the interval between Virtual Router Redundancy Protocol (VRRP) IPv6 advertisement packets.

### Options

***milliseconds***—Interval, in milliseconds, between advertisement packets.

- **Range:** 100 to 40,000 ms

- **Default:** 1 second

## Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 10.0.

## RELATED DOCUMENTATION

| [Configuring VRRP for IPv6 \(CLI Procedure\)](#)

# interface

## IN THIS SECTION

- [Syntax | 1162](#)
- [Hierarchy Level | 1163](#)
- [Description | 1163](#)
- [Options | 1163](#)
- [Required Privilege Level | 1163](#)
- [Release Information | 1163](#)

## Syntax

```
interface interface-name {
    bandwidth-threshold bits-per-second priority-cost priority;
    priority-cost priority;
}
```

## Hierarchy Level

```
[edit interfaces interface-name unit logical-unit-number family inet address address vrrp-group group-id track],
[edit interfaces interface-name unit logical-unit-number family inet6 address address vrrp-inet6-group group-id track],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family inet address address vrrp-group group-id track],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family inet6 address address vrrp-inet6-group group-id track]
```

## Description

Enable logical interface tracking for a Virtual Router Redundancy Protocol (VRRP) group.

## Options

***interface-name***—Interface to be tracked for this VRRP group.

- **Range:** 1 through 10 interfaces

The remaining statements are described separately.

## Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

## Release Information

Statement introduced before Junos OS Release 7.4.

**bandwidth-threshold** statement added in Junos OS Release 8.1.

## RELATED DOCUMENTATION

Configuring a Logical Interface to Be Tracked for a VRRP Group

[Junos OS Services Interfaces Library for Routing Devices](#)

## preempt (VRRP)

### IN THIS SECTION

- [Syntax | 1164](#)
- [Hierarchy Level | 1164](#)
- [Description | 1164](#)
- [Default | 1165](#)
- [Required Privilege Level | 1165](#)
- [Release Information | 1165](#)

### Syntax

```
(preempt | no-preempt) {
    hold-time seconds;
}
```

### Hierarchy Level

```
[edit interfaces interface-name unit logical-unit-number family inet address address vrrp-
group group-id],
[edit interfaces interface-name unit logical-unit-number family inet6 address address vrrp-inet6-
group group-id],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number
family inet address address vrrp-group group-id],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number
family inet6 address address vrrp-inet6-group group-id]
```

### Description

In a Virtual Router Redundancy Protocol (VRRP) configuration, determine whether or not a backup router can preempt a primary router:

- `preempt`—Allow the primary router to be preempted.

**NOTE:** By default, a higher-priority backup router can preempt a lower-priority primary router.

- **no-preempt**—Prohibit the preemption of the primary router. When **no-preempt** is configured, the backup router cannot preempt the primary router even if the backup router has a higher priority.

The remaining statement is explained separately. See [CLI Explorer](#).

## Default

By default the **preempt** statement is enabled, and a higher-priority backup router preempts a lower-priority primary router even if the **preempt** statement is not explicitly configured.

## Required Privilege Level

**interface**—To view this statement in the configuration.

**interface-control**—To add this statement to the configuration.

## Release Information

Statement introduced before Junos OS Release 7.4.

## RELATED DOCUMENTATION

Configuring a Backup Router to Preempt the VRRP Primary Router

Configuring VRRP Preemption and Hold Time

## preempt

### IN THIS SECTION

- [Syntax | 1166](#)
- [Hierarchy Level | 1166](#)
- [Description | 1166](#)

- Required Privilege Level | **1166**
- Release Information | **1166**

## Syntax

```
(preempt | no-preempt) {  
    hold-time seconds;  
}
```

## Hierarchy Level

```
[edit interfaces interface-name unit logical-unit-number family inet6 address address vrrp-inet6-  
group group-id]
```

## Description

Configure whether a backup router can preempt a primary router:

- **preempt**—Allow the primary router to be preempted.
- **no-preempt**—Prohibit the preemption of the primary router.

The remaining statement is explained separately. See [CLI Explorer](#).

## Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 10.0.



## RELATED DOCUMENTATION

Configuring VRRP for IPv6 (CLI Procedure)

## priority (Protocols VRRP)

### IN THIS SECTION

- [Syntax | 1167](#)
- [Hierarchy Level | 1167](#)
- [Description | 1168](#)
- [Options | 1168](#)
- [Required Privilege Level | 1168](#)
- [Release Information | 1168](#)

### Syntax

```
priority priority;
```

### Hierarchy Level

```
[edit interfaces interface-name unit logical-unit-number family inet address address vrrp-  
group group-id],  
[edit interfaces interface-name unit logical-unit-number family inet6 address address vrrp-inet6-  
group group-id],  
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number  
family inet address address vrrp-group group-id],  
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number  
family inet6 address address vrrp-inet6-group group-id]
```

## Description

Configure a Virtual Router Redundancy Protocol (VRRP) device's priority for becoming the primary default device. The device with the highest priority within the group becomes the primary. VRRP is designed to eliminate the single point of failure inherent in the static default routed environment. VRRP specifies an election protocol that dynamically assigns responsibility for a virtual router to one of the VRRP routers on a LAN. The VRRP router controlling the IP address(es) associated with a virtual router is called the Primary, and forwards packets sent to these IP addresses. The election process provides dynamic fail-over in the forwarding responsibility when the Primary become unavailable. Any of the virtual router's IP addresses on a LAN can then be used as the default first hop router by end-hosts. The advantage gained from using VRRP is a higher availability default path without requiring configuration of dynamic routing or router discovery protocols on every end-host.

## Options

**priority** Device's priority for being elected to be the primary device in the VRRP group. A larger value indicates a higher priority for being elected.

- **Range:** 0 through 255
- **Default:** 100. If two or more devices have the highest priority in the VRRP group, the device with the VRRP interface that has the highest IP address becomes the primary, and the others serve as backups.

## Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

## Release Information

Statement introduced before Junos OS Release 7.4.

## RELATED DOCUMENTATION

[Configuring Basic VRRP Support](#)

*Understanding VRRP on SRX Series Devices*

*Example: Configuring VRRP/VRRPv3 on Chassis Cluster Redundant Ethernet Interfaces*

## priority

### IN THIS SECTION

- [Syntax | 1169](#)
- [Hierarchy Level | 1169](#)
- [Description | 1169](#)
- [Options | 1169](#)
- [Required Privilege Level | 1170](#)
- [Release Information | 1170](#)

### Syntax

```
priority number;
```

### Hierarchy Level

```
[edit interfaces interface-name unit logical-unit-number family inet address address vrrp-group  
group-id],  
[edit interfaces interface-name unit logical-unit-number family inet6 address address vrrp-inet6-  
group group-id]
```

### Description

Configure a switch's priority for becoming the primary default routing platform. The routing platform with the highest priority within the group becomes the primary.

### Options

***number***—Routing platform's priority for being elected to be the primary router in the VRRP group. A larger value indicates a higher priority for being elected.

- **Range:** 1 through 255

- **Default:** 100 (for backup routers)

**NOTE:** Priority 255 cannot be assigned to routed VLAN interfaces (RVIs).

## Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 10.0.

## RELATED DOCUMENTATION

| [Configuring VRRP for IPv6 \(CLI Procedure\)](#)

## priority-cost (VRRP)

### IN THIS SECTION

- [Syntax | 1171](#)
- [Hierarchy Level | 1171](#)
- [Description | 1171](#)
- [Options | 1171](#)
- [Required Privilege Level | 1171](#)
- [Release Information | 1171](#)

## Syntax

```
priority-cost priority;
```

## Hierarchy Level

```
[edit interfaces interface-name unit logical-unit-number family inet address address vrrp-  
group group-id track interface interface-name],  
[edit interfaces interface-name unit logical-unit-number family inet6 address address vrrp-inet6-  
group group-id track interface interface-name],  
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number  
family inet address address vrrp-group group-id track interface interface-name],  
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number  
family inet6 address address vrrp-inet6-group group-id track interface interface-name]
```

## Description

Configure a Virtual Router Redundancy Protocol (VRRP) router's priority cost for becoming the primary default router. The router with the highest priority within the group becomes the primary.

## Options

***priority***—The value subtracted from the configured VRRP priority when the tracked interface or route is down to force a new primary router election. The sum of all the costs for all interfaces or routes that are tracked must be less than or equal to the configured priority of the VRRP group.

- **Range:** 1 through 254

## Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

## Release Information

Statement introduced before Junos OS Release 7.4.

Statement introduced in Junos OS Release 12.2 for ACX2000 Universal Metro Routers.

## RELATED DOCUMENTATION

Configuring a Logical Interface to Be Tracked for a VRRP Group

## priority-hold-time

### IN THIS SECTION

- [Syntax | 1172](#)
- [Hierarchy Level | 1172](#)
- [Description | 1173](#)
- [Options | 1173](#)
- [Required Privilege Level | 1173](#)
- [Release Information | 1173](#)

### Syntax

```
priority-hold-time seconds;
```

### Hierarchy Level

```
[edit interfaces interface-name unit logical-unit-number family inet address address vrrp-group group-id track],  
[edit interfaces interface-name unit logical-unit-number family inet6 address address vrrp-inet6-group group-id track],  
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family inet address address vrrp-group group-id track],  
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family inet6 address address vrrp-inet6-group group-id track]
```

## Description

Configure a Virtual Router Redundancy Protocol (VRRP) router's priority hold time to define the minimum length of time that must elapse between dynamic priority changes. If the dynamic priority changes because of a tracking event, the priority hold timer begins running. If another tracking event or manual configuration change occurs while the timer is running, the new dynamic priority update is postponed until the timer expires.

**NOTE:** When the track feature is configured, and if VRRP should pre-empt due to the tracking interface or route transition, any configured pre-empt hold time will be ignored. VRRP primary will pre-empt according to the configuration of the priority-hold time.

## Options

***seconds***—Minimum length of time that must elapse between dynamic priority changes.

- **Range:** 0 through 3600 seconds

## Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 8.1.

## RELATED DOCUMENTATION

| [Configuring a Logical Interface to Be Tracked for a VRRP Group](#)

## route (Interfaces)

### IN THIS SECTION

- [Syntax | 1174](#)
- [Hierarchy Level | 1174](#)
- [Description | 1174](#)
- [Options | 1174](#)
- [Required Privilege Level | 1175](#)
- [Release Information | 1175](#)

### Syntax

```
route prefix routing-instance instance-name priority-cost priority;
```

### Hierarchy Level

```
[edit interfaces interface-name unit logical-unit-number family inet address address vrrp-group group-id track],
[edit interfaces interface-name unit logical-unit-number family inet6 address address vrrp-inet6-group group-id track],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family inet address address vrrp-group group-id track],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family inet6 address address vrrp-inet6-group group-id track]
```

### Description

Enable route tracking for a Virtual Router Redundancy Protocol (VRRP) group.

### Options

*prefix*—Route to be tracked for this VRRP group.



**priority-cost** *priority*—The value subtracted from the configured VRRP priority when the tracked interface or route is down, forcing a new primary router election. The sum of all the costs for all interfaces or routes that are tracked must be less than or equal to the configured priority of the VRRP group.

**routing-instance** *instance-name*—Routing instance in which the route is to be tracked. If the route is in the default, or global, routing instance, the value for *instance-name* must be **default**.

## Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 9.0.

## RELATED DOCUMENTATION

| [Configuring a Route to Be Tracked for a VRRP Group](#)

## skew-timer-disable

### IN THIS SECTION

- [Syntax | 1176](#)
- [Hierarchy Level | 1176](#)
- [Description | 1176](#)
- [Default | 1176](#)
- [Required Privilege Level | 1176](#)
- [Release Information | 1176](#)

## Syntax

```
skew-timer-disable;
```

## Hierarchy Level

```
[edit protocols vrrp]
```

## Description

Disable the skew timer, thereby reducing the time required to transition from the backup state to the primary state.

**NOTE:** The `skew-timer-disable` statement is used when there is only one primary router and one backup router in the network.

## Default

By default, the skew timer is enabled for all the VRRP groups.

## Required Privilege Level

routing—To view this statement in the configuration.

routing-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 12.2.

## RELATED DOCUMENTATION

Improving the Convergence Time for VRRP

Configuring VRRP to Improve Convergence Time

## startup-silent-period

### IN THIS SECTION

- [Syntax | 1177](#)
- [Hierarchy Level | 1177](#)
- [Description | 1177](#)
- [Options | 1177](#)
- [Required Privilege Level | 1178](#)
- [Release Information | 1178](#)

### Syntax

```
startup-silent-period seconds;
```

### Hierarchy Level

```
[edit protocols vrrp]
```

### Description

Instruct the system to ignore the Primary Down Event when an interface transitions from the down state to the up state. This statement is used to avoid incorrect error alarms caused by the delay or interruption of incoming Virtual Router Redundancy Protocol (VRRP) advertisement packets during the interface startup phase.

### Options

***seconds***—Number of seconds for the startup period.

- **Default:** 4 seconds
- **Range:** 1 through 2000 seconds

## Required Privilege Level

routing—To view this statement in the configuration.

routing-control—To add this statement to the configuration.

## Release Information

Statement introduced before Junos OS Release 7.4.

## RELATED DOCUMENTATION

Configuring the Startup Period for VRRP Operations

# traceoptions (Protocols VRRP)

## IN THIS SECTION

- [Syntax | 1178](#)
- [Hierarchy Level | 1179](#)
- [Description | 1179](#)
- [Default | 1179](#)
- [Options | 1179](#)
- [Required Privilege Level | 1180](#)
- [Release Information | 1180](#)

## Syntax

```
traceoptions {  
    file filename <files number> <match regular-expression> <microsecond-stamp> <size size>  
    <world-readable | no-world-readable>;  
    flag flag;
```

```
no-remote-trace;
}
```

## Hierarchy Level

```
[edit protocols vrrp]
```

## Description

Define tracing operations for the Virtual Router Redundancy Protocol (VRRP) process.

To specify more than one tracing operation, include multiple `flag` statements.

By default, VRRP logs the error, dcd configuration, and routing socket events in a file in the directory `/var/log`.

## Default

If you do not include this statement, no VRRP-specific tracing operations are performed.

## Options

**file *filename***—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory `/var/log`. By default, VRRP tracing output is placed in the file `vrrpd`.

**files *number***—(Optional) Maximum number of trace files. When a trace file named *trace-file* reaches its maximum size, it is renamed *trace-file.0*, then *trace-file.1*, and so on, until the maximum number of trace files is reached. When the maximum number is reached, the oldest trace file is overwritten.

- **Range:** 0 through 4,294,967,296 files
- **Default:** 3 files

If you specify a maximum number of files, you also must specify a maximum file size with the **size** option.

**flag *flag***—Tracing operation to perform. To specify more than one tracing operation, include multiple `flag` statements. These are the VRRP-specific tracing options:

- **all**—All VRRP tracing operations
- **database**—Database changes

- **general**—General events
- **interfaces**—Interface changes
- **normal**—Normal events
- **packets**—Packets sent and received
- **state**—State transitions
- **timer**—Timer events

**match *regular-expression***—(Optional) Refine the output to include only those lines that match the given regular expression.

**microsecond-stamp**—(Optional) Provide a timestamp with microsecond granularity.

**no-world-readable**—(Optional) Restrict users from reading the log file.

**size *size***—(Optional) Maximum size of each trace file, in kilobytes, megabytes, or gigabytes. When a trace file named *trace-file* reaches this size, it is renamed *trace-file.0*. When the *trace-file* again reaches its maximum size, *trace-file.0* is renamed *trace-file.1* and *trace-file* is renamed *trace-file.0*. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

- **Syntax:** *xk* to specify KB, *xm* to specify MB, or *xg* to specify GB
- **Range:** 10 KB through the maximum file size supported on your routing platform
- **Default:** 1 MB

If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option.

**world-readable**—(Optional) Allow users to read the log file.

## Required Privilege Level

**trace**—To view this statement in the configuration.

**trace-control**—To add this statement to the configuration.

## Release Information

Statement introduced before Junos OS Release 7.4.

## RELATED DOCUMENTATION

| [Tracing VRRP Operations](#)

## traceoptions

### IN THIS SECTION

- [Syntax | 1181](#)
- [Hierarchy Level | 1181](#)
- [Description | 1181](#)
- [Default | 1182](#)
- [Options | 1182](#)
- [Required Privilege Level | 1183](#)
- [Release Information | 1183](#)

### Syntax

```
traceoptions {  
    file <filename> <files number> <match regular-expression> <microsecond-stamp> <size size>  
<world-readable | no-world-readable>;  
    flag flag;  
    no-remote-trace;  
}
```

### Hierarchy Level

```
[edit protocols vrrp]
```

### Description

Define tracing operations for the Virtual Router Redundancy Protocol (VRRP) process.

To specify more than one tracing operation, include multiple `flag` statements.

By default, VRRP logs the error, dcd configuration, and routing socket events in a file in the directory `/var/log`.

**NOTE:** The `traceoptions` statement is not supported on a QFabric system.

## Default

If you do not include this statement, no VRRP-specific tracing operations are performed.

## Options

**filename** *filename*—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory `/var/log`. By default, VRRP tracing output is placed in the file `vrrpd`.

**files** *number*—(Optional) Maximum number of trace files. When a trace file named *trace-file* reaches its maximum size, it is renamed *trace-file.0*, then *trace-file.1*, and so on, until the maximum number of trace files is reached. When the maximum number is reached, the oldest trace file is overwritten.

- **Range:** 0 through 4,294,967,296 files
- **Default:** 3 files

If you specify a maximum number of files, you also must specify a maximum file size with the **size** option.

**flag** *flag*—Tracing operation to perform. To specify more than one tracing operation, include multiple `flag` statements. These are the VRRP-specific tracing options:

- **all**—All VRRP tracing operations
- **database**—Database changes
- **general**—General events
- **interfaces**—Interface changes
- **normal**—Normal events
- **packets**—Packets sent and received
- **state**—State transitions



- **timer**—Timer events

**match *regex***—(Optional) Refine the output to include only those lines that match the given regular expression.

**microsecond-stamp**—(Optional) Provide a timestamp with microsecond granularity.

**no-world-readable**—Restrict users from reading the log file.

**size *size***—(Optional) Maximum size of each trace file, in kilobytes, megabytes, or gigabytes. When a trace file named *trace-file* reaches this size, it is renamed *trace-file.0*. When the *trace-file* again reaches its maximum size, *trace-file.0* is renamed *trace-file.1* and *trace-file* is renamed *trace-file.0*. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

- **Syntax:** *xk* to specify KB, *xm* to specify MB, or *xg* to specify GB
- **Range:** 10 KB through the maximum file size supported on your routing platform
- **Default:** 1 MB

If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option.

**world-readable**—Allow users to read the log file.

## Required Privilege Level

**interface**—To view this statement in the configuration.

**interface-control**—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 11.3.

## RELATED DOCUMENTATION

| Tracing VRRP Operations

## track (VRRP)

### IN THIS SECTION

- [Syntax | 1184](#)
- [Syntax for cRPD | 1184](#)
- [Hierarchy Level | 1185](#)
- [Description | 1185](#)
- [Options | 1185](#)
- [Required Privilege Level | 1185](#)
- [Release Information | 1186](#)

### Syntax

```
track {
    interface interface-name {
        bandwidth-threshold bits-per-second priority-cost priority;
        priority-cost priority;
    }
    priority-hold-time seconds;
    route prefix/prefix-length routing-instance instance-name priority-cost priority;
}
```

### Syntax for cRPD

```
track {
    interface interface-name
    notify-backup {script-name name of script;
    username username}
    notify-fault {script-name name of script;
    username username}
    notify-master {script-name name of script;
    username username}
    notify-script {Notify script for VRRP group}
    track-script {Script instance;
```

```

    keepalived_check fall/interval/rise script-name name of script/time-out;
    weight cost/reverse;}
}

```

## Hierarchy Level

```

[edit interfaces interface-name unit logical-unit-number family inet address address vrrp-
group group-id],
[edit interfaces interface-name unit logical-unit-number family inet6 address address vrrp-inet6-
group group-id],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number
family inet address address vrrp-group group-id],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number
family inet6 address address vrrp-inet6-group group-id]

```

## Description

Enable logical interface tracking, route tracking, or both, for a Virtual Router Redundancy Protocol (VRRP) group.

## Options

The remaining statements are described separately.

<b>notify-backup</b>	Notify script to BACKUP transition
<b>notify-fault</b>	Notify script to FAULT transition
<b>notify-master</b>	Notify script to MASTER transition
<b>notify-script</b>	Notify script for VRRP group
<b>track-script</b>	Tracking script for VRRP group

## Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

## Release Information

Statement introduced before Junos OS Release 7.4.

priority-hold-time statement added in Junos OS Release 8.1.

route statement added in Junos OS Release 9.0.

## RELATED DOCUMENTATION

[Configuring a Logical Interface to Be Tracked for a VRRP Group](#)

[Configuring a Route to Be Tracked for a VRRP Group](#)

## version-3

### IN THIS SECTION

- [Syntax | 1186](#)
- [Hierarchy Level | 1186](#)
- [Description | 1187](#)
- [Default | 1187](#)
- [Required Privilege Level | 1187](#)
- [Release Information | 1187](#)

## Syntax

```
version-3;
```

## Hierarchy Level

```
[edit protocols vrrp]
```

## Description

Enable Virtual Router Redundancy Protocol version 3 (VRRPv3).

### NOTE:

- Even though the `version-3` statement can be configured only at the `[edit protocols vrrp]` hierarchy level, VRRPv3 is enabled on all the configured logical systems as well.
- When enabling VRRPv3, you must ensure that VRRPv3 is enabled on all the VRRP routers in the network. This is because VRRPv3 does not interoperate with the previous versions of VRRP.

## Default

### Required Privilege Level

routing—To view this statement in the configuration.

routing-control—To add this statement to the configuration.

### Release Information

Statement introduced in Junos OS Release 12.2.

### RELATED DOCUMENTATION

| Junos OS Support for VRRPv3

## virtual-address

### IN THIS SECTION

- [Syntax | 1188](#)
- [Hierarchy Level | 1188](#)

- [Description | 1188](#)
- [Options | 1188](#)
- [Required Privilege Level | 1188](#)
- [Release Information | 1189](#)

## Syntax

```
virtual-address [ addresses ];
```

## Hierarchy Level

```
[edit interfaces interface-name unit logical-unit-number family inet address address vrrp-  
group group-id],  
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number  
family inet address address vrrp-group group-id]
```

## Description

Configure the addresses of the devices in a Virtual Router Redundancy Protocol (VRRP) IPv4 or IPv6 group. You can configure up to eight addresses.

## Options

**addresses** Addresses of one or more devices. Do not include a prefix length. If the address is the same as the interface's physical address, the interface becomes the primary device for the group.

## Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

## Release Information

Statement introduced before Junos OS Release 7.4.

## RELATED DOCUMENTATION

[Configuring Basic VRRP Support](#)

*Understanding VRRP on SRX Series Devices*

*Example: Configuring VRRP/VRRPv3 on Chassis Cluster Redundant Ethernet Interfaces*

## virtual-inet6-address

### IN THIS SECTION

- [Syntax | 1189](#)
- [Hierarchy Level | 1189](#)
- [Description | 1190](#)
- [Options | 1190](#)
- [Required Privilege Level | 1190](#)
- [Release Information | 1190](#)

## Syntax

```
virtual-inet6-address [ addresses ];
```

## Hierarchy Level

```
[edit interfaces interface-name unit logical-unit-number family inet6 address address vrrp-inet6-group group-id],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number
family inet6 address address vrrp-inet6-group group-id]
```

## Description

Configure the addresses of the virtual routers in a Virtual Router Redundancy Protocol (VRRP) IPv6 group. You can configure up to eight addresses.

## Options

**addresses**—Addresses of one or more virtual routers. Do not include a prefix length. If the address is the same as the interface's physical address, the interface becomes the primary virtual router for the group.

## Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

## Release Information

Statement introduced before Junos OS Release 7.4.

## RELATED DOCUMENTATION

| [Configuring Basic VRRP Support](#)

## virtual-link-local-address

### IN THIS SECTION

- [Syntax | 1191](#)
- [Hierarchy Level | 1191](#)
- [Description | 1191](#)
- [Options | 1191](#)
- [Required Privilege Level | 1191](#)
- [Release Information | 1191](#)



## Syntax

```
virtual-link-local-address ipv6-address;
```

## Hierarchy Level

```
[edit interfaces interface-name unit logical-unit-number family inet6 address address vrrp-inet6-group group-id],  
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number  
family inet6 address address vrrp-inet6-group group-id]
```

## Description

Used to explicitly configure a virtual link-local address for a Virtual Router Redundancy Protocol (VRRP) IPv6 group. The virtual link-local address must be configured to be on a fe80::/64 subnet for proper operation. Early versions of the Junos OS required manual configuration of this parameter. In current Junos releases a virtual link local address is automatically created based on the interface's MAC address.

**NOTE:** In current Junos releases you do *not* need to configure link-local addresses and virtual link-local addresses when configuring VRRP for IPv6. Junos OS automatically generates link-local addresses and virtual link-local addresses. However, if link local addresses and virtual link-local addresses are configured, Junos OS honors the explicitly configured addresses.

## Options

*ipv6-address*—virtual link-local IPv6 address for VRRP for an IPv6 group.

- **Range:** 0 through 255

## Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 8.4.

## RELATED DOCUMENTATION

Configuring Basic VRRP Support

Junos OS Support for VRRPv3

## vrrp-group

### IN THIS SECTION

- [Syntax | 1192](#)
- [Hierarchy Level | 1193](#)
- [Description | 1193](#)
- [Options | 1193](#)
- [Required Privilege Level | 1194](#)
- [Release Information | 1194](#)

## Syntax

```
vrrp-group group-id {  
    (accept-data | no-accept-data);  
    advertise-interval seconds;  
    global-advertisements-threshold number;  
    authentication-key key;  
    authentication-type authentication;  
    fast-interval milliseconds;  
    (preempt | no-preempt) {  
        hold-time seconds;  
    }  
    priority number;  
    track {  
        interface interface-name {  
            bandwidth-threshold bits-per-second priority-cost priority;  
            priority-cost priority;  
        }  
        priority-hold-time seconds;  
    }  
}
```

```

    route prefix/prefix-length routing-instance instance-name priority-cost priority;
  }
  virtual-address [ addresses ];
  vrrp-inherit-from vrrp-group;

}

```

## Hierarchy Level

```

[edit interfaces interface-name unit logical-unit-number family inet address address],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number
family inet address address]

```

## Description

Configure a Virtual Router Redundancy Protocol (VRRP) IPv4 group. As of Junos OS Release 13.2, VRRP nonstop active routing (NSR) is enabled only when you configure the `nonstop-routing` statement at the `[edit routing-options]` or `[edit logical system logical-system-name routing-options hierarchy level`.

## Options

*group-id*—VRRP group identifier. If you enable MAC source address filtering on the interface, you must include the virtual MAC address in the list of source MAC addresses that you specify in the `source-address-filter` statement. MAC addresses ranging from 00:00:5e:00:53:01 through 00:00:5e:00:53:ff are reserved for VRRP, as defined in RFC 2338. The VRRP group number must be the decimal equivalent of the last hexadecimal byte of the virtual MAC address.

- **Range:** 0 through 255

**NOTE:** Under certain circumstances, the group identifier that you enter must be different from any other group identifiers that you configured for logical units of this same physical interface. See [Configuring Basic VRRP Support](#) for more information.

The remaining statements are explained separately. Click a linked statement in the Syntax section for more information about that statement.

## Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

## Release Information

Statement introduced before Junos OS Release 7.4.

## RELATED DOCUMENTATION

Configuring Basic VRRP Support

Configuring VRRP

Example: Configuring VRRP for Load Sharing

[vrrp-inet6-group](#) | **1194**

[nonstop-routing](#) | **1064**

## vrrp-inet6-group

### IN THIS SECTION

- [Syntax](#) | **1194**
- [Hierarchy Level](#) | **1195**
- [Description](#) | **1195**
- [Options](#) | **1195**
- [Required Privilege Level](#) | **1196**
- [Release Information](#) | **1196**

## Syntax

```
vrrp-inet6-group group-id {
  (accept-data | no-accept-data);
```

```

advertisements-threshold number;
fast-interval milliseconds;
inet6-advertise-interval seconds;
(preempt | no-preempt) {
    hold-time seconds;
}
priority number;
track {
    interface interface-name {
        bandwidth-threshold bits-per-second priority-cost priority;
        priority-cost priority;
    }
    priority-hold-time seconds;
    route prefix/prefix-length routing-instance instance-name priority-cost priority;
}
virtual-inet6-address [ addresses ];
virtual-link-local-address ipv6-address;
vrrp-inherit-from vrrp-group;
}

```

## Hierarchy Level

```

[edit interfaces interface-name unit logical-unit-number family inet6 address address],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number
family inet6 address address]

```

## Description

Configure a Virtual Router Redundancy Protocol (VRRP) IPv6 group.

**NOTE:** The group identifier that you enter must be different from any other group identifiers that you configured for logical units of this same physical interface.

## Options

***group-id***—VRRP group identifier. If you enable MAC source address filtering on the interface, you must include the virtual MAC address in the list of source MAC addresses that you specify in the `source-address-filter` statement. MAC addresses ranging from **00:00:5e:00:01:00** through **00:00:5e:00:01:ff** are

reserved for VRRP, as defined in RFC 2338. The VRRP group number must be the decimal equivalent of the last hexadecimal byte of the virtual MAC address.

- **Range:** 0 through 255

The remaining statements are explained separately. See [CLI Explorer](#).

## Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

## Release Information

Statement introduced before Junos OS Release 7.4.

## RELATED DOCUMENTATION

| [Configuring Basic VRRP Support](#)

## vrrp-inherit-from

### IN THIS SECTION

- [Syntax | 1197](#)
- [Hierarchy Level | 1197](#)
- [Description | 1197](#)
- [Options | 1197](#)
- [Required Privilege Level | 1197](#)
- [Release Information | 1197](#)

## Syntax

```

vrp-inherit-from {
    active-group group-index;
    active-interface active-interface-name;
}

```

## Hierarchy Level

```

[edit interfaces interface-name unit logical-unit-number family inet6 vrp-inet6-group group-id]
[edit interfaces interface-name unit logical-unit-number family inet vrp-group group-id]

```

## Description

VRRP group to follow for the vrrp-group or vrrp-inet6-group.

## Options

*group-index*—Identifier for VRRP active group.

- **Range:** 0 through 255

*active-interface-name*—Interface name of VRRP active group.

## Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

## Release Information

Statement introduced before Junos OS Release 7.4.

## RELATED DOCUMENTATION

| Understanding VRRP

# Administration

## IN THIS CHAPTER

- [Upgrading Software on an EX6200 or EX8200 Standalone Switch Using Nonstop Software Upgrade \(CLI Procedure\) | 1198](#)
- [Upgrading Software on an EX8200 Virtual Chassis Using Nonstop Software Upgrade \(CLI Procedure\) | 1209](#)
- [Upgrading Software Using Nonstop Software Upgrade on EX Series Virtual Chassis and Mixed Virtual Chassis \(CLI Procedure\) | 1215](#)

## Upgrading Software on an EX6200 or EX8200 Standalone Switch Using Nonstop Software Upgrade (CLI Procedure)

## IN THIS SECTION

- [Preparing the Switch for Software Installation | 1199](#)
- [Upgrading Both Routing Engines Using NSSU | 1200](#)
- [Upgrading One Routing Engine Using NSSU \(EX8200 Switch Only\) | 1204](#)
- [Upgrading the Original Primary Routing Engine \(EX8200 Switch Only\) | 1207](#)

You can use nonstop software upgrade (NSSU) to upgrade the software on standalone EX6200 or EX8200 switches with redundant Routing Engines. NSSU upgrades the software running on the Routing Engines and line cards with minimal traffic disruption during the upgrade. NSSU is supported on EX8200 switches running Junos OS Release 10.4 or later and on EX6200 switches running Junos OS Release 12.2 or later.

This topic covers:



## Preparing the Switch for Software Installation

Before you begin software installation using NSSU:

- (Optional) Configure line-card upgrade groups as described in [Configuring Line-Card Upgrade Groups for Nonstop Software Upgrade](#). By default, an NSSU upgrades line cards one at a time to allow aggregated Ethernet links that have members on different line cards to remain up through the upgrade process. Configuring line-card upgrade groups reduces the time an upgrade takes because the line cards in each upgrade group are upgraded at the same time rather than sequentially.
- Verify that the Routing Engines are running the same version of the software. Enter the following command:

```
{master}
user@switch> show version invoke-on all-routing-engines
re0:
-----
Hostname: switch
Model: ex8208
JUNOS Base OS boot [11.3-20110429.1]
JUNOS Base OS Software Suite [11.3-20110429.1]
JUNOS Kernel Software Suite [11.3-20110429.1]
JUNOS Crypto Software Suite [11.3-20110429.1]
JUNOS Online Documentation [11.3-20110429.1]
JUNOS Enterprise Software Suite [11.3-20110429.1]
LC JUNOS Installation Software [11.3-20110429.1]
JUNOS Routing Software Suite [11.3-20110429.1]
JUNOS Web Management [11.3-20110429.1]

re1:
-----
Hostname: switch
Model: ex8208
JUNOS Base OS boot [11.3-20110429.1]
JUNOS Base OS Software Suite [11.3-20110429.1]
JUNOS Kernel Software Suite [11.3-20110429.1]
JUNOS Crypto Software Suite [11.3-20110429.1]
JUNOS Online Documentation [11.3-20110429.1]
JUNOS Enterprise Software Suite [11.3-20110429.1]
LC JUNOS Installation Software [11.3-20110429.1]
```

JUNOS Routing Software Suite [11.3-20110429.1]

JUNOS Web Management [11.3-20110429.1]

If the Routing Engines are not running the same version of the software, use the [request system software add](#) command to upgrade the Routing Engine that is running the earlier software version.

- Ensure that nonstop active routing (NSR) and graceful Routing Engine switchover (GRES) are enabled. To verify that they are enabled, you need to check only the state of nonstop active routing—if nonstop active routing is enabled, then graceful Routing Engine switchover is enabled.

To verify that nonstop active routing is enabled, execute the following command:

```
{master}
user@switch> show task replication
    Stateful Replication: Enabled
    RE mode: Master

    Protocol          Synchronization Status
    OSPF              Complete
    RIP               Complete
    PIM               Complete
    RSVP              Complete
```

If nonstop active routing is not enabled (**Stateful Replication is Disabled**), see [Configuring Nonstop Active Routing on Switches](#) for information on how to enable it.

- (Optional) Enable nonstop bridging (NSB). Enabling NSB ensures that all NSB-supported Layer 2 protocols operate seamlessly during the Routing Engine switchover that is part of the NSSU.
- (Optional) Back up the system software on each Routing Engine to an external storage device with the [request system snapshot](#) command.

## Upgrading Both Routing Engines Using NSSU

This procedure describes how to upgrade both Routing Engines using NSSU. When the upgrade completes, both Routing Engines are running the new version of the software, and the backup Routing Engine is the new primary Routing Engine.

To upgrade both Routing Engines using NSSU:

1. Download the software package.
2. Copy the software package to the switch. We recommend that you use FTP to copy the file to the `/var/tmp` directory.

3. Log in to the primary Routing Engine using the console connection. You can perform an NSSU from the management interface, but a console connection allows you to monitor the progress of the primary Routing Engine reboot.
4. Install the new software package:

```
{master}
user@switch> request system software nonstop-upgrade reboot
/var/tmp/package-name-m.nZx-distribution.tgz
```

where *package-name-m.nZx-distribution.tgz* is, for example, *jinstall-ex-8200-10.4R1.5-domestic-signed.tgz*.

The switch displays the following status messages as the upgrade executes:

```
Chassis ISSU Check Done
ISSU: Validating Image
ISSU: Preparing Backup RE
Pushing bundle to re1
WARNING: A reboot is required to install the software
WARNING: Use the 'request system reboot' command immediately
Backup upgrade done
Rebooting Backup RE

Rebooting re1
ISSU: Backup RE Prepare Done
Waiting for Backup RE reboot
GRES operational
Initiating Chassis In-Service-Upgrade
Chassis ISSU Started
ISSU: Preparing Daemons
ISSU: Daemons Ready for ISSU
ISSU: Starting Upgrade for FRUs
ISSU: Preparing for Switchover
ISSU: Ready for Switchover
Checking In-Service-Upgrade status
```

Item	Status	Reason
FPC 0	Online (ISSU)	
FPC 1	Online (ISSU)	
FPC 2	Online (ISSU)	
FPC 3	Offline	Offlined by CLI command
FPC 4	Online (ISSU)	

```

FPC 5      Online (ISSU)
FPC 6      Online (ISSU)
FPC 7      Online (ISSU)
Resolving mastership...
Complete. The other routing engine becomes the master.
ISSU: RE switchover Done
ISSU: Upgrading Old Master RE
WARNING: A reboot is required to install the software
WARNING: Use the 'request system reboot' command immediately
ISSU: Old Master Upgrade Done
ISSU: IDLE

*** FINAL System shutdown message from user@switch ***
System going down IMMEDIATELY

Shutdown NOW!
[pid 2635]

```

**NOTE:** If you omit the **reboot** option in this step when using an EX8200 switch, you must manually reboot the original primary Routing Engine with the `request system reboot` command for the upgrade to complete.

The original primary Routing Engine reboots automatically after updating the new primary Routing Engine when an NSSU is used to upgrade an EX6200 switch with dual Routing Engines.

5. Log in after the reboot completes. To verify that both Routing Engines have been upgraded, enter the following command:

```

{backup}
user@switch> show version invoke-on all-routing-engines
re0:
-----
Hostname: switch
Model: ex8208
JUNOS Base OS boot [12.1-20111229.0]
JUNOS Base OS Software Suite [12.1-20111229.0]
JUNOS Kernel Software Suite [12.1-20111229.0]
JUNOS Crypto Software Suite [12.1-20111229.0]
JUNOS Online Documentation [12.1-20111229.0]

```

```

JUNOS Enterprise Software Suite [12.1-20111229.0]
LC JUNOS Installation Software [12.1-20111229.0]
JUNOS Routing Software Suite [12.1-20111229.0]
JUNOS Web Management [12.1-20111229.0]

re1:
-----

Hostname: switch
Model: ex8208
JUNOS Base OS boot [12.1-20111229.0]
JUNOS Base OS Software Suite [12.1-20111229.0]
JUNOS Kernel Software Suite [12.1-20111229.0]
JUNOS Crypto Software Suite [12.1-20111229.0]
JUNOS Online Documentation [12.1-20111229.0]
JUNOS Enterprise Software Suite [12.1-20111229.0]
LC JUNOS Installation Software [12.1-20111229.0]
JUNOS Routing Software Suite [12.1-20111229.0]
JUNOS Web Management [12.1-20111229.0]

```

6. To verify that the line cards that were online before the upgrade are online after the upgrade, log in to the primary Routing Engine and enter the `show chassis nonstop-upgrade` command:

```

{backup}
user@switch> request routing-engine login master

{master}
user@switch> show chassis nonstop-upgrade

```

Item	Status	Reason
FPC 0	Online (ISSU)	
FPC 1	Online (ISSU)	
FPC 2	Online (ISSU)	
FPC 3	Offline	Offlined by CLI command
FPC 4	Online (ISSU)	
FPC 5	Online (ISSU)	
FPC 6	Online (ISSU)	
FPC 7	Online (ISSU)	

7. If you want to make **re0** the primary Routing Engine again, enter the following command:

```
{master}
user@switch> request chassis routing-engine master switch
Toggle mastership between routing engines ? [yes,no] (no) yes
```

You can verify that **re0** is the primary Routing Engine by executing the `show chassis routing-engine` command.

8. To ensure that the resilient dual-root partitions feature operates correctly, execute the following command to copy the new Junos OS image into the alternate root partition on each Routing Engine:

```
user@switch> request system snapshot slice alternate routing-engine both
```

Resilient dual-root partitions allow the switch to boot transparently from the alternate root partition if the system fails to boot from the primary root partition.

## Upgrading One Routing Engine Using NSSU (EX8200 Switch Only)

This procedure describes how to upgrade one of the Routing Engines using NSSU on an EX8200 switch. When the upgrade completes, the backup Routing Engine is running the new software version and is the new primary. The original primary Routing Engine, now the backup Routing Engine, continues to run the previous software version.

**NOTE:** NSSU always upgrades the software on both Routing Engines on an EX6200 switch. Therefore, you cannot upgrade software on one Routing Engine using NSSU on an EX6200 switch.

To upgrade one Routing Engine using NSSU:

1. Download the software package.
2. Copy the software package to the switch. We recommend that you use FTP to copy the file to the `/var/tmp` directory.
3. Log in to the primary Routing Engine.

4. Request an NSSU. On an EX8200 switch, specify the **no-old-master-upgrade** option when requesting the NSSU:

```
{master}
user@switch> request system software nonstop-upgrade
no-old-master-upgrade /var/tmp/package-name-m.nZx-distribution.tgz
```

where *package-name-m.nZx-distribution.tgz* is, for example, **jinstall-ex-8200-10.4R2.5-domestic-signed.tgz**.

The switch displays the following status messages as the upgrade executes:

```
Chassis ISSU Check Done
ISSU: Validating Image
ISSU: Preparing Backup RE
Pushing bundle to re1
WARNING: A reboot is required to install the software
WARNING: Use the 'request system reboot' command immediately
Backup upgrade done
Rebooting Backup RE

Rebooting re1
ISSU: Backup RE Prepare Done
Waiting for Backup RE reboot
GRES operational
Initiating Chassis In-Service-Upgrade
Chassis ISSU Started
ISSU: Preparing Daemons
ISSU: Daemons Ready for ISSU
ISSU: Starting Upgrade for FRUs
ISSU: Preparing for Switchover
ISSU: Ready for Switchover
Checking In-Service-Upgrade status
```

Item	Status	Reason
FPC 0	Online (ISSU)	
FPC 1	Online (ISSU)	
FPC 2	Online (ISSU)	
FPC 3	Offline	Offlined by CLI command
FPC 4	Online (ISSU)	
FPC 5	Online (ISSU)	
FPC 6	Online (ISSU)	
FPC 7	Online (ISSU)	

```

Resolving mastership...
Complete. The other routing engine becomes the master.
ISSU: RE switchover Done
Skipping Old Master Upgrade
ISSU: IDLE

```

When the upgrade is complete, the original primary Routing Engine (**re0**) becomes the backup Routing Engine.

5. To verify that the original backup Routing Engine (**re1**) has been upgraded, enter the following command:

```

{backup}
user@switch> show version invoke-on all-routing-engines
re0:
-----
Hostname: switch
Model: ex8208
JUNOS Base OS boot [11.3-20110429.1]
JUNOS Base OS Software Suite [11.3-20110429.1]
JUNOS Kernel Software Suite [11.3-20110429.1]
JUNOS Crypto Software Suite [11.3-20110429.1]
JUNOS Online Documentation [11.3-20110429.1]
JUNOS Enterprise Software Suite [11.3-20110429.1]
LC JUNOS Installation Software [11.3-20110429.1]
JUNOS Routing Software Suite [11.3-20110429.1]
JUNOS Web Management [11.3-20110429.1]

re1:
-----
Hostname: switch
Model: ex8208
JUNOS Base OS boot [12.1-20111229.0]
JUNOS Base OS Software Suite [12.1-20111229.0]
JUNOS Kernel Software Suite [12.1-20111229.0]
JUNOS Crypto Software Suite [12.1-20111229.0]
JUNOS Online Documentation [12.1-20111229.0]
JUNOS Enterprise Software Suite [12.1-20111229.0]
LC JUNOS Installation Software [12.1-20111229.0]
JUNOS Routing Software Suite [12.1-20111229.0]
JUNOS Web Management [12.1-20111229.0]

```



6. To verify that the line cards that were online before the upgrade are online after the upgrade, log in to the new primary Routing Engine and enter the `show chassis nonstop-upgrade` command:

```
{backup}
user@switch> request routing-engine login master

--- JUNOS 12.1-20111229.0 built 2011-12-29 04:12:22 UTC
{master}
user@switch> show chassis nonstop-upgrade
```

Item	Status	Reason
FPC 0	Online	
FPC 1	Online	
FPC 2	Online	
FPC 3	Offline	Offlined by CLI command
FPC 4	Online	
FPC 5	Online	
FPC 6	Online	
FPC 7	Online	

7. To ensure that the resilient dual-root partitions feature operates correctly, copy the new Junos OS image into the alternate root partition of the Routing Engine:

```
user@switch> request system snapshot slice alternate
```

Resilient dual-root partitions allow the switch to boot transparently from the alternate root partition if the system fails to boot from the primary root partition.

## Upgrading the Original Primary Routing Engine (EX8200 Switch Only)

This procedure describes how to upgrade the original primary Routing Engine after you have upgraded the original backup Routing Engine as described in ["Upgrading One Routing Engine Using NSSU \(EX8200 Switch Only\)" on page 1204](#) for an EX8200 switch.

1. Log in to the current primary Routing Engine (**re1**).
2. Enter configuration mode and disable nonstop active routing:

```
{master}[edit]
user@switch# delete routing-options nonstop-routing
```

3. Deactivate graceful Routing Engine switchover and commit the configuration:

```
{master}[edit]
user@switch# deactivate chassis redundancy graceful-switchover

{master}[edit]
user@switch# commit
```

4. Log in to the current backup Routing Engine (**re0**) using a console connection.
5. Request a software installation:

```
user@switch> request system software add reboot /var/tmp/package-name-m.nZx-distribution.tgz
```

**NOTE:** When you use NSSU to upgrade only one Routing Engine, the installation package is not automatically deleted from **/var/tmp**, leaving the package available to be used to upgrade the original primary Routing Engine.

6. After the upgrade completes, log in to the current primary Routing Engine (**re1**) and enter CLI configuration mode.
7. Re-enable nonstop active routing and graceful Routing Engine switchover:

```
[edit]
user@switch# activate chassis redundancy graceful-switchover

[edit]
user@switch# set routing-options nonstop-routing

[edit]
user@switch# commit
```

8. To ensure that the resilient dual-root partitions feature operates correctly, exit the CLI configuration mode and copy the new Junos OS image into the alternate root partition of the Routing Engine:

```
user@switch> request system snapshot slice alternate
```

Resilient dual-root partitions allow the switch to boot transparently from the alternate root partition if the system fails to boot from the primary root partition.

9. (Optional) To return control to the original primary Routing Engine (**re0**), enter the following command:

```
{master}
user@switch> request chassis routing-engine master switch
Toggle mastership between routing engines ? [yes,no] (no) yes
```

You can verify that **re0** is the primary Routing Engine by executing the `show chassis routing-engine` command.

## RELATED DOCUMENTATION

[Understanding Nonstop Software Upgrade on EX Series Switches | 593](#)

*Configuring Dual-Root Partitions*

*Troubleshooting Software Installation on EX Series Switches*

## Upgrading Software on an EX8200 Virtual Chassis Using Nonstop Software Upgrade (CLI Procedure)

### IN THIS SECTION

- [Preparing the Switch for Software Installation | 1210](#)
- [Upgrading the Software Using NSSU | 1211](#)

You can use nonstop software upgrade (NSSU) to upgrade the software on an EX8200 Virtual Chassis. NSSU upgrades the software running on all Routing Engines with minimal traffic disruption during the upgrade. NSSU is supported on EX8200 Virtual Chassis with redundant XRE200 External Routing Engines running Junos OS Release 11.1 or later.

**NOTE:** NSSU upgrades all Routing Engines on all members of the Virtual Chassis and on the XRE200 External Routing Engines. Using NSSU, you cannot choose to upgrade the backup Routing Engines only, nor can you choose to upgrade a specific member of the Virtual Chassis. If

you need to upgrade a specific member of the Virtual Chassis, see [Installing Software for a Single Device in an EX8200 Virtual Chassis](#).

This topic covers:

## Preparing the Switch for Software Installation

Before you begin software installation using NSSU:

- (Optional) Configure line-card upgrade groups as described in [Configuring Line-Card Upgrade Groups for Nonstop Software Upgrade](#). By default, NSSU upgrades line cards one at a time, starting with the line card in slot 0 of member 0. This permits aggregated Ethernet links that have members on different line cards remain up through the upgrade process. Configuring line-card upgrade groups reduces the time an upgrade takes because the line cards in each upgrade group are upgraded at the same time rather than sequentially.
- Verify that the members are running the same version of the software:

```
{master:8}
user@external-routing-engine> show version all-members
```

If the Virtual Chassis members are not running the same version of the software, use the [request system software add](#) command to upgrade the software on the inconsistent members. For instructions, see [Installing Software for a Single Device in an EX8200 Virtual Chassis](#).

- Ensure that nonstop active routing (NSR) and graceful Routing Engine switchover (GRES) are enabled. To verify that they are enabled, you need to check only the state of nonstop active routing—if nonstop active routing is enabled, then graceful Routing Engine switchover is enabled.

To verify that nonstop active routing is enabled:

```
{master:8}
user@switch> show task replication
    Stateful Replication: Enabled
    RE mode: Master

Protocol                Synchronization Status
PIM                      Complete
```

If nonstop active routing is not enabled (**Stateful Replication is Disabled**), see [Configuring Nonstop Active Routing on Switches](#) for information on how to enable it.

## Upgrading the Software Using NSSU

This procedure describes how to upgrade the software running on all Routing Engines using NSSU. When the upgrade completes, all Routing Engines are running the new version of the software. The backup external Routing Engine is now the primary external Routing Engine, and the internal backup Routing Engines in the member switches are now the internal primary Routing Engines in those member switches.

To upgrade all Routing Engines using NSSU:

1. Download the software package for the XRE200 External Routing Engine by following one of the procedures in [Downloading Software](#). The name of the software package for the XRE200 External Routing Engine contains the term **xre200**.
2. Copy the software package to the switch. We recommend that you use FTP to copy the file to the **/var/tmp** directory.
3. Log in to the primary external Routing Engine using the console connection. You can perform an NSSU from the management interface, but a console connection allows you to monitor the progress of the primary Routing Engine reboot.
4. Install the new software package:

```
{master:8}
user@external-routing-engine> request system software nonstop-upgrade reboot
/var/tmp/package-name-m.nZx-distribution.tgz
```

where *package-name-m.nZx-distribution.tgz* is, for example, **jinstall-ex-xre200-11.1R2.5-domestic-signed.tgz**.

**NOTE:** You can omit **reboot** option. When you include the **reboot** option, NSSU automatically reboots the original primary Routing Engines after the new image has been installed on them. If you omit the **reboot** option, you must manually reboot the original primary Routing Engines (now the backup Routing Engines) to complete the upgrade. To perform the reboot, you must establish a connection to the console port on the Switch Fabric and Routing Engine (SRE) module or Routing Engine (RE) module.

The switch displays status messages similar to the following messages as the upgrade executes:

```
Chassis ISSU Check Done
ISSU: Validating Image
ISSU: Preparing LCC Backup REs
```

```
ISSU: Preparing Backup RE
Pushing bundle /var/tmp/jinstall-ex-xre200-11.1-20110208.0-domestic-signed.tgz to member9
member9:
```

```
-----
WARNING: A reboot is required to install the software
WARNING:   Use the 'request system reboot' command immediately
VC Backup upgrade done
Rebooting VC Backup RE
```

```
Rebooting member9
ISSU: Backup RE Prepare Done
Waiting for VC Backup RE reboot
Pushing bundle to member0-backup
Pushing bundle to member1-backup
WARNING: A reboot is required to install the software
WARNING:   Use the 'request system reboot' command immediately
WARNING: A reboot is required to install the software
WARNING:   Use the 'request system reboot' command immediately
```

```
Rebooting member0-backup
Rebooting LCC [member0-backup]
```

```
Rebooting member1-backup
Rebooting LCC [member1-backup]
ISSU: LCC Backup REs Prepare Done
GRES operational
Initiating Chassis Nonstop-Software-Upgrade
Chassis ISSU Started
ISSU: Preparing Daemons
ISSU: Daemons Ready for ISSU
ISSU: Starting Upgrade for FRUs
ISSU: Preparing for Switchover
ISSU: Ready for Switchover
Checking Nonstop-Upgrade status
member0:
```

```
-----
Item           Status           Reason
FPC 0          Online (ISSU)
FPC 1          Online (ISSU)
FPC 2          Online (ISSU)
FPC 5          Online (ISSU)
```

```
member1:
```

```

-----
Item          Status          Reason
FPC 0         Online (ISSU)
FPC 1         Online (ISSU)
FPC 2         Online (ISSU)
FPC 5         Online (ISSU)

```

member0:

```

-----
Item          Status          Reason
FPC 0         Online (ISSU)
FPC 1         Online (ISSU)
FPC 2         Online (ISSU)
FPC 5         Online (ISSU)

```

member1:

```

-----
Item          Status          Reason
FPC 0         Online (ISSU)
FPC 1         Online (ISSU)
FPC 2         Online (ISSU)
FPC 5         Online (ISSU)

```

ISSU: Upgrading Old Master RE

Pushing bundle /var/tmp/incoming-package-8200.tgz to member0-master

Pushing bundle /var/tmp/incoming-package-8200.tgz to member1-master

ISSU: RE switchover Done

WARNING: A reboot is required to install the software

WARNING: Use the 'request system reboot' command immediately

ISSU: Old Master Upgrade Done

ISSU: IDLE

\*\*\* FINAL System shutdown message from root@ \*\*\*

System going down

IMMEDIATELY

Shutdown NOW!

**NOTE:** If you omit the **reboot** option in this step, you must complete the upgrade by separately rebooting the original primary Routing Engine on each Virtual Chassis member and

the original primary external Routing Engine. To reboot the original primary Routing Engine on a Virtual Chassis member, you must establish a connection to the console port on the Switch Fabric and Routing Engine (SRE) module or Routing Engine (RE) module.

5. Log in after the reboot completes. To verify that the software on all Routing Engines in the Virtual Chassis members has been upgraded, enter the following command:

```
{backup:8}
user@external-routing-engine> show version all-members
```

6. Verify that the line cards that were online before the upgrade are online after the upgrade by entering the `show chassis nonstop-upgrade` command:

```
{backup:8}
user@external-routing-engine> show chassis nonstop-upgrade
member0:
-----
  Item      Status      Reason
  FPC 0     Online
  FPC 1     Online
  FPC 2     Online
  FPC 5     Online

member1:
-----
  Item      Status      Reason
  FPC 0     Online
  FPC 1     Online
  FPC 2     Online
  FPC 5     Online
```

## RELATED DOCUMENTATION

[Upgrading Software Using Nonstop Software Upgrade on EX Series Virtual Chassis and Mixed Virtual Chassis \(CLI Procedure\) | 1215](#)

[Upgrading Software on an EX6200 or EX8200 Standalone Switch Using Nonstop Software Upgrade \(CLI Procedure\)](#)

[Understanding Nonstop Software Upgrade on EX Series Switches | 593](#)



---

[Configuring Dual-Root Partitions](#)

---

[Troubleshooting Software Installation on EX Series Switches](#)

---

[Understanding Nonstop Software Upgrade on EX Series Switches | 593](#)

---

[Understanding Software Installation on EX Series Switches](#)

## Upgrading Software Using Nonstop Software Upgrade on EX Series Virtual Chassis and Mixed Virtual Chassis (CLI Procedure)

### IN THIS SECTION

- [Preparing the Switch for Software Installation | 1215](#)
- [Upgrading the Software Using NSSU | 1217](#)

You can use nonstop software upgrade (NSSU) to upgrade the software running on all member switches in most EX Series Virtual Chassis with minimal traffic disruption during the upgrade.

NSSU is supported on the following EX Series Virtual Chassis platforms:

- EX3300 Virtual Chassis
- EX3400 Virtual Chassis
- EX4200 Virtual Chassis
- EX4300 Virtual Chassis
- EX4500 Virtual Chassis
- EX4550 Virtual Chassis
- All mixed Virtual Chassis composed of EX4200, EX4500, and EX4550 switches
- EX8200 Virtual Chassis

This topic covers:

### Preparing the Switch for Software Installation

Before you begin software installation using NSSU:

- Ensure that the Virtual Chassis is configured correctly to support NSSU. Verify that:
  - The Virtual Chassis members are connected in a ring topology. A ring topology prevents the Virtual Chassis from splitting during an NSSU.
  - The Virtual Chassis primary and backup are adjacent to each other in the ring topology. Adjacency permits the primary and backup to always be in sync, even when the switches in linecard roles are rebooting.
  - The Virtual Chassis is preprovisioned so that the linecard role has been explicitly assigned to member switches acting in the linecard role. During an NSSU, the Virtual Chassis members must maintain their roles—the primary and backup must maintain their primary and backup roles (although primary role will change), and the other member switches must maintain their linecard roles.

For information on configuring a preprovisioned Virtual Chassis, see [Configuring an EX3300 Virtual Chassis \(CLI Procedure\)](#), [Configuring an EX4200, EX4500, or EX4550 Virtual Chassis \(CLI Procedure\)](#), [Configuring an EX2300, EX3400, or EX4300 Virtual Chassis](#), and [Configuring an EX8200 Virtual Chassis \(CLI Procedure\)](#).

- A two-member Virtual Chassis has `no-split-detection` configured so that the Virtual Chassis does not split when an NSSU upgrades a member.
- Verify that the members are running the same version of the software:

```
user@switch> show version
```

If the Virtual Chassis members are not running the same version of the software, use the `request system software add` command to upgrade the software on the inconsistent members.

- Ensure that nonstop active routing (NSR) and graceful Routing Engine switchover (GRES) are enabled. To verify that they are enabled, you need to check only the state of nonstop active routing—if nonstop active routing is enabled, then graceful Routing Engine switchover is enabled.

To verify that nonstop active routing is enabled:

```
user@switch> show task replication
      Stateful Replication: Enabled
      RE mode: Master

Protocol           Synchronization Status
-----
OSPF                Complete
```

BGP	Complete
PIM	Complete

If nonstop active routing is not enabled (Stateful Replication is Disabled), see [Configuring Nonstop Active Routing on Switches](#) for information on how to enable it.

- For the EX4300 Virtual Chassis, you should enable the `vcp-no-hold-time` statement at the `[edit virtual-chassis]` hierarchy level before performing a software upgrade using NSSU. If you do not enable the `vcp-no-hold-time` statement, the Virtual Chassis may split during the upgrade. A split Virtual Chassis can cause disruptions to your network, and you may have to manually reconfigure your Virtual Chassis after the NSSU if the split and merge feature was disabled. For more information about a split Virtual Chassis, see [Understanding Split and Merge in a Virtual Chassis](#).
- (Optional) Enable nonstop bridging (NSB). Enabling NSB ensures that all NSB-supported Layer 2 protocols operate seamlessly during the Routing Engine switchover that is part of the NSSU.
- (Optional) Back up the system software—Junos OS, the active configuration, and log files—on each member to an external storage device with the `request system snapshot` command.

## Upgrading the Software Using NSSU

This procedure describes how to upgrade the software running on all Virtual Chassis members using NSSU. When the upgrade completes, all members are running the new version of the software. Because a graceful Routing Engine switchover occurs during the upgrade, the original Virtual Chassis backup is the new primary.

To upgrade all members using NSSU:

1. Download the software package. If you are upgrading the software running on a mixed Virtual Chassis, download the software packages for both switch types.
2. Copy the software package or packages to the Virtual Chassis. We recommend that you copy the file to the `/var/tmp` directory on the primary.
3. Log in to the Virtual Chassis using the console connection or the virtual management Ethernet (VME) interface. Using a console connection allows you to monitor the progress of the primary switch reboot.
4. Start the NSSU:
  - On an EX3300 Virtual Chassis, EX3400 Virtual Chassis, EX4200 Virtual Chassis, EX4300 Virtual Chassis, EX4500 Virtual Chassis, or EX4550 Virtual Chassis, enter:

```
user@switch> request system software nonstop-upgrade /var/tmp/package-name.tgz
```

where *package-name.tgz* is, for example, *jinstall-ex4200-12.1R2.5-domestic-signed.tgz*.

- On a mixed Virtual Chassis, enter:

```
user@switch> request system software nonstop-upgrade set [/var/tmp/package-  
name.tgz /var/tmp/package-name.tgz]
```

where *[/var/tmp/package-name.tgz /var/tmp/package-name.tgz]* specifies the EX4200 and EX4500 software packages.

The switch displays status messages similar to the following messages as the upgrade executes:

```
Chassis ISSU Check Done
ISSU: Validating Image
ISSU: Preparing Backup RE
Installing image on other FPC's along with the backup

Checking pending install on fpc1
Pushing bundle to fpc1
WARNING: A reboot is required to install the software
WARNING:   Use the 'request system reboot' command immediately
Completed install on fpc1

Checking pending install on fpc2
Pushing bundle to fpc2
WARNING: A reboot is required to install the software
WARNING:   Use the 'request system reboot' command immediately
Completed install on fpc2

Rebooting fpc1
ISSU: Backup RE Prepare Done
Waiting for Backup RE reboot
GRES operational
Initiating Chassis In-Service-Upgrade
Chassis ISSU Started
ISSU: Preparing Daemons
ISSU: Daemons Ready for ISSU
ISSU: Starting Upgrade for FRUs
ISSU: Preparing for Switchover
ISSU: Ready for Switchover
Checking In-Service-Upgrade status
```

Item	Status	Reason
FPC 0	Online	
FPC 1	Online	
FPC 2	Online (ISSU)	

Going to install image on master

WARNING: A reboot is required to install the software

WARNING: Use the 'request system reboot' command immediately  
relinquish mastership

ISSU: IDLE

\*\*\* FINAL System shutdown message from user@switch \*\*\*

System going down IMMEDIATELY

Shutdown NOW!

[pid 9336]

5. Log in after the reboot of the original primary switch completes. To verify that the software on all Routing Engines in the Virtual Chassis members has been upgraded, enter the following command:

```
user@switch> show version
```

6. To ensure that the resilient dual-root partitions feature operates correctly, copy the new Junos OS image into the alternate root partitions of all members:

```
user@switch> request system snapshot slice alternate all-members
```

Resilient dual-root partitions allow the switch to boot transparently from the alternate root partition if the system fails to boot from the primary root partition.

## RELATED DOCUMENTATION

[Understanding Nonstop Software Upgrade on EX Series Switches | 593](#)

[Configuring Dual-Root Partitions](#)

[Understanding Software Installation on EX Series Switches](#)

[Troubleshooting Software Installation on EX Series Switches](#)

[Understanding Nonstop Software Upgrade on EX Series Switches | 593](#)

# Verification Tasks

## IN THIS CHAPTER

- [Verifying Power Configuration and Use | 1220](#)

## Verifying Power Configuration and Use

## IN THIS SECTION

- [Purpose | 1220](#)
- [Action | 1221](#)
- [Meaning | 1222](#)

### Purpose

Verify on an EX Series switch:

- The power redundancy and line card priority settings
- The PoE power budgets for line cards that support PoE
- Whether the  $N+1$  or  $N+N$  power requirements are being met
- Whether the switch has sufficient power for a new line card or an  $N+N$  configuration

## Action

Enter the following command:

```
user@switch> show chassis power-budget-statistics
```

Example output for an EX6200 switch:

```

PSU  0    (EX6200-PWR-AC2500)          :   2500 W   Online
PSU  1    (EX6200-PWR-AC2500)          :   2500 W   Online
PSU  2    (EX6200-PWR-AC2500)          :   2500 W   Online
PSU  3    (EX6200-PWR-AC2500)          :   2500 W   Online
Total Power supplied by all Online PSUs :  10000 W
Power Redundancy Configuration         :    N+1
Power Reserved for the Chassis         :    500 W

Fan Tray Statistics      Base power   Power Used
FTC  0                   :    300 W    43.04 W

FPC Statistics          Base power   Power Used   PoE power   Priority
FPC  1  (EX6200-48P)    :    220 W    49.47 W    1440 W      1
FPC  2  (EX6200-48P)    :    220 W    47.20 W     800 W      2
FPC  3  (EX6200-48P)    :    220 W   1493.57 W    1440 W      0
FPC  4  (EX6200-SRE64-4XS) :   100 W    51.38 W      0 W        0
FPC  5  (EX6200-SRE64-4XS) :   100 W    50.28 W      0 W        0
FPC  6  (EX6200-48P)    :    220 W    49.38 W     800 W      6
FPC  8  (EX6200-48P)    :    220 W    61.41 W    1440 W      9
FPC  9  (EX6200-48T)    :    150 W    12.49 W      0 W        9

Total (non-PoE) Power allocated         :   1750 W
Total Power allocated for PoE           :   5920 W
Power Available (Redundant case)         :   5750 W
Total Power Available                    :   2515 W

```

Example output for an EX8200 switch:

```

PSU  0    (EX8200-AC2K)                :   1200 W   Online
PSU  1    (EX8200-AC2K)                :   1200 W   Online
PSU  2    (EX8200-AC2K)                :   1200 W   Online
PSU  3    (EX8200-AC2K)                :   1200 W   Online

```

Total Power supplied by all Online PSUs		:	4800 W	
Power Redundancy Configuration		:	N+1	
Power Reserved for the Chassis		:	1600 W	
FPC Statistics			Base power	PoE power    Priority
FPC 0	(EX8200-48T)	:	350 W	0 W    2
FPC 1	(EX8200-2XS-40P)	:	387 W	300 W    0
FPC 2	(EX8200-48PL)	:	267 W	350 W    15
FPC 4	(EX8200-2XS-40P)	:	387 W	300 W    1
FPC 5	(EX8200-48TL)	:	230 W	0 W    15
FPC 6	(EX8200-48TL)	:	230 W	0 W    15
Total (non-PoE) Power allocated		:	3451 W	
Total Power allocated for PoE		:	950 W	
Power Available (Redundant case)		:	149 W	
Total Power Available		:	510 W	

## Meaning

- Example output for an EX6200 switch —The online power supplies can supply a total of 10,000 W to the switch. The switch is configured for *N*+1 redundancy, which means 7500 W of redundant power can be supplied. The **Power Available (Redundant case)** field shows that the switch is meeting the *N*+1 power requirements, with an additional 5750 W available. This value is calculated by subtracting all power allocations except PoE power allocations from redundant power (7500 W).

The total amount of power available on the switch is 2515 W. This value is calculated by subtracting all power allocations, including PoE power allocations, from the total power (10,000 W). On a switch with PoE line cards, if **Total Power Available** is 0, some or all of the PoE line cards might not be allocated their configured PoE power budgets, which means power to some or all PoE ports might be disabled.

The power priority order of the line cards, from highest priority line card to the lowest priority line card, is 4, 5, 3, 1, 2, 6, 8, 9. Slots 4 and 5, which contain the Switch Fabric and Routing Engine (SRE) modules, always have highest priority, even if a lower-numbered slot, such as slot 3 in this example, has a priority of 0. Should two or more 2500 W power supplies fail, power management will remove or reduce the PoE power allocations from the PoE line cards in the following order to balance the power budget: 8, 6, 2, 1, and 3.

The **Power Used** values for the fan tray and line cards shows the actual power being consumed for these components at the time the command was executed. These values are for your information only; power management uses allocated power, which is based on the maximum power the component might consume, and not actual power consumed, in determining its power budget.



- Example output for an EX8200 switch—The online power supplies can supply a total of 4800 W to the switch. The switch is configured for  $N+1$  redundancy, which means 3600 W of redundant power can be supplied. The **Power Available (Redundant case)** field shows that the switch is meeting the  $N+1$  power requirements, with an additional 149 W available. This value is calculated by subtracting all power allocations except PoE power allocations from redundant power (3600 W). Because 149 W is insufficient power for a line card, another line card cannot be added to the switch while maintaining  $N+1$  redundancy.

The total amount of power available on the switch is 510 W. This value is calculated by subtracting all power allocations, including PoE power allocations, from the total power (4800 W). On a switch with PoE line cards, if **Total Power Available** is 0, some or all of the PoE line cards might not be allocated their configured PoE power budgets, which means power to some or all PoE ports might be disabled.

The power priority order of the line cards, from highest priority line card to the lowest priority line card, is 1, 4, 0, 2, 5, 6. Should one or more 1200 W power supplies fail, power management will remove or reduce the PoE power allocations from the PoE line cards in the following order to balance the power budget: 2, 4, and 1.

## RELATED DOCUMENTATION

---

Configuring Power Supply Redundancy (CLI Procedure)

Configuring the Power Priority of Line Cards (CLI Procedure)

# Operational Commands

## IN THIS CHAPTER

- clear chassis high-availability data-plane statistics | 1226
- clear chassis high-availability information | 1227
- clear security pki node-local certificate-request | 1229
- clear security pki node-local local-certificate | 1230
- clear security pki node-local key-pair | 1232
- clear vrrp | 1233
- request chassis high-availability failover services-redundancy-group | 1235
- request chassis redundancy feb slot | 1236
- request chassis routing-engine master | 1238
- request chassis sfm master switch | 1246
- request chassis ssb master switch | 1248
- request redundant-power-system multi-backup | 1250
- request security pki node-local local-certificate verify | 1252
- request security pki node-local local-certificate re-enroll | 1254
- request security pki node-local local-certificate load | 1255
- request security pki node-local local-certificate export | 1257
- request security pki node-local local-certificate enroll | 1259
- request security pki node-local key-pair export | 1262
- request security pki node-local generate-key-pair | 1264
- request security pki sync-from-peer | 1266
- request security pki node-local generate-certificate-request | 1267
- request system software in-service-upgrade | 1270
- request system software in-service-upgrade (MX Series 5G Universal Routing Platforms and EX9200 Switches) | 1291
- request system software nonstop-upgrade | 1314
- request system software validate in-service-upgrade | 1327

- [show bgp neighbor | 1332](#)
- [show log | 1372](#)
- [show \(ospf | ospf3\) overview | 1379](#)
- [show chassis dedicated-ukern-cpu | 1388](#)
- [show chassis in-service-upgrade | 1389](#)
- [show chassis realtime-ukern-thread | 1395](#)
- [show chassis redundancy feb | 1396](#)
- [show chassis high-availability data-plane statistics | 1401](#)
- [show chassis high-availability information | 1406](#)
- [show chassis high-availability peer-info | 1415](#)
- [show chassis high-availability prefix-srgid-table | 1417](#)
- [show chassis high-availability services-redundancy-group | 1419](#)
- [show chassis nonstop-upgrade | 1426](#)
- [show chassis nonstop-upgrade node-group | 1429](#)
- [show chassis power-budget-statistics | 1431](#)
- [show chassis redundant-power-system | 1436](#)
- [show protection-group ethernet-ring aps | 1439](#)
- [show protection-group ethernet-ring configuration | 1445](#)
- [show protection-group ethernet-ring data-channel | 1453](#)
- [show protection-group ethernet-ring flush-info | 1457](#)
- [show protection-group ethernet-ring interface | 1459](#)
- [show protection-group ethernet-ring node-state | 1465](#)
- [show protection-group ethernet-ring statistics | 1472](#)
- [show protection-group ethernet-ring vlan | 1479](#)
- [show redundant-power-system led | 1486](#)
- [show redundant-power-system multi-backup | 1489](#)
- [show redundant-power-system network | 1490](#)
- [show redundant-power-system power-supply | 1492](#)
- [show redundant-power-system status | 1494](#)
- [show redundant-power-system upgrade | 1497](#)
- [show redundant-power-system version | 1499](#)
- [show security pki node-local local-certificate | 1501](#)

- [show security pki node-local certificate-request | 1507](#)
- [show chassis ssb | 1510](#)
- [show nonstop-routing | 1513](#)
- [show pfe ssb | 1517](#)
- [show system switchover | 1526](#)
- [show task replication | 1535](#)
- [show vrrp | 1538](#)
- [show vrrp track | 1555](#)

## clear chassis high-availability data-plane statistics

### IN THIS SECTION

- [Syntax | 1226](#)
- [Description | 1226](#)
- [Required Privilege Level | 1227](#)
- [Output Fields | 1227](#)
- [Sample Output | 1227](#)
- [Release Information | 1227](#)

### Syntax

```
clear chassis high-availability data-plane statistics
```

### Description

Clear the data plane statistics of Multinode High Availability.

## Required Privilege Level

clear

## Output Fields

## Sample Output

**clear chassis high-availability data-plane statistics**

```
user@host> clear chassis high-availability data-plane statistics
Cleared data-plane statistics
```

## Release Information

Command introduced in Junos OS Release 20.4R1.

## RELATED DOCUMENTATION

| [show chassis high-availability data-plane statistics](#) | [1401](#)

## clear chassis high-availability information

### IN THIS SECTION

- [Syntax](#) | [1228](#)
- [Description](#) | [1228](#)
- [Required Privilege Level](#) | [1228](#)
- [Output Fields](#) | [1228](#)
- [Sample Output](#) | [1228](#)
- [Release Information](#) | [1228](#)

## Syntax

```
clear chassis high-availability information
```

## Description

Clear Multinode High Availability information.

## Required Privilege Level

clear

## Output Fields

## Sample Output

**clear chassis high-availability information**

```
user@host> clear chassis high-availability information
```

```
Cleared chassis l3-ha information
```

## Release Information

Command introduced in Junos OS Release 20.4R1.

## RELATED DOCUMENTATION

| [show chassis high-availability information](#) | 1406

# clear security pki node-local certificate-request

IN THIS SECTION

- [Syntax | 1229](#)
- [Description | 1229](#)
- [Options | 1229](#)
- [Required Privilege Level | 1229](#)
- [Output Fields | 1230](#)
- [Sample Output | 1230](#)
- [Release Information | 1230](#)

## Syntax

```
clear security pki node-local certificate-request (all | certificate-id certificate-id-name)
```

## Description

Delete node-local digital certificate, certificate requests, and the corresponding public/private key pairs from the device in a Multinode High Availability setup.

## Options

<b>all</b>	Delete all local digital certificate requests from the router.
<b>certificate-id</b> <i>certificate-id-name</i>	Delete the specified local digital certificate and corresponding public/private key pair.

## Required Privilege Level

clear

## Output Fields

When you enter this command, you are provided feedback on the status of your request.

## Sample Output

When you enter this command, you are provided feedback on the status of your request.

## Release Information

Command introduced in Junos OS Release 22.3R1.

## RELATED DOCUMENTATION

[Multinode High Availability /](#)

[show pki security node-local certificate-request /](#)

# clear security pki node-local local-certificate

## IN THIS SECTION

- [Syntax | 1231](#)
- [Description | 1231](#)
- [Options | 1231](#)
- [Required Privilege Level | 1231](#)
- [Output Fields | 1231](#)
- [Sample Output | 1231](#)
- [Release Information | 1231](#)



## Syntax

```
clear security pki node-local local-certificate (all | certificate-id certificate-id | system-generated)
```

## Description

Clear public key infrastructure (PKI) information for local digital certificates on the local device in a Multinode High Availability system.

## Options

- **all**—Clear information for all the local digital certificates on the device.

You cannot clear the automatically generated self-signed certificate using `clear security pki local-certificate all` command. To clear the self-signed certificate you need to use `system-generated` as an option.

- **certificate-id *certificate-id***—Clear the specified local digital certificate with this certificate ID.
- **system-generated**—Clear the existing automatically generated self-signed certificate and generate a new self-signed certificate.

## Required Privilege Level

clear and security

## Output Fields

When you enter this command, you are provided feedback on the status of your request.

## Sample Output

This command produces no output.

## Release Information

Command modified in Junos OS Release 22.3R1

## RELATED DOCUMENTATION

[Multinode High Availability](#) /

[show security pki node-local local-certificate](#) /

[request security pki node-local local-certificate load](#) /

[request security pki node-local local-certificate export](#)

[request security pki node-local local-certificate enroll](#) /

[request security pki node-local local-certificate re-enroll](#) /

## clear security pki node-local key-pair

### IN THIS SECTION

- [Syntax](#) | 1232
- [Description](#) | 1232
- [Options](#) | 1232
- [Required Privilege Level](#) | 1233
- [Output Fields](#) | 1233
- [Release Information](#) | 1233

### Syntax

```
clear security pki node-local key-pair (all | certificate-id certificate-id)
```

### Description

Clear public key infrastructure (PKI) key pair information for local digital certificates on the local device in a Multinode High Availability system.

### Options

- `all`—Clear key pair information for all local certificates.

- `certificate-id certificate-id` —Clear key pair information for the local certificate with this certificate ID.

## Required Privilege Level

clear and security

## Output Fields

This command produces no output.

## Release Information

Command introduced in Junos OS Release 22.3R1

## RELATED DOCUMENTATION

[Multinode High Availability /](#)

[request security pki node-local generate-key-pair /](#)

[request security pki node-local key-pair export /](#)

## clear vrrp

### IN THIS SECTION

- [Syntax | 1234](#)
- [Description | 1234](#)
- [Options | 1234](#)
- [Required Privilege Level | 1234](#)
- [Output Fields | 1234](#)
- [Sample Output | 1234](#)
- [Release Information | 1234](#)

## Syntax

```
clear vrrp (all | interface interface-name)
```

## Description

Set Virtual Router Redundancy Protocol (VRRP) interface statistics to zero.

## Options

- all** Clear statistics on all interfaces.
- interface *interface-name*** Clear statistics on the specified interface only.

## Required Privilege Level

clear

## Output Fields

When you enter this command, you are provided feedback on the status of your request.

## Sample Output

**clear vrrp all**

```
user@host> clear vrrp all
```

## Release Information

Command introduced before Junos OS Release 7.4.

## RELATED DOCUMENTATION

| [show vrrp](#) | 1538

# request chassis high-availability failover services-redundancy-group

IN THIS SECTION

- [Syntax | 1235](#)
- [Description | 1235](#)
- [Options | 1235](#)
- [Required Privilege Level | 1235](#)
- [Output Fields | 1236](#)
- [Sample Output | 1236](#)
- [Release Information | 1236](#)

## Syntax

```
request chassis high-availability failover services-redundancy-group group-id peer-id peer-id
```

## Description

Initiate a manual failover on service redundancy group of the peer node. Use the command from the active node of the service redundancy group.

## Options

- |                                  |  |
|----------------------------------|--|
| <b>services-redundancy-group</b> | Service redundancy group on which to initiate manual failover. <ul style="list-style-type: none"><li>● <b>Range:</b> 1 through 256</li></ul>                               |
| <b>peer-id</b>                   | Node identifier of the SRG. After the failover, this node transitions as the new active node. <ul style="list-style-type: none"><li>● <b>Range:</b> 1 through 10</li></ul> |

## Required Privilege Level

maintenance

## Output Fields

When you enter this command, you are provided feedback on the status of your request.

## Sample Output

### request chassis high-availability failover services-redundancy-group 1

```
user@host> request chassis high-availability failover services-redundancy-group 1 peer-id 2
Initiated manual failover for redundancy group 1
```

## Release Information

Command introduced in Junos OS 20.4R1.

## RELATED DOCUMENTATION

[Hardware Upgrade for SRX5000-Line SPC3 in a Multinode High Availability Setup](#)

## request chassis redundancy feb slot

### IN THIS SECTION

- [Syntax | 1237](#)
- [Description | 1237](#)
- [Options | 1237](#)
- [Required Privilege Level | 1237](#)
- [Output Fields | 1237](#)
- [Sample Output | 1237](#)
- [Release Information | 1238](#)

## Syntax

```
request chassis redundancy feb slot slot-number (switch-to-backup | revert-from-backup)
```

## Description

(M120 routers only) Control the operation of the specified Forwarding Engine Board (FEB) in a redundancy group.

## Options

<b><i>slot-number</i></b>	FEB slot number. Replace <b><i>slot-number</i></b> with a value from <b>0</b> through <b>5</b> .
<b>switch-to-backup</b>	Initiate a switchover from the specified active FEB to the backup FEB for the redundancy group.
<b>revert-from-backup</b>	Initiate a revert to the specified FEB following a switchover from the backup FEB for a redundancy group.

## Required Privilege Level

maintenance

## Output Fields

When you enter this command, you are provided feedback on the status of your request.

## Sample Output

**request chassis redundancy feb slot 2 switch-to-backup**

```
user@host> request chassis redundancy feb slot 2 switch-to-backup
Switch initiated, use "show chassis redundancy febs" to verify
```

## request chassis redundancy feb slot 3 revert-from-backup

```
user@host> request chassis redundancy feb slot 3 revert-from-backup
Revert initiated, use "show chassis redundancy febs" to verify
```

## Release Information

Command introduced in Junos OS Release 8.2.

## RELATED DOCUMENTATION

[show chassis redundancy feb | 1396](#)

Configuring FEB Redundancy on the M120 Router

[Understanding Switching Control Board Redundancy | 15](#)

## request chassis routing-engine master

### IN THIS SECTION

- [Syntax | 1239](#)
- [Syntax \(M Series, MX Series, T Series Routers, ACX7509, ACX1000 Devices\) | 1239](#)
- [Syntax \(TX Matrix Routers\) | 1239](#)
- [Syntax \(TX Matrix Plus Routers\) | 1239](#)
- [Syntax \(MX Series Virtual Chassis\) | 1239](#)
- [Syntax \(QFX Series\) | 1240](#)
- [Syntax | 1240](#)
- [Description | 1240](#)
- [Options | 1241](#)
- [Additional Information | 1242](#)
- [Required Privilege Level | 1243](#)
- [Output Fields | 1243](#)
- [Sample Output | 1243](#)



## Syntax

```
request chassis routing-engine master (acquire | release | switch)
<no-confirm>
```

### Syntax (M Series, MX Series, T Series Routers, ACX7509, ACX1000 Devices)

```
request chassis routing-engine master (acquire | release | switch)
<no-confirm>
<check>
```

### Syntax (TX Matrix Routers)

```
request chassis routing-engine master (acquire | release | switch) (lcc number |
scc | all-chassis)
<no-confirm>
```

### Syntax (TX Matrix Plus Routers)

```
request chassis routing-engine master (acquire | release | switch) (lcc number |
sfc | all-chassis | all-lcc)
<no-confirm>
```

### Syntax (MX Series Virtual Chassis)

```
request chassis routing-engine master (acquire | release | switch)
<all-members>
<check>
<local>
```

```
<member member-id>
<no-confirm>
```

## Syntax (QFX Series)

```
request chassis routing-engine master (release | switch)
<check>
<interconnect-device name>
<node-group name>
<no-confirm>
```

## Syntax

## Description

For routers or switches with multiple Routing Engines, control which Routing Engine is the primary.



**CAUTION:** (Routing matrix based on the TX Matrix or TX Matrix Plus routers only)  
Within the routing matrix, we recommend that all Routing Engines run the same Junos OS Release. If you run different releases on the Routing Engines and a change in primary role occurs on any backup Routing Engine in the routing matrix, one or all routers (in a routing matrix based on the TX Matrix router or in a routing matrix based on a TX Matrix Plus router) might become logically disconnected from the TX Matrix router and cause data loss. For more information, see the [TX Matrix Router Hardware Guide](#) or the [Junos OS High Availability User Guide](#).

**NOTE:** Successive graceful Routing Engine switchover events must be a minimum of 240 seconds (4 minutes) apart after both Routing Engines have come up.

If the router or switch displays a warning message similar to “Standby Routing Engine is not ready for graceful switchover. Packet Forwarding Engines that are not ready for graceful switchover might be reset,” do not attempt switchover. If you choose to proceed with switchover, only the Packet Forwarding Engines that were not ready for graceful switchover are reset. None of the Flexible PIC concentrators (FPCs) should spontaneously restart. We recommend that you wait until the warning no longer appears and then proceed with the switchover.

You will receive an error message stating “Command terminated. Not ready for primary role switch, try after n seconds” when this command is re-entered before 240 seconds have elapsed on EX Series switches.

**NOTE:** On a QFabric system, to avoid traffic loss on the network Node group, switch primary role of the routing engine to the backup routing engine, and then reboot.

## Options

**acquire** (Not available for Junos OS Evolved) Attempt to become the primary Routing Engine.

**release** (Not available for Junos OS Evolved) Request that the other Routing Engine become the primary.

**switch** Toggle primary role between Routing Engines.

**NOTE:** The acquire option should be used with caution because acquiring a Routing Engine may result in a corrupted database. If possible, use the switch option instead.

The acquire, release, and switch options have the following suboptions:

- |                    |  |
|--------------------|--|
| <b>all-chassis</b> | (TX Matrix and TX Matrix Plus routers only) On a routing matrix composed of a TX Matrix router and the attached T640 routers, switch primary role on all the Routing Engines in the routing matrix. Likewise, on a routing matrix composed of a TX Matrix Plus router and the attached T1600 or T4000 routers, switch primary role on all the Routing Engines in the routing matrix. |
| <b>all-lcc</b>     | (TX Matrix Plus routers only) Request to acquire primary role for all line-card chassis (LCC).   |
| <b>all-members</b> | (MX Series routers only) (Optional) Control Routing Engine primary role on the Routing Engines in all member routers of the Virtual Chassis configuration.   |
| <b>check</b>       | (ACX7509, MX104, MX480, MX960, MX2010, MX2020, and MX2008 routers, QFabric systems, and PTX5000 routers only) (Optional) Available with the switch, release, and acquire options. Check graceful switchover status of the standby Routing  |

Engine before toggling primary role between Routing Engines (RE). Check if the RE is ready for a switchover.

<b>interconnect-device <i>name</i></b>	(QFabric systems only) (Optional) Control Routing Engine primary role on the Routing Engines on an Interconnect device.
<b>lcc <i>number</i></b>	<p>(TX Matrix router and TX Matrix Plus router only) (Optional) Line-card chassis number.</p> <p>Replace <i>number</i> with the following values depending on the LCC configuration:</p> <ul style="list-style-type: none"> <li>• 0 through 3, when T640 routers are connected to a TX Matrix router in a routing matrix.</li> <li>• 0 through 3, when T1600 routers are connected to a TX Matrix Plus router in a routing matrix.</li> <li>• 0 through 7, when T1600 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.</li> <li>• 0, 2, 4, or 6, when T4000 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.</li> </ul>
<b>local</b>	(MX Series routers only) (Optional) Control Routing Engine primary role on the Routing Engines in the local Virtual Chassis member.
<b>member <i>member-id</i></b>	<p>(MX Series routers only) (Optional) Control Routing Engine primary role on the Routing Engines of the specified member in the Virtual Chassis configuration.</p> <p>Replace <i>member-id</i> with a value of 0 or 1.</p>
<b>no-confirm</b>	(Optional) Do not request confirmation for the switch.
<b>node-group <i>name</i></b>	(QFabric systems only) (Optional) Control Routing Engine primary role on the Routing Engines on a Node group.
<b>scc</b>	(TX Matrix routers only) TX Matrix (switch-card chassis).
<b>sfc</b>	(TX Matrix Plus routers only) TX Matrix Plus router (or switch-fabric chassis).

## Additional Information

Always use the `show system switchover` command on the backup Routing Engine to determine if the backup is ready to take over as the primary Routing Engine.

Because both Routing Engines are always running, the transition from one to the other as the primary Routing Engine is immediate. However, the changeover interrupts communication to the System and Switch Board (SSB). The SSB takes several seconds to reinitialize the Flexible PIC Concentrators (FPCs) and restart the PICs. Interior gateway protocol (IGP) and BGP convergence times depend on the specific network environment.

By default, the Routing Engine in slot 0 (RE0) is the primary and the Routing Engine in slot 1 (RE1) is the backup. To change the default primary Routing Engine, include the `routing-engine` statement at the `[edit chassis redundancy]` hierarchy level in the configuration.

To have the backup Routing Engine become the primary Routing Engine, use the `request chassis routing-engine master switch` command. If you use this command to change the primary and then restart the chassis software for any reason, the primary reverts to the default setting.

**NOTE:** Although the configurations on the two Routing Engines do not have to be the same and are not automatically synchronized, we recommend making both configurations the same.

## Required Privilege Level

maintenance

## Output Fields

When you enter this command, you are provided feedback on the status of your request.

## Sample Output

### `request chassis routing-engine primary acquire`

```
user@host> request chassis routing-engine master acquire

warning: Traffic will be interrupted while the PFE is re-initialized

warning: The other routing engine's file system could be corrupted

Reset other routing engine and become master ? [yes,no] (no)
```

## request chassis routing-engine primary switch

```
user@host> request chassis routing-engine master switch

warning: Traffic will be interrupted while the PFE is re-initialized
Toggle mastership between Routing Engines ? [yes,no] (no) yes

Resolving mastership...
Complete. The other Routing Engine becomes the master.
```

Switch primary role back to the local Routing Engine:

```
user@host> request chassis routing-engine master switch

warning: Traffic will be interrupted while the PFE is re-initialized
Toggle mastership between routing engines ? [yes,no] (no) yes

Resolving mastership...
Complete. The local routing engine becomes the master.
```

## request chassis routing-engine master switch (Junos OS Evolved)

```
user@host> request chassis routing-engine master switch
Resolving mastership...
Complete. The other Routing Engine becomes the master.
```

Switching back to primary router:

```
user@host> request chassis routing-engine master switch
Resolving mastership...
Complete. The local Routing Engine becomes the master.
```

If you did not switch back and tried to enter configuration mode, you would get the following error message:

```
user@host> configure
error: unknown command: configure
Configuration is allowed only from the master Routing Engine.
```

### **request chassis routing-engine primary switch check (ACX7509, M Series, MX Series, and T Series Devices)**

```
warning: Standby Routing Engine is not ready for graceful switchover.
{master}[edit]

user@host> request chassis routing-engine master switch check
Platform specific components not ready for switchover
```

Output when system is ready for graceful switchover.

```
user@host> request chassis routing-engine master switch check
Switchover Ready
```

You can similarly check the backup Routing Engine for the switchover readiness.

### **request chassis routing-engine master switch check (DRAM Size Mismatch Between Primary and Standby)**

```
user@host> request chassis routing-engine master switch check
error: Standby mirror connection is not up:RE DRAM Size Mismatch

{master}
```

To check switchover readiness, use the `show system switchover` command before changing the mastership. Please note that the switchover is denied until 360 seconds have passed from the previous switchover.

## Release Information

Command introduced before Junos OS Release 7.4.

all-chassis option added in Junos OS Release 8.0.

sfc option introduced for the TX Matrix Plus router in Junos OS Release 9.6.

Command support added to ACX7509 platform in Junos OS Evo Release 22.1.

## RELATED DOCUMENTATION

| [show system switchover](#) | [1526](#)

## request chassis sfm master switch

### IN THIS SECTION

- [Syntax](#) | [1246](#)
- [Description](#) | [1247](#)
- [Options](#) | [1247](#)
- [Additional Information](#) | [1247](#)
- [Required Privilege Level](#) | [1247](#)
- [Output Fields](#) | [1247](#)
- [Sample Output](#) | [1247](#)
- [Release Information](#) | [1248](#)

## Syntax

```
request chassis sfm master switch  
<no-confirm>
```



## Description

(M40e and M160 routers only) Control which Switching and Forwarding Module (SFM) is primary.

## Options

**no-confirm** (Optional) Do not display a switch warning or query.

## Additional Information

By default, the SFM in slot 0 (SFM0) is the primary and the SFM in slot 1 (SFM1) is the backup. If you use this command to change the primary, and then restart the chassis software for any reason, the primary reverts to the default setting. To change the default primary SFM, include the `sfm` statement at the `[edit chassis redundancy]` hierarchy level in the configuration. For more information, see the [Junos OS Administration Library for Routing Devices](#).

All installed SFMs are always working together to forward packets. If an SFM fails, the other SFMs take over and traffic continues to flow uninterrupted.

## Required Privilege Level

maintenance

## Output Fields

When you enter this command, you are provided feedback on the status of your request.

## Sample Output

**request chassis sfm primary switch**

```
user@host> request chassis sfm master switch
warning: Traffic will be interrupted while the PFE is re-initialized
Toggle mastership between system forwarding module? [yes,no] (no) yes

Switch initiated, use "show chassis sfm" to verify
```

## request chassis sfm primary switch no-confirm

```
user@host> request chassis sfm master switch no-confirm  
Switch initiated, use "show chassis sfm" to verify
```

### Release Information

Command introduced before Junos OS Release 7.4.

### RELATED DOCUMENTATION

*show chassis sfm*

*Switching the Global Primary and Backup Roles in a Virtual Chassis Configuration*

## request chassis ssb master switch

### IN THIS SECTION

- [Syntax | 1248](#)
- [Description | 1249](#)
- [Options | 1249](#)
- [Additional Information | 1249](#)
- [Required Privilege Level | 1249](#)
- [Output Fields | 1249](#)
- [Sample Output | 1249](#)
- [Release Information | 1250](#)

### Syntax

```
request chassis ssb master switch  
<no-confirm>
```

## Description

(M20 router only) Control which System and Switch Board (SSB) is primary.

## Options

**no-confirm** (Optional) Do not request confirmation for the switch.

## Additional Information

By default, the SSB in slot 0 (SSB0) is the primary and the SSB in slot 1 (SSB1) is the backup. If you use this command to change the primary, and then restart the chassis software for any reason, the primary reverts to the default setting. To change the default primary SSB, include the `ssb` statement at the **[edit chassis redundancy]** hierarchy level in the configuration. For more information, see the [Junos OS Administration Library for Routing Devices](#).

The configurations on the two SSBs do not have to be the same, and they are not automatically synchronized. If you configure both SSBs as primaries, when the chassis software restarts for any reason, the SSB in slot 0 becomes the primary and the one in slot 1 becomes the backup.

The switchover from the primary SSB to the backup SSB is immediate. The SSB takes several seconds to reinitialize the Flexible PIC Concentrators (FPCs) and restart the PICs. The interior gateway protocol (IGP) and BGP convergence times depend on the specific network environment.

## Required Privilege Level

maintenance

## Output Fields

When you enter this command, you are provided feedback on the status of your request.

## Sample Output

**request chassis ssb primary switch**

```
user@host> request chassis ssb master switch
warning: Traffic will be interrupted while the PFE is re-initialized
Toggle mastership between system switch boards ? [yes,no] (no) yes
```

Switch initiated, use “show chassis ssb” to verify

## **request chassis ssb primary switch no-confirm**

```
user@host> request chassis ssb master switch no-confirm
```

Switch initiated, use “show chassis ssb” to verify

## **Release Information**

Command introduced before Junos OS Release 7.4.

## **RELATED DOCUMENTATION**

| [show chassis ssb](#) | [1510](#)

## **request redundant-power-system multi-backup**

### **IN THIS SECTION**

- [Syntax](#) | [1251](#)
- [Description](#) | [1251](#)
- [Required Privilege Level](#) | [1251](#)
- [Sample Output](#) | [1251](#)
- [Release Information](#) | [1251](#)

## Syntax

EX2200 switch:

```
request redundant-power-system multi-backup
request redundant-power-system no-multi-backup
```

EX3300 switch:

```
request redundant-power-system multi-backup member member-number

request redundant-power-system no-multi-backup member member-number
```

## Description

Configure a redundant power system (RPS) to back up six non-Power-over-Ethernet (PoE) powered switches instead of the default which is to back up three PoE-powered switches.

## Required Privilege Level

admin—To view this statement in the configuration.

admin-control—To add this statement to the configuration.

## Sample Output

**request redundant-power-system multi-backup**

```
user@switch> request redundant-power-system multi-backup member 1
Sending multi-backup setting to RPS
```

## Release Information

Command introduced in Junos OS Release 12.1.

## RELATED DOCUMENTATION

| EX Series Redundant Power System Hardware Overview

## request security pki node-local local-certificate verify

### IN THIS SECTION

- [Syntax | 1252](#)
- [Description | 1252](#)
- [Options | 1252](#)
- [Required Privilege Level | 1252](#)
- [Output Fields | 1252](#)
- [Sample Output | 1253](#)
- [Release Information | 1253](#)

### Syntax

```
request security pki node-local local-certificate verify certificate-id certificate-id-name
```

### Description

Verify the validity of the local digital certificate identifier on the local node in Multinode High Availability setup.

### Options

`certificate-id` *certificate-id-name* — Name of the local digital certificate identifier.

### Required Privilege Level

maintenance and security

### Output Fields

When you enter this command, you are provided feedback on the status of your request.

## Sample Output

### **request security pki node-local local-certificate verify certificate-id bme1 (not downloaded)**

You receive the following response before the certificate revocation list (CRL) is downloaded:

```
user@host> request security pki node-local local-certificate verify certificate-id
bme1
Local certificate bme1: CRL verification in progress. Please check the PKId debug logs for
completion status
```

### **request security pki local-certificate verify certificate bme1 (downloaded)**

You receive the following response after the certificate revocation list (CRL) is downloaded:

```
user@host> request security pki node-local local-certificate verify certificate-id
bme1
Local certificate bme1 verification success
```

## Release Information

Command introduced in Junos OS Release 22.3R1.

## RELATED DOCUMENTATION

[Multinode High Availability](#) /

[show security pki node-local local-certificate](#) /

[request security pki node-local local-certificate re-enroll](#) /

[request security pki node-local local-certificate load](#) /

[request security pki node-local local-certificate export](#)

[request security pki node-local local-certificate enroll](#) /

# request security pki node-local local-certificate re-enroll

## IN THIS SECTION

- [Syntax | 1254](#)
- [Description | 1254](#)
- [Options | 1254](#)
- [Required Privilege Level | 1255](#)
- [Output Fields | 1255](#)
- [Release Information | 1255](#)

## Syntax

```
request security pki node-local local-certificate re-enroll (cmpv2 | scep) certificate-id
certificate-id ca-profile profile-name challenge-password password
<re-generate-keypair>
<scep-digest-algorithm>
<scep-encryption-algorithm>
```

## Description

Manually reenroll an end-entity (EE) certificate with Certificate Management Protocol version 2 (CMPv2) or with Simple Certificate Enrollment Protocol (SCEP). This command initiates renewal of the EE certificate using the selected protocol and you can use the command in conjunction with the set security pki auto-re-enrollment command for automatic enrollment.

## Options

scep	Enroll end-entity certificate using SCEP protocol
cmpv2	Enroll certificate using CMPv2 protocol
ca-profile-name <i>ca-profile-name</i>	(Optional) CA profile name.
certificate-id <i>certificate-id-name</i>	Name of the local digital certificate.
challenge-password	Password used by CA for enrollment and revocation



<b>re-generate-keypair</b>	(Optional) Generate a PKI public/private key pair for the EE certificate.  Key generation might take a few seconds.
<b>scep-digest-algorithm</b>	Hash algorithm used for SCEP-PKCS7
<b>scep-encryption-algorithm</b>	Encryption algorithm used for SCEP-PKCS7

**Required Privilege Level**

maintenance and security

**Output Fields**

This command produces no output.

**Release Information**

Command introduced in Junos OS Release 22.3R1.

**RELATED DOCUMENTATION**

<a href="#">Multinode High Availability /</a>
<a href="#">show security pki node-local local-certificate /</a>
<a href="#">request security pki node-local local-certificate enroll /</a>
<a href="#">request security pki node-local local-certificate load /</a>
<a href="#">request security pki node-local local-certificate export</a>

**request security pki node-local local-certificate load**

**IN THIS SECTION**

- [Syntax | 1256](#)
- [Description | 1256](#)
- [Options | 1256](#)

- [Required Privilege Level | 1256](#)
- [Output Fields | 1256](#)
- [Sample Output | 1257](#)
- [Release Information | 1257](#)

## Syntax

```
request security pki node-local local-certificate load certificate-id certificate-id  
filename file-name key key-string  
<passphrase passphrase-string>
```

## Description

Manually load a local digital certificate from a specified location on the local device in a Multinode High Availability setup.

## Options

<b>certificate-id</b>	Name of the certificate identifier
<b>filename</b>	Filename that contains the certificate to load
<b>key</b>	File pathname that contains the private key/key-pair to loaded
<b>passphrase</b>	Passphrase of the private key/key-pair (PEM) file

## Required Privilege Level

maintenance and security

## Output Fields

When you enter this command, you are provided feedback on the status of your request.

## Sample Output

### request security pki node-local local-certificate load

```
user@host> request security pki node-local local-certificate load filename cert_name.crt key
key_name.key certificate-id test
Local certificate cert_name.crt loaded successfully
```

## Release Information

Command introduced in Junos OS Release 22.3R1

## RELATED DOCUMENTATION

[Multinode High Availability](#) /

[show security pki node-local local-certificate](#) /

[request security pki node-local local-certificate enroll](#) /

[request security pki node-local local-certificate export](#)

[request security pki node-local local-certificate re-enroll](#) /

## request security pki node-local local-certificate export

### IN THIS SECTION

- [Syntax](#) | 1258
- [Description](#) | 1258
- [Options](#) | 1258
- [Required Privilege Level](#) | 1258
- [Output Fields](#) | 1258
- [Sample Output](#) | 1258
- [Release Information](#) | 1259

## Syntax

```
request security pki node-local local-certificate export certificate id certificate-id-name
filename path/filename
<type (der | pem)>
```

## Description

Export a generated self-signed certificate from the default location (var/db/certs/common/local) to a specific location within the local device in a Multinode High Availability setup.

## Options

<b>certificate id</b> <i>certificate-id-name</i>	Name of the local digital certificate.
<b>filename</b> <i>path/filename</i>	Target directory location and filename of the CA digital certificate.
<b>type</b> (der   pem)	Certificate format: DER (distinguished encoding rules) or PEM (privacy-enhanced mail).

## Required Privilege Level

maintenance

## Output Fields

When you enter this command, you are provided feedback on the status of your request.

## Sample Output

**request security pki node-local local-certificate export**

```
user@host> request security pki node-local local-certificate export filename /var/tmp/my-
cert.pem certificate-id nss-cert type pem
certificate exported successfully
```

## Release Information

Command introduced in Junos OS Release 22.3R1

## RELATED DOCUMENTATION

[Multinode High Availability](#) /

[show security pki node-local local-certificate](#) /

[request security pki node-local local-certificate enroll](#) /

[request security pki node-local local-certificate load](#) /

[request security pki node-local local-certificate re-enroll](#) /

## request security pki node-local local-certificate enroll

### IN THIS SECTION

- [Syntax](#) | **1259**
- [Description](#) | **1260**
- [Options](#) | **1260**
- [Required Privilege Level](#) | **1261**
- [Output Fields](#) | **1261**
- [Sample Output](#) | **1261**
- [Release Information](#) | **1262**

## Syntax

```
request security pki node-local local-certificate enroll
  ca-dn subject-dn
  ca-profile ca-profile name
  ca-reference reference
  ca-secret shared-secret
  certificate-id certificate-id-name
  challenge-password password
```

```

cmpv2
digiSt
domain-name domain-name
email email-address
ip-address ip-address
ipv6-address ipv6-address
scep
scep-digest-algorithm
scep-encryption-algorithm
subject subject-distinguished-name

```

## Description

Enroll and install a local digital certificate online by using CMPv2 or Simple Certificate Enrollment Protocol (SCEP). This command loads both end-entity (EE) and CA certificates based on the CA server configuration. Certificate revocation list (CRL) or Online Certificate Status Protocol (OCSP) can be used to check the revocation status of a certificate.

## Options

<b>ca-profile</b> <i>ca-profile-name</i>	CA profile name.
<b>certificate-id</b> <i>certificate-id-name</i>	Name of the local digital certificate and the public/private key pair.
<b>challenge-password</b> <i>password</i>	Password set by the administrator and normally obtained from the SCEP enrollment webpage of the CA. The password is 16 characters in length
<b>cmpv2</b>	Enroll certificate using CMPv2 protocol.
<b>domain-name</b> <i>domain-name</i>	Fully qualified domain name (FQDN). The FQDN provides the identity of the certificate owner for Internet Key Exchange (IKE) negotiations and provides an alternative to the subject name.
<b>email</b> <i>email-address</i>	E-mail address of the certificate holder.
<b>ip-address</b> <i>ip-address</i>	IP address of the router.
<b>ipv6-address</b> <i>ipv6-address</i>	IPv6 address of the router for the alternate subject.
<b>scep</b>	Enroll certificate using Simple Certificate Enrollment Protocol (SCEP) protocol.

<b>scep-digest-algorithm</b>	Hash algorithm digest, either MD5 or SHA-1; SHA-1 is the default.
<b>scep-encryption-algorithm</b>	Encryption algorithm, either DES or DES3; DES3 is the default.
<b>subject <i>subject-distinguished-name</i></b>	<p>Distinguished Name (DN) format that contains the domain component, common name, department, serial number, company name, state, and country in the following format: DC, CN, OU, O, SN, L, ST, C.</p> <ul style="list-style-type: none"> <li>• DC—Domain component</li> <li>• CN—Common name</li> <li>• OU—Organizational unit name</li> <li>• O—Organization name</li> <li>• SN—Serial number of the device</li> </ul> <p>If you define SN in the subject field without the serial number, then the serial number is read directly from the device and added to the certificate signing request (CSR).</p> <ul style="list-style-type: none"> <li>• ST—State</li> <li>• C—Country</li> </ul>

## Required Privilege Level

maintenance and security

## Output Fields

When you enter this command, you are provided feedback on the status of your request.

## Sample Output

### command-name

```
user@host> request security pki node-local local-certificate enroll cmpv2 ca-profile root-552 ca-
dn DC=example,CN=root-552 certificate-id tc552 email tc552-root@example.net domain-name
example.net ip-address 10.192.0.22 ca-secret example ca-reference 51892 subject
CN=example,OU=SBU,O=552-22
```

Certificate enrollment has started. To view the status of your enrollment, check the public key infrastructure log (pkid) log file at /var/log/pkid.

## Release Information

Command introduced in Junos OS Release 22.3R1.

## RELATED DOCUMENTATION

[Multinode High Availability](#) /

[show security pki node-local local-certificate](#) /

[request security pki node-local local-certificate load](#) /

[request security pki node-local local-certificate export](#)

[request security pki node-local local-certificate re-enroll](#) /

## request security pki node-local key-pair export

### IN THIS SECTION

- [Syntax](#) | 1262
- [Description](#) | 1263
- [Options](#) | 1263
- [Required Privilege Level](#) | 1263
- [Output Fields](#) | 1263
- [Release Information](#) | 1263

## Syntax

```
request security pki node-local key-pair export certificate-id certificate-id filename filename
<passphrase string>
< type (der | pem)>
```



Description

Export the keypair for an end-entity (EE) certificate. Junos OS encrypts the exported keypair.

You can export the PKI key-pairs file as a backup or to check the file for troubleshooting purposes.

We recommend providing permission to the `request security pki node-local key-pair export` command only to the privileged users.

Options

<b>certificate-id</b> <i>certificate-id</i>	Name of the local digital certificate.
<b>filename</b> <i>filename</i>	Target directory location and filename of the CA digital certificate.
<b>passphrase</b> <i>passphrase</i>	(Optional) Passphrase to protect the keypair data for PEM format. The passphrase can be up to 64 characters. If specified, the passphrase must be used when importing the keypair.
<b>type</b> ( <i>der</i>   <i>pem</i> )	(Optional) Type of format, either DER or PEM. PEM is the default.

Required Privilege Level

maintenance

Output Fields

This command produces no output.

Release Information

Command introduced in Junos OS Release 22.3R1

RELATED DOCUMENTATION

<a href="#">Multinode High Availability</a> /
<a href="#">request security pki node-local generate-key-pair</a> /
<a href="#">clear security pki node-local key-pair</a> /

# request security pki node-local generate-key-pair

IN THIS SECTION

- [Syntax | 1264](#)
- [Description | 1264](#)
- [Options | 1264](#)
- [Required Privilege Level | 1265](#)
- [Output Fields | 1265](#)
- [Sample Output | 1265](#)
- [Release Information | 1265](#)

## Syntax

```
request security pki node-local generate-key-pair certificate-id certificate-id-name
<size (256 | 384 | 521 | 1024 | 2048 | 4096)>
<type (dsa | ecdsa | rsa)>
```

## Description

Generate a public key infrastructure (PKI) public/private key pair for a local digital certificate on the local node in a Multinode High Availability setup.

## Options

<b>certificate-id</b> <b><i>certificate-id-name</i></b>	Name of the local digital certificate and the public/private key pair.
<b>size</b>	Key pair size. The key pair size can be 256, 384, 521, 1024, 2048, or 4096 bits.
	Key size compatibility
	<ul style="list-style-type: none"><li>• ECDSA-256, 384, and 521</li></ul>

- DSA and RSA - 1024, 2048, or 4096. The default key pair size is 1024 for DSA and 2048 for RSA.

When you use ECDSA-521 signatures, you can:

- Load a complete certificate, which is generated using an external tool like OpenSSL into PKI.
- Manually generate a Certificate Signing Request (CSR) for a local certificate and sending the CSR to a (Certificate Authority) CA server to enroll.
- Automatic enroll with CA server.

**type** The algorithm to be used for encrypting the public/private key pair:

- `ecdsa`—ECDSA encryption
- `dsa`— DSA encryption
- `rsa`—RSA encryption (default)

## Required Privilege Level

maintenance

## Output Fields

When you enter this command, you are provided feedback on the status of your request.

## Sample Output

**request security pki generate-key-pair**

```
user@host> request security pki node-local generate-key-pair certificate-id cert-123 type rsa
size 4096
Generated key pair cert-123, key size [4096] bits
```

## Release Information

Command introduced in Junos OS Release 22.3R1.

## RELATED DOCUMENTATION

[Multinode High Availability](#) /

[clear security pki node-local key-pair](#) /

[request security pki node-local key-pair export](#) /

## request security pki sync-from-peer

### IN THIS SECTION

- [Syntax](#) | 1266
- [Description](#) | 1266
- [Required Privilege Level](#) | 1267
- [Output Fields](#) | 1267
- [Sample Output](#) | 1267
- [Release Information](#) | 1267

### Syntax

```
request security pki sync-from-peer
```

### Description

Synchronize the PKI file system on the peer node in a Multinode High Availability setup. You can use this command to replicate the PKI directory in the remote node to your local node. Replicating PKI directory is helpful when one of the two nodes or ICL goes down.

Note that you can run this command only you've enabled Multinode High Availability.

Consider a set up with node 0 (local node) and node 1 (remote node). To replicate the PKI directory of the remote node (node 1), run this command in your local node (node 0).

When you run this command on your local node, all the local PKI files are deleted and replaced by the remote node PKI directory. Hence, be sure on which node you are executing this command. After running this command, we recommend you to verify whether the files are synchronized between the two nodes.

## Required Privilege Level

maintenance

## Output Fields

This command produces no output.

## Sample Output

### request security pki sync-from-peer

```
user@host> request security pki sync-from-peer
File syncing is in progress... This will take a few seconds. Please confirm that the files are
synched. If not, run this command once again.
```

## Release Information

Command introduced in Junos OS Release 20.4R1.

## RELATED DOCUMENTATION

*ike (High Availability)*

*ipsec (High Availability)*

[High-Availability \(Chassis\)](#)

[Multinode High Availability](#)

## request security pki node-local generate-certificate-request

### IN THIS SECTION

- [Syntax | 1268](#)
- [Description | 1268](#)

- Options | 1268
- Required Privilege Level | 1269
- Output Fields | 1269
- Sample Output | 1269
- Release Information | 1270

## Syntax

```
request security pki node-local generate-certificate-request certificate-id certificate-id-name
domain-name domain-name subject subject-distinguished-name
<digest (sha1 | sha256)>
<email email-address>
<filename (path | terminal)>
<ip-address ip-address>
```

## Description

Manually generate a local digital certificate request in the Public-Key Cryptography Standards #10 (PKCS-10) format on the local device in a Multinode High Availability setup.

## Options

<b>certificate-id</b> <i>certificate-id-name</i>	Name of the local digital certificate and the public/private key pair.
<b>domain-name</b> <i>domain-name</i>	Fully qualified domain name (FQDN) provides the identity of the certificate owner for Internet Key Exchange (IKE) negotiations and provides an alternative to the subject name.
<b>subject</b> <i>subject-distinguished-name</i>	Distinguished name format contains the following information: <ul style="list-style-type: none"> <li>● DC—Domain component</li> <li>● CN—Common name</li> <li>● OU—Organizational unit name</li> </ul>

- `o`—Organization name
- `L`—Locality
- `ST`—State
- `C`—Country

<b>digest</b>	(Optional) Hash algorithm used to sign the certificate request.
	<ul style="list-style-type: none"> <li>• <code>sha-1</code>—SHA-1 digests (default value for RSA or DSA only).</li> <li>• <code>sha-256</code>—SHA-256 digests for RSA or ECDSA only (default value for ECDSA).</li> <li>• <code>sha-384</code>—SHA-384 digests for ECDSA only.</li> </ul>
<b>email</b> <i>email-address</i>	(Optional) E-mail address of the certificate holder.
<b>filename</b> ( <i>path</i>   <i>terminal</i> )	(Optional) Location where the local digital certificate request should be placed or the login terminal.
<b>ip-address</b> <i>ip-address</i>	(Optional) IP address of the router.

## Required Privilege Level

maintenance

## Output Fields

When you enter this command, you are provided feedback on the status of your request.

## Sample Output

**request security pki generate-certificate-request**

```
user@host> request security pki node-local generate-certificate-request certificate-id local-entrust2 domain-name router2.example.net filename entrust-req2 subject cn=router2.example.net
```

Generated certificate request

-----BEGIN CERTIFICATE REQUEST-----

```
MIIBoTCCAQoCAQAwGjEYMBYGA1UEAxMPdHxLmp1bm1wZXIubmV0MIGfMA0GCSqG
SIb3DQEBAQUAA4GNADCBiQKBgQCiUFk1Qws1Ud+AqN5DDxRs2kVyKEhh9qoVFnz+
```

```

Hz4c9vsy3B8ElwTJlkmIt2cB3yifB6zePd+6WYpf57Crwre7YqPkiXM31F6z3YjX
H+1BPNbCxNWYvyrnSyVYDbFj8o0Xyqog8ACDfVL2JBWrPNBYy7imq/K9soDBbAs6
5hZqqwIDAQABoEcwRQYJKoZIhvcNAQkOMTgwNjA0BgNVHQ8BAf8EBAMCB4AwJAYD
VR0RAQH/BBowGIIWdHAXLmVuZ2xhYi5qdW5pcGVyLm5ldDANBgkqhkiG9w0BAQQF
AA0BgQBc2rq1v5S0QXH7LCb/FdqAL8ZM6GoaN5d6cGwq4bB6a7UQFgtoH406gQ3G
3iH0Zfz4xMIBpJYuGd1dkqgvcDoH3AgTsLkfn7Wi3x5H2qeQVs9bvL4P5nvEZLND
EIMUHwteolZCiZ70f09Fer9cXWHSQs1UtXtgPqQJy2xIeImLgw==
-----END CERTIFICATE REQUEST-----
Fingerprint:
0d:90:b8:d2:56:74:fc:84:59:62:b9:78:71:9c:e4:9c:54:ba:16:97 (sha1)
1b:08:d4:f7:90:f1:c4:39:08:c9:de:76:00:86:62:b8 (md5)

```

## Release Information

Command introduced in Junos OS Release 22.3R1

## RELATED DOCUMENTATION

[Multinode High Availability](#) /

## request system software in-service-upgrade

### IN THIS SECTION

- [Syntax](#) | **1271**
- [Syntax](#) | **1271**
- [Description](#) | **1271**
- [Options](#) | **1271**
- [Additional Information](#) | **1273**
- [Required Privilege Level](#) | **1273**
- [Output Fields](#) | **1273**
- [Sample Output](#) | **1274**
- [Release Information](#) | **1290**



## Syntax

```
request system software in-service-upgrade package-name
<no-old-master-upgrade>
<reboot>
<status>
<enhanced-mode>
<no-validate>
<handle-incompatible-config>
```

## Syntax

### Syntax (QFX Series)

```
request system software in-service-upgrade package-name
```

## Description

Perform a unified in-service software upgrade (ISSU). A unified ISSU enables you to upgrade from one Junos OS release to another with no disruption on the control plane and with minimal disruption of traffic.

On QFX5100 and QFX5200 switches, enable nonstop active routing (NSR) and nonstop bridging (NSB).

## Options

- package-name*** Location from which the software package or bundle is to be installed. For example:
- */var/tmp/package-name*— For a software package or bundle that is being installed from a local directory on the router.
  - *protocol://hostname/pathname/package-name*— For a software package or bundle that is to be downloaded and installed from a remote location. Replace *protocol* with one of the following:
    - ftp—File Transfer Protocol
    - http—Hypertext Transfer Protocol
    - scp—Secure copy (available only for Canada and U.S. version)

**no-old-master-upgrade** (Optional) When the `no-old-master-upgrade` option is included, after the backup Routing Engine is rebooted with the new software package and a switchover occurs to make it the new primary Routing Engine, the former primary (new backup) Routing Engine will not be upgraded to the new software. In this case, you must manually upgrade the former primary (new backup) Routing Engine. If you do not include the `no-old-master-upgrade` option, the system will automatically upgrade the former primary Routing Engine.

**NOTE:** This option is not available on QFX5100 and QFX5200 switches.

**reboot** (Optional) When the `reboot` option is included, the former primary (new backup) Routing Engine is automatically rebooted after being upgraded to the new software. When the `reboot` option is not included, you must manually reboot the former primary (new backup) Routing Engine using the `request system reboot` command.

**NOTE:** This option is not available on the QFX Series switches.

**status** (Optional) Starting in Junos OS Release 19.4R1, use this option to display the status of a unified ISSU during the upgrade. You will need to run this command on the Routing Engine where the ISSU was triggered to display the correct ISSU log file.

**NOTE:** This option is only available on MX240, MX480, MX960, MX2010, MX2020, PTX3000, and PTX5000 routers.

**enhanced-mode** (Optional) Starting in Junos OS Release 20.1R1, runs unified ISSU in enhanced mode, a mode of ISSU that eliminates packet loss during the unified ISSU process.

**NOTE:** This option is only available on MPC8E, and MPC9E line cards. Support for MPC11E line cards is provided from Junos OS Release 21.4R1 onwards.

**no-validate** (Optional) Starting in Junos OS Release 20.4R2, skip the validation step of the unified ISSU process.

**handle-incompatible-config** (Optional) Starting in Junos OS Release 22.1R1, automatically deactivate the incompatible configurations at the start of an ISSU and reactivate them once the ISSU

is completed. If the ISSU is aborted, the deactivated configurations are automatically reactivated. This is currently applicable only to clock synchronization configurations for Precision Time Protocol (PTP) and Synchronous Ethernet.

**NOTE:** This option is available only for the MX960, MX10003, MX10008, MX10016, MX2010, and MX2020 routers.

## Additional Information

The following conditions apply to unified ISSUs:

- Unified ISSU is not supported on every platform. For a list of supported platforms, see "[Unified ISSU System Requirements](#)" on page 504.
- Unsupported PICs are restarted during a unified ISSU on certain routing devices. For information about supported PICs, see the [Junos OS High Availability User Guide](#).
- Unsupported protocols will experience packet loss during a unified ISSU. For information about supported protocols, see the [Junos OS High Availability User Guide](#).
- During a unified ISSU, you cannot bring any PICs online or offline on certain routing devices.
- The `no-validate` option is required when upgrading to Junos OS Releases 21.2R1 or 22.1R1. If you are upgrading from a release prior to Junos OS Release 20.4R2, then you will need to upgrade to a release that supports the `no-validate` option before using unified ISSU to upgrade to Junos OS Releases 21.2R1 or 22.1R1.

For more information, see the [Junos OS High Availability User Guide](#).

## Required Privilege Level

view

## Output Fields

When you enter this command, you are provided feedback on the status of your request.

## Sample Output

### request system software in-service-upgrade reboot

```
{master}
user@host> request system software in-service-upgrade /var/tmp/jinstall-9.0-20080114.2-domestic-signed.tgz
reboot
ISSU: Validating Image
PIC 0/3 will be offlined (In-Service-Upgrade not supported)
Do you want to continue with these actions being taken ? [yes,no] (no) yes

ISSU: Preparing Backup RE
Pushing bundle to re1
Checking compatibility with configuration
Initializing...
Using jbase-9.0-20080114.2
Verified manifest signed by PackageProduction_9_0_0
Using /var/tmp/jinstall-9.0-20080114.2-domestic-signed.tgz
Verified jinstall-9.0-20080114.2-domestic.tgz signed by PackageProduction_9_0_0
Using jinstall-9.0-20080114.2-domestic.tgz
Using jbundle-9.0-20080114.2-domestic.tgz
Checking jbundle requirements on /
Using jbase-9.0-20080114.2.tgz
Verified manifest signed by PackageProduction_9_0_0
Using jkernel-9.0-20080114.2.tgz
Verified manifest signed by PackageProduction_9_0_0
Using jcrypto-9.0-20080114.2.tgz
Verified manifest signed by PackageProduction_9_0_0
Using jpfe-9.0-20080114.2.tgz
Using jdocs-9.0-20080114.2.tgz
Verified manifest signed by PackageProduction_9_0_0
Using jroute-9.0-20080114.2.tgz
Verified manifest signed by PackageProduction_9_0_0
Hardware Database regeneration succeeded
Validating against /config/juniper.conf.gz
mgd: commit complete
Validation succeeded
Installing package '/var/tmp/jinstall-9.0-20080114.2-domestic-signed.tgz' ...
Verified jinstall-9.0-20080114.2-domestic.tgz signed by PackageProduction_9_0_0
Adding jinstall...
Verified manifest signed by PackageProduction_9_0_0
```

```

WARNING:      This package will load JUNOS 9.0-20080114.2 software.
WARNING:      It will save JUNOS configuration files, and SSH keys
WARNING:      (if configured), but erase all other files and information
WARNING:      stored on this machine. It will attempt to preserve dumps
WARNING:      and log files, but this can not be guaranteed. This is the
WARNING:      pre-installation stage and all the software is loaded when
WARNING:      you reboot the system.

```

Saving the config files ...

NOTICE: uncommitted changes have been saved in /var/db/config/juniper.conf.pre-install

Installing the bootstrap installer ...

```

WARNING:      A REBOOT IS REQUIRED TO LOAD THIS SOFTWARE CORRECTLY. Use the
WARNING:      'request system reboot' command when software installation is
WARNING:      complete. To abort the installation, do not reboot your system,
WARNING:      instead use the 'request system software delete jinstall'
WARNING:      command as soon as this operation completes.

```

Saving package file in /var/sw/pkg/jinstall-9.0-20080114.2-domestic-signed.tgz ...

Saving state for rollback ...

Backup upgrade done

Rebooting Backup RE

Rebooting re1

ISSU: Backup RE Prepare Done

Waiting for Backup RE reboot

GRES operational

Initiating Chassis In-Service-Upgrade

Chassis ISSU started

ISSU: Backup RE Prepare Done

ISSU: Preparing Daemons

ISSU: Daemons Ready for ISSU

ISSU: Starting Upgrade for FRUs

ISSU: Preparing for Switchover

ISSU: Ready for Switchover

Checking In-Service-Upgrade status

Item	Status	Reason
FPC 0	Online (ISSU)	
FPC 1	Online (ISSU)	
FPC 2	Online (ISSU)	
FPC 6	Online (ISSU)	
FPC 7	Online (ISSU)	

Resolving mastership...

```

Complete. The other routing engine becomes the master.
ISSU: RE switchover Done
ISSU: Upgrading Old Master RE
Installing package '/var/tmp/paKEuy' ...
Verified jinstall-9.0-20080114.2-domestic.tgz signed by PackageProduction_9_0_0
Adding jinstall...
Verified manifest signed by PackageProduction_9_0_0

WARNING:      This package will load JUNOS 9.0-20080114.2 software.
WARNING:      It will save JUNOS configuration files, and SSH keys
WARNING:      (if configured), but erase all other files and information
WARNING:      stored on this machine. It will attempt to preserve dumps
WARNING:      and log files, but this can not be guaranteed. This is the
WARNING:      pre-installation stage and all the software is loaded when
WARNING:      you reboot the system.

Saving the config files ...
NOTICE: uncommitted changes have been saved in /var/db/config/juniper.conf.pre-install
Installing the bootstrap installer ...

WARNING:      A REBOOT IS REQUIRED TO LOAD THIS SOFTWARE CORRECTLY. Use the
WARNING:      'request system reboot' command when software installation is
WARNING:      complete. To abort the installation, do not reboot your system,
WARNING:      instead use the 'request system software delete jinstall'
WARNING:      command as soon as this operation completes.

Saving package file in /var/sw/pkg/jinstall-9.0-20080114.2-domestic-signed.tgz ...
cp: /var/tmp/paKEuy is a directory (not copied).
Saving state for rollback ...
ISSU: Old Master Upgrade Done
ISSU: IDLE
Shutdown NOW!
Reboot consistency check bypassed - jinstall 9.0-20080114.2 will complete installation upon
reboot
[pid 30227]

*** FINAL System shutdown message from root@host ***

System going down IMMEDIATELY

Connection to host closed.

```

**request system software in-service-upgrade reboot (TX Matrix Plus Router)**

```

{master}
user@host> request system software in-service-upgrade /var/tmp/jinstall-12.3R2-domestic-signed.tgz
Chassis ISSU Check Done
ISSU: Validating Image
PIC 8/1 will be offlined (In-Service-Upgrade not supported)
PIC 19/2 will be offlined (In-Service-Upgrade not supported)
PIC 15/3 will be offlined (In-Service-Upgrade not supported)
Do you want to continue with these actions being taken ? [yes,no] (no) yes

Checking compatibility with configuration
Initializing...
Using jbase-12.3R2
Verified manifest signed by PackageProduction_12_3_0
Using /var/tmp/jinstall-12.3R2-domestic-signed.tgz
Verified jinstall-12.3R2-domestic.tgz signed by PackageProduction_12_3_0
Using jinstall-12.3R2-domestic.tgz
Using jbundle-12.3R2-domestic.tgz
Checking jbundle requirements on /
Using jbase-12.3R2.tgz
Verified manifest signed by PackageProduction_12_3_0
Verified jbase-12.3R2 signed by PackageProduction_12_3_0
Using /var/validate/chroot/tmp/jbundle/jboot-12.3R2.tgz
Using jcrypto-12.3R2.tgz
Verified manifest signed by PackageProduction_12_3_0
Verified jcrypto-12.3R2 signed by PackageProduction_12_3_0
Using jdocs-12.3R2.tgz
Verified manifest signed by PackageProduction_12_3_0
Verified jdocs-12.3R2 signed by PackageProduction_12_3_0
Using jkernel-12.3R2.tgz
Verified manifest signed by PackageProduction_12_3_0
Verified jkernel-12.3R2 signed by PackageProduction_12_3_0
Using jpfe-12.3R2.tgz
WARNING: jpfe-12.3R2.tgz: not a signed package
WARNING: jpfe-common-12.3R2.tgz: not a signed package
Verified jpfe-common-12.3R2 signed by PackageProduction_12_3_0
WARNING: jpfe-T-12.3R2.tgz: not a signed package
Verified jpfe-T-12.3R2 signed by PackageProduction_12_3_0
Using jplatform-12.3R2.tgz
Verified manifest signed by PackageProduction_12_3_0
Verified jplatform-12.3R2 signed by PackageProduction_12_3_0

```

```

Using jroute-12.3R2.tgz
Verified manifest signed by PackageProduction_12_3_0
Verified jroute-12.3R2 signed by PackageProduction_12_3_0
Using jruntime-12.3R2.tgz
Verified manifest signed by PackageProduction_12_3_0
Verified jruntime-12.3R2 signed by PackageProduction_12_3_0
Using jservices-12.3R2.tgz
Using jservices-crypto-12.3R2.tgz
Hardware Database regeneration succeeded
Validating against /config/juniper.conf.gz
mgd: commit complete
Validation succeeded
ISSU: Preparing LCC Backup REs
Pushing bundle to lcc0-re1
Pushing bundle to lcc1-re1
Pushing bundle to lcc2-re1
Pushing bundle to lcc3-re1
Pushing bundle to sfc0-re1
Installing package '/var/tmp/jinstall-12.3R2-domestic-signed.tgz' ...
Verified jinstall-12.3R2-domestic.tgz signed by PackageProduction_12_3_0
Adding jinstall...
Verified manifest signed by PackageProduction_12_3_0

WARNING:    This package will load JUNOS 12.3R2 software.
WARNING:    It will save JUNOS configuration files, and SSH keys
WARNING:    (if configured), but erase all other files and information
WARNING:    stored on this machine. It will attempt to preserve dumps
WARNING:    and log files, but this can not be guaranteed. This is the
WARNING:    pre-installation stage and all the software is loaded when
WARNING:    you reboot the system.

Saving the config files ...
NOTICE: uncommitted changes have been saved in /var/db/config/juniper.conf.pre-install
Installing the bootstrap installer ...

WARNING:    A REBOOT IS REQUIRED TO LOAD THIS SOFTWARE CORRECTLY. Use the
WARNING:    'request system reboot' command when software installation is
WARNING:    complete. To abort the installation, do not reboot your system,
WARNING:    instead use the 'request system software delete jinstall'
WARNING:    command as soon as this operation completes.

Saving package file in /var/sw/pkg/jinstall-12.3R2-domestic-signed.tgz ...
Saving state for rollback ...

```



```
Installing package '/var/tmp/jinstall-12.3R2-domestic-signed.tgz' ...
Verified jinstall-12.3R2-domestic.tgz signed by PackageProduction_12_3_0
Adding jinstall...
Verified manifest signed by PackageProduction_12_3_0
```

```
WARNING:    This package will load JUNOS 12.3R2 software.
WARNING:    It will save JUNOS configuration files, and SSH keys
WARNING:    (if configured), but erase all other files and information
WARNING:    stored on this machine. It will attempt to preserve dumps
WARNING:    and log files, but this can not be guaranteed. This is the
WARNING:    pre-installation stage and all the software is loaded when
WARNING:    you reboot the system.
```

```
Saving the config files ...
NOTICE: uncommitted changes have been saved in /var/db/config/juniper.conf.pre-install
Installing the bootstrap installer ...
```

```
WARNING:    A REBOOT IS REQUIRED TO LOAD THIS SOFTWARE CORRECTLY. Use the
WARNING:    'request system reboot' command when software installation is
WARNING:    complete. To abort the installation, do not reboot your system,
WARNING:    instead use the 'request system software delete jinstall'
WARNING:    command as soon as this operation completes.
```

```
Saving package file in /var/sw/pkg/jinstall-12.3R2-domestic-signed.tgz ...
Saving state for rollback ...
Installing package '/var/tmp/jinstall-12.3R2-domestic-signed.tgz' ...
Verified jinstall-12.3R2-domestic.tgz signed by PackageProduction_12_3_0
Adding jinstall...
Verified manifest signed by PackageProduction_12_3_0
```

```
WARNING:    This package will load JUNOS 12.3R2 software.
WARNING:    It will save JUNOS configuration files, and SSH keys
WARNING:    (if configured), but erase all other files and information
WARNING:    stored on this machine. It will attempt to preserve dumps
WARNING:    and log files, but this can not be guaranteed. This is the
WARNING:    pre-installation stage and all the software is loaded when
WARNING:    you reboot the system.
```

```
Saving the config files ...
NOTICE: uncommitted changes have been saved in /var/db/config/juniper.conf.pre-install
Installing the bootstrap installer ...
```

```
WARNING:    A REBOOT IS REQUIRED TO LOAD THIS SOFTWARE CORRECTLY. Use the
```

```

WARNING:      'request system reboot' command when software installation is
WARNING:      complete. To abort the installation, do not reboot your system,
WARNING:      instead use the 'request system software delete jinstall'
WARNING:      command as soon as this operation completes.

```

```
Saving package file in /var/sw/pkg/jinstall-12.3R2-domestic-signed.tgz ...
```

```
Saving state for rollback ...
```

```
Installing package '/var/tmp/jinstall-12.3R2-domestic-signed.tgz' ...
```

```
Verified jinstall-12.3R2-domestic.tgz signed by PackageProduction_12_3_0
```

```
Adding jinstall...
```

```
Verified manifest signed by PackageProduction_12_3_0
```

```
WARNING:      This package will load JUNOS 12.3R2 software.
```

```
WARNING:      It will save JUNOS configuration files, and SSH keys
```

```
WARNING:      (if configured), but erase all other files and information
```

```
WARNING:      stored on this machine. It will attempt to preserve dumps
```

```
WARNING:      and log files, but this can not be guaranteed. This is the
```

```
WARNING:      pre-installation stage and all the software is loaded when
```

```
WARNING:      you reboot the system.
```

```
Saving the config files ...
```

```
NOTICE: uncommitted changes have been saved in /var/db/config/juniper.conf.pre-install
```

```
Installing the bootstrap installer ...
```

```
WARNING:      A REBOOT IS REQUIRED TO LOAD THIS SOFTWARE CORRECTLY. Use the
```

```
WARNING:      'request system reboot' command when software installation is
```

```
WARNING:      complete. To abort the installation, do not reboot your system,
```

```
WARNING:      instead use the 'request system software delete jinstall'
```

```
WARNING:      command as soon as this operation completes.
```

```
Saving package file in /var/sw/pkg/jinstall-12.3R2-domestic-signed.tgz ...
```

```
Saving state for rollback ...
```

```
ISSU: Preparing SFC Backup RE
```

```
NOTICE: Validating configuration against jinstall-12.3R2-domestic-signed.tgz.
```

```
NOTICE: Use the 'no-validate' option to skip this if desired.
```

```
Checking compatibility with configuration
```

```
Initializing...
```

```
Using jbase-12.3R2
```

```
Verified manifest signed by PackageProduction_12_3_0
```

```
Using /var/tmp/jinstall-12.3R2-domestic-signed.tgz
```

```
Verified jinstall-12.3R2-domestic.tgz signed by PackageProduction_12_3_0
```

```
Using jinstall-12.3R2-domestic.tgz
```

```
Using jbundle-12.3R2-domestic.tgz
```

```

Checking jbundle requirements on /
Using jbase-12.3R2.tgz
Verified manifest signed by PackageProduction_12_3_0
Verified jbase-12.3R2 signed by PackageProduction_12_3_0
Using /var/validate/chroot/tmp/jbundle/jboot-12.3R2.tgz
Using jcrypto-12.3R2.tgz
Verified manifest signed by PackageProduction_12_3_0
Verified jcrypto-12.3R2 signed by PackageProduction_12_3_0
Using jdocs-12.3R2.tgz
Verified manifest signed by PackageProduction_12_3_0
Verified jdocs-12.3R2 signed by PackageProduction_12_3_0
Using jkernel-12.3R2.tgz
Verified manifest signed by PackageProduction_12_3_0
Verified jkernel-12.3R2 signed by PackageProduction_12_3_0
Using jpfe-12.3R2.tgz
WARNING: jpfe-12.3R2.tgz: not a signed package
WARNING: jpfe-common-12.3R2.tgz: not a signed package
Verified jpfe-common-12.3R2 signed by PackageProduction_12_3_0
WARNING: jpfe-T-12.3R2.tgz: not a signed package
Verified jpfe-T-12.3R2 signed by PackageProduction_12_3_0
Using jplatform-12.3R2.tgz
Verified manifest signed by PackageProduction_12_3_0
Verified jplatform-12.3R2 signed by PackageProduction_12_3_0
Using jroute-12.3R2.tgz
Verified manifest signed by PackageProduction_12_3_0
Verified jroute-12.3R2 signed by PackageProduction_12_3_0
Using jruntime-12.3R2.tgz
Verified manifest signed by PackageProduction_12_3_0
Verified jruntime-12.3R2 signed by PackageProduction_12_3_0
Using jservices-12.3R2.tgz
Using jservices-crypto-12.3R2.tgz
Hardware Database regeneration succeeded
Validating against /config/juniper.conf.gz
mgd: commit complete
Validation succeeded
Installing package '/var/tmp/jinstall-12.3R2-domestic-signed.tgz' ...
Verified jinstall-12.3R2-domestic.tgz signed by PackageProduction_12_3_0
Adding jinstall...
Verified manifest signed by PackageProduction_12_3_0

WARNING:      This package will load JUNOS 12.3R2 software.
WARNING:      It will save JUNOS configuration files, and SSH keys
WARNING:      (if configured), but erase all other files and information

```

```

WARNING:    stored on this machine.  It will attempt to preserve dumps
WARNING:    and log files, but this can not be guaranteed.  This is the
WARNING:    pre-installation stage and all the software is loaded when
WARNING:    you reboot the system.

```

```
Saving the config files ...
```

```
NOTICE: uncommitted changes have been saved in /var/db/config/juniper.conf.pre-install
```

```
Installing the bootstrap installer ...
```

```

WARNING:    A REBOOT IS REQUIRED TO LOAD THIS SOFTWARE CORRECTLY. Use the
WARNING:    'request system reboot' command when software installation is
WARNING:    complete. To abort the installation, do not reboot your system,
WARNING:    instead use the 'request system software delete jinstall'
WARNING:    command as soon as this operation completes.

```

```
Saving package file in /var/sw/pkg/jinstall-12.3R2-domestic-signed.tgz ...
```

```
Saving state for rollback ...
```

```
SFC Backup upgrade done
```

```
Rebooting SFC Backup RE
```

```
Rebooting sfc0-re1
```

```
ISSU: SFC Backup RE Prepare Done
```

```
Waiting for SFC Backup RE reboot
```

```
Rebooting lcc0-re1
```

```
Rebooting LCC [lcc0-re1]
```

```
Rebooting lcc1-re1
```

```
Rebooting LCC [lcc1-re1]
```

```
Rebooting lcc2-re1
```

```
Rebooting LCC [lcc2-re1]
```

```
Rebooting lcc3-re1
```

```
Rebooting LCC [lcc3-re1]
```

```
LCC Backup REs have rebooted
```

```
Waiting for LCC Backup REs come back online
```

```
ISSU: LCC Backup REs Prepare Done
```

```
GRES operational
```

```
Initiating Chassis In-Service-Upgrade
```

```
Chassis ISSU Started
```

```
ISSU: Preparing Daemons
```

```
ISSU: Daemons Ready for ISSU
```

ISSU: Starting Upgrade for FRUs

ISSU: Preparing for Switchover

ISSU: Ready for Switchover

Checking In-Service-Upgrade status

lcc0-re0:

---

Item	Status	Reason
FPC 1	Online (ISSU)	
PIC 0	Online (ISSU)	
FPC 2	Online (ISSU)	
FPC 3	Online (ISSU)	
PIC 1	Online (ISSU)	
FPC 4	Online (ISSU)	
FPC 6	Online (ISSU)	
FPC 7	Online (ISSU)	

lcc1-re0:

---

Item	Status	Reason
FPC 0	Online (ISSU)	
PIC 3	Online (ISSU)	
FPC 1	Online (ISSU)	
FPC 2	Online (ISSU)	
FPC 4	Online (ISSU)	
FPC 6	Online (ISSU)	
FPC 7	Online (ISSU)	

lcc2-re0:

---

Item	Status	Reason
FPC 0	Online (ISSU)	
FPC 2	Online (ISSU)	
FPC 3	Online (ISSU)	
PIC 0	Online (ISSU)	
FPC 4	Online (ISSU)	
FPC 6	Online (ISSU)	
FPC 7	Online (ISSU)	
PIC 1	Online (ISSU)	

lcc3-re0:

---

Item	Status	Reason
FPC 0	Online (ISSU)	

```

    PIC 0      Online (ISSU)
    FPC 1      Online (ISSU)
    FPC 2      Online (ISSU)
    FPC 3      Online (ISSU)
    PIC 2      Online (ISSU)
    FPC 4      Online (ISSU)
    FPC 5      Online (ISSU)
    FPC 6      Online (ISSU)
    FPC 7      Online (ISSU)
    PIC 1      Online (ISSU)

lcc0-re0:
-----
Resolving mastership...
Complete. The other routing engine becomes the master.

lcc1-re0:
-----
Resolving mastership...
Complete. The other routing engine becomes the master.

lcc2-re0:
-----
Resolving mastership...
Complete. The other routing engine becomes the master.

lcc3-re0:
-----
Resolving mastership...
Complete. The other routing engine becomes the master.
Resolving mastership...
Complete. The other routing engine becomes the master.
ISSU: RE switchover Done
ISSU: Upgrading SFC Old Master RE

lcc0-re0:
Installing package '/var/tmp/jinstall-12.3R2-domestic-signed.tgz' ...
Verified jinstall-12.3R2-domestic.tgz signed by PackageProduction_12_3_0
Adding jinstall...
Verified manifest signed by PackageProduction_12_3_0

WARNING:      This package will load JUNOS 12.3R2 software.
WARNING:      It will save JUNOS configuration files, and SSH keys

```

```

WARNING:      (if configured), but erase all other files and information
WARNING:      stored on this machine. It will attempt to preserve dumps
WARNING:      and log files, but this can not be guaranteed. This is the
WARNING:      pre-installation stage and all the software is loaded when
WARNING:      you reboot the system.

```

Saving the config files ...

NOTICE: uncommitted changes have been saved in /var/db/config/juniper.conf.pre-install

Installing the bootstrap installer ...

```

WARNING:      A REBOOT IS REQUIRED TO LOAD THIS SOFTWARE CORRECTLY. Use the
WARNING:      'request system reboot' command when software installation is
WARNING:      complete. To abort the installation, do not reboot your system,
WARNING:      instead use the 'request system software delete jinstall'
WARNING:      command as soon as this operation completes.

```

Saving package file in /var/sw/pkg/jinstall-12.3R2-domestic-signed.tgz ...

Saving state for rollback ...

lcc1-re0:

Installing package '/var/tmp/jinstall-12.3R2-domestic-signed.tgz' ...

Verified jinstall-12.3R2-domestic.tgz signed by PackageProduction\_12\_3\_0

Adding jinstall...

Verified manifest signed by PackageProduction\_12\_3\_0

```

WARNING:      This package will load JUNOS 12.3R2 software.
WARNING:      It will save JUNOS configuration files, and SSH keys
WARNING:      (if configured), but erase all other files and information
WARNING:      stored on this machine. It will attempt to preserve dumps
WARNING:      and log files, but this can not be guaranteed. This is the
WARNING:      pre-installation stage and all the software is loaded when
WARNING:      you reboot the system.

```

Saving the config files ...

NOTICE: uncommitted changes have been saved in /var/db/config/juniper.conf.pre-install

Installing the bootstrap installer ...

```

WARNING:      A REBOOT IS REQUIRED TO LOAD THIS SOFTWARE CORRECTLY. Use the
WARNING:      'request system reboot' command when software installation is
WARNING:      complete. To abort the installation, do not reboot your system,
WARNING:      instead use the 'request system software delete jinstall'
WARNING:      command as soon as this operation completes.

```

```
Saving package file in /var/sw/pkg/jinstall-12.3R2-domestic-signed.tgz ...
Saving state for rollback ...
```

```
lcc2-re0:
```

```
Installing package '/var/tmp/jinstall-12.3R2-domestic-signed.tgz' ...
Verified jinstall-12.3R2-domestic.tgz signed by PackageProduction_12_3_0
Adding jinstall...
Verified manifest signed by PackageProduction_12_3_0
```

```
WARNING:    This package will load JUNOS 12.3R2 software.
WARNING:    It will save JUNOS configuration files, and SSH keys
WARNING:    (if configured), but erase all other files and information
WARNING:    stored on this machine. It will attempt to preserve dumps
WARNING:    and log files, but this can not be guaranteed. This is the
WARNING:    pre-installation stage and all the software is loaded when
WARNING:    you reboot the system.
```

```
Saving the config files ...
```

```
NOTICE: uncommitted changes have been saved in /var/db/config/juniper.conf.pre-install
Installing the bootstrap installer ...
```

```
WARNING:    A REBOOT IS REQUIRED TO LOAD THIS SOFTWARE CORRECTLY. Use the
WARNING:    'request system reboot' command when software installation is
WARNING:    complete. To abort the installation, do not reboot your system,
WARNING:    instead use the 'request system software delete jinstall'
WARNING:    command as soon as this operation completes.
```

```
Saving package file in /var/sw/pkg/jinstall-12.3R2-domestic-signed.tgz ...
Saving state for rollback ...
```

```
lcc3-re0:
```

```
Installing package '/var/tmp/jinstall-12.3R2-domestic-signed.tgz' ...
Verified jinstall-12.3R2-domestic.tgz signed by PackageProduction_12_3_0
Adding jinstall...
Verified manifest signed by PackageProduction_12_3_0
```

```
WARNING:    This package will load JUNOS 12.3R2 software.
WARNING:    It will save JUNOS configuration files, and SSH keys
WARNING:    (if configured), but erase all other files and information
WARNING:    stored on this machine. It will attempt to preserve dumps
WARNING:    and log files, but this can not be guaranteed. This is the
WARNING:    pre-installation stage and all the software is loaded when
WARNING:    you reboot the system.
```



Saving the config files ...

NOTICE: uncommitted changes have been saved in /var/db/config/juniper.conf.pre-install

Installing the bootstrap installer ...

WARNING: A REBOOT IS REQUIRED TO LOAD THIS SOFTWARE CORRECTLY. Use the  
 WARNING: 'request system reboot' command when software installation is  
 WARNING: complete. To abort the installation, do not reboot your system,  
 WARNING: instead use the 'request system software delete jinstall'  
 WARNING: command as soon as this operation completes.

Saving package file in /var/sw/pkg/jinstall-12.3R2-domestic-signed.tgz ...

Saving state for rollback ...

Installing package '/var/tmp/paBWTg' ...

Verified jinstall-12.3R2-domestic.tgz signed by PackageProduction\_12\_3\_0

Adding jinstall...

Verified manifest signed by PackageProduction\_12\_3\_0

WARNING: This package will load JUNOS 12.3R2 software.  
 WARNING: It will save JUNOS configuration files, and SSH keys  
 WARNING: (if configured), but erase all other files and information  
 WARNING: stored on this machine. It will attempt to preserve dumps  
 WARNING: and log files, but this can not be guaranteed. This is the  
 WARNING: pre-installation stage and all the software is loaded when  
 WARNING: you reboot the system.

Saving the config files ...

NOTICE: uncommitted changes have been saved in /var/db/config/juniper.conf.pre-install

Installing the bootstrap installer ...

WARNING: A REBOOT IS REQUIRED TO LOAD THIS SOFTWARE CORRECTLY. Use the  
 WARNING: 'request system reboot' command when software installation is  
 WARNING: complete. To abort the installation, do not reboot your system,  
 WARNING: instead use the 'request system software delete jinstall'  
 WARNING: command as soon as this operation completes.

Saving package file in /var/sw/pkg/jinstall-12.3R2-domestic-signed ...

cp: /var/tmp/paBWTg is a directory (not copied).

Saving state for rollback ...

ISSU: SFC Old Master Upgrade Done

ISSU: IDLE

## request system software in-service-upgrade (QFX5100 Switch)

```
{master}
user@switch> request system software in-service-upgrade /var/tmp/jinstall-qfx-132_x51_vjunos.0-domestic.tgz
ISSU: Validating Image
Prepare for ISSU
spawn the backup VM
ISSU: Preparing Backup RE
Backup upgrade done
ISSU: Backup RE Prepare Done
waiting for backup RE switchover ready
GRES operational
Initiating Chassis In-Service-Upgrade
Chassis ISSU Started
ISSU: Preparing Daemons
ISSU: Daemons Ready for ISSU
ISSU: Starting Upgrade for FRUs
ISSU: FPC Warm Booting
ISSU: FPC Warm Booted
ISSU: Preparing for Switchover
ISSU: Ready for Switchover
Checking In-Service-Upgrade status
  Item           Status           Reason
  FPC 0         Online (ISSU)
send ISSU done to chassisd on backup VM
Chassis ISSU Completed
ISSU: IDLE
mgd_package_opus_issu: Initiate em0 device handoff
```

## request system software in-service-upgrade status

```
{master}
user@host> request system software in-service-upgrade /var/tmp/jinstall-12.3R2-domestic-signed.tgz
[Apr 29 01:31:11]:ISSU: Validating Image
[Apr 29 01:43:13]:ISSU: Validating Image Done
[Apr 29 01:43:13]:ISSU: Preparing Backup RE
[Apr 29 01:43:13]:ISSU: Pushing /var/tmp/jinstall-12.3R2-domestic-signed.tgz to re1:/var/tmp/
jinstall-12.3R2-domestic-signed.tgz
[Apr 29 01:44:48]:ISSU: Pushing package /var/tmp/jinstall-12.3R2-domestic-signed.tgz to re1 done
[Apr 29 01:44:48]:ISSU: Installing package /var/tmp/jinstall-12.3R2-domestic-signed.tgz on re1
```

```

[Apr 29 01:52:35]:ISSU: Installing package /var/tmp/jinstall-12.3R2-domestic-signed.tgz on re1
done
[Apr 29 01:52:35]:ISSU: Rebooting Backup RE
[Apr 29 01:52:36]:ISSU: Backup RE Prepare Done
[Apr 29 01:52:36]:ISSU: Waiting for Backup RE reboot
[Apr 29 01:56:45]:ISSU: Backup RE reboot done. Backup RE is up
[Apr 29 01:56:45]:ISSU: Waiting for Backup RE state synchronization
[Apr 29 01:57:10]:ISSU: Backup RE state synchronization done
[Apr 29 01:57:10]:ISSU: GRES operational
[Apr 29 01:58:16]:ISSU: Preparing Daemons
[Apr 29 01:58:40]:ISSU: Daemons Ready for ISSU
[Apr 29 01:58:46]:ISSU: Offline Incompatible FRUs
[Apr 29 01:58:51]:ISSU: Starting Upgrade for FRUs
[Apr 29 02:03:32]:ISSU: Preparing for Switchover
[Apr 29 02:03:57]:ISSU: Ready for Switchover
[Apr 29 02:03:59]:ISSU: RE switchover Done
[Apr 29 02:03:59]:ISSU: Upgrading Old Master RE
[Apr 29 02:12:51]:ISSU: Old Master Upgrade Done
[Apr 29 02:12:51]:ISSU: IDLE

```

## request system software in-service-upgrade enhanced-mode

```

{master}
user@host> request system software in-service-upgrade /var/tmp/junos-install-mx-x86-32-20.1.tgz reboot
enhanced-mode
Chassis ISSU enhanced-mode
ISSU: set chassis enhanced-mode
Chassis ISSU Check Done
ISSU: Validating Image
..
mgd: commit complete
Validation succeeded
  Validating Image Done
  Preparing Backup RE
  Pushing /var/tmp/junos-install-mx-x86-32-20.1.tgz to re1:/var/tmp/junos-install-mx-
x86-32-20.1.tgz
  Pushing package /var/tmp/junos-install-mx-x86-32-20.1.tgz to re1 done
  Installing package /var/tmp/junos-install-mx-x86-32-20.1.tgz on re1
...
Verified sflow-mx signed by PackageDevelopmentEc_2019 method ECDSA256+SHA256
NOTICE: 'pending' set will be activated at next reboot...

```

```
ISSU: Installing package /var/tmp/junos-install-mx-x86-32-20.1.tgz on re1 done
ISSU: Rebooting Backup RE
```

```
Rebooting re1
```

```
Backup RE Prepare Done
```

```
Waiting for Backup RE reboot
```

```
Backup RE reboot done. Backup RE is up
```

```
Waiting for Backup RE state synchronization
```

```
Backup RE state synchronization done
```

```
GRES operational
```

```
"Initiating Chassis In-Service-Upgrade"
```

```
Chassis ISSU Started
```

```
ISSU: Preparing Daemons
```

```
ISSU: Daemons Ready for ISSU
```

```
ISSU: Offline Incompatible FRUs
```

```
ISSU: Starting Upgrade for FRUs
```

```
...
```

```
ISSU: Preparing for Switchover
```

```
ISSU: Ready for Switchover
```

```
Checking In-Service-Upgrade status
```

Item	Status	Reason
FPC 1	Online (ISSU)	
FPC 2	Offline	Configured power off

```
Resolving mastership...
```

```
Complete. The other routing engine becomes the master.
```

## Release Information

Command introduced in Junos OS Release 9.0.

status option introduced in Junos OS Release 19.4R1 for MX240, MX480, MX960, MX2010, MX2020, PTX3000, and PTX5000 routers.

handle-incompatible-config option introduced in Junos OS Release 22.1R1 for MX960, MX10003, MX10008, MX10016, MX2010, and MX2020 routers.

## RELATED DOCUMENTATION

*request system software abort*

[show chassis in-service-upgrade](#) | 1389

---

Getting Started with Unified In-Service Software Upgrade

---

Performing an In-Service Software Upgrade (ISSU) with Non-Stop Routing

---

Example: Performing a Unified ISSU

## request system software in-service-upgrade (MX Series 5G Universal Routing Platforms and EX9200 Switches)

### IN THIS SECTION

- [Syntax | 1291](#)
- [Description | 1291](#)
- [Options | 1292](#)
- [Additional Information | 1293](#)
- [Required Privilege Level | 1293](#)
- [Output Fields | 1293](#)
- [Sample Output | 1293](#)
- [Release Information | 1314](#)

### Syntax

```
request system software in-service-upgrade package-name  
<no-copy>  
<no-old-master-upgrade>  
<reboot>  
<unlink>
```

### Description

Perform a unified in-service software upgrade (unified ISSU). Unified ISSU enables you to upgrade from one Junos OS release to another with no disruption on the control plane and with minimal disruption of traffic. Unified ISSU is supported only by dual Routing Engine platforms. In addition, graceful Routing Engine switchover (GRES) and nonstop active routing (NSR) must be enabled.

## Options

<b><i>package-name</i></b>	<p>Location from which the software package or bundle is to be installed. For example:</p> <ul style="list-style-type: none"> <li>• <b><i>/var/tmp/package-name</i></b>— For a software package or bundle that is being installed from a local directory on the router.</li> <li>• <b><i>protocol://hostname/pathname/package-name</i></b>—For a software package or bundle that is to be downloaded and installed from a remote location. Replace <b><i>protocol</i></b> with one of the following: <ul style="list-style-type: none"> <li>• <b>ftp</b>—File Transfer Protocol</li> <li>• <b>http</b>—Hypertext Transfer Protocol</li> <li>• <b>scp</b>—Secure copy (available only for Canada and U.S. version)</li> </ul> </li> </ul>
<b>no-copy</b>	<p>(Optional) When the <b>no-copy</b> option is included, copies of package files are not saved on the Packet Forwarding Engine.</p> <p>The <b>no-copy</b> option is not available for an MX Series Virtual Chassis or an EX9200 Virtual Chassis.</p>
<b>no-old-master-upgrade</b>	<p>(Optional) When the <b>no-old-master-upgrade</b> option is included, after the backup Routing Engine is rebooted with the new software package and a switchover occurs to make it the new primary Routing Engine, the former primary (new backup) Routing Engine is not upgraded to the new software. In this case, you must manually upgrade the former primary (new backup) Routing Engine. If you do not include the <b>no-old-master-upgrade</b> option, the system automatically upgrades the former primary Routing Engine.</p> <p>The <b>no-old-master-upgrade</b> option is not available for an MX Series Virtual Chassis or an EX9200 Virtual Chassis.</p>
<b>reboot</b>	<p>(Optional) When the <b>reboot</b> option is included, the former primary (new backup) Routing Engine is automatically rebooted after being upgraded to the new software. When the <b>reboot</b> option is not included, you must manually reboot the former primary (new backup) Routing Engine using the <code>request system reboot</code> command.</p> <p>The <b>reboot</b> option is accepted but ignored for an MX Series Virtual Chassis or an EX9200 Virtual Chassis. A unified ISSU in an MX Series Virtual Chassis or EX9200 Virtual Chassis always reboots all Routing Engines in the member routers or switches.</p>
<b>unlink</b>	<p>(Optional) When the <b>unlink</b> option is included, the package is removed from <b>/var/home</b> whether the installation is successful or unsuccessful.</p>

The unlink option is not available for an MX Series Virtual Chassis or an EX9200 Virtual Chassis.

## Additional Information

The following conditions apply to unified ISSUs:

- Unified ISSUs are supported on MX Series 5G Universal Routing Platforms and EX9200 switches.
- Unsupported PICs (on EX9200, PICs are known as “line cards”) are restarted during a unified ISSU. For information about supported PICs, see the [Junos OS High Availability User Guide](#). For information about supported EX9200 line cards, see ["Unified ISSU System Requirements" on page 504](#).
- Unsupported protocols will experience packet loss during a unified ISSU. For information about supported protocols, see the [Junos OS High Availability User Guide](#) or, for EX9200, see ["Unified ISSU System Requirements" on page 504](#).
- During a unified ISSU, you cannot bring any PICs online or offline.

For more information, see the [Junos OS High Availability User Guide](#).

## Required Privilege Level

view

## Output Fields

When you enter this command, you are provided feedback about the status of your request.

## Sample Output

### request system software in-service-upgrade reboot

```
{master}
user@host> request system software in-service-upgrade /var/tmp/jinstall-11.2B2.1-domestic-
signed.tgz reboot
Chassis ISSU Check Done
ISSU: Validating Image
Checking compatibility with configuration
Initializing...
Using jbase-11.2B1.5
```

```

Verified manifest signed by PackageProduction_11_2_0
Verified jbase-11.2B1.5 signed by PackageProduction_11_2_0
Using /var/tmp/jinstall-11.2B2.1-domestic-signed.tgz
Verified jinstall-11.2B2.1-domestic.tgz signed by PackageProduction_11_2_0
Using jinstall-11.2B2.1-domestic.tgz
Using jbundle-11.2B2.1-domestic.tgz
Checking jbundle requirements on /
Using jbase-11.2B2.1.tgz
Verified manifest signed by PackageProduction_11_2_0
Verified jbase-11.2B2.1 signed by PackageProduction_11_2_0
Using /var/validate/chroot/tmp/jbundle/jboot-11.2B2.1.tgz
Using jcrypto-11.2B2.1.tgz
Verified manifest signed by PackageProduction_11_2_0
Verified jcrypto-11.2B2.1 signed by PackageProduction_11_2_0
Using jdocs-11.2B2.1.tgz
Verified manifest signed by PackageProduction_11_2_0
Verified jdocs-11.2B2.1 signed by PackageProduction_11_2_0
Using jkernel-11.2B2.1.tgz
Verified manifest signed by PackageProduction_11_2_0
Verified jkernel-11.2B2.1 signed by PackageProduction_11_2_0
Using jpfe-11.2B2.1.tgz
Using jroute-11.2B2.1.tgz
Verified manifest signed by PackageProduction_11_2_0
Verified jroute-11.2B2.1 signed by PackageProduction_11_2_0
Using jruntime-11.2B2.1.tgz
Verified manifest signed by PackageProduction_11_2_0
Verified jruntime-11.2B2.1 signed by PackageProduction_11_2_0
Using jservices-11.2B2.1.tgz
Auto-deleting old jservices-voice ...
Removing /opt/sdk/service-packages/jservices-voice ...
Removing jservices-voice-bsg-11.2B1.5.tgz from /var/sw/pkg ...
Notifying mspd ...
Installing new jservices-voice ...
Verified jservices-voice-bsg-11.2B2.1.tgz signed by PackageProduction_11_2_0
Creating /var/sw/pkg ...
Creating /opt/sdk/service-packages/jservices-voice ...
Storing jservices-voice-bsg-11.2B2.1.tgz in /var/sw/pkg ...
Link: /opt/sdk/service-packages/jservices-voice/jservices-voice-bsg -> /var/sw/pkg/jservices-voice-bsg-11.2B2.1.tgz...
Auto-deleting old jservices-bgf ...
Removing /opt/sdk/service-packages/jservices-bgf ...
Removing jservices-bgf-pic-11.2B1.5.tgz from /var/sw/pkg ...
Notifying mspd ...

```



```

Installing new jservices-bgf ...
Verified jservices-bgf-pic-11.2B2.1.tgz signed by PackageProduction_11_2_0
Creating /opt/sdk/service-packages/jservices-bgf ...
Storing jservices-bgf-pic-11.2B2.1.tgz in /var/sw/pkg ...
Link: /opt/sdk/service-packages/jservices-bgf/jservices-bgf-pic -> /var/sw/pkg/jservices-bgf-
pic-11.2B2.1.tgz...
Auto-deleting old jservices-aacl ...
Removing /opt/sdk/service-packages/jservices-aacl ...
Removing jservices-aacl-pic-11.2B1.5.tgz from /var/sw/pkg ...
Notifying mspd ...
Installing new jservices-aacl ...
Verified jservices-aacl-pic-11.2B2.1.tgz signed by PackageProduction_11_2_0
Creating /opt/sdk/service-packages/jservices-aacl ...
Storing jservices-aacl-pic-11.2B2.1.tgz in /var/sw/pkg ...
Link: /opt/sdk/service-packages/jservices-aacl/jservices-aacl-pic -> /var/sw/pkg/jservices-aacl-
pic-11.2B2.1.tgz...
Auto-deleting old jservices-llpdf ...
Removing /opt/sdk/service-packages/jservices-llpdf ...
Removing jservices-llpdf-pic-11.2B1.5.tgz from /var/sw/pkg ...
Notifying mspd ...
Installing new jservices-llpdf ...
Verified jservices-llpdf-pic-11.2B2.1.tgz signed by PackageProduction_11_2_0
Creating /opt/sdk/service-packages/jservices-llpdf ...
Storing jservices-llpdf-pic-11.2B2.1.tgz in /var/sw/pkg ...
Link: /opt/sdk/service-packages/jservices-llpdf/jservices-llpdf-pic -> /var/sw/pkg/jservices-
llpdf-pic-11.2B2.1.tgz...
Auto-deleting old jservices-ptsp ...
Removing /opt/sdk/service-packages/jservices-ptsp ...
Removing jservices-ptsp-pic-11.2B1.5.tgz from /var/sw/pkg ...
Notifying mspd ...
Installing new jservices-ptsp ...
Verified jservices-ptsp-pic-11.2B2.1.tgz signed by PackageProduction_11_2_0
Creating /opt/sdk/service-packages/jservices-ptsp ...
Storing jservices-ptsp-pic-11.2B2.1.tgz in /var/sw/pkg ...
Link: /opt/sdk/service-packages/jservices-ptsp/jservices-ptsp-pic -> /var/sw/pkg/jservices-ptsp-
pic-11.2B2.1.tgz...
Auto-deleting old jservices-sfw ...
Removing /opt/sdk/service-packages/jservices-sfw ...
Removing jservices-sfw-pic-11.2B1.5.tgz from /var/sw/pkg ...
Notifying mspd ...
Installing new jservices-sfw ...
Verified jservices-sfw-pic-11.2B2.1.tgz signed by PackageProduction_11_2_0
Creating /opt/sdk/service-packages/jservices-sfw ...

```

```

Storing jservices-sfw-pic-11.2B2.1.tgz in /var/sw/pkg ...
Link: /opt/sdk/service-packages/jservices-sfw/jservices-sfw-pic -> /var/sw/pkg/jservices-sfw-
pic-11.2B2.1.tgz...
Auto-deleting old jservices-nat ...
Removing /opt/sdk/service-packages/jservices-nat ...
Removing jservices-nat-pic-11.2B1.5.tgz from /var/sw/pkg ...
Notifying mspd ...
Installing new jservices-nat ...
Verified jservices-nat-pic-11.2B2.1.tgz signed by PackageProduction_11_2_0
Creating /opt/sdk/service-packages/jservices-nat ...
Storing jservices-nat-pic-11.2B2.1.tgz in /var/sw/pkg ...
Link: /opt/sdk/service-packages/jservices-nat/jservices-nat-pic -> /var/sw/pkg/jservices-nat-
pic-11.2B2.1.tgz...
Auto-deleting old jservices-alg ...
Removing /opt/sdk/service-packages/jservices-alg ...
Removing jservices-alg-pic-11.2B1.5.tgz from /var/sw/pkg ...
Notifying mspd ...
Installing new jservices-alg ...
Verified jservices-alg-pic-11.2B2.1.tgz signed by PackageProduction_11_2_0
Creating /opt/sdk/service-packages/jservices-alg ...
Storing jservices-alg-pic-11.2B2.1.tgz in /var/sw/pkg ...
Link: /opt/sdk/service-packages/jservices-alg/jservices-alg-pic -> /var/sw/pkg/jservices-alg-
pic-11.2B2.1.tgz...
Auto-deleting old jservices-cpcd ...
Removing /opt/sdk/service-packages/jservices-cpcd ...
Removing jservices-cpcd-pic-11.2B1.5.tgz from /var/sw/pkg ...
Notifying mspd ...
Installing new jservices-cpcd ...
Verified jservices-cpcd-pic-11.2B2.1.tgz signed by PackageProduction_11_2_0
Creating /opt/sdk/service-packages/jservices-cpcd ...
Storing jservices-cpcd-pic-11.2B2.1.tgz in /var/sw/pkg ...
Link: /opt/sdk/service-packages/jservices-cpcd/jservices-cpcd-pic -> /var/sw/pkg/jservices-cpcd-
pic-11.2B2.1.tgz...
Auto-deleting old jservices-rpm ...
Removing /opt/sdk/service-packages/jservices-rpm ...
Removing jservices-rpm-pic-11.2B1.5.tgz from /var/sw/pkg ...
Notifying mspd ...
Installing new jservices-rpm ...
Verified jservices-rpm-pic-11.2B2.1.tgz signed by PackageProduction_11_2_0
Creating /opt/sdk/service-packages/jservices-rpm ...
Storing jservices-rpm-pic-11.2B2.1.tgz in /var/sw/pkg ...
Link: /opt/sdk/service-packages/jservices-rpm/jservices-rpm-pic -> /var/sw/pkg/jservices-rpm-
pic-11.2B2.1.tgz...

```

```

Auto-deleting old jservices-hcm ...
Removing /opt/sdk/service-packages/jservices-hcm ...
Removing jservices-hcm-pic-11.2B1.5.tgz from /var/sw/pkg ...
Notifying mspd ...
Installing new jservices-hcm ...
Verified jservices-hcm-pic-11.2B2.1.tgz signed by PackageProduction_11_2_0
Creating /opt/sdk/service-packages/jservices-hcm ...
Storing jservices-hcm-pic-11.2B2.1.tgz in /var/sw/pkg ...
Link: /opt/sdk/service-packages/jservices-hcm/jservices-hcm-pic -> /var/sw/pkg/jservices-hcm-
pic-11.2B2.1.tgz...
Auto-deleting old jservices-appid ...
Removing /opt/sdk/service-packages/jservices-appid ...
Removing jservices-appid-pic-11.2B1.5.tgz from /var/sw/pkg ...
Notifying mspd ...
Installing new jservices-appid ...
Verified jservices-appid-pic-11.2B2.1.tgz signed by PackageProduction_11_2_0
Creating /opt/sdk/service-packages/jservices-appid ...
Storing jservices-appid-pic-11.2B2.1.tgz in /var/sw/pkg ...
Link: /opt/sdk/service-packages/jservices-appid/jservices-appid-pic -> /var/sw/pkg/jservices-
appid-pic-11.2B2.1.tgz...
Auto-deleting old jservices-idp ...
Removing /opt/sdk/service-packages/jservices-idp ...
Removing jservices-idp-pic-11.2B1.5.tgz from /var/sw/pkg ...
Notifying mspd ...
Installing new jservices-idp ...
Verified jservices-idp-pic-11.2B2.1.tgz signed by PackageProduction_11_2_0
Creating /opt/sdk/service-packages/jservices-idp ...
Storing jservices-idp-pic-11.2B2.1.tgz in /var/sw/pkg ...
Link: /opt/sdk/service-packages/jservices-idp/jservices-idp-pic -> /var/sw/pkg/jservices-idp-
pic-11.2B2.1.tgz...
Using jservices-crypto-11.2B2.1.tgz
Auto-deleting old jservices-crypto-base ...
Removing /opt/sdk/service-packages/jservices-crypto-base ...
Removing jservices-crypto-base-pic-11.2B1.5.tgz from /var/sw/pkg ...
Notifying mspd ...
Installing new jservices-crypto-base ...
Verified jservices-crypto-base-pic-11.2B2.1.tgz signed by PackageProduction_11_2_0
Creating /opt/sdk/service-packages/jservices-crypto-base ...
Storing jservices-crypto-base-pic-11.2B2.1.tgz in /var/sw/pkg ...
Link: /opt/sdk/service-packages/jservices-crypto-base/jservices-crypto-base-pic -> /var/sw/pkg/
jservices-crypto-base-pic-11.2B2.1.tgz...
Auto-deleting old jservices-ssl ...
Removing /opt/sdk/service-packages/jservices-ssl ...

```

```
Removing jservices-ssl-pic-11.2B1.5.tgz from /var/sw/pkg ...
Notifying mspd ...
Installing new jservices-ssl ...
Verified jservices-ssl-pic-11.2B2.1.tgz signed by PackageProduction_11_2_0
Creating /opt/sdk/service-packages/jservices-ssl ...
Storing jservices-ssl-pic-11.2B2.1.tgz in /var/sw/pkg ...
Link: /opt/sdk/service-packages/jservices-ssl/jservices-ssl-pic -> /var/sw/pkg/jservices-ssl-
pic-11.2B2.1.tgz...
Hardware Database regeneration succeeded
Validating against /config/juniper.conf.gz
mgd: commit complete
Validation succeeded
ISSU: Preparing Backup RE
Pushing bundle to re1
NOTICE: Validating configuration against jinstall-11.2B2.1-domestic-signed.tgz.
NOTICE: Use the 'no-validate' option to skip this if desired.
Checking compatibility with configuration
Initializing...
Using jbase-11.2B1.5
Verified manifest signed by PackageProduction_11_2_0
Verified jbase-11.2B1.5 signed by PackageProduction_11_2_0
Using /var/tmp/jinstall-11.2B2.1-domestic-signed.tgz
Verified jinstall-11.2B2.1-domestic.tgz signed by PackageProduction_11_2_0
Using jinstall-11.2B2.1-domestic.tgz
Using jbundle-11.2B2.1-domestic.tgz
Checking jbundle requirements on /
Using jbase-11.2B2.1.tgz
Verified manifest signed by PackageProduction_11_2_0
Verified jbase-11.2B2.1 signed by PackageProduction_11_2_0
Using /var/validate/chroot/tmp/jbundle/jboot-11.2B2.1.tgz
Using jcrypto-11.2B2.1.tgz
Verified manifest signed by PackageProduction_11_2_0
Verified jcrypto-11.2B2.1 signed by PackageProduction_11_2_0
Using jdocs-11.2B2.1.tgz
Verified manifest signed by PackageProduction_11_2_0
Verified jdocs-11.2B2.1 signed by PackageProduction_11_2_0
Using jkernel-11.2B2.1.tgz
Verified manifest signed by PackageProduction_11_2_0
Verified jkernel-11.2B2.1 signed by PackageProduction_11_2_0
Using jpfe-11.2B2.1.tgz
Using jroute-11.2B2.1.tgz
Verified manifest signed by PackageProduction_11_2_0
Verified jroute-11.2B2.1 signed by PackageProduction_11_2_0
```

```

Using jruntime-11.2B2.1.tgz
Verified manifest signed by PackageProduction_11_2_0
Verified jruntime-11.2B2.1 signed by PackageProduction_11_2_0
Using jservices-11.2B2.1.tgz
Auto-deleting old jservices-voice ...
Removing /opt/sdk/service-packages/jservices-voice ...
Removing jservices-voice-bsg-11.2B1.5.tgz from /var/sw/pkg ...
Notifying mspd ...
Installing new jservices-voice ...
Verified jservices-voice-bsg-11.2B2.1.tgz signed by PackageProduction_11_2_0
Creating /var/sw/pkg ...
Creating /opt/sdk/service-packages/jservices-voice ...
Storing jservices-voice-bsg-11.2B2.1.tgz in /var/sw/pkg ...
Link: /opt/sdk/service-packages/jservices-voice/jservices-voice-bsg -> /var/sw/pkg/jservices-voice-bsg-11.2B2.1.tgz...
Auto-deleting old jservices-bgf ...
Removing /opt/sdk/service-packages/jservices-bgf ...
Removing jservices-bgf-pic-11.2B1.5.tgz from /var/sw/pkg ...
Notifying mspd ...
Installing new jservices-bgf ...
Verified jservices-bgf-pic-11.2B2.1.tgz signed by PackageProduction_11_2_0
Creating /opt/sdk/service-packages/jservices-bgf ...
Storing jservices-bgf-pic-11.2B2.1.tgz in /var/sw/pkg ...
Link: /opt/sdk/service-packages/jservices-bgf/jservices-bgf-pic -> /var/sw/pkg/jservices-bgf-pic-11.2B2.1.tgz...
Auto-deleting old jservices-aacl ...
Removing /opt/sdk/service-packages/jservices-aacl ...
Removing jservices-aacl-pic-11.2B1.5.tgz from /var/sw/pkg ...
Notifying mspd ...
Installing new jservices-aacl ...
Verified jservices-aacl-pic-11.2B2.1.tgz signed by PackageProduction_11_2_0
Creating /opt/sdk/service-packages/jservices-aacl ...
Storing jservices-aacl-pic-11.2B2.1.tgz in /var/sw/pkg ...
Link: /opt/sdk/service-packages/jservices-aacl/jservices-aacl-pic -> /var/sw/pkg/jservices-aacl-pic-11.2B2.1.tgz...
Auto-deleting old jservices-llpdf ...
Removing /opt/sdk/service-packages/jservices-llpdf ...
Removing jservices-llpdf-pic-11.2B1.5.tgz from /var/sw/pkg ...
Notifying mspd ...
Installing new jservices-llpdf ...
Verified jservices-llpdf-pic-11.2B2.1.tgz signed by PackageProduction_11_2_0
Creating /opt/sdk/service-packages/jservices-llpdf ...
Storing jservices-llpdf-pic-11.2B2.1.tgz in /var/sw/pkg ...

```

```

Link: /opt/sdk/service-packages/jservices-llpdf/jservices-llpdf-pic -> /var/sw/pkg/jservices-
llpdf-pic-11.2B2.1.tgz...
Auto-deleting old jservices-ptsp ...
Removing /opt/sdk/service-packages/jservices-ptsp ...
Removing jservices-ptsp-pic-11.2B1.5.tgz from /var/sw/pkg ...
Notifying mspd ...
Installing new jservices-ptsp ...
Verified jservices-ptsp-pic-11.2B2.1.tgz signed by PackageProduction_11_2_0
Creating /opt/sdk/service-packages/jservices-ptsp ...
Storing jservices-ptsp-pic-11.2B2.1.tgz in /var/sw/pkg ...
Link: /opt/sdk/service-packages/jservices-ptsp/jservices-ptsp-pic -> /var/sw/pkg/jservices-ptsp-
pic-11.2B2.1.tgz...
Auto-deleting old jservices-sfw ...
Removing /opt/sdk/service-packages/jservices-sfw ...
Removing jservices-sfw-pic-11.2B1.5.tgz from /var/sw/pkg ...
Notifying mspd ...
Installing new jservices-sfw ...
Verified jservices-sfw-pic-11.2B2.1.tgz signed by PackageProduction_11_2_0
Creating /opt/sdk/service-packages/jservices-sfw ...
Storing jservices-sfw-pic-11.2B2.1.tgz in /var/sw/pkg ...
Link: /opt/sdk/service-packages/jservices-sfw/jservices-sfw-pic -> /var/sw/pkg/jservices-sfw-
pic-11.2B2.1.tgz...
Auto-deleting old jservices-nat ...
Removing /opt/sdk/service-packages/jservices-nat ...
Removing jservices-nat-pic-11.2B1.5.tgz from /var/sw/pkg ...
Notifying mspd ...
Installing new jservices-nat ...
Verified jservices-nat-pic-11.2B2.1.tgz signed by PackageProduction_11_2_0
Creating /opt/sdk/service-packages/jservices-nat ...
Storing jservices-nat-pic-11.2B2.1.tgz in /var/sw/pkg ...
Link: /opt/sdk/service-packages/jservices-nat/jservices-nat-pic -> /var/sw/pkg/jservices-nat-
pic-11.2B2.1.tgz...
Auto-deleting old jservices-alg ...
Removing /opt/sdk/service-packages/jservices-alg ...
Removing jservices-alg-pic-11.2B1.5.tgz from /var/sw/pkg ...
Notifying mspd ...
Installing new jservices-alg ...
Verified jservices-alg-pic-11.2B2.1.tgz signed by PackageProduction_11_2_0
Creating /opt/sdk/service-packages/jservices-alg ...
Storing jservices-alg-pic-11.2B2.1.tgz in /var/sw/pkg ...
Link: /opt/sdk/service-packages/jservices-alg/jservices-alg-pic -> /var/sw/pkg/jservices-alg-
pic-11.2B2.1.tgz...
Auto-deleting old jservices-cpcd ...

```

```

Removing /opt/sdk/service-packages/jservices-cpcd ...
Removing jservices-cpcd-pic-11.2B1.5.tgz from /var/sw/pkg ...
Notifying mspd ...
Installing new jservices-cpcd ...
Verified jservices-cpcd-pic-11.2B2.1.tgz signed by PackageProduction_11_2_0
Creating /opt/sdk/service-packages/jservices-cpcd ...
Storing jservices-cpcd-pic-11.2B2.1.tgz in /var/sw/pkg ...
Link: /opt/sdk/service-packages/jservices-cpcd/jservices-cpcd-pic -> /var/sw/pkg/jservices-cpcd-
pic-11.2B2.1.tgz...
Auto-deleting old jservices-rpm ...
Removing /opt/sdk/service-packages/jservices-rpm ...
Removing jservices-rpm-pic-11.2B1.5.tgz from /var/sw/pkg ...
Notifying mspd ...
Installing new jservices-rpm ...
Verified jservices-rpm-pic-11.2B2.1.tgz signed by PackageProduction_11_2_0
Creating /opt/sdk/service-packages/jservices-rpm ...
Storing jservices-rpm-pic-11.2B2.1.tgz in /var/sw/pkg ...
Link: /opt/sdk/service-packages/jservices-rpm/jservices-rpm-pic -> /var/sw/pkg/jservices-rpm-
pic-11.2B2.1.tgz...
Auto-deleting old jservices-hcm ...
Removing /opt/sdk/service-packages/jservices-hcm ...
Removing jservices-hcm-pic-11.2B1.5.tgz from /var/sw/pkg ...
Notifying mspd ...
Installing new jservices-hcm ...
Verified jservices-hcm-pic-11.2B2.1.tgz signed by PackageProduction_11_2_0
Creating /opt/sdk/service-packages/jservices-hcm ...
Storing jservices-hcm-pic-11.2B2.1.tgz in /var/sw/pkg ...
Link: /opt/sdk/service-packages/jservices-hcm/jservices-hcm-pic -> /var/sw/pkg/jservices-hcm-
pic-11.2B2.1.tgz...
Auto-deleting old jservices-appid ...
Removing /opt/sdk/service-packages/jservices-appid ...
Removing jservices-appid-pic-11.2B1.5.tgz from /var/sw/pkg ...
Notifying mspd ...
Installing new jservices-appid ...
Verified jservices-appid-pic-11.2B2.1.tgz signed by PackageProduction_11_2_0
Creating /opt/sdk/service-packages/jservices-appid ...
Storing jservices-appid-pic-11.2B2.1.tgz in /var/sw/pkg ...
Link: /opt/sdk/service-packages/jservices-appid/jservices-appid-pic -> /var/sw/pkg/jservices-
appid-pic-11.2B2.1.tgz...
Auto-deleting old jservices-idp ...
Removing /opt/sdk/service-packages/jservices-idp ...
Removing jservices-idp-pic-11.2B1.5.tgz from /var/sw/pkg ...
Notifying mspd ...

```

```

Installing new jservices-idp ...
Verified jservices-idp-pic-11.2B2.1.tgz signed by PackageProduction_11_2_0
Creating /opt/sdk/service-packages/jservices-idp ...
Storing jservices-idp-pic-11.2B2.1.tgz in /var/sw/pkg ...
Link: /opt/sdk/service-packages/jservices-idp/jservices-idp-pic -> /var/sw/pkg/jservices-idp-
pic-11.2B2.1.tgz...
Using jservices-crypto-11.2B2.1.tgz
Auto-deleting old jservices-crypto-base ...
Removing /opt/sdk/service-packages/jservices-crypto-base ...
Removing jservices-crypto-base-pic-11.2B1.5.tgz from /var/sw/pkg ...
Notifying mspd ...
Installing new jservices-crypto-base ...
Verified jservices-crypto-base-pic-11.2B2.1.tgz signed by PackageProduction_11_2_0
Creating /opt/sdk/service-packages/jservices-crypto-base ...
Storing jservices-crypto-base-pic-11.2B2.1.tgz in /var/sw/pkg ...
Link: /opt/sdk/service-packages/jservices-crypto-base/jservices-crypto-base-pic -> /var/sw/pkg/
jservices-crypto-base-pic-11.2B2.1.tgz...
Auto-deleting old jservices-ssl ...
Removing /opt/sdk/service-packages/jservices-ssl ...
Removing jservices-ssl-pic-11.2B1.5.tgz from /var/sw/pkg ...
Notifying mspd ...
Installing new jservices-ssl ...
Verified jservices-ssl-pic-11.2B2.1.tgz signed by PackageProduction_11_2_0
Creating /opt/sdk/service-packages/jservices-ssl ...
Storing jservices-ssl-pic-11.2B2.1.tgz in /var/sw/pkg ...
Link: /opt/sdk/service-packages/jservices-ssl/jservices-ssl-pic -> /var/sw/pkg/jservices-ssl-
pic-11.2B2.1.tgz...
Hardware Database regeneration succeeded
Validating against /config/juniper.conf.gz
mgd: commit complete
Validation succeeded
Installing package '/var/tmp/jinstall-11.2B2.1-domestic-signed.tgz' ...
Verified jinstall-11.2B2.1-domestic.tgz signed by PackageProduction_11_2_0
Adding jinstall...
Verified manifest signed by PackageProduction_11_2_0

WARNING:    This package will load JUNOS 11.2B2.1 software.
WARNING:    It will save JUNOS configuration files, and SSH keys
WARNING:    (if configured), but erase all other files and information
WARNING:    stored on this machine. It will attempt to preserve dumps
WARNING:    and log files, but this can not be guaranteed. This is the
WARNING:    pre-installation stage and all the software is loaded when
WARNING:    you reboot the system.

```



```

Saving the config files ...
NOTICE: uncommitted changes have been saved in /var/db/config/juniper.conf.pre-install
Installing the bootstrap installer ...

WARNING:      A REBOOT IS REQUIRED TO LOAD THIS SOFTWARE CORRECTLY. Use the
WARNING:      'request system reboot' command when software installation is
WARNING:      complete. To abort the installation, do not reboot your system,
WARNING:      instead use the 'request system software delete jinstall'
WARNING:      command as soon as this operation completes.

Saving package file in /var/sw/pkg/jinstall-11.2B2.1-domestic-signed.tgz ...
Saving state for rollback ...
Backup upgrade done
Rebooting Backup RE

Rebooting re1
ISSU: Backup RE Prepare Done
Waiting for Backup RE reboot
GRES operational
Initiating Chassis In-Service-Upgrade
Chassis ISSU Started
ISSU: Preparing Daemons
ISSU: Daemons Ready for ISSU
ISSU: Starting Upgrade for FRUs
ISSU: Preparing for Switchover
ISSU: Ready for Switchover
Checking In-Service-Upgrade status
  Item           Status           Reason
  FPC 1          Online (ISSU)
  FPC 4          Online (ISSU)
  FPC 8          Online (ISSU)
  FPC 10         Online (ISSU)
Resolving mastership...
Complete. The other routing engine becomes the master.
ISSU: RE switchover Done
ISSU: Upgrading Old Master RE
NOTICE: Validating configuration against jinstall-11.2B2.1-domestic-signed.tgz.
NOTICE: Use the 'no-validate' option to skip this if desired.
Checking compatibility with configuration
Initializing...
Using jbase-11.2B1.5
Verified manifest signed by PackageProduction_11_2_0

```

```

Verified jbase-11.2B1.5 signed by PackageProduction_11_2_0
Using /var/tmp/jinstall-11.2B2.1-domestic-signed.tgz
Verified jinstall-11.2B2.1-domestic.tgz signed by PackageProduction_11_2_0
Using jinstall-11.2B2.1-domestic.tgz
Using jbundle-11.2B2.1-domestic.tgz
Checking jbundle requirements on /
Using jbase-11.2B2.1.tgz
Verified manifest signed by PackageProduction_11_2_0
Verified jbase-11.2B2.1 signed by PackageProduction_11_2_0
Using /var/validate/chroot/tmp/jbundle/jboot-11.2B2.1.tgz
Using jcrypto-11.2B2.1.tgz
Verified manifest signed by PackageProduction_11_2_0
Verified jcrypto-11.2B2.1 signed by PackageProduction_11_2_0
Using jdocs-11.2B2.1.tgz
Verified manifest signed by PackageProduction_11_2_0
Verified jdocs-11.2B2.1 signed by PackageProduction_11_2_0
Using jkernel-11.2B2.1.tgz
Verified manifest signed by PackageProduction_11_2_0
Verified jkernel-11.2B2.1 signed by PackageProduction_11_2_0
Using jpfe-11.2B2.1.tgz
Using jroute-11.2B2.1.tgz
Verified manifest signed by PackageProduction_11_2_0
Verified jroute-11.2B2.1 signed by PackageProduction_11_2_0
Using jruntime-11.2B2.1.tgz
Verified manifest signed by PackageProduction_11_2_0
Verified jruntime-11.2B2.1 signed by PackageProduction_11_2_0
Using jservices-11.2B2.1.tgz
Auto-deleting old jservices-voice ...
Removing /opt/sdk/service-packages/jservices-voice ...
Removing jservices-voice-bsg-11.2B1.5.tgz from /var/sw/pkg ...
Notifying mspd ...
Installing new jservices-voice ...
Verified jservices-voice-bsg-11.2B2.1.tgz signed by PackageProduction_11_2_0
Creating /var/sw/pkg ...
Creating /opt/sdk/service-packages/jservices-voice ...
Storing jservices-voice-bsg-11.2B2.1.tgz in /var/sw/pkg ...
Link: /opt/sdk/service-packages/jservices-voice/jservices-voice-bsg -> /var/sw/pkg/jservices-voice-bsg-11.2B2.1.tgz...
Auto-deleting old jservices-bgf ...
Removing /opt/sdk/service-packages/jservices-bgf ...
Removing jservices-bgf-pic-11.2B1.5.tgz from /var/sw/pkg ...
Notifying mspd ...
Installing new jservices-bgf ...

```

```

Verified jservices-bgf-pic-11.2B2.1.tgz signed by PackageProduction_11_2_0
Creating /opt/sdk/service-packages/jservices-bgf ...
Storing jservices-bgf-pic-11.2B2.1.tgz in /var/sw/pkg ...
Link: /opt/sdk/service-packages/jservices-bgf/jservices-bgf-pic -> /var/sw/pkg/jservices-bgf-
pic-11.2B2.1.tgz...
Auto-deleting old jservices-aacl ...
Removing /opt/sdk/service-packages/jservices-aacl ...
Removing jservices-aacl-pic-11.2B1.5.tgz from /var/sw/pkg ...
Notifying mspd ...
Installing new jservices-aacl ...
Verified jservices-aacl-pic-11.2B2.1.tgz signed by PackageProduction_11_2_0
Creating /opt/sdk/service-packages/jservices-aacl ...
Storing jservices-aacl-pic-11.2B2.1.tgz in /var/sw/pkg ...
Link: /opt/sdk/service-packages/jservices-aacl/jservices-aacl-pic -> /var/sw/pkg/jservices-aacl-
pic-11.2B2.1.tgz...
Auto-deleting old jservices-llpdf ...
Removing /opt/sdk/service-packages/jservices-llpdf ...
Removing jservices-llpdf-pic-11.2B1.5.tgz from /var/sw/pkg ...
Notifying mspd ...
Installing new jservices-llpdf ...
Verified jservices-llpdf-pic-11.2B2.1.tgz signed by PackageProduction_11_2_0
Creating /opt/sdk/service-packages/jservices-llpdf ...
Storing jservices-llpdf-pic-11.2B2.1.tgz in /var/sw/pkg ...
Link: /opt/sdk/service-packages/jservices-llpdf/jservices-llpdf-pic -> /var/sw/pkg/jservices-
llpdf-pic-11.2B2.1.tgz...
Auto-deleting old jservices-ptsp ...
Removing /opt/sdk/service-packages/jservices-ptsp ...
Removing jservices-ptsp-pic-11.2B1.5.tgz from /var/sw/pkg ...
Notifying mspd ...
Installing new jservices-ptsp ...
Verified jservices-ptsp-pic-11.2B2.1.tgz signed by PackageProduction_11_2_0
Creating /opt/sdk/service-packages/jservices-ptsp ...
Storing jservices-ptsp-pic-11.2B2.1.tgz in /var/sw/pkg ...
Link: /opt/sdk/service-packages/jservices-ptsp/jservices-ptsp-pic -> /var/sw/pkg/jservices-ptsp-
pic-11.2B2.1.tgz...
Auto-deleting old jservices-sfw ...
Removing /opt/sdk/service-packages/jservices-sfw ...
Removing jservices-sfw-pic-11.2B1.5.tgz from /var/sw/pkg ...
Notifying mspd ...
Installing new jservices-sfw ...
Verified jservices-sfw-pic-11.2B2.1.tgz signed by PackageProduction_11_2_0
Creating /opt/sdk/service-packages/jservices-sfw ...
Storing jservices-sfw-pic-11.2B2.1.tgz in /var/sw/pkg ...

```

```

Link: /opt/sdk/service-packages/jservices-sfw/jservices-sfw-pic -> /var/sw/pkg/jservices-sfw-
pic-11.2B2.1.tgz...
Auto-deleting old jservices-nat ...
Removing /opt/sdk/service-packages/jservices-nat ...
Removing jservices-nat-pic-11.2B1.5.tgz from /var/sw/pkg ...
Notifying mspd ...
Installing new jservices-nat ...
Verified jservices-nat-pic-11.2B2.1.tgz signed by PackageProduction_11_2_0
Creating /opt/sdk/service-packages/jservices-nat ...
Storing jservices-nat-pic-11.2B2.1.tgz in /var/sw/pkg ...
Link: /opt/sdk/service-packages/jservices-nat/jservices-nat-pic -> /var/sw/pkg/jservices-nat-
pic-11.2B2.1.tgz...
Auto-deleting old jservices-alg ...
Removing /opt/sdk/service-packages/jservices-alg ...
Removing jservices-alg-pic-11.2B1.5.tgz from /var/sw/pkg ...
Notifying mspd ...
Installing new jservices-alg ...
Verified jservices-alg-pic-11.2B2.1.tgz signed by PackageProduction_11_2_0
Creating /opt/sdk/service-packages/jservices-alg ...
Storing jservices-alg-pic-11.2B2.1.tgz in /var/sw/pkg ...
Link: /opt/sdk/service-packages/jservices-alg/jservices-alg-pic -> /var/sw/pkg/jservices-alg-
pic-11.2B2.1.tgz...
Auto-deleting old jservices-cpcd ...
Removing /opt/sdk/service-packages/jservices-cpcd ...
Removing jservices-cpcd-pic-11.2B1.5.tgz from /var/sw/pkg ...
Notifying mspd ...
Installing new jservices-cpcd ...
Verified jservices-cpcd-pic-11.2B2.1.tgz signed by PackageProduction_11_2_0
Creating /opt/sdk/service-packages/jservices-cpcd ...
Storing jservices-cpcd-pic-11.2B2.1.tgz in /var/sw/pkg ...
Link: /opt/sdk/service-packages/jservices-cpcd/jservices-cpcd-pic -> /var/sw/pkg/jservices-cpcd-
pic-11.2B2.1.tgz...
Auto-deleting old jservices-rpm ...
Removing /opt/sdk/service-packages/jservices-rpm ...
Removing jservices-rpm-pic-11.2B1.5.tgz from /var/sw/pkg ...
Notifying mspd ...
Installing new jservices-rpm ...
Verified jservices-rpm-pic-11.2B2.1.tgz signed by PackageProduction_11_2_0
Creating /opt/sdk/service-packages/jservices-rpm ...
Storing jservices-rpm-pic-11.2B2.1.tgz in /var/sw/pkg ...
Link: /opt/sdk/service-packages/jservices-rpm/jservices-rpm-pic -> /var/sw/pkg/jservices-rpm-
pic-11.2B2.1.tgz...
Auto-deleting old jservices-hcm ...

```

```

Removing /opt/sdk/service-packages/jservices-hcm ...
Removing jservices-hcm-pic-11.2B1.5.tgz from /var/sw/pkg ...
Notifying mspd ...
Installing new jservices-hcm ...
Verified jservices-hcm-pic-11.2B2.1.tgz signed by PackageProduction_11_2_0
Creating /opt/sdk/service-packages/jservices-hcm ...
Storing jservices-hcm-pic-11.2B2.1.tgz in /var/sw/pkg ...
Link: /opt/sdk/service-packages/jservices-hcm/jservices-hcm-pic -> /var/sw/pkg/jservices-hcm-
pic-11.2B2.1.tgz...
Auto-deleting old jservices-appid ...
Removing /opt/sdk/service-packages/jservices-appid ...
Removing jservices-appid-pic-11.2B1.5.tgz from /var/sw/pkg ...
Notifying mspd ...
Installing new jservices-appid ...
Verified jservices-appid-pic-11.2B2.1.tgz signed by PackageProduction_11_2_0
Creating /opt/sdk/service-packages/jservices-appid ...
Storing jservices-appid-pic-11.2B2.1.tgz in /var/sw/pkg ...
Link: /opt/sdk/service-packages/jservices-appid/jservices-appid-pic -> /var/sw/pkg/jservices-
appid-pic-11.2B2.1.tgz...
Auto-deleting old jservices-idp ...
Removing /opt/sdk/service-packages/jservices-idp ...
Removing jservices-idp-pic-11.2B1.5.tgz from /var/sw/pkg ...
Notifying mspd ...
Installing new jservices-idp ...
Verified jservices-idp-pic-11.2B2.1.tgz signed by PackageProduction_11_2_0
Creating /opt/sdk/service-packages/jservices-idp ...
Storing jservices-idp-pic-11.2B2.1.tgz in /var/sw/pkg ...
Link: /opt/sdk/service-packages/jservices-idp/jservices-idp-pic -> /var/sw/pkg/jservices-idp-
pic-11.2B2.1.tgz...
Using jservices-crypto-11.2B2.1.tgz
Auto-deleting old jservices-crypto-base ...
Removing /opt/sdk/service-packages/jservices-crypto-base ...
Removing jservices-crypto-base-pic-11.2B1.5.tgz from /var/sw/pkg ...
Notifying mspd ...
Installing new jservices-crypto-base ...
Verified jservices-crypto-base-pic-11.2B2.1.tgz signed by PackageProduction_11_2_0
Creating /opt/sdk/service-packages/jservices-crypto-base ...
Storing jservices-crypto-base-pic-11.2B2.1.tgz in /var/sw/pkg ...
Link: /opt/sdk/service-packages/jservices-crypto-base/jservices-crypto-base-pic -> /var/sw/pkg/
jservices-crypto-base-pic-11.2B2.1.tgz...
Auto-deleting old jservices-ssl ...
Removing /opt/sdk/service-packages/jservices-ssl ...
Removing jservices-ssl-pic-11.2B1.5.tgz from /var/sw/pkg ...

```

```

Notifying mspd ...
Installing new jservices-ssl ...
Verified jservices-ssl-pic-11.2B2.1.tgz signed by PackageProduction_11_2_0
Creating /opt/sdk/service-packages/jservices-ssl ...
Storing jservices-ssl-pic-11.2B2.1.tgz in /var/sw/pkg ...
Link: /opt/sdk/service-packages/jservices-ssl/jservices-ssl-pic -> /var/sw/pkg/jservices-ssl-
pic-11.2B2.1.tgz...
Hardware Database regeneration succeeded
Validating against /config/juniper.conf.gz
mgd: commit complete
Validation succeeded
Installing package '/var/tmp/jinstall-11.2B2.1-domestic-signed.tgz' ...
Verified jinstall-11.2B2.1-domestic.tgz signed by PackageProduction_11_2_0
Adding jinstall...
Verified manifest signed by PackageProduction_11_2_0

WARNING:      This package will load JUNOS 11.2B2.1 software.
WARNING:      It will save JUNOS configuration files, and SSH keys
WARNING:      (if configured), but erase all other files and information
WARNING:      stored on this machine. It will attempt to preserve dumps
WARNING:      and log files, but this can not be guaranteed. This is the
WARNING:      pre-installation stage and all the software is loaded when
WARNING:      you reboot the system.

Saving the config files ...
NOTICE: uncommitted changes have been saved in /var/db/config/juniper.conf.pre-install
Installing the bootstrap installer ...

WARNING:      A REBOOT IS REQUIRED TO LOAD THIS SOFTWARE CORRECTLY. Use the
WARNING:      'request system reboot' command when software installation is
WARNING:      complete. To abort the installation, do not reboot your system,
WARNING:      instead use the 'request system software delete jinstall'
WARNING:      command as soon as this operation completes.

Saving package file in /var/sw/pkg/jinstall-11.2B2.1-domestic-signed.tgz ...
Saving state for rollback ...
ISSU: Old Master Upgrade Done
ISSU: IDLE
Shutdown NOW!
Reboot consistency check bypassed - jinstall 11.2B2.1 will complete installation upon reboot
[pid 66780]

```

```
*** FINAL System shutdown message from user@host> ***
System going down IMMEDIATELY
```

## request system software in-service-upgrade (MX Series Virtual Chassis)

```
{master:member0-re0}
user@host> request system software in-service-upgrade jinstall-14.1-20140114.2-domestic-
signed.tgz
[Jan 30 10:45:32]:ISSU: IDLE

Beginning in-service-upgrade at Jan 30, 2014; 10:45:34
[Jan 30 10:45:34]:ISSU: Validating Image
Validating VC readiness...
Validating required configuration...
Validating release compatibility...
Validation successful
Initiating chassis in-service-upgrade
[Jan 30 10:46:56]:ISSU: Preparing LCC Backup REs
Copying new release to all RE's
Pushing bundle to member0-re0
Pushing bundle to member1-re0
Pushing bundle to member1-re1
[Jan 30 10:51:11]:ISSU: Preparing Backup RE
Arming new release on all RE's
member0-re0:
-----
Installing package '/var/tmp/jinstall-14.1-20140114_ib_14_1_psd.1-domestic-signed.tgz' ...
Verified jinstall-14.1-20140114_ib_14_1_psd.1-domestic.tgz signed by PackageDevelopmentEc_2014
Adding jinstall...

WARNING:      The software that is being installed has limited support.
WARNING:      Run 'file show /etc/notices/unsupported.txt' for details.

verixec: accepting signer: PackageDevelopmentEc_2014
Verified manifest signed by PackageDevelopmentEc_2014

WARNING:      This package will load JUNOS 14.1-20140114_ib_14_1_psd.1 software.
WARNING:      It will save JUNOS configuration files, and SSH keys
WARNING:      (if configured), but erase all other files and information
WARNING:      stored on this machine. It will attempt to preserve dumps
WARNING:      and log files, but this can not be guaranteed. This is the
```

WARNING: pre-installation stage and all the software is loaded when  
 WARNING: you reboot the system.

Saving the config files ...

NOTICE: uncommitted changes have been saved in /var/db/config/juniper.conf.pre-install

Installing the bootstrap installer ...

WARNING: A REBOOT IS REQUIRED TO LOAD THIS SOFTWARE CORRECTLY. Use the  
 WARNING: 'request system reboot' command when software installation is  
 WARNING: complete. To abort the installation, do not reboot your system,  
 WARNING: instead use the 'request system software delete jinstall'  
 WARNING: command as soon as this operation completes.

Saving package file in /var/sw/pkg/jinstall-14.1-20140114\_ib\_14\_1\_psd.1-domestic-signed.tgz ...

Saving state for rollback ...

member1-re0:

-----  
 Installing package '/var/tmp/jinstall-14.1-20140114\_ib\_14\_1\_psd.1-domestic-signed.tgz' ...  
 Verified jinstall-14.1-20140114\_ib\_14\_1\_psd.1-domestic.tgz signed by PackageDevelopmentEc\_2014  
 Adding jinstall...

WARNING: The software that is being installed has limited support.  
 WARNING: Run 'file show /etc/notices/unsupported.txt' for details.

verixec: accepting signer: PackageDevelopmentEc\_2014

Verified manifest signed by PackageDevelopmentEc\_2014

WARNING: This package will load JUNOS 14.1-20140114\_ib\_14\_1\_psd.1 software.  
 WARNING: It will save JUNOS configuration files, and SSH keys  
 WARNING: (if configured), but erase all other files and information  
 WARNING: stored on this machine. It will attempt to preserve dumps  
 WARNING: and log files, but this can not be guaranteed. This is the  
 WARNING: pre-installation stage and all the software is loaded when  
 WARNING: you reboot the system.

Saving the config files ...

NOTICE: uncommitted changes have been saved in /var/db/config/juniper.conf.pre-install

Installing the bootstrap installer ...

WARNING: A REBOOT IS REQUIRED TO LOAD THIS SOFTWARE CORRECTLY. Use the  
 WARNING: 'request system reboot' command when software installation is  
 WARNING: complete. To abort the installation, do not reboot your system,



WARNING: instead use the 'request system software delete jinstall'  
 WARNING: command as soon as this operation completes.

Saving package file in /var/sw/pkg/jinstall-14.1-20140114\_ib\_14\_1\_psd.1-domestic-signed.tgz ...  
 Saving state for rollback ...

member1-rel:

-----  
 Installing package '/var/tmp/jinstall-14.1-20140114\_ib\_14\_1\_psd.1-domestic-signed.tgz' ...  
 Verified jinstall-14.1-20140114\_ib\_14\_1\_psd.1-domestic.tgz signed by PackageDevelopmentEc\_2014  
 Adding jinstall...

WARNING: The software that is being installed has limited support.  
 WARNING: Run 'file show /etc/notices/unsupported.txt' for details.

verixec: accepting signer: PackageDevelopmentEc\_2014  
 Verified manifest signed by PackageDevelopmentEc\_2014

WARNING: This package will load JUNOS 14.1-20140114\_ib\_14\_1\_psd.1 software.  
 WARNING: It will save JUNOS configuration files, and SSH keys  
 WARNING: (if configured), but erase all other files and information  
 WARNING: stored on this machine. It will attempt to preserve dumps  
 WARNING: and log files, but this can not be guaranteed. This is the  
 WARNING: pre-installation stage and all the software is loaded when  
 WARNING: you reboot the system.

Saving the config files ...  
 NOTICE: uncommitted changes have been saved in /var/db/config/juniper.conf.pre-install  
 Installing the bootstrap installer ...

WARNING: A REBOOT IS REQUIRED TO LOAD THIS SOFTWARE CORRECTLY. Use the  
 WARNING: 'request system reboot' command when software installation is  
 WARNING: complete. To abort the installation, do not reboot your system,  
 WARNING: instead use the 'request system software delete jinstall'  
 WARNING: command as soon as this operation completes.

Saving package file in /var/sw/pkg/jinstall-14.1-20140114\_ib\_14\_1\_psd.1-domestic-signed.tgz ...  
 Saving state for rollback ...

Installing package '/var/tmp/jinstall-14.1-20140114\_ib\_14\_1\_psd.1-domestic-signed.tgz' ...  
 Verified jinstall-14.1-20140114\_ib\_14\_1\_psd.1-domestic.tgz signed by PackageDevelopmentEc\_2014  
 Adding jinstall...

WARNING: The software that is being installed has limited support.

WARNING: Run 'file show /etc/notices/unsupported.txt' for details.

verexec: accepting signer: PackageDevelopmentEc\_2014

Verified manifest signed by PackageDevelopmentEc\_2014

WARNING: This package will load JUNOS 14.1-20140114\_ib\_14\_1\_psd.1 software.

WARNING: It will save JUNOS configuration files, and SSH keys

WARNING: (if configured), but erase all other files and information

WARNING: stored on this machine. It will attempt to preserve dumps

WARNING: and log files, but this can not be guaranteed. This is the

WARNING: pre-installation stage and all the software is loaded when

WARNING: you reboot the system.

Saving the config files ...

NOTICE: uncommitted changes have been saved in /var/db/config/juniper.conf.pre-install

Installing the bootstrap installer ...

WARNING: A REBOOT IS REQUIRED TO LOAD THIS SOFTWARE CORRECTLY. Use the

WARNING: 'request system reboot' command when software installation is

WARNING: complete. To abort the installation, do not reboot your system,

WARNING: instead use the 'request system software delete jinstall'

WARNING: command as soon as this operation completes.

Saving package file in /var/sw/pkg/jinstall-14.1-20140114\_ib\_14\_1\_psd.1-domestic-signed.tgz ...

Saving state for rollback ...

[Jan 30 11:03:12]:ISSU: Backup RE Prepare Done

Rebooting standby RE's

Sending Reboot Command to member0-re0

Shutdown NOW!

Reboot consistency check bypassed - jinstall 14.1-20140114\_ib\_14\_1\_psd.1 will complete installation upon reboot

[pid 2757]

Sending Reboot Command to member1-re1

Shutdown NOW!

Reboot consistency check bypassed - jinstall 14.1-20140114\_ib\_14\_1\_psd.1 will complete installation upon reboot

[pid 2670]

Waiting for standby RE's to boot

[Jan 30 11:18:26]:ISSU: LCC Backup REs Prepare Done

Waiting for standby RE's to have the correct ISSU state

Waiting for protocol backup to be ready to switch mastership

Switching mastership on the protocol backup chassis to slot 1

Waiting for protocol backup chassis master switch to complete

```

Globally updating ISSU state
Waiting for protocol backup chassis to become GRES ready
[Jan 30 11:19:18]:ISSU: VC Protocol Backup has Switched
Passing ISSU control to chassisd
Chassis ISSU Started
[Jan 30 11:21:01]:ISSU: Preparing Daemons
[Jan 30 11:22:02]:ISSU: Daemons Ready for ISSU
[Jan 30 11:22:06]:ISSU: Starting Upgrade for FRUs
[Jan 30 11:25:42]:ISSU: Preparing for Switchover
[Jan 30 11:26:06]:ISSU: Ready for Switchover
[Jan 30 11:26:20]:ISSU: All VC Members Ready for Switchover
Waiting for master chassis to be switch ready
Switching mastership locally
Resolving mastership...
Complete. The other routing engine becomes the master.
Waiting for virtual chassis roles to switch
Globally updating ISSU state to IDLE
[Jan 30 11:26:33]:ISSU: IDLE
Rebooting protocol backup standby RE.
Sending Reboot Command to member1-re0

member1-re0:
-----
Shutdown NOW!
Reboot consistency check bypassed - jinstall 14.1-20140114_ib_14_1_psd.1 will complete
installation upon reboot
[pid 10462]
Rebooting locally to complete the in service upgrade.
Shutdown NOW!
Reboot consistency check bypassed - jinstall 14.1-20140114_ib_14_1_psd.1 will complete
installation upon reboot
[pid 13458]

{local:member0-re1}
user@host>
*** FINAL System shutdown message from user@host ***

System going down IMMEDIATELY

Connection closed by foreign host.

```

## Release Information

Command introduced in Junos OS Release 11.2.

## RELATED DOCUMENTATION

*request system software abort*

[show chassis in-service-upgrade](#) | [1389](#)

# request system software nonstop-upgrade

## IN THIS SECTION

- [Syntax](#) | [1314](#)
- [Description](#) | [1315](#)
- [Options](#) | [1317](#)
- [Required Privilege Level](#) | [1318](#)
- [Output Fields](#) | [1318](#)
- [Sample Output](#) | [1319](#)
- [Release Information](#) | [1326](#)

## Syntax

```
request system software nonstop-upgrade (package-name | set [package-name package-name])
<force-host>
<no-copy>
<no-old-master-upgrade>
<reboot >
<unlink>
```

## Description

Perform a nonstop software upgrade (NSSU) on a switch with redundant Routing Engines or on a Virtual Chassis or Virtual Chassis Fabric (VCF). The behavior of this command depends on the type of switch, Virtual Chassis, or VCF where you run it, as follows:

- When you run this command on any of the following Virtual Chassis or VCF configurations, NSSU upgrades all members of the Virtual Chassis:
  - EX3300, EX3400, EX4200, EX4300, EX4400, EX4500, EX4550, EX4600, or EX4650-48Y Virtual Chassis
  - Mixed Virtual Chassis composed of any combination of EX4200, EX4500, and EX4550 switches, or EX4300 and EX4600 switches
  - QFX3500 and QFX3600 Virtual Chassis
  - QFX5100 Virtual Chassis
  - QFX5120-48Y, QFX5120-48T or QFX5120-32C Virtual Chassis
  - Fixed configuration of switches in a VCF (QFX3500/QFX3600 and QFX5100 switches)
  - Mixed VCF composed of any combination of QFX3500/QFX3600, QFX5100, and EX4300 switches

The original Virtual Chassis or VCF backup becomes the primary. The new primary automatically upgrades and reboots the original primary, which then rejoins the Virtual Chassis or VCF as the backup.

- When you run this command on an EX6200 or EX8200 switch, NSSU upgrades both the backup and primary Routing Engines. The original backup Routing Engine becomes the new primary at the end of the upgrade.
  - On an EX6200 switch, NSSU automatically reboots the original primary Routing Engine.
  - On an EX8200 switch, NSSU does not automatically reboot the original primary Routing Engine unless you specify the `reboot` option.
- When you run this command on an EX8200 Virtual Chassis, NSSU upgrades all primary and backup Routing Engines in the Virtual Chassis, including the external Routing Engines. The original backup Routing Engines become the new primary Routing Engines. NSSU does not automatically reboot the original primary Routing Engines unless you specify the `reboot` option.

This command has the following requirements:

- All Virtual Chassis members, VCF members, and all Routing Engines must be running the same Junos OS release.

- You must enable Graceful Routing Engine switchover (GRES)..
- You must enable Nonstop active routing (NSR).

**NOTE:** Although not required, we recommend you also enable nonstop bridging (NSB). NSB ensures that all NSB-supported Layer 2 protocols operate seamlessly during the Routing Engine switchover during NSSU. See [Configuring Nonstop Bridging on EX Series Switches \(CLI Procedure\)](#).

- You must run the command from the primary Routing Engine on a standalone switch or from the primary on a Virtual Chassis.
- For minimal traffic disruption, you must define link aggregation groups (LAGs) such that the member links reside on different Virtual Chassis or VCF member switches (or on different line cards for EX6200 and EX8200 switches and EX8200 Virtual Chassis).
- For all Virtual Chassis (except EX8200 Virtual Chassis):
  - The Virtual Chassis members must be connected in a ring topology. A ring topology prevents the Virtual Chassis from splitting during an NSSU.
  - The Virtual Chassis primary and backup must be adjacent to each other in the ring topology. With adjacent placement, the primary and backup are always in sync while the switches in line-card roles are rebooting.
  - The Virtual Chassis must be preprovisioned so the line-card role is explicitly assigned to member switches acting in a line-card role. During an NSSU, the primary and backup member switches must maintain their Routing Engine roles (although the primary role switches to the backup), and the remaining switches must maintain their line-card roles.
  - In a two-member Virtual Chassis, you must configure no-split-detection so the Virtual Chassis doesn't split during NSSU.
- For Virtual Chassis Fabric:
  - You can only have two members preprovisioned in the Routing Engine role. If more than two Routing Engines are configured, NSSU issues a warning message and the NSSU process stops.
  - The VCF members should be connected in a spine and leaf topology. A spine and leaf topology prevents the VCF from splitting during NSSU. Each leaf device must be connected to both spine devices.
  - The VCF must be preprovisioned so that the line-card role has been explicitly assigned to member switches acting in a line-card role, and likewise the Routing Engine role has been explicitly assigned to the member switches acting in a Routing Engine role. During an NSSU, the primary

and backup member switches must maintain their Routing Engine roles (although the primary role switches to the backup), and the remaining switches must maintain their line-card roles.

- You must configure no-split-detection in a two-member VCF so the VCF does not split during NSSU.

## Options

***package-name***

Location of the software package or bundle to be installed. For example:

- */var/tmp/package-name*—For a software package or bundle installed from a local directory on the switch.
- *protocol://hostname/pathname/package-name*—For a software package or bundle downloaded and installed from a remote location. Replace *protocol* with one of the following:
  - *ftp*—File Transfer Protocol.  
Use *ftp://hostname/pathname/package-name*.  
To specify authentication credentials, use *ftp://<username>:<password>@hostname/pathname/package-name*.  
To have the system prompt you for the password, specify *prompt* in place of the password.  
The command displays an error message if a password is required and you do not specify the password or prompt.
  - *http*—Hypertext Transfer Protocol.  
Use *http://hostname/pathname/package-name*.  
To specify authentication credentials, use *http://<username>:<password>@hostname/pathname/package-name*.  
The command prompts you for a password if one is required and you didn't include it.
  - *scp*—Secure copy (available only for Canada and U.S. version).  
Use *scp://hostname/pathname/package-name*.  
To specify authentication credentials, use *scp://<username>:<password>@hostname/pathname/package-name*.

**NOTE:** The *pathname* in the protocol is the relative path to the user home directory on the remote system and not the root directory.

**set**  
**[*package-name*]**

(Mixed Virtual Chassis only) Locations of the different installation packages required by the different types of member switches. These packages must be for the same Junos OS

<b><i>package-name]</i></b>	release. See this command's <i>package-name</i> option for information about how to specify the installation packages.
<b>force-host</b>	(Optional) Force adding the host software package or bundle (and ignore warnings) on EX4650, QFX5100, or QFX5120 devices.
<b>no-copy</b>	(Optional) Install a software package or bundle, but do not save copies of the package or bundle files.
<b>no-old-master-upgrade</b>	(Optional) (EX8200 switches only) Upgrade the backup Routing Engine only. After the upgrade completes, the original primary Routing Engine becomes the backup Routing Engine and continues running the previous software version.
<b>reboot</b>	(Optional) (EX8200 switches and EX8200 Virtual Chassis only) When you include the reboot option, NSSU automatically reboots the original primary (new backup) Routing Engine after being upgraded to the new software. When you omit the reboot option, you must manually reboot the original primary (new backup) Routing Engine using the <a href="#">request system reboot</a> command.

**NOTE:** If you do not use the `reboot` option on an EX8200 Virtual Chassis, you must establish a connection to the console port on the Switch Fabric and Routing Engine (SRE) module or Routing Engine (RE) module to manually reboot the backup Routing Engines.

<b>unlink</b>	(Optional) Remove the software package after a successful upgrade.
---------------	--

## Required Privilege Level

maintenance

## Output Fields

This command reports feedback on the status of the request. Some functions are shared between NSSU and the in-service software upgrade (ISSU) feature, so you might see what appear to be ISSU messages as well as NSSU messages in the output from this command.



## Sample Output

### request system software nonstop-upgrade (EX4200 Virtual Chassis)

```
user@switch> request system software nonstop-upgrade
/var/tmp/jinstall-ex-4200-12.1R5.5-domestic-signed.tgz
Chassis ISSU Check Done
ISSU: Validating Image
ISSU: Preparing Backup RE
Installing image on other FPC's along with the backup

Checking pending install on fpc1
Pushing bundle to fpc1
WARNING: A reboot is required to install the software
WARNING: Use the 'request system reboot' command immediately
Completed install on fpc1

Checking pending install on fpc2
Pushing bundle to fpc2
WARNING: A reboot is required to install the software
WARNING: Use the 'request system reboot' command immediately
Completed install on fpc2

Checking pending install on fpc3
Pushing bundle to fpc3
WARNING: A reboot is required to install the software
WARNING: Use the 'request system reboot' command immediately
Completed install on fpc3

Checking pending install on fpc4
Pushing bundle to fpc4
WARNING: A reboot is required to install the software
WARNING: Use the 'request system reboot' command immediately
Completed install on fpc4

Checking pending install on fpc5
Pushing bundle to fpc5
WARNING: A reboot is required to install the software
WARNING: Use the 'request system reboot' command immediately
Completed install on fpc5

Checking pending install on fpc6
```

Pushing bundle to fpc6  
 WARNING: A reboot is required to install the software  
 WARNING: Use the 'request system reboot' command immediately  
 Completed install on fpc6

Checking pending install on fpc7  
 Pushing bundle to fpc7  
 WARNING: A reboot is required to install the software  
 WARNING: Use the 'request system reboot' command immediately  
 Completed install on fpc7  
 Backup upgrade done  
 Rebooting Backup RE

Rebooting fpc1  
 ISSU: Backup RE Prepare Done  
 Waiting for Backup RE reboot  
 GRES operational  
 Initiating Chassis In-Service-Upgrade  
 Chassis ISSU Started  
 ISSU: Preparing Daemons  
 ISSU: Daemons Ready for ISSU  
 ISSU: Starting Upgrade for FRUs  
 ISSU: Preparing for Switchover  
 ISSU: Ready for Switchover  
 Checking In-Service-Upgrade status

Item	Status	Reason
FPC 0	Online	
FPC 1	Online	
FPC 2	Online (ISSU)	
FPC 3	Online (ISSU)	
FPC 4	Online (ISSU)	
FPC 5	Online (ISSU)	
FPC 6	Online (ISSU)	
FPC 7	Online (ISSU)	

Going to install image on master  
 WARNING: A reboot is required to install the software  
 WARNING: Use the 'request system reboot' command immediately  
 relinquish mastership  
 ISSU: IDLE

\*\*\* FINAL System shutdown message from root@switch \*\*\*

System going down IMMEDIATELY

Shutdown NOW!  
[pid 9336]

### request system software nonstop-upgrade (EX6200 Switch)

```
{master}
user@switch> request system software nonstop-upgrade
/var/tmp/jinstall-ex-6200-12.2R5.5-domestic-signed.tgz
Chassis ISSU Check Done
ISSU: Validating Image
ISSU: Preparing Backup RE
Pushing bundle to re0
NOTICE: Validating configuration against jinstall-ex-6200-12.2R5.5-domestic-signed.tgz.
NOTICE: Use the 'no-validate' option to skip this if desired.
WARNING: A reboot is required to install the software
WARNING: Use the 'request system reboot' command immediately
Backup upgrade done
Rebooting Backup RE

Rebooting re0
ISSU: Backup RE Prepare Done
Waiting for Backup RE reboot
GRES operational
Initiating Chassis In-Service-Upgrade
Chassis ISSU Started
ISSU: Preparing Daemons
ISSU: Daemons Ready for ISSU
ISSU: Starting Upgrade for FRUs
ISSU: Preparing for Switchover
ISSU: Ready for Switchover
Checking In-Service-Upgrade status
```

Item	Status	Reason
FPC 0	Online (ISSU)	
FPC 1	Online (ISSU)	
FPC 2	Online (ISSU)	
FPC 3	Online (ISSU)	
FPC 4	Online	
FPC 5	Online	

```

FPC 6      Online (ISSU)
FPC 7      Online (ISSU)
FPC 8      Online (ISSU)
FPC 9      Online (ISSU)
Going to install image on master
NOTICE: Validating configuration against jinstall-ex-6200-12.2R5.5-domestic-signed.tgz.
NOTICE: Use the 'no-validate' option to skip this if desired.
WARNING: A reboot is required to install the software
WARNING:   Use the 'request system reboot' command immediately
relinquish mastership
ISSU: IDLE
Trying to relinquish mastership before rebooting...
Resolving mastership...
Complete. The other routing engine becomes the master.

*** FINAL System shutdown message from user@switch ***

System going down IMMEDIATELY

```

### **request system software nonstop-upgrade reboot (EX8200 Switch)**

```

{master}
user@switch> request system software nonstop-upgrade reboot
/var/tmp/jinstall-ex-8200-10.4R1.5-domestic-signed.tgz
Chassis ISSU Check Done
ISSU: Validating Image
ISSU: Preparing Backup RE
Pushing bundle to re1
WARNING: A reboot is required to install the software
WARNING:   Use the 'request system reboot' command immediately
Backup upgrade done
Rebooting Backup RE

Rebooting re1
ISSU: Backup RE Prepare Done
Waiting for Backup RE reboot
GRES operational
Initiating Chassis In-Service-Upgrade
Chassis ISSU Started
ISSU: Preparing Daemons
ISSU: Daemons Ready for ISSU

```

```

ISSU: Starting Upgrade for FRUs
ISSU: Preparing for Switchover
ISSU: Ready for Switchover
Checking In-Service-Upgrade status
  Item           Status           Reason
  FPC 0          Online (ISSU)
  FPC 2          Offline           Offlined by CLI command
  FPC 3          Online (ISSU)
Resolving mastership...
Complete. The other routing engine becomes the master.
ISSU: RE switchover Done
ISSU: Upgrading Old Master RE
WARNING: A reboot is required to install the software
WARNING:   Use the 'request system reboot' command immediately
ISSU: Old Master Upgrade Done
ISSU: IDLE
Shutdown NOW!
[pid 2635]

*** FINAL System shutdown message from user@switch ***
System going down IMMEDIATELY

```

### **request system software nonstop-upgrade no-old-master-upgrade (EX8200 Switch)**

```

{master}
user@switch> request system software nonstop-upgrade no-old-master-upgrade
/var/tmp/jinstall-ex-8200-10.4R1.5-domestic-signed.tgz
Chassis ISSU Check Done
ISSU: Validating Image
ISSU: Preparing Backup RE
Pushing bundle to re1
WARNING: A reboot is required to install the software
WARNING:   Use the 'request system reboot' command immediately
Backup upgrade done
Rebooting Backup RE

Rebooting re1
ISSU: Backup RE Prepare Done
Waiting for Backup RE reboot
GRES operational

```

```

Initiating Chassis In-Service-Upgrade
Chassis ISSU Started
ISSU: Preparing Daemons
ISSU: Daemons Ready for ISSU
ISSU: Starting Upgrade for FRUs
ISSU: Preparing for Switchover
ISSU: Ready for Switchover
Checking In-Service-Upgrade status
  Item           Status           Reason
  FPC 0          Online (ISSU)
  FPC 1          Online (ISSU)
  FPC 2          Online (ISSU)
  FPC 3          Offline           Offlined by CLI command
  FPC 4          Online (ISSU)
  FPC 5          Online (ISSU)
  FPC 6          Online (ISSU)
  FPC 7          Online (ISSU)
Resolving mastership...
Complete. The other routing engine becomes the master.
ISSU: RE switchover Done
Skipping Old Master Upgrade
ISSU: IDLE

```

### request system software nonstop-upgrade reboot (EX8200 Virtual Chassis)

```

{master:9}
user@external-routing-engine> request system software nonstop-upgrade reboot
/var/tmp/jinstall-ex-xre200-11.1-20101130.0-domestic-signed.tgz
Chassis ISSU Check Done
ISSU: Validating Image
ISSU: Preparing LCC Backup REs
ISSU: Preparing Backup RE
Pushing bundle /var/tmp/jinstall-ex-xre200-11.1-20101130.0-domestic-signed.tgz to member8
-----
WARNING: A reboot is required to install the software
WARNING:   Use the 'request system reboot' command immediately
VC Backup upgrade done
Rebooting VC Backup RE

Rebooting member8
ISSU: Backup RE Prepare Done

```

```

Waiting for VC Backup RE reboot
Pushing bundle to member0-backup
Pushing bundle to member1-backup
WARNING: A reboot is required to install the software
WARNING: Use the 'request system reboot' command immediately
WARNING: A reboot is required to install the software
WARNING: Use the 'request system reboot' command immediately

```

```

Rebooting member0-backup
Rebooting LCC [member0-backup]

```

```

Rebooting member1-backup
Rebooting LCC [member1-backup]
ISSU: LCC Backup REs Prepare Done
GRES operational
Initiating Chassis Nonstop-Software-Upgrade
Chassis ISSU Started
ISSU: Preparing Daemons
ISSU: Daemons Ready for ISSU
ISSU: Starting Upgrade for FRUs
ISSU: Preparing for Switchover
ISSU: Ready for Switchover
Checking Nonstop-Upgrade status
member0:

```

---

Item	Status	Reason
FPC 0	Online (ISSU)	
FPC 1	Online (ISSU)	
FPC 2	Online (ISSU)	
FPC 5	Online (ISSU)	

```
member1:
```

---

Item	Status	Reason
FPC 0	Online (ISSU)	
FPC 1	Offline	Offlined due to config
FPC 2	Online (ISSU)	
FPC 3	Online (ISSU)	
FPC 4	Online (ISSU)	
FPC 5	Online (ISSU)	
FPC 7	Online (ISSU)	

```
member0:
```

```

-----
Item           Status           Reason
FPC 0          Online (ISSU)
FPC 1          Online (ISSU)
FPC 2          Online (ISSU)
FPC 5          Online (ISSU)

member1:
-----
Item           Status           Reason
FPC 0          Online (ISSU)
FPC 1          Offline           Offlined due to config
FPC 2          Online (ISSU)
FPC 3          Online (ISSU)
FPC 4          Online (ISSU)
FPC 5          Online (ISSU)
FPC 7          Online (ISSU)
ISSU: Upgrading Old Master RE
Pushing bundle /var/tmp/incoming-package-8200.tgz to member0-master
Pushing bundle /var/tmp/incoming-package-8200.tgz to member1-master

ISSU: RE switchover Done
WARNING: A reboot is required to install the software
WARNING:   Use the 'request system reboot' command immediately
Rebooting ...
shutdown: [pid 2188]
Shutdown NOW!
ISSU: Old Master Upgrade Done
ISSU: IDLE
Shutdown NOW!

*** FINAL System shutdown message from root@ ***
System going down IMMEDIATELY

```

## Release Information

Command introduced in Junos OS Release 10.4.

Option set `[package-name package-name]` added in Junos OS Release 12.1 for EX Series switches.



## RELATED DOCUMENTATION

[show chassis nonstop-upgrade | 1426](#)

[Upgrading Software on an EX6200 or EX8200 Standalone Switch Using Nonstop Software Upgrade \(CLI Procedure\)](#)

[Upgrading Software on an EX8200 Virtual Chassis Using Nonstop Software Upgrade \(CLI Procedure\)](#)

[Upgrading Software on a Virtual Chassis and Mixed Virtual Chassis Using Nonstop Software Upgrade](#)

[Upgrading Software on a Virtual Chassis Fabric Using Nonstop Software Upgrade](#)

## request system software validate in-service-upgrade

### IN THIS SECTION

- [Syntax | 1327](#)
- [Description | 1327](#)
- [Options | 1328](#)
- [Additional Information | 1328](#)
- [Required Privilege Level | 1328](#)
- [Output Fields | 1328](#)
- [Sample Output | 1329](#)
- [Release Information | 1332](#)

### Syntax

```
request system software validate in-service-upgrade package-name
<enhanced-mode>
```

### Description

Perform a compatibility check to ensure that the software and hardware components and the configuration on the device support unified ISSU. The `request system software validate in-service-upgrade` command enables you to detect any compatibility issues before actually issuing the `request system software in-service-upgrade` command to initiate unified ISSU.

## Options

### *package-name*

Location from which the software package or bundle is to be installed. For example:

- */var/tmp/package-name*—For a software package or bundle that is being installed from a local directory on the router.
- *protocol://hostname/pathname/package-name*—For a software package or bundle that is to be downloaded and installed from a remote location. Replace *protocol* with one of the following:
  - *ftp*—File Transfer Protocol
  - *http*—Hypertext Transfer Protocol
  - *scp*—Secure copy (available only for Canada and U.S. version)

### **enhanced-mode**

(Optional) Checks for compatibility with enhanced mode—a mode of ISSU that eliminates packet loss during the unified ISSU process.

**NOTE:** The enhanced mode option is available on MPC7E, MPC8E, and MPC9E line cards starting from Junos OS Release 20.1R1. Support for MPC11E line cards is provided from Junos OS Release 21.4R1 onwards.

## Additional Information

Unified ISSU is not supported on every platform. For a list of supported platforms, see ["Unified ISSU System Requirements" on page 504](#).

## Required Privilege Level

view

## Output Fields

When you enter this command, Junos OS displays the status of your request.

## Sample Output

### request system software validate in-service-upgrade

```
{master}
user@host> request system software validate in-service-upgrade /var/tmp/jinstall-9.0-20080114.2-domestic-
signed.tgz reboot
Checking compatibility with configuration
Initializing...
Using jbase-9.5-20090127.0
Verified manifest signed by PackageProduction_9_5_0
Using /var/tmp/jinstall-9.6-daily-domestic-signed.tgz
Verified jinstall-9.6-20090706.0-domestic.tgz signed by PackageProduction_9_6_0
Using jinstall-9.6-20090706.0-domestic.tgz
Using jbundle-9.6-20090706.0-domestic.tgz
Checking jbundle requirements on /
Using jbase-9.6-20090706.0.tgz
Verified manifest signed by PackageProduction_9_6_0
Using jkernel-9.6-20090706.0.tgz
Verified manifest signed by PackageProduction_9_6_0
Using jcrypto-9.6-20090706.0.tgz
Verified manifest signed by PackageProduction_9_6_0
Using jpfe-9.6-20090706.0.tgz
Using jdocs-9.6-20090706.0.tgz
Verified manifest signed by PackageProduction_9_6_0
Using jroute-9.6-20090706.0.tgz
Verified manifest signed by PackageProduction_9_6_0
Using jservices-9.6-20090706.0.tgz
[: /var/validate/chroot/tmp/jservices/packages/jservices-voice-9.6-20090706.0.tgz: unexpected
operator
Auto-deleting old jservices-voice ...
Removing /opt/sdk/jservices-voice ...
Removing jservices-voice-bsg-9.5-20090127.0.tgz from /var/sw/pkg ...
Notifying mspd ...
Installing new jservices-voice ...
Verified jservices-voice-bsg-9.6-20090706.0.tgz signed by PackageProduction_9_6_0
Creating /var/sw/pkg ...
Creating /opt/sdk/jservices-voice ...
Storing jservices-voice-bsg-9.6-20090706.0.tgz in /var/sw/pkg ...
Link: /opt/sdk/jservices-voice/jservices-voice-bsg -> /var/sw/pkg/jservices-voice-
bsg-9.6-20090706.0.tgz...
Installing new jservices-bgf ...
```

```

Verified jservices-bgf-pic-9.6-20090706.0.tgz signed by PackageProduction_9_6_0
Creating /opt/sdk/jservices-bgf ...
Storing jservices-bgf-pic-9.6-20090706.0.tgz in /var/sw/pkg ...
Link: /opt/sdk/jservices-bgf/jservices-bgf-pic -> /var/sw/pkg/jservices-bgf-
pic-9.6-20090706.0.tgz...
Auto-deleting old jservices-aacl ...
Removing /opt/sdk/jservices-aacl ...
Removing jservices-aacl-pic-9.5-20090127.0.tgz from /var/sw/pkg ...
Notifying mspd ...
Installing new jservices-aacl ...
Verified jservices-aacl-pic-9.6-20090706.0.tgz signed by PackageProduction_9_6_0
Creating /opt/sdk/jservices-aacl ...
Storing jservices-aacl-pic-9.6-20090706.0.tgz in /var/sw/pkg ...
Link: /opt/sdk/jservices-aacl/jservices-aacl-pic -> /var/sw/pkg/jservices-aacl-
pic-9.6-20090706.0.tgz...
Auto-deleting old jservices-llpdf ...
Removing /opt/sdk/jservices-llpdf ...
Removing jservices-llpdf-pic-9.5-20090127.0.tgz from /var/sw/pkg ...
Notifying mspd ...
Installing new jservices-llpdf ...
Verified jservices-llpdf-pic-9.6-20090706.0.tgz signed by PackageProduction_9_6_0
Creating /opt/sdk/jservices-llpdf ...
Storing jservices-llpdf-pic-9.6-20090706.0.tgz in /var/sw/pkg ...
Link: /opt/sdk/jservices-llpdf/jservices-llpdf-pic -> /var/sw/pkg/jservices-llpdf-
pic-9.6-20090706.0.tgz...
Auto-deleting old jservices-sfw ...
Removing /opt/sdk/jservices-sfw ...
Removing jservices-sfw-pic-9.5-20090127.0.tgz from /var/sw/pkg ...
Notifying mspd ...
Installing new jservices-sfw ...
Verified jservices-sfw-pic-9.6-20090706.0.tgz signed by PackageProduction_9_6_0
Creating /opt/sdk/jservices-sfw ...
Storing jservices-sfw-pic-9.6-20090706.0.tgz in /var/sw/pkg ...
Link: /opt/sdk/jservices-sfw/jservices-sfw-pic -> /var/sw/pkg/jservices-sfw-
pic-9.6-20090706.0.tgz...
Auto-deleting old jservices-appid ...
Removing /opt/sdk/jservices-appid ...
Removing jservices-appid-pic-9.5-20090127.0.tgz from /var/sw/pkg ...
Notifying mspd ...
Installing new jservices-appid ...
Verified jservices-appid-pic-9.6-20090706.0.tgz signed by PackageProduction_9_6_0
Creating /opt/sdk/jservices-appid ...
Storing jservices-appid-pic-9.6-20090706.0.tgz in /var/sw/pkg ...

```

```

Link: /opt/sdk/jservices-appid/jservices-appid-pic -> /var/sw/pkg/jservices-appid-
pic-9.6-20090706.0.tgz...
Auto-deleting old jservices-idp ...
Removing /opt/sdk/jservices-idp ...
Removing jservices-idp-pic-9.5-20090127.0.tgz from /var/sw/pkg ...
Notifying mspd ...
Installing new jservices-idp ...
Verified jservices-idp-pic-9.6-20090706.0.tgz signed by PackageProduction_9_6_0
Creating /opt/sdk/jservices-idp ...
Storing jservices-idp-pic-9.6-20090706.0.tgz in /var/sw/pkg ...
Link: /opt/sdk/jservices-idp/jservices-idp-pic -> /var/sw/pkg/jservices-idp-
pic-9.6-20090706.0.tgz...
Hardware Database regeneration succeeded
Validating against /config/juniper.conf.gz
mgd: commit complete
Validation succeeded
PIC 7/0 will be offlined (In-Service-Upgrade not supported)
PIC 7/1 will be offlined (In-Service-Upgrade not supported)
PIC 4/2 will be offlined (In-Service-Upgrade not supported)
PIC 4/3 will be offlined (In-Service-Upgrade not supported)

```

### request system software validate in-service-upgrade enhanced-mode

```

{master}
user@host> request system software validate in-service-upgrade /var/tmp/junos-install-mx-x86-32-20.1.tgz
enhanced-mode
ISSU: enhanced-mode check passed
Verified junos-install-mx-x86-32-20.1 signed by PackageDevelopmentEc_2019 method ECDSA256+SHA256
Verified manifest signed by PackageDevelopmentEc_2019 method ECDSA256+SHA256
...
Checking PIC combinations
Adding junos-mx-x86-32-20.1 ...
Verified fips-mode signed by PackageDevelopmentEc_2019 method ECDSA256+SHA256
...
Hardware Database regeneration succeeded
Validating against /config/juniper.conf.gz
...
Validation succeeded
ISSU: Validating Image Done

```

## Release Information

Command introduced in Junos OS Release 9.6.

## RELATED DOCUMENTATION

---

*request system software validate*

---

[request system software in-service-upgrade](#) | 1270

---

*request system software abort*

---

[show chassis in-service-upgrade](#) | 1389

---

Getting Started with Unified In-Service Software Upgrade

---

Example: Performing a Unified ISSU

## show bgp neighbor

### IN THIS SECTION

- [Syntax](#) | 1333
- [Syntax \(EX Series Switch, QFX Series, OCX Series, and cRPD\)](#) | 1333
- [Syntax \(SRX Series\)](#) | 1333
- [Description](#) | 1333
- [Options](#) | 1333
- [Additional Information](#) | 1334
- [Required Privilege Level](#) | 1334
- [Output Fields](#) | 1334
- [Sample Output](#) | 1351
- [Release Information](#) | 1372

## Syntax

```
show bgp neighbor
<exact-instance instance-name>
<instance instance-name>
<logical-system (all | logical-system-name)>
<neighbor-address>
<output-queue>
<orf (detail | neighbor-address)>
<rib-sharding (main | rib-shard-name)>
```

## Syntax (EX Series Switch, QFX Series, OCX Series, and cRPD)

```
show bgp neighbor
<instance instance-name>
<exact-instance instance-name>
<neighbor-address>
<orf (neighbor-address | detail)>
<rib-sharding neighbor-address>
```

## Syntax (SRX Series)

```
show bgp neighbor
<neighbor-address>
<instance instance-name>
```

## Description

Display information about BGP peers.

## Options

<b>none</b>	Display information about all BGP peers.
<b>exact-instance <i>instance-name</i></b>	(Optional) Display information for the specified instance only.

<b>instance</b> <i>instance-name</i>	(Optional) Display information about BGP peers for all routing instances whose name begins with this string (for example, cust1, cust11, and cust111 are all displayed when you run the <code>show bgp neighbor instance cust1</code> command).
<b>logical-system</b> (all   <i>logical-system-name</i> )	(Optional) Perform this operation on all logical systems or on a particular logical system.
<b>neighbor-address</b>	(Optional) Display information for only the BGP peer at the specified IP address.
<b>orf</b> (detail   <i>neighbor-address</i> )	(Optional) Display outbound route-filtering information for all BGP peers or only for the BGP peer at the specified IP address. The default is to display brief output. Use the <code>detail</code> option to display detailed output.
<b>output-queue</b>	(Optional) Display information regarding the number of routes currently queued in the 17 prioritized BGP output queues.
<b>rib-sharding</b> (main   junos-bgpshard <i>shard-number</i> )	(Optional) Display information for specific shard only. When NSR is configured, display information in the backup Routing Engine. For example, junos-bgpshard0. If omitted, displays aggregated data from all shards including main shard.

## Additional Information

For information about the `local-address`, `nlri`, `hold-time`, and preference statements, see the [Junos OS Routing Protocols Library for Routing Devices](#).

## Required Privilege Level

view

## Output Fields

[Table 50 on page 1335](#) describes the output fields for the `show bgp neighbor` command. Output fields are listed in the approximate order in which they appear.



**Table 50: show bgp neighbor Output Fields**

Field Name	Field Description
Peer	Address of the BGP neighbor. The address is followed by the neighbor port number.
AS	AS number of the peer.
Local	Address of the local routing device. The address is followed by the peer port number.
Type	Type of peer: Internal or External.
State	<p>Current state of the BGP session:</p> <ul style="list-style-type: none"> <li>• Active—BGP is initiating a transport protocol connection in an attempt to connect to a peer. If the connection is successful, BGP sends an Open message.</li> <li>• Connect—BGP is waiting for the transport protocol connection to be completed.</li> <li>• Established—The BGP session has been established, and the peers are exchanging update messages.</li> <li>• Idle—This is the first stage of a connection. BGP is waiting for a Start event.</li> <li>• OpenConfirm—BGP has acknowledged receipt of an open message from the peer and is waiting to receive a keepalive or notification message.</li> <li>• OpenSent—BGP has sent an open message and is waiting to receive an open message from the peer.</li> <li>• route reflector client—The BGP session is established with a route reflector client.</li> </ul>

Table 50: show bgp neighbor Output Fields (*Continued*)

Field Name	Field Description
Flags	<p>Internal BGP flags:</p> <ul style="list-style-type: none"> <li>• <b>Aggregate Label</b>—BGP has aggregated a set of incoming labels (labels received from the peer) into a single forwarding label.</li> <li>• <b>CleanUp</b>—The peer session is being shut down.</li> <li>• <b>Delete</b>—This peer has been deleted.</li> <li>• <b>Idled</b>—This peer has been permanently idled.</li> <li>• <b>ImportEval</b>—At the last commit operation, this peer was identified as needing to reevaluate all received routes.</li> <li>• <b>Initializing</b>—The peer session is initializing.</li> <li>• <b>PurgePending</b>—This flag marks one or more routing table (also known as routing information base [RIB]) entries for deletion. The purge job to delete these entries begins after the peer is closed. A purge job keeps running if new routing table entries are marked for deletion.</li> <li>• <b>PurgeInProgress</b>—The purge job has started and is not yet complete.</li> <li>• <b>PurgeImpatient</b>—The purge begins as a low priority background job. The Adj-RIB-Out can be cleaned up and a new peering can be established in the background before all routes are deleted. After the peer goes down and the group has closed, the purge becomes a normal priority job.</li> <li>• <b>SendRtn</b>—Messages are being sent to the peer.</li> <li>• <b>Sync</b>—This peer is synchronized with the rest of the peer group.</li> <li>• <b>RSync</b>—This peer in the backup Routing Engine is synchronized with the BGP peer in the primary Routing Engine for nonstop active routing.</li> <li>• <b>TryConnect</b>—Another attempt is being made to connect to the peer.</li> <li>• <b>Unconfigured</b>—This peer is not configured.</li> <li>• <b>WriteFailed</b>—An attempt to write to this peer failed.</li> </ul>

Table 50: show bgp neighbor Output Fields (*Continued*)

Field Name	Field Description
Last state	<p>Previous state of the BGP session:</p> <ul style="list-style-type: none"><li>• Active—BGP is initiating a transport protocol connection in an attempt to connect to a peer. If the connection is successful, BGP sends an Open message.</li><li>• Connect—BGP is waiting for the transport protocol connection to be completed.</li><li>• Established—The BGP session has been established, and the peers are exchanging update messages.</li><li>• Idle—This is the first stage of a connection. BGP is waiting for a Start event.</li><li>• OpenConfirm—BGP has acknowledged receipt of an open message from the peer and is waiting to receive a keepalive or notification message.</li><li>• OpenSent—BGP has sent an open message and is waiting to receive an open message from the peer.</li></ul>

Table 50: show bgp neighbor Output Fields (*Continued*)

Field Name	Field Description
Last event	<p>Last activity that occurred in the BGP session:</p> <ul style="list-style-type: none"> <li>• Closed—The BGP session closed.</li> <li>• ConnectRetry—The transport protocol connection failed, and BGP is trying again to connect.</li> <li>• HoldTime—The session ended because the hold timer expired.</li> <li>• KeepAlive—The local routing device sent a BGP keepalive message to the peer.</li> <li>• Open—The local routing device sent a BGP open message to the peer.</li> <li>• OpenFail—The local routing device did not receive an acknowledgment of a BGP open message from the peer.</li> <li>• RecvKeepAlive—The local routing device received a BGP keepalive message from the peer.</li> <li>• RecvNotify—The local routing device received a BGP notification message from the peer.</li> <li>• RecvOpen—The local routing device received a BGP open message from the peer.</li> <li>• RecvUpdate—The local routing device received a BGP update message from the peer.</li> <li>• Start—The peering session started.</li> <li>• Stop—The peering session stopped.</li> <li>• TransportError—A TCP error occurred.</li> </ul>

**Table 50: show bgp neighbor Output Fields (Continued)**

Field Name	Field Description
Last error	<p>Last error that occurred in the BGP session:</p> <ul style="list-style-type: none"> <li>• Cease—An error occurred, such as a version mismatch, that caused the session to close.</li> <li>• Finite State Machine Error—In setting up the session, BGP received a message that it did not understand.</li> <li>• Hold Time Expired—The session's hold time expired.</li> <li>• Message Header Error—The header of a BGP message was malformed.</li> <li>• Open Message Error—A BGP open message contained an error.</li> <li>• None—No errors occurred in the BGP session.</li> <li>• Update Message Error—A BGP update message contained an error.</li> </ul>
Export	Name of the export policy that is configured on the peer.
Import	Name of the import policy that is configured on the peer.

Table 50: show bgp neighbor Output Fields (Continued)

Field Name	Field Description
Options	<p>Configured BGP options:</p> <ul style="list-style-type: none"> <li>• AddressFamily—Configured address family: inet or inet-vpn.</li> <li>• AdvertiseBGPStatic—Configured BGP static routes are advertised.</li> <li>• AuthKeyChain—Authentication key change is enabled.</li> <li>• BfdEnabled—Status of BFD.</li> <li>• DontGRHelpFateSharingBfdDown—Status of the dont-help-shared-fate-bfd-down option. If this option is configured the device does not go into graceful restart helper mode.</li> <li>• DropPathAttributes—Certain path attributes are configured to be dropped from neighbor updates during inbound processing.</li> <li>• GracefulRestart—Graceful restart is configured.</li> <li>• HoldTime—Hold time configured with the hold-time statement. The hold time is three times the interval at which keepalive messages are sent.</li> <li>• IgnorePathAttributes—Certain path attributes are configured to be ignored in neighbor updates during inbound processing.</li> <li>• Local Address—Address configured with the local-address statement.</li> <li>• LLGR—BGP long-lived graceful restart capability is configured.</li> <li>• LLGRHelperDisabled—BGP long-lived graceful restart is completely disabled for a neighbor.</li> <li>• Multihop—Allow BGP connections to external peers that are not on a directly connected network.</li> <li>• NLRI—Configured MBGP state for the BGP group: multicast, unicast, or both if you have configured nlri any.</li> <li>• Peer AS—Configured peer autonomous system (AS).</li> <li>• Preference—Preference value configured with the preference statement.</li> <li>• Refresh—Configured to refresh automatically when the policy changes.</li> <li>• Rib-group—Configured routing table group.</li> </ul>

**Table 50: show bgp neighbor Output Fields (Continued)**

Field Name	Field Description
	<ul style="list-style-type: none"> <li>• RFC6514CompliantSafi129—Configured SAFI 129 according to RFC 6514 (BGP VPN multicast used to use SAFI 128).</li> </ul>
Path-attributes dropped	Path attribute codes that are dropped from neighbor updates.
Path-attributes ignored	Path attribute codes that are ignored during neighbor updates.
Peer does not support LLGR Restarter or Receiver functionality	BGP neighbor does not support long-lived graceful restart (LLGR) restarter mode completely.
Peer does not support LLGR Restarter functionality	BGP neighbor does not support long-lived graceful restart (LLGR) restarter mode for any family.
Authentication key change	(Appears only if the authentication-keychain statement has been configured) Name of the authentication keychain enabled.
Authentication algorithm	(Appears only if the authentication-algorithm statement has been configured) Type of authentication algorithm enabled: hmac or md5.
Prefixlimit configured for NLRI	(Appears only if the drop-excess <percentage> or hide-excess <percentage> option in the prefix-limit statement is configured) NLRI for which the prefix-limit statement is configured.
Acceptedprefixlimit configured for NLRI	(Appears only if the drop-excess <percentage> or hide-excess <percentage> option in the accepted-prefix-limit statement is configured) NLRI for which the accepted-prefix-limit statement is configured.

**Table 50: show bgp neighbor Output Fields (Continued)**

Field Name	Field Description
Action	<p>(Appears only if the drop-excess &lt;percentage&gt; or hide-excess &lt;percentage&gt; option in the prefix-limit and accepted-prefix-limit statements are configured) Performs the configured action:</p> <ul style="list-style-type: none"> <li>teardown &lt;percentage&gt;— Tears down the session when the maximum number of prefixes is reached.</li> <li>drop-excess &lt;percentage&gt;— Drops excess routes when the maximum number of prefixes is exceeded.</li> <li>hide-excess &lt;percentage&gt;— Hides excess routes when the maximum number of prefixes is exceeded.</li> </ul>
Limit	<p>(Appears only if the drop-excess &lt;percentage&gt; or hide-excess &lt;percentage&gt; option in the prefix-limit and accepted-prefix-limit statements are configured) Number of the maximum prefixes if exceeded, the configured action in the Action field takes place.</p>
Warning percentage	<p>(Appears only if the drop-excess &lt;percentage&gt; or hide-excess &lt;percentage&gt; option in the prefix-limit and accepted-prefix-limit statements are configured) Percentage of the maximum dropped or hidden routes if exceeded, displays a warning message in the logs.</p>
Count	<p>(Appears only if the drop-excess &lt;percentage&gt; or hide-excess &lt;percentage&gt; option in the prefix-limit and accepted-prefix-limit statements are configured) Displays the number of routes that are dropped or hidden after exceeding the limit configured in the Limit field. The counter resets only after the peer resets.</p>
Address families configured	Names of configured address families for the VPN.
BGP-Static Advertisement Policy	Name of the BGP static policy that is configured on the peer.
Local Address	Address of the local routing device.



**Table 50: show bgp neighbor Output Fields (Continued)**

Field Name	Field Description
Remove-private options	Options associated with the <code>remove-private</code> statement.
Holdtime	Hold time configured with the <code>hold-time</code> statement. The hold time is three times the interval at which keepalive messages are sent.
Flags for NLRI inet-label-unicast	Flags related to labeled-unicast: <ul style="list-style-type: none"> <li>• TrafficStatistics—Collection of statistics for labeled-unicast traffic is enabled.</li> </ul>
Traffic statistics	Information about labeled-unicast traffic statistics: <ul style="list-style-type: none"> <li>• Options—Options configured for collecting statistics about labeled-unicast traffic.</li> <li>• File—Name and location of statistics log files.</li> <li>• size—Size of all the log files, in bytes.</li> <li>• files—Number of log files.</li> </ul>
Traffic Statistics Interval	Time between sample periods for labeled-unicast traffic statistics, in seconds.
Preference	Preference value configured with the <code>preference</code> statement.
Outbound Timer	Time for which the route is available in Junos OS routing table before it is exported to BGP. This field is displayed in the output only if the <code>out-delay</code> parameter is configured to a non-zero value.
Number of flaps	Number of times the BGP session has gone down and then come back up.

**Table 50: show bgp neighbor Output Fields (Continued)**

Field Name	Field Description
Threads related state	<p>Displays thread related state if update threading is enabled:</p> <ul style="list-style-type: none"> <li>• Thread sync pending—Thread sync is yet to begin.</li> <li>• Update thread sync—Syncing peer up with update threads.</li> <li>• Shard sync—Syncing peer up with shards. If the peer is in shard sync state, it also displays a hex value indicating which shards are yet to send peer up acknowledgement.</li> <li>• Thread sync complete—Peer has been synced in update threads and shards.</li> <li>• Peer UP acknowledgement received from Update Thread—Display peer up acknowledgement received from update threads.</li> </ul>
Peer ID	Router identifier of the peer.
Group index	Index number for the BGP peer group. The index number differentiates between groups when a single BGP group is split because of different configuration options at the group and peer levels.
Peer index	Index that is unique within the BGP group to which the peer belongs.
Local ID	Router identifier of the local routing device.
Local Interface	Name of the interface on the local routing device.
Active holdtime	Hold time that the local routing device negotiated with the peer.
Keepalive Interval	Keepalive interval, in seconds.
I/O Session Thread	Displays the BGP I/O session thread and its state if update threading is enabled.
I/O Session Thread	Displays the BGP I/O session thread and its state if update threading is enabled.

**Table 50: show bgp neighbor Output Fields (Continued)**

Field Name	Field Description
BFD	Status of BFD failure detection.
Local Address	Name of directly connected interface over which direct EBGp peering is established.
NLRI and times for LLGR configured on peer	<p>Names of address families and stale time for BGP long-lived graceful restart configured on the BGP peer or neighbor.</p> <p>Times are displayed using the routing protocol daemon (rpd) %OT format:</p> <p>&lt;weeks&gt;w&lt;days&gt;d &lt;hours&gt;:&lt;minutes&gt;:&lt;seconds&gt;</p> <p>Zero leading elements are omitted, for example, a value less than one week do not include the weeks.</p>
NLRI and times that peer supports LLGR Restarter for	<p>Names of address families and stale time that the BGP peer supports for restarter mode for BGP long-lived graceful restart.</p> <p>Times are displayed using the routing protocol daemon (rpd) %OT format:</p> <p>&lt;weeks&gt;w&lt;days&gt;d &lt;hours&gt;:&lt;minutes&gt;:&lt;seconds&gt;</p> <p>Zero leading elements are omitted, for example, a value less than one week do not include the weeks.</p>
NLRI that peer saved LLGR forwarding for	Name of the address family for which the BGP peer saved BGP long-lived graceful restart forwarding.
Graceful Restart Details	Amount of time that is remaining until LLGR expires and the time remaining on the GR stale timer, along with RIB details, are displayed while LLGR receiver mode is active (a peer that negotiated LLGR has disconnected and not yet reconnected).
NLRI we are holding stale routes for	Names of address families (NLRIs) for which that stale routes are held or preserved when BGP graceful restart receiver mode is active for a neighbor.

**Table 50: show bgp neighbor Output Fields (Continued)**

Field Name	Field Description
Time until end-of-rib is assumed for stale routes	<p>Amount of time remaining on the stale timer until which end-of-RIB (EoR) markers are assumed when BGP graceful restart receiver mode is active for a neighbor.</p> <p>Time is displayed in Coordinated Universal Time (UTC) format (YYYY-MM-DD-HH:MM:SS). Note that the stale timer display ('Time until end-of-rib is assumed') is also present when a session is active, but the neighbor has not yet sent all of the end-of-rib indications.</p>
Time until stale routes are deleted or become long-lived stale	Amount of time up to which stale routes are deleted or become long-lived stale routes when BGP graceful restart receiver mode is active for a neighbor.
NLRI for restart configured on peer	Names of address families configured for restart.
NLRI advertised by peer	Address families supported by the peer: unicast or multicast.
NLRI for this session	Address families being used for this session.
Peer supports Refresh capability	Remote peer's ability to send and request full routing table readvertisement (route refresh capability). For more information, see RFC 2918, <i>Route Refresh Capability for BGP-4</i> .
Restart time configured on peer	Configured time allowed for restart on the neighbor.
Stale routes from peer are kept for	When graceful restart is negotiated, the maximum time allowed to hold routes from neighbors after the BGP session has gone down.
Peer does not support Restarter functionality	Graceful restart restarter-mode is disabled on the peer.

**Table 50: show bgp neighbor Output Fields (Continued)**

Field Name	Field Description
Peer does not support Receiver functionality	Graceful restart helper-mode is disabled on the peer.
Restart time requested by this peer	Restart time requested by this neighbor during capability negotiation.
Restart flag received from the peer	When this field appears, the BGP speaker has restarted (Restarting), and this peer should not wait for the end-of-rib marker from the speaker before advertising routing information to the speaker.
NLRI that peer supports restart for	Neighbor supports graceful restart for this address family.
NLRI peer can save forwarding state	Neighbor supporting this address family saves all forwarding states.
NLRI that peer saved forwarding for	Neighbor saves all forwarding states for this address family.
NLRI that restart is negotiated for	Router supports graceful restart for this address family.
NLRI of received end-of-rib markers	Address families for which end-of-routing-table markers are received from the neighbor.
NLRI of all end-of-rib markers sent	Address families for which end-of-routing-table markers are sent to the neighbor.
Peer supports 4 byte AS extension (peer-as 1)	Peer understands 4-byte AS numbers in BGP messages. The peer is running Junos OS Release 9.1 or later.

Table 50: show bgp neighbor Output Fields (Continued)

Field Name	Field Description
NLRIs for which peer can receive multiple paths	<p>Appears in the command output of the local router if the downstream peer is configured to receive multiple BGP routes to a single destination, instead of only receiving the active route.</p> <p>Possible value is inet-unicast.</p>
NLRIs for which peer can send multiple paths: inet-unicast	<p>Appears in the command output of the local router if the upstream peer is configured to send multiple BGP routes to a single destination, instead of only sending the active route.</p> <p>Possible value is inet-unicast.</p>
Table inet.number	<p>Information about the routing table:</p> <ul style="list-style-type: none"> <li>• RIB State—BGP is in the graceful restart process for this routing table: restart is complete or restart in progress.</li> <li>• Bit—Number that represents the entry in the routing table for this peer.</li> <li>• Send state—State of the BGP group: in sync, not in sync, or not advertising.</li> <li>• Active prefixes—Number of prefixes received from the peer that are active in the routing table.</li> <li>• Received prefixes—Total number of prefixes from the peer, both active and inactive, that are in the routing table.</li> <li>• Accepted prefixes—Total number of prefixes from the peer that have been accepted by a routing policy.</li> <li>• Suppressed due to damping—Number of routes currently inactive because of damping or other reasons. These routes do not appear in the forwarding table and are not exported by routing protocols.</li> </ul>
Last traffic (seconds)	Last time any traffic was received from the peer or sent to the peer, and the last time the local routing device checked.
Input messages	Messages that BGP has received from the receive socket buffer, showing the total number of messages, number of update messages, number of times a policy is changed and refreshed, and the buffer size in octets. The buffer size is 16 KB.

Table 50: show bgp neighbor Output Fields (*Continued*)

Field Name	Field Description
Output messages	Messages that BGP has written to the transmit socket buffer, showing the total number of messages, number of update messages, number of times a policy is changed and refreshed, and the buffer size in octets. The buffer size is 16 KB.
Input dropped path attributes	Information about dropped path attributes: <ul style="list-style-type: none"> <li>• Code—Path attribute code.</li> <li>• Count—Path attribute count.</li> </ul>
Input ignored path attributes	Information about ignored path attributes: <ul style="list-style-type: none"> <li>• Code—Path attribute code.</li> <li>• Count—Path attribute count.</li> </ul>
Output queue	<p>Number of BGP packets that are queued to be transmitted to a particular neighbor for a particular routing table. Output queue 0 is for unicast NLRIs, and queue 1 is for multicast NLRIs.</p> <p>It also specifies the routing table name and the NLRI that the table was advertised through, in the format (<i>routing table name</i>, <i>NLRI</i>).</p> <p>If update threading is enabled, the Output Queue field will display the Output Queue count from update threads with an additional field that displays the Output Queue count per RIB as fetched from main or shards.</p> <p><b>NOTE:</b> The output queue of routing tables that are not advertised, will only show up at extensive output level.</p>
Trace options	Configured tracing of BGP protocol packets and operations.
Trace file	Name of the file to receive the output of the tracing operation.

Table 50: show bgp neighbor Output Fields (Continued)

Field Name	Field Description
Filter Updates rcv	<p>(orf option only) Number of outbound-route filters received for each configured address family.</p> <p><b>NOTE:</b> The counter is cumulative. For example, the counter is increased after the remote peer either resends or clears the outbound route filtering prefix list.</p>
Immediate	<p>(orf option only) Number of route updates received with the immediate flag set. The immediate flag indicates that the BGP peer should readvertise the updated routes.</p> <p><b>NOTE:</b> The counter is cumulative. For example, the counter is increased after the remote peer either resends or clears the outbound route filtering prefix list.</p>
Filter	(orf option only) Type of prefix filter received: prefix-based or extended-community.
Received filter entries	(orf option only) List of received filters displayed.
seq	(orf option only) Numerical order assigned to this prefix entry among all the received outbound route filter prefix entries.
prefix	(orf option only) Address for the prefix entry that matches the filter.
minlength	(orf option only) Minimum prefix length, in bits, required to match this prefix.
maxlength	(orf option only) Maximum prefix length, in bits, required to match this prefix.
match	(orf option only) For this prefix match, whether to permit or deny route updates.



## Sample Output

### show bgp neighbor

```
user@host > show bgp neighbor
```

For M Series, MX Series, and T Series routers running Junos OS Release 16.1 or later, the `show bgp neighbor` output includes the BGP group the peer belongs to, the routing instance (if any) that the peer is configured in, and the routing instance that the peer is using for the forwarding context (if applicable). An example follows.

```
Peer: 10.255.7.250+179 AS 65010   Local: 10.255.7.248+63740 AS 65010
  Group: toAsbr2                  Routing-Instance: master
  Forwarding routing-instance: toAsbr2
    Type: Internal   State: Established   Flags: <Sync>
  Last State: OpenConfirm   Last Event: RecvKeepAlive
  Last Error: None
  Export: [ redistrib_static ]
  Options: <Preference LocalAddress PeerAS Refresh>
  Options: <AdvertiseBGPStatic>
  Local Address: 10.255.7.248 Holdtime: 90 Preference: 170 Outbound Timer: 50
  Number of flaps: 0
  Peer ID: 10.255.7.250   Local ID: 10.255.7.248   Active Holdtime: 90
  Keepalive Interval: 30   Group index: 0   Peer index: 0
  BFD: disabled, down
  NLRI for restart configured on peer: inet-unicast
  NLRI advertised by peer: inet-unicast
  NLRI for this session: inet-unicast
  Peer supports Refresh capability (2)
  Stale routes from peer are kept for: 300
  Peer does not support Restarter functionality
  NLRI that restart is negotiated for: inet-unicast
  NLRI of received end-of-rib markers: inet-unicast
  NLRI of all end-of-rib markers sent: inet-unicast
  Peer supports 4 byte AS extension (peer-as 65010)
  Peer does not support Addpath
  NLRI that we support extended nexthop encoding for: inet-unicast
  NLRI that peer supports extended nexthop encoding for: inet-unicast

Table inet.0 Bit: 10000
  RIB State: BGP restart is complete
```

```

    Send state: in sync
    Active prefixes:          1
    Received prefixes:        1
    Accepted prefixes:        1
    Suppressed due to damping: 0
    Advertised prefixes:      1
    Last traffic (seconds): Received 9    Sent 5    Checked 5
    Input messages:  Total 36    Updates 2    Refreshes 0    Octets 718
    Output messages: Total 37    Updates 1    Refreshes 0    Octets 796
    Output Queue[0]: 0          (inet.0, inet-unicast)

Peer: 10.255.162.214+52193 AS 65100 Local: 10.255.167.205+179 AS 65100
  Type: Internal    State: Established (route reflector client)Flags: <Sync>
  Last State: OpenConfirm  Last Event: RecvKeepAlive
  Last Error: None
  Options: <Preference LocalAddress Cluster AddressFamily Rib-group Refresh>
  Address families configured: inet-unicast inet-vpn-unicast route-target
  Local Address: 10.255.167.205 Holdtime: 90 Preference: 170
  Number of flaps: 0
  Peer ID: 10.255.162.214  Local ID: 10.255.167.205    Active Holdtime: 90
  Keepalive Interval: 30    Group index: 0    Peer index: 1

```

### show bgp neighbor (dont-help-shared-fate-bfd-down is configured)

```

user@host> show bgp neighbor

Peer: 10.1.1.1 AS 200          Local: unspecified AS 65017
  Group: one                   Routing-Instance: master
  Forwarding routing-instance: master
  Type: External    State: Idle          Flags: <PeerInterfaceError>
  Last State: NoState    Last Event: NoEvent
  Last Error: None
  Options: <Preference PeerAS Refresh>
  Options: <BfdEnabled>
  Options: <DontGRHelpFateSharingBfdDown>
  Holdtime: 90 Preference: 170
  Number of flaps: 0
  Trace options: bridge
  Trace file: /var/log/bgp-log size 131072 files 10

Peer: 10.20.1.1 AS 200          Local: unspecified AS 65017

```

```

Group: one                      Routing-Instance: master
Forwarding routing-instance: master
Type: External    State: Idle          Flags: <PeerInterfaceError>
Last State: NoState    Last Event: NoEvent
Last Error: None
Options: <Preference PeerAS Refresh>
Options: <BfdEnabled>
Options: <DontGRHelpFateSharingBfdDown>
Holdtime: 90 Preference: 170
Number of flaps: 0
Peer: 10.30.1.1 AS 200          Local: unspecified AS 65017
Group: two                      Routing-Instance: master
Forwarding routing-instance: master
Type: External    State: Idle          Flags: <PeerInterfaceError>
Last State: NoState    Last Event: NoEvent
Last Error: None
Options: <Preference PeerAS Refresh>
Options: <BfdEnabled>
Options: <DontGRHelpFateSharingBfdDown>
Holdtime: 90 Preference: 170
Number of flaps: 0

```

## show bgp neighbor (CLNS)

```

user@host> show bgp neighbor
Peer: 10.245.245.1+179 AS 65200 Local: 10.245.245.3+3770 AS 65100
Type: External    State: Established    Flags: <ImportEval Sync>
Last State: OpenConfirm    Last Event: RecvKeepAlive
Last Error: None
Options: <Multihop Preference LocalAddress HoldTime AddressFamily PeerAS    Rib-group Refresh>
Address families configured: iso-vpn-unicast
Local Address: 10.245.245.3 Holdtime: 90 Preference: 170
Number of flaps: 0
Peer ID: 10.245.245.1    Local ID: 10.245.245.3    Active Holdtime: 90
Keepalive Interval: 30    Peer index: 0
NLRI advertised by peer: iso-vpn-unicast
NLRI for this session: iso-vpn-unicast
Peer supports Refresh capability (2)
Table bgp.isovpn.0 Bit: 10000
RIB State: BGP restart is complete
RIB State: VPN restart is complete

```

```

Send state: in sync
Active prefixes:      3
Received prefixes:    3
Suppressed due to damping: 0
Advertised prefixes:  3
Table aaaa.iso.0
RIB State: BGP restart is complete
RIB State: VPN restart is complete
Send state: not advertising
Active prefixes:      3
Received prefixes:    3
Suppressed due to damping: 0
Last traffic (seconds): Received 6    Sent 5    Checked 5
Input messages:  Total 1736    Updates 4    Refreshes 0    Octets 33385
Output messages: Total 1738    Updates 3    Refreshes 0    Octets 33305
Output Queue[0]: 0            (bgp.isovpn.0, iso-vpn-unicast)
Output Queue[1]: 0            (aaaa.iso.0, iso-vpn-unicast)

```

### show bgp neighbor (Layer 2 VPN)

```

user@host> show bgp neighbor
Peer: 10.69.103.2    AS 65536 Local: 10.69.103.1    AS 65539
Type: External      State: Active      Flags: <ImportEval>
Last State: Idle      Last Event: Start
Last Error: None
Export: [ BGP-INET-import ]
Options: <Preference LocalAddress HoldTime GracefulRestart AddressFamily PeerAS Refresh>
Address families configured: inet-unicast
Local Address: 10.69.103.1 Holdtime: 90 Preference: 170
Number of flaps: 0
Peer: 10.69.104.2    AS 65539 Local: 10.69.104.1    AS 65539
Type: External      State: Active      Flags: <ImportEval>
Last State: Idle      Last Event: Start
Last Error: None
Export: [ BGP-L-import ]
Options: <Preference LocalAddress HoldTime GracefulRestart AddressFamily PeerAS Refresh>
Address families configured: inet-labeled-unicast
Local Address: 10.69.104.1 Holdtime: 90 Preference: 170
Number of flaps: 0
Peer: 10.255.14.182+179 AS 65069    Local: 10.255.14.176+2131 AS 65069
Type: Internal      State: Established  Flags: <ImportEval>

```

```

Last State: OpenConfirm   Last Event: RecvKeepAlive
Last Error: None
Options: <Preference LocalAddress HoldTime GracefulRestart AddressFamily   Rib-group Refresh>
Address families configured: inet-vpn-unicast l2vpn
Local Address: 10.255.14.176 Holdtime: 90 Preference: 170
Number of flaps: 0
Peer ID: 10.255.14.182    Local ID: 10.255.14.176    Active Holdtime: 90
Keepalive Interval: 30
NLRI for restart configured on peer: inet-vpn-unicast l2vpn
NLRI advertised by peer: inet-vpn-unicast l2vpn
NLRI for this session: inet-vpn-unicast l2vpn
Peer supports Refresh capability (2)
Restart time configured on the peer: 120
Stale routes from peer are kept for: 300
Restart time requested by this peer: 120
NLRI that peer supports restart for: inet-vpn-unicast l2vpn
NLRI peer can save forwarding state: inet-vpn-unicast l2vpn
NLRI that peer saved forwarding for: inet-vpn-unicast l2vpn
NLRI that restart is negotiated for: inet-vpn-unicast l2vpn
NLRI of received end-of-rib markers: inet-vpn-unicast l2vpn
Table bgp.l3vpn.0 Bit: 10000
  RIB State: BGP restart in progress
  RIB State: VPN restart in progress
  Send state: in sync
  Active prefixes:          10
  Received prefixes:        10
  Suppressed due to damping: 0
Table bgp.l2vpn.0 Bit: 20000
  RIB State: BGP restart in progress
  RIB State: VPN restart in progress
  Send state: in sync
  Active prefixes:          1
  Received prefixes:        1
  Suppressed due to damping: 0
Table BGP-INET.inet.0 Bit: 30000
  RIB State: BGP restart in progress
  RIB State: VPN restart in progress
  Send state: in sync
  Active prefixes:          2
  Received prefixes:        2
  Suppressed due to damping: 0
Table BGP-L.inet.0 Bit: 40000
  RIB State: BGP restart in progress

```

```

RIB State: VPN restart in progress
Send state: in sync
Active prefixes:          2
Received prefixes:        2
Suppressed due to damping: 0
Table LDP.inet.0 Bit: 50000
RIB State: BGP restart is complete
RIB State: VPN restart in progress
Send state: in sync
Active prefixes:          1
Received prefixes:        1
Suppressed due to damping: 0
Table OSPF.inet.0 Bit: 60000
RIB State: BGP restart is complete
RIB State: VPN restart in progress
Send state: in sync
Active prefixes:          2
Received prefixes:        2
Suppressed due to damping: 0
Table RIP.inet.0 Bit: 70000
RIB State: BGP restart is complete
RIB State: VPN restart in progress
Send state: in sync
Active prefixes:          2
Received prefixes:        2
Suppressed due to damping: 0
Table STATIC.inet.0 Bit: 80000
RIB State: BGP restart is complete
RIB State: VPN restart in progress
Send state: in sync
Active prefixes:          1
Received prefixes:        1
Suppressed due to damping: 0
Table L2VPN.l2vpn.0 Bit: 90000
RIB State: BGP restart is complete
RIB State: VPN restart in progress
Send state: in sync
Active prefixes:          1
Received prefixes:        1
Suppressed due to damping: 0
Last traffic (seconds): Received 0    Sent 0    Checked 0
Input messages:  Total 14    Updates 13    Refreshes 0    Octets 1053
Output messages: Total 3     Updates 0     Refreshes 0     Octets 105

```

```

Output Queue[0]: 0      (bgp.l3vpn.0, inet-vpn-unicast)
Output Queue[1]: 0      (bgp.l2vpn.0, inet-vpn-unicast)
Output Queue[2]: 0      (BGP-INET.inet.0, inet-vpn-unicast)
Output Queue[3]: 0      (BGP-L.inet.0, inet-vpn-unicast)
Output Queue[4]: 0      (LDP.inet.0, inet-vpn-unicast)
Output Queue[5]: 0      (OSPF.inet.0, inet-vpn-unicast)
Output Queue[6]: 0      (RIP.inet.0, inet-vpn-unicast)
Output Queue[7]: 0      (STATIC.inet.0, inet-vpn-unicast)
Output Queue[8]: 0      (L2VPN.l2vpn.0, inet-vpn-unicast)

```

### **show bgp neighbor (Layer 3 VPN) (Not supported on the OCX Series.)**

```

user@host> show bgp neighbor
Peer: 192.0.2.0.179      AS 65045 Local: 192.0.2.1+1214      AS 65045
  Type: Internal      State: Established      Flags: <ImportEval>
  Last State: OpenConfirm  Last Event: RecvKeepAlive
  Last Error: None
  Export: [ match-all ] Import: [ match-all ]
  Options: <Preference LocalAddress HoldTime GracefulRestart AddressFamily      Rib-group Refresh>
  Address families configured: inet-vpn-unicast
  Local Address: 192.0.2.1 Holdtime: 90 Preference: 170
  Flags for NLRI inet-labeled-unicast: TrafficStatistics
  Traffic Statistics: Options: all File: /var/log/bstat.log
                                size 131072 files 10

  Traffic Statistics Interval: 60
  Number of flaps: 0
  Peer ID: 192.168.1.110      Local ID: 192.168.1.111      Active Holdtime: 90
  Keepalive Interval: 30
  NLRI for restart configured on peer: inet-vpn-unicast
  NLRI advertised by peer: inet-vpn-unicast
  NLRI for this session: inet-vpn-unicast
  Peer supports Refresh capability (2)
  Restart time configured on the peer: 120
  Stale routes from peer are kept for: 300
  Restart time requested by this peer: 120
  NLRI that peer supports restart for: inet-vpn-unicast
  NLRI peer can save forwarding state: inet-vpn-unicast
  NLRI that peer saved forwarding for: inet-vpn-unicast
  NLRI that restart is negotiated for: inet-vpn-unicast
  NLRI of received end-of-rib markers: inet-vpn-unicast
  NLRI of all end-of-rib markers sent: inet-vpn-unicast

```

```

Table bgp.l3vpn.0 Bit: 10000
  RIB State: BGP restart is complete
  RIB State: VPN restart is complete
  Send state: in sync
  Active prefixes:          2
  Received prefixes:        2
  Suppressed due to damping: 0
Table vpn-green.inet.0 Bit: 20001
  RIB State: BGP restart is complete
  RIB State: VPN restart is complete
  Send state: in sync
  Active prefixes:          2
  Received prefixes:        2
  Suppressed due to damping: 0
Last traffic (seconds): Received 15   Sent 20   Checked 20
Input messages:  Total 40      Updates 2      Refreshes 0      Octets 856
Output messages: Total 44      Updates 2      Refreshes 0      Octets 1066
Output Queue[0]: 0           (bgp.l3vpn.0, inet-vpn-unicast)
Output Queue[1]: 0           (vpn-green.inet.0, inet-vpn-unicast)
Trace options: detail packets
Trace file: /var/log/bgpr.log size 131072 files 10

```

## show bgp neighbor neighbor-address

```

user@host> show bgp neighbor 10.255.245.12
Peer: 10.255.245.12+179 AS 65035 Local: 10.255.245.13+2884 AS 65035
  Type: Internal   State: Established (route reflector client)Flags: <Sync>
  Last State: OpenConfirm   Last Event: RecvKeepAlive
  Last Error: None
  Options: <Preference LocalAddress HoldTime Cluster AddressFamily Rib-group Refresh>
  Options: RFC6514CompliantSafi129
  Address families configured: inet-vpn-unicast inet-labeled-unicast
  Local Address: 10.255.245.13 Holdtime: 90 Preference: 170
  Flags for NLRI inet-vpn-unicast: AggregateLabel
  Flags for NLRI inet-labeled-unicast: AggregateLabel
  Number of flaps: 0
  Peer ID: 10.255.245.12   Local ID: 10.255.245.13   Active Holdtime: 90
  Keepalive Interval: 30
BFD: disabled
  NLRI advertised by peer: inet-vpn-unicast inet-labeled-unicast
  NLRI for this session: inet-vpn-unicast inet-labeled-unicast

```



```

Peer supports Refresh capability (2)
Restart time configured on the peer: 300
Stale routes from peer are kept for: 60
Restart time requested by this peer: 300
NLRI that peer supports restart for: inet-unicast inet6-unicast
NLRI that restart is negotiated for: inet-unicast inet6-unicast
NLRI of received end-of-rib markers: inet-unicast inet6-unicast
NLRI of all end-of-rib markers sent: inet-unicast inet6-unicast
Table inet.0 Bit: 10000
  RIB State: restart is complete
  Send state: in sync
  Active prefixes: 4
  Received prefixes: 6
  Suppressed due to damping: 0
Table inet6.0 Bit: 20000
  RIB State: restart is complete
  Send state: in sync
  Active prefixes: 0
  Received prefixes: 2
  Suppressed due to damping: 0
Last traffic (seconds): Received 3    Sent 3    Checked 3
Input messages:  Total 9      Updates 6      Refreshes 0      Octets 403
Output messages: Total 7      Updates 3      Refreshes 0      Octets 365
Output Queue[0]: 0          (inet.0, inet-unicast)
Output Queue[1]: 0          (inet6.0, inet6-unicast)
Trace options: detail packets
Trace file: /var/log/bgpr size 131072 files 10

```

## show bgp neighbor neighbor-address

```

user@host> show bgp neighbor 192.168.4.222
Peer: 192.168.4.222+4902 AS 65501 Local: 192.168.4.221+179 AS 65500
  Type: External    State: Established    Flags: <Sync>
  Last State: OpenConfirm    Last Event: RecvKeepAlive
  Last Error: Cease
  Export: [ export-policy ] Import: [ import-policy ]
  Options: <Preference HoldTime AddressFamily PeerAS PrefixLimit Refresh>
  Address families configured: inet-unicast inet-multicast
  Holdtime: 60000 Preference: 170
  Number of flaps: 4
  Last flap event: RecvUpdate

```

```

Error: 'Cease' Sent: 5 Recv: 0
Peer ID: 10.255.245.6    Local ID: 10.255.245.5    Active Holdtime: 60000
Keepalive Interval: 20000    Peer index: 0
BFD: disabled, down
Local Interface: fxp0.0
NLRI advertised by peer: inet-unicast inet-multicast
NLRI for this session: inet-unicast inet-multicast
Peer supports Refresh capability (2)
Table inet.0 Bit: 10000
  RIB State: BGP restart is complete
  Send state: in sync
  Active prefixes:          8
  Received prefixes:        10
  Accepted prefixes:        10
  Suppressed due to damping: 0
  Advertised prefixes:      3
Table inet.2 Bit: 20000
  RIB State: BGP restart is complete
  Send state: in sync
  Active prefixes:          0
  Received prefixes:        0
  Accepted prefixes:        0
  Suppressed due to damping: 0
  Advertised prefixes:      0
Last traffic (seconds): Received 357 Sent 357 Checked 357
Input messages: Total 4    Updates 2    Refreshes 0    Octets 211
Output messages: Total 4    Updates 1    Refreshes 0    Octets 147
Output Queue[0]: 0        (inet.0, inet-unicast)
Output Queue[1]: 0        (inet.2, inet-multiicast)
Trace options: all
Trace file: /var/log/bgp size 10485760 files 10

```

### show bgp neighbor neighbor-address (BGP Graceful Restart Enabled)

```

user@router> show bgp neighbor 10.255.255.16

Peer: 10.255.255.16 AS 65100    Local: 10.255.255.12 AS 65100
  Type: Internal    State: Active    Flags: <>
  Last State: Idle    Last Event: Start
  Last Error: None
  Options: <Preference LocalAddress AddressFamily Rib-group Refresh>

```

```

Options: <LLGR>
Address families configured: l2vpn
Local Address: 10.255.255.12 Holdtime: 90 Preference: 170
NLRI l2vpn:
Number of flaps: 6
Last flap event: Restart
NLRI we are holding stale routes for: inet-vpn-unicast
Time until stale routes are deleted or become long-lived stale: 00:01:57
Time until end-of-rib is assumed for stale routes: 00:04:43
Table bgp.l3vpn.0
  RIB State: BGP restart is complete
  RIB State: VPN restart is complete
  Send state: not advertising
  Active prefixes:          0
  Received prefixes:        7
  Accepted prefixes:        7
  Suppressed due to damping: 0
Table foo.inet.0 Bit: 30000
  RIB State: BGP restart is complete
  RIB State: VPN restart is complete
  Send state: not in sync
  Active prefixes:          0
  Received prefixes:        7
  Accepted prefixes:        7
  Suppressed due to damping: 0

```

### **show bgp neighbor neighbor-address (BGP Long-Lived Graceful Restart)**

```

user@router> show bgp neighbor 10.4.12.11

Peer: 10.4.12.11 AS 65100      Local: 10.6.128.225 AS 65100
Type: Internal    State: Active    Flags: <>
Last State: Idle      Last Event: Start
Last Error: None
Export: [ foo ]
Options: <Preference LocalAddress Refresh GracefulRestart>
Options: <LLGR>
Local Address: 10.6.128.225 Holdtime: 90 Preference: 170
Number of flaps: 3
Last flap event: Restart
Error: 'Cease' Sent: 0 Recv: 1

```

```

Time until long-lived stale routes deleted: inet-vpn-unicast 10:00:22 route-target 10:00:22
Table bgp.l3vpn.0
  RIB State: BGP restart is complete
  RIB State: VPN restart is complete
  Send state: not advertising
  Active prefixes:          0
  Received prefixes:        7
  Accepted prefixes:        7
  Suppressed due to damping: 0
Table foo.inet.0 Bit: 30000
  RIB State: BGP restart is complete
  RIB State: VPN restart is complete
  Send state: not in sync
  Active prefixes:          0
  Received prefixes:        7
  Accepted prefixes:        7
  Suppressed due to damping: 0

```

### show bgp neighbor orf neighbor-address detail

```

user@host > show bgp neighbor orf 192.168.165.56 detail
Peer: 192.168.165.56+179 Type: External
Group: ext1

inet-unicast
  Filter updates rcv:          1 Immediate:          1
  Filter: prefix-based receive
  Received filter entries:
    seq 1: prefix 10.2.2.2/32: minlen 32: maxlen 32: match deny:

inet6-unicast
  Filter updates rcv:          0 Immediate:          1
  Filter: prefix-based receive
  Received filter entries:
    *:*

```

### show bgp neighbor logical-system

```

user@host > show bgp neighbor logical-system ITR1
Peer: 10.79.8.2+179 AS 65536 Local: 10.79.8.1+50891 AS 65500

```

```

Description: MX1
Type: External    State: Established    Flags: <ImportEval Sync>
Last State: OpenConfirm    Last Event: RecvKeepAlive
Last Error: None
....
Table inet.0 Bit: 10000
  RIB State: BGP restart is complete
  Send state: in sync
  Active prefixes:          1
  Received prefixes:        1
  Accepted prefixes:        1
  Suppressed due to damping: 0
  Advertised prefixes:      10
  Stale prefixes:           4: <=new, line only appears if count is non-0
It is the Number of prefixes marked as stale;
  LLGR-stale prefixes:      5: <=new, line only appears if count is non-0
It is the Number of prefixes marked as LLGR-stale

```

### show bgp neighbor output-queue

```

user@host > show bgp neighbor output-queue
Peer: 192.0.2.2+179 AS 65103      Local: 192.0.2.1+50799 AS 65102
Output Queue[0]: 0                (inet.0, inet-unicast)
  Priority 1 : 0
  Priority 2 : 0
  Priority 3 : 0
  Priority 4 : 0
  Priority 5 : 0
  Priority 6 : 0
  Priority 7 : 0
  Priority 8 : 0
  Priority 9 : 0
  Priority 10: 0
  Priority 11: 0
  Priority 12: 0
  Priority 13: 0
  Priority 14: 0
  Priority 15: 0
  Priority 16: 0
  Expedited  : 0

```

## show bgp neighbor (Segment Routing Traffic Engineering)

```

user@host > show bgp neighbor
run show bgp neighbor 10.1.1.254
  Peer: 10.1.1.254+60180 AS 65100   Local: 10.1.1.1+179 AS 65100
  Group: toB                        Routing-Instance: master
  Forwarding routing-instance: master
  Type: Internal   State: Established   Flags: <Sync>
  Last State: OpenConfirm   Last Event: RecvKeepAlive
  Last Error: None
  Options: <Preference LocalAddress>
  Address families configured: inet-segment-routing-te
  Local Address: 10.1.1.1 Holdtime: 90 Preference: 170 Local AS: 65100 Local System AS: 0
  Number of flaps: 0
  Peer ID: 10.128.150.15   Local ID: 10.128.150.110   Active Holdtime: 90
  Keepalive Interval: 30   Group index: 0   Peer index: 0
  I/O Session Thread: bgpio-0 State: Enabled
  BFD: disabled, down
  NLRI for restart configured on peer: inet-segment-routing-te
  NLRI advertised by peer: inet-segment-routing-te
  NLRI for this session: inet-segment-routing-te
  Peer supports Refresh capability (2)
  Stale routes from peer are kept for: 300
  Peer does not support Restarter functionality
  Restart flag received from the peer: Notification
  NLRI that restart is negotiated for: inet-segment-routing-te
  Peer does not support LLGR Restarter functionality
  Peer supports 4 byte AS extension (peer-as 65100)
  Peer does not support Addpath
  Last traffic (seconds): Received 17628 Sent 25   Checked 17628
  Input messages:   Total 2       Updates 0       Refreshes 0       Octets 82
  Output messages: Total 1       Updates 0       Refreshes 0       Octets 19
  Trace options: all
  Trace file: /var/log/bgp.log size 10485760 files 10

```

## show bgp neighbor (with rib-sharding configured)

```

user@host > show bgp neighbor rib-sharding main
Peer: 10.1.1.1+179 AS 65001   Local: 10.2.2.1+60231 AS 65001
Group: toFeeder              Routing-Instance: master

```

```

Forwarding routing-instance: master
Type: Internal    State: Established    Flags: <Sync>
Last State: OpenConfirm    Last Event: RecvKeepAlive
Last Error: None
Options: <Preference LocalAddress Refresh>
Options: <ConnectRetryInterval>
Options: <GracefulShutdownRcv>
Local Address: 10.2.2.1 Holdtime: 90 Preference: 170
Graceful Shutdown Receiver local-preference: 0
Number of flaps: 0
Threads related state:
    Internal State: Thread sync complete
    Peer UP acknowledgement received from Update Thread
Peer ID: 10.1.1.1          Local ID: 10.2.2.1          Active Holdtime: 90
Keepalive Interval: 30      Group index: 0      Peer index: 0      SNMP index: 0
I/O Session Thread: bgp-updio-2 State: Enabled
BFD: disabled, down
NLRI for restart configured on peer: inet-unicast
NLRI advertised by peer: inet-unicast
NLRI for this session: inet-unicast
Peer supports Refresh capability (2)
Stale routes from peer are kept for: 300
Peer does not support Restarter functionality
Restart flag received from the peer: Notification
NLRI that restart is negotiated for: inet-unicast
NLRI of received end-of-rib markers: inet-unicast
NLRI of all end-of-rib markers sent: inet-unicast
Peer does not support LLGR Restarter functionality
Peer supports 4 byte AS extension (peer-as 65001)
Peer does not support Addpath
NLRI(s) enabled for color nexthop resolution: inet-unicast
Table inet.0 Bit: 20002
    RIB State: BGP restart is complete
    Send state: in sync
    Active prefixes:          0
    Received prefixes:        0
    Accepted prefixes:        0
    Suppressed due to damping: 0
    Advertised prefixes:      0
Last traffic (seconds): Received 7    Sent 11    Checked 3910
Input messages:  Total 145    Updates 1      Refreshes 0      Octets 2759
Output messages: Total 135    Updates 0      Refreshes 0      Octets 2569

```

```
Output Queue[1]: 0          (inet.0, inet-unicast)
Output Queue[1]: 0          (inet.0, inet-unicast) (Main/Shards)
```

### show bgp neighbor (with rib-sharding configured on crpd)

```
user@host > show bgp neighbor rib-sharding junos-bgpshard14
```

```
Peer: 10.2.2.1 AS 65100          Local: 10.20.255.10 AS 65100
Description: To_Adolf
Group: G101_V4                  Routing-Instance: master
Forwarding routing-instance: master
Type: Internal    State: Idle      (route reflector client)Flags: <>
Last State: Established    Last Event: Stop
Last Error: None
Import: [ Block_bgp ]
Options: <Preference LocalAddress HoldTime Cluster AddressFamily Rib-group Refresh>
Options: <GracefulShutdownRcv>
Address families configured: inet-unicast inet-vpn-unicast inet6-vpn-unicast route-target
Local Address: 10.20.255.10 Holdtime: 10 Preference: 170
Graceful Shutdown Receiver local-preference: 0
Number of flaps: 1
Last flap event: Stop

Peer: 10.5.1.1 AS 65100          Local: 10.20.255.10 AS 65100
Description: To_stonepark
Group: G201_V4                  Routing-Instance: master
Forwarding routing-instance: master
Type: Internal    State: Idle      (route reflector client)Flags: <>
Last State: Established    Last Event: Stop
Last Error: None
Import: [ Block_bgp ]
Options: <Preference LocalAddress HoldTime Cluster AddressFamily Rib-group Refresh>
Options: <GracefulShutdownRcv>
Address families configured: inet-vpn-unicast inet6-vpn-unicast route-target
Local Address: 10.20.255.10 Holdtime: 10 Preference: 170
Graceful Shutdown Receiver local-preference: 0
Number of flaps: 2
Last flap event: Stop
Trace options: all
```



Trace file: /var/log/aaaaaa size 1073741824 files 10

**show bgp neighbor (with drop-excess <percentage> option configured and not exceeding the maximum configured percentage.)**

```

user@host > show bgp neighbor
Peer: 10.128.139.6+179 AS 65100 Local: 10.128.139.63+55782 AS 65100
  Group: ibgp Routing-Instance: master
  Forwarding routing-instance: master
  Type: Internal State: Established (route reflector client)Flags: <Sync>
  Last State: OpenConfirm Last Event: RecvKeepAlive
  Last Error: None
  Import: [ list_based_on_as ]
  Options: <LocalAddress KeepNone Cluster AddressFamily PrefixLimit Rib-group Refresh>
  Options: <GracefulShutdownRcv>
  Address families configured: inet-unicast
  Local Address: 10.128.139.63 Holdtime: 90 Preference: 170
  Graceful Shutdown Receiver local-preference: 0
  Prefixlimit configured for NLRI: inet-unicast Limit: 800000 Action: Drop excess
  Number of flaps: 0
  Peer ID: 10.128.139.6 Local ID: 10.128.139.63 Active Holdtime: 90
  Keepalive Interval: 30 Group index: 0 Peer index: 0 SNMP index: 0
  I/O Session Thread: bgpio-0 State: Enabled
  BFD: disabled, down
  NLRI for restart configured on peer: inet-unicast
  NLRI advertised by peer: inet-unicast inet-vpn-unicast inet-vpn-multicast
  NLRI for this session: inet-unicast
  Peer supports Refresh capability (2)
  Stale routes from peer are kept for: 300
  Peer does not support Restarter functionality
  Restart flag received from the peer: Notification
  NLRI that restart is negotiated for: inet-unicast
  NLRI of received end-of-rib markers: inet-unicast
  NLRI of all end-of-rib markers sent: inet-unicast
  Peer does not support LLGR Restarter functionality
  Peer supports 4 byte AS extension (peer-as 65100)
  Peer does not support Addpath
  NLRI(s) enabled for color nexthop resolution: inet-unicast
  Table inet.0 Bit: 20000
    RIB State: BGP restart is complete

```

```

Send state: in sync
Active prefixes:      800000
Received prefixes:    800000
Accepted prefixes:    800000
Suppressed due to damping: 0
Advertised prefixes:  29788
Last traffic (seconds): Received 1   Sent 0   Checked 538
Input messages:  Total 137090 Updates 137070 Refreshes 0 Octets 17371127
Output messages: Total 23022  Updates 23001 Refreshes 0 Octets 3539841
Output Queue[1]: 0          (inet.0, inet-unicast)
Trace options: send refresh
Trace file: /var/log/bgp_refresh size 5242880 files 10

```

**NOTE:** Such similar output is displayed when you configure the `hide-excess <percentage>` option and does not exceed the maximum configured percentage. This sample output is applicable for both the `prefix-limit` and `accepted-prefix-limit` configuration statements.

### **show bgp neighbor (with drop-excess <percentage> option configured and exceeding the maximum configured percentage.)**

```

user@host > show bgp neighbor
Peer: 10.128.139.6+179 AS 65100 Local: 10.128.139.63+55782 AS 65100
Group: ibgp Routing-Instance: master
Forwarding routing-instance: master
Type: Internal State: Established (route reflector client)Flags: <Sync>
Last State: OpenConfirm Last Event: RecvKeepAlive
Last Error: None
Import: [ list_based_on_as ]
Options: <LocalAddress KeepNone Cluster AddressFamily PrefixLimit Rib-group Refresh>
Options: <GracefulShutdownRcv>
Address families configured: inet-unicast
Local Address: 10.128.139.63 Holdtime: 90 Preference: 170
Graceful Shutdown Receiver local-preference: 0
Prefixlimit configured for NLRI: inet-unicast Limit: 800000 Action: Drop excess
Number of flaps: 0
Dropped prefixes - Exceeded configured prefix-limits
Peer ID: 10.128.139.6 Local ID: 10.128.139.63 Active Holdtime: 90
Keepalive Interval: 30 Group index: 0 Peer index: 0 SNMP index: 0
I/O Session Thread: bgpio-0 State: Enabled

```

```

BFD: disabled, down
NLRI for restart configured on peer: inet-unicast
NLRI advertised by peer: inet-unicast inet-vpn-unicast inet-vpn-multicast
NLRI for this session: inet-unicast
Peer supports Refresh capability (2)
Stale routes from peer are kept for: 300
Peer does not support Restarter functionality
Restart flag received from the peer: Notification
NLRI that restart is negotiated for: inet-unicast
NLRI of received end-of-rib markers: inet-unicast
NLRI of all end-of-rib markers sent: inet-unicast
Peer does not support LLGR Restarter functionality
Peer supports 4 byte AS extension (peer-as 65100)
Peer does not support Addpath
NLRI(s) enabled for color nexthop resolution: inet-unicast
Table inet.0 Bit: 20000
  RIB State: BGP restart is complete
  Send state: in sync
  Active prefixes:          800000
  Received prefixes:       800000
  Accepted prefixes:       800000
  Suppressed due to damping: 0
  Advertised prefixes:     29788
Prefix-limit dropped routes NLRI: inet-unicast count: 27850
Last traffic (seconds): Received 1   Sent 0   Checked 538
Input messages:  Total 137090   Updates 137070   Refreshes 0   Octets 17371127
Output messages: Total 23022   Updates 23001   Refreshes 0   Octets 3539841
Output Queue[1]: 0               (inet.0, inet-unicast)
Trace options: send refresh
Trace file: /var/log/bgp_refresh size 5242880 files 10

```

```
user@host > show bgp neighbor
```

```
Threading mode: BGP I/O
```

```
Default eBGP mode: advertise - accept, receive - accept
```

```
Groups: 1 Peers: 2 Down peers: 0
```

Table	Tot Paths	Act Paths	Suppressed	History	Damp	State	Pending
inet.0	1629784	829784	0	0	0	0	
bgp.13vpn.0	0	0	0	0	0	0	
bgp.13vpn.2							

Peer	AS	InPkt	OutPkt	OutQ	Flaps	Last Up/Dwn	State #Active/ Received/Accepted/Damped...
10.128.139.6	65100	137070	23013	0	0	8:49	Establ
inet.0: 800000/800000/800000/0							

**NOTE:** This sample output is applicable for both the `prefix-limit` and `accepted-prefix-limit` configuration statements.

**show bgp neighbor (with `hide-excess <percentage>` option configured and exceeding the maximum configured percentage.)**

```

user@host > show bgp neighbor
Peer: 10.128.139.6+50420 AS 65100 Local: 10.128.139.63+179 AS 65100
  Group: ibgp          Routing-Instance: master
  Forwarding routing-instance: master
  Type: Internal      State: Established (route reflector client)Flags: <Sync>
  Last State: OpenConfirm  Last Event: RecvKeepAlive
  Last Error: Cease
  Import: [ list_based_on_as ]
  Options: <LocalAddress KeepNone Cluster AddressFamily PrefixLimit Rib-group Refresh>
  Options: <GracefulShutdownRcv>
  Address families configured: inet-unicast
  Local Address: 10.128.139.63 Holdtime: 90 Preference: 170
  Graceful Shutdown Receiver local-preference: 0
  Prefixlimit configured for NLRI: inet-unicast Limit: 800000 Action: Hide excess
  Number of flaps: 1
  Last flap event: Stop
  Error: 'Cease' Sent: 1 Recv: 0
  Hidden prefixes - Exceeded configured prefix-limits
  Peer ID: 10.128.139.6   Local ID: 10.128.139.63   Active Holdtime: 90
  Keepalive Interval: 30   Group index: 0   Peer index: 0   SNMP index: 0
  I/O Session Thread: bgpio-0 State: Enabled
  BFD: disabled, down
  NLRI for restart configured on peer: inet-unicast
  NLRI advertised by peer: inet-unicast inet-vpn-unicast inet-vpn-multicast
  NLRI for this session: inet-unicast
  Peer supports Refresh capability (2)
  Stale routes from peer are kept for: 300

```

```

Peer does not support Restarter functionality
Restart flag received from the peer: Notification
NLRI that restart is negotiated for: inet-unicast
NLRI of received end-of-rib markers: inet-unicast
NLRI of all end-of-rib markers sent: inet-unicast
Peer does not support LLGR Restarter functionality
Peer supports 4 byte AS extension (peer-as 65100)
Peer does not support Addpath
NLRI(s) enabled for color nexthop resolution: inet-unicast
Table inet.0 Bit: 20000
  RIB State: BGP restart is complete
  Send state: in sync
  Active prefixes:          799908
  Received prefixes:        827581
  Accepted prefixes:        799908
  Suppressed due to damping: 0
  Advertised prefixes:      29826
Prefix-limit hidden routes NLRI: inet-unicast count: 28484
Last traffic (seconds): Received 0   Sent 0   Checked 1028
Input messages:  Total 140272 Updates 140232 Refreshes 0 Octets 17794222
Output messages: Total 46362  Updates 46324 Refreshes 0 Octets 6473287
Output Queue[1]: 0          (inet.0, inet-unicast)
Trace options: send refresh
Trace file: /var/log/bgp_refresh size 5242880 files 10

```

```

user@host > show bgp neighbor
Threading mode: BGP I/O
Default eBGP mode: advertise - accept, receive - accept
Groups: 1 Peers: 2 Down peers: 0
Table      Tot Paths  Act Paths Suppressed    History Damp State    Pending
inet.0
          1657319    829736         0         0         0         0
bgp.l3vpn.0
           0         0         0         0         0         0
bgp.l3vpn.2
           0         0         0         0         0         0
Peer      AS      InPkt    OutPkt    OutQ    Flaps Last Up/Dwn State|#Active/
Received/Accepted/Damped...
10.128.139.6    65100    140669    46482      0        1    18:46 Establ
inet.0: 799916/827583/799916/0

```

**NOTE:** This sample output is applicable for both the `prefix-limit` and `accepted-prefix-limit` configuration statements.

## Release Information

Command introduced before Junos OS Release 7.4.

`orf` option introduced in Junos OS Release 9.2.

`exact-instance` option introduced in Junos OS Release 11.4.

`output-queue` option introduced in Junos OS Release 16.1.

`DontGRHeIpFateSharingBfdDown` is added to the `options` field of the command output in Junos OS Release 18.3R1.

`PurgePending`, `PurgeInProgress`, and `PurgeImpatient` are added to the `Flags` field of the command output in Junos OS Release 19.4R1.

`rib-sharding` option introduced in cRPD Release 20.1R1.

`Prefixlimit` configured for NLRI, `Acceptedprefixlimit` configured for NLRI, `Action`, `Limit`, `Warning percentage`, and `Count` fields are introduced to the `show bgp neighbor` output in Junos OS Release 21.2R1.

`Prefixlimit` configured for NLRI, `Acceptedprefixlimit` configured for NLRI, `Action`, `Limit`, `Warning percentage`, and `Count` fields are introduced to the `show bgp neighbor` output in Junos OS Evolved Release 21.3R1.

## RELATED DOCUMENTATION

| *clear bgp neighbor*

## show log

### IN THIS SECTION

- [Syntax | 1373](#)
- [Syntax \(QFX Series and OCX Series\) | 1373](#)

- Syntax (TX Matrix Router) | 1373
- Description | 1373
- Options | 1374
- Required Privilege Level | 1375
- Sample Output | 1375
- Release Information | 1379

## Syntax

```
show log
<filename / user <username>>
```

## Syntax (QFX Series and OCX Series)

```
show log filename
<device-type (device-id | device-alias)>
```

## Syntax (TX Matrix Router)

```
show log
<all-lcc | lcc number | scc>
<filename / user <username>>
```

## Description

List log files, display log file contents, or display information about users who have logged in to the router or switch.

**NOTE:** On MX Series routers, modifying a configuration to replace a service interface with another service interface is treated as a catastrophic event. When you modify a configuration, the entire configuration associated with the service interface—including NAT pools, rules, and

service sets—is deleted and then re-created for the newly specified service interface. If there are active sessions associated with the service interface that is being replaced, these sessions are deleted and the NAT pools are then released, which leads to the generation of the NAT\_POOL\_RELEASE system log messages. However, because NAT pools are already deleted as a result of the catastrophic configuration change and no longer exist, the NAT\_POOL\_RELEASE system log messages are not generated for the changed configuration.

Options

<b>none</b>	List all log files.
<b>&lt;all-lcc   lcc number   scc&gt;</b>	(Routing matrix only)(Optional) Display logging information about all T640 routers (or line-card chassis) or a specific T640 router (replace <i>number</i> with a value from 0 through 3) connected to a TX Matrix router. Or, display logging information about the TX Matrix router (or switch-card chassis).
<b>device-type</b>	<p>(QFabric system only) (Optional) Display log messages for only one of the following device types:</p> <ul style="list-style-type: none"><li>• director-device—Display logs for Director devices.</li><li>• infrastructure-device—Display logs for the logical components of the QFabric system infrastructure, including the diagnostic Routing Engine, fabric control Routing Engine, fabric manager Routing Engine, and the default network Node group and its backup (NW-NG-0 and NW-NG-0-backup).</li><li>• interconnect-device—Display logs for Interconnect devices.</li><li>• node-device—Display logs for Node devices.</li></ul> <div><p><b>NOTE:</b> If you specify the device-type optional parameter, you must also specify either the device-id or device-alias optional parameter.</p></div>
<b>(device-id   device-alias)</b>	If a device type is specified, display logs for a device of that type. Specify either the device ID or the device alias (if configured).
<b>filename</b>	(Optional) Display the log messages in the specified log file. For the routing matrix, the filename must include the chassis information.



**NOTE:** The *filename* parameter is mandatory for the QFabric system. If you did not configure a syslog filename, specify the default filename of **messages**.

**user**  
**<username>** (Optional) Display logging information about users who have recently logged in to the router or switch. If you include *username*, display logging information about the specified user.

## Required Privilege Level

trace

## Sample Output

### show log

```
user@host> show log
total 57518
-rw-r--r-- 1 root bin      211663 Oct  1 19:44 dcd
-rw-r--r-- 1 root bin      999947 Oct  1 19:41 dcd.0
-rw-r--r-- 1 root bin      999994 Oct  1 17:48 dcd.1
-rw-r--r-- 1 root bin      238815 Oct  1 19:44 rpd
-rw-r--r-- 1 root bin     1049098 Oct  1 18:00 rpd.0
-rw-r--r-- 1 root bin     1061095 Oct  1 12:13 rpd.1
-rw-r--r-- 1 root bin     1052026 Oct  1 06:08 rpd.2
-rw-r--r-- 1 root bin     1056309 Sep 30 18:21 rpd.3
-rw-r--r-- 1 root bin     1056371 Sep 30 14:36 rpd.4
-rw-r--r-- 1 root bin     1056301 Sep 30 10:50 rpd.5
-rw-r--r-- 1 root bin     1056350 Sep 30 07:04 rpd.6
-rw-r--r-- 1 root bin     1048876 Sep 30 03:21 rpd.7
-rw-rw-r-- 1 root bin       19656 Oct  1 19:37 wtmp
```

### show log filename

```
user@host> show log rpd
Oct  1 18:00:18 trace_on: Tracing to ?/var/log/rpd? started
Oct  1 18:00:18 EVENT <MTU> ds-5/2/0.0 index 24 <Broadcast PointToPoint Multicast
```

```

Oct  1 18:00:18
Oct  1 18:00:19 KRT rcv len 56 V9 seq 148 op add Type route/if af 2 addr 192.0.2.21 nhop type
local nhop 192.0.2.21
Oct  1 18:00:19 KRT rcv len 56 V9 seq 149 op add Type route/if af 2 addr 192.0.2.22 nhop type
unicast nhop 192.0.2.22
Oct  1 18:00:19 KRT rcv len 48 V9 seq 150 op add Type ifaddr index 24 devindex 43
Oct  1 18:00:19 KRT rcv len 144 V9 seq 151 op chnge Type ifdev devindex 44
Oct  1 18:00:19 KRT rcv len 144 V9 seq 152 op chnge Type ifdev devindex 45
Oct  1 18:00:19 KRT rcv len 144 V9 seq 153 op chnge Type ifdev devindex 46
Oct  1 18:00:19 KRT rcv len 1272 V9 seq 154 op chnge Type ifdev devindex 47
...

```

```

user@host:LSYS1> show log flow_lsys1.log

```

```

Nov  7 07:34:09 07:34:09.491800:CID-0:THREAD_ID-00:LSYS_ID-01:RT:got route table lock

Nov  7 07:34:09 07:34:09.491809:CID-0:THREAD_ID-00:LSYS_ID-01:RT:released route table lock

Nov  7 07:34:09 07:34:09.491840:CID-0:THREAD_ID-00:LSYS_ID-01:RT:got route table lock

Nov  7 07:34:09 07:34:09.491841:CID-0:THREAD_ID-00:LSYS_ID-01:RT:released route table lock

Nov  7 07:34:09 07:34:09.491854:CID-0:THREAD_ID-00:LSYS_ID-01:RT:cache final sw_nh 0x0

Nov  7 07:34:09 07:34:09.491868:CID-0:THREAD_ID-00:LSYS_ID-01:RT:got route table lock

Nov  7 07:34:09 07:34:09.491869:CID-0:THREAD_ID-00:LSYS_ID-01:RT:released route table lock

Nov  7 07:34:09 07:34:09.491881:CID-0:THREAD_ID-00:LSYS_ID-01:RT:cache final sw_nh 0x0
user@host:TSYS1> show log flow_tsys1.log
Nov  7 13:21:47 13:21:47.217744:CID-0:THREAD_ID-05:LSYS_ID-32:RT:<192.0.2.0/0-
>198.51.100.0/9011;1,0x0> :

```

```

Nov  7 13:21:47 13:21:47.217747:CID-0:THREAD_ID-05:LSYS_ID-32:RT:packet [84] ipid = 39281,
@0x7f490ae56d52

```

```

Nov  7 13:21:47 13:21:47.217749:CID-0:THREAD_ID-05:LSYS_ID-32:RT:---- flow_process_pkt: (thd 5):
flow_ctxt type 0, common flag 0x0, mbuf 0x4882b600, rtbl7

```

```

Nov  7 13:21:47 13:21:47.217752:CID-0:THREAD_ID-05:LSYS_ID-32:RT: flow process pak fast ifl 88
in_ifp lt-0/0/0.101

```

```

Nov  7 13:21:47 13:21:47.217753:CID-0:THREAD_ID-05:LSYS_ID-32:RT: lt-0/0/0.101:192.0.2.0-
>198.51.100.0, icmp, (0/0)

```

```

Nov  7 13:21:47 13:21:47.217756:CID-0:THREAD_ID-05:LSYS_ID-32:RT: find flow: table 0x11d0a2680,
hash 20069(0xffff), sa 192.0.2.0, da 198.51.100.0, sp 0, d0

Nov  7 13:21:47 13:21:47.217760:CID-0:THREAD_ID-05:LSYS_ID-32:RT:Found: session id 0x12. sess
tok 28685

Nov  7 13:21:47 13:21:47.217761:CID-0:THREAD_ID-05:LSYS_ID-32:RT:  flow got session.

Nov  7 13:21:47 13:21:47.217761:CID-0:THREAD_ID-05:LSYS_ID-32:RT:  flow session id 18

Nov  7 13:21:47 13:21:47.217763:CID-0:THREAD_ID-05:LSYS_ID-32:RT: vector bits 0x200 vector
0x84ae85f0

Nov  7 13:21:47 13:21:47.217764:CID-0:THREAD_ID-05:LSYS_ID-32:RT:set nat 0x11e463550(18) timeout
const to 2

Nov  7 13:21:47 13:21:47.217765:CID-0:THREAD_ID-05:LSYS_ID-32:RT: set_nat_timeout 2 on session 18

Nov  7 13:21:47 13:21:47.217765:CID-0:THREAD_ID-05:LSYS_ID-32:RT:refresh nat 0x11e463550(18)
timeout to 2

Nov  7 13:21:47 13:21:47.217767:CID-0:THREAD_ID-05:LSYS_ID-32:RT:insert usp tag for apps

Nov  7 13:21:47 13:21:47.217768:CID-0:THREAD_ID-05:LSYS_ID-32:RT:mbuf 0x4882b600, exit nh
0xffffb0006

```

### show log filename (QFabric System)

```

user@qfabric> show log messages

Mar 28 18:00:06 qfabric chassisd: QFABRIC_INTERNAL_SYSLOG: Mar 28 18:00:06 ED1486 chassisd:
CHASSISD_SNMP_TRAP10: SNMP trap generated: FRU power on (jnxFruContentsIndex 8, jnxFruL1Index 1,
jnxFruL2Index 1, jnxFruL3Index 0, jnxFruName PIC: 48x 10G-SFP+ @ 0/0/*, jnxFruType 11,
jnxFruSlot 0, jnxFruOfflineReason 2, jnxFruLastPowerOff 0, jnxFruLastPowerOn 2159)

Mar 28 18:00:07 qfabric chassisd: QFABRIC_INTERNAL_SYSLOG: Mar 28 18:00:07 ED1486 chassisd:
CHASSISD_SNMP_TRAP10: SNMP trap generated: FRU power on (jnxFruContentsIndex 8, jnxFruL1Index 1,
jnxFruL2Index 2, jnxFruL3Index 0, jnxFruName PIC: @ 0/1/*, jnxFruType 11, jnxFruSlot 0,
jnxFruOfflineReason 2, jnxFruLastPowerOff 0, jnxFruLastPowerOn 2191)

Mar 28 18:00:07 qfabric chassisd: QFABRIC_INTERNAL_SYSLOG: Mar 28 18:00:07 ED1492 chassisd:
CHASSISD_SNMP_TRAP10: SNMP trap generated: FRU power on (jnxFruContentsIndex 8, jnxFruL1Index 1,
jnxFruL2Index 1, jnxFruL3Index 0, jnxFruName PIC: 48x 10G-SFP+ @ 0/0/*, jnxFruType 11,

```

```
jnxFruSlot 0, jnxFruOfflineReason 2, jnxFruLastPowerOff 0, jnxFruLastPowerOn 242726)
Mar 28 18:00:07 qfabric chassisd: QFABRIC_INTERNAL_SYSLOG: Mar 28 18:00:07 ED1492 chassisd:
CHASSISD_SNMP_TRAP10: SNMP trap generated: FRU power on (jnxFruContentsIndex 8, jnxFruL1Index 1,
jnxFruL2Index 2, jnxFruL3Index 0, jnxFruName PIC: @ 0/1/*, jnxFruType 11, jnxFruSlot 0,
jnxFruOfflineReason 2, jnxFruLastPowerOff 0, jnxFruLastPowerOn 242757)
Mar 28 18:00:16 qfabric file: QFABRIC_INTERNAL_SYSLOG: Mar 28 18:00:16 ED1486 file: UI_COMMIT:
User 'root' requested 'commit' operation (comment: none)
Mar 28 18:00:27 qfabric file: QFABRIC_INTERNAL_SYSLOG: Mar 28 18:00:27 ED1486 file: UI_COMMIT:
User 'root' requested 'commit' operation (comment: none)
Mar 28 18:00:50 qfabric file: QFABRIC_INTERNAL_SYSLOG: Mar 28 18:00:50 _DCF_default___NW-
INE-0_RE0_ file: UI_COMMIT: User 'root' requested 'commit' operation (comment: none)
Mar 28 18:00:50 qfabric file: QFABRIC_INTERNAL_SYSLOG: Mar 28 18:00:50 _DCF_default___NW-
INE-0_RE0_ file: UI_COMMIT: User 'root' requested 'commit' operation (comment: none)
Mar 28 18:00:55 qfabric file: QFABRIC_INTERNAL_SYSLOG: Mar 28 18:00:55 ED1492 file: UI_COMMIT:
User 'root' requested 'commit' operation (comment: none)
Mar 28 18:01:10 qfabric file: QFABRIC_INTERNAL_SYSLOG: Mar 28 18:01:10 ED1492 file: UI_COMMIT:
User 'root' requested 'commit' operation (comment: none)
Mar 28 18:02:37 qfabric chassisd: QFABRIC_INTERNAL_SYSLOG: Mar 28 18:02:37 ED1491 chassisd:
CHASSISD_SNMP_TRAP10: SNMP trap generated: FRU power on (jnxFruContentsIndex 8, jnxFruL1Index 1,
jnxFruL2Index 1, jnxFruL3Index 0, jnxFruName PIC: 48x 10G-SFP+ @ 0/0/*, jnxFruType 11,
jnxFruSlot 0, jnxFruOfflineReason 2, jnxFruLastPowerOff 0, jnxFruLastPowerOn 33809)
```

## show log user

```
user@host> show log user
```

usera	mg2546		Thu Oct 1 19:37	still logged in
usera	mg2529		Thu Oct 1 19:08 - 19:36	(00:28)
usera	mg2518		Thu Oct 1 18:53 - 18:58	(00:04)
root	mg1575		Wed Sep 30 18:39 - 18:41	(00:02)
root	ttyp2	aaa.bbbb.com	Wed Sep 30 18:39 - 18:41	(00:02)
userb	ttyp1	192.0.2.0	Wed Sep 30 01:03 - 01:22	(00:19)

## show log accepted-traffic (SRX4600, SRX5400, SRX5600, and SRX5800)

```
user@host> show log accepted-traffic
```

```
Jul 17 20:26:04 sourpunch RT_FLOW: RT_FLOW_SESSION_CREATE: session created 3.3.3.5/2-
>4.4.4.2/63 0x0 None 3.3.3.5/2->4.4.4.2/63 0x0 N/A N/A N/A N/A 17 p2 TRUST UNTRUST 2617282058
N/A(N/A) xe-7/0/0.0 UNKNOWN UNKNOWN UNKNOWN N/A N/A -1 N/A N/A N/A
Jul 17 20:26:04 sourpunch RT_FLOW: RT_FLOW_SESSION_CREATE: session created 3.3.3.4/4-
```

```

>4.4.4.2/63 0x0 None 3.3.3.4/4->4.4.4.2/63 0x0 N/A N/A N/A N/A 17 p2 TRUST UNTRUST 2550162754
N/A(N/A) xe-7/0/0.0 UNKNOWN UNKNOWN UNKNOWN N/A N/A -1 N/A N/A N/A
Jul 17 20:26:04 sourpunch RT_FLOW: RT_FLOW_SESSION_CREATE: session created 3.3.3.4/1-
>4.4.4.2/63 0x0 None 3.3.3.4/1->4.4.4.2/63 0x0 N/A N/A N/A N/A 17 p2 TRUST UNTRUST 2550162755
N/A(N/A) xe-7/0/0.0 UNKNOWN UNKNOWN UNKNOWN N/A N/A -1 N/A N/A N/A
Jul 17 20:26:04 sourpunch RT_FLOW: RT_FLOW_SESSION_CREATE: session created 3.3.3.3/0-
>4.4.4.2/63 0x0 None 3.3.3.3/0->4.4.4.2/63 0x0 N/A N/A N/A N/A 17 p2 TRUST UNTRUST 2550162752
N/A(N/A) xe-7/0/0.0 UNKNOWN UNKNOWN UNKNOWN N/A N/A -1 N/A N/A N/A
Jul 17 20:26:04 sourpunch RT_FLOW: RT_FLOW_SESSION_CREATE: session created 3.3.3.5/5-
>4.4.4.2/63 0x0 None 3.3.3.5/5->4.4.4.2/63 0x0 N/A N/A N/A N/A 17 p2 TRUST UNTRUST 2550162751
N/A(N/A) xe-7/0/0.0 UNKNOWN UNKNOWN UNKNOWN N/A N/A -1 N/A N/A N/A
Jul 17 20:26:04 sourpunch RT_FLOW: RT_FLOW_SESSION_CREATE: session created 3.3.3.3/3-
>4.4.4.2/63 0x0 None 3.3.3.3/3->4.4.4.2/63 0x0 N/A N/A N/A N/A 17 p2 TRUST UNTRUST 2550162753
N/A(N/A) xe-7/0/0.0 UNKNOWN UNKNOWN UNKNOWN N/A N/A -1 N/A N/A N/A

```

## Release Information

Command introduced before Junos OS Release 7.4.

Option *device-type* (*device-id* | *device-alias*) is introduced in Junos OS Release 13.1 for the QFX Series.

## RELATED DOCUMENTATION

| [syslog \(System\)](#)

## show (ospf | ospf3) overview

### IN THIS SECTION

- [Syntax | 1380](#)
- [Syntax \(EX Series Switch and QFX Series\) | 1380](#)
- [Description | 1380](#)
- [Options | 1380](#)
- [Required Privilege Level | 1381](#)
- [Output Fields | 1381](#)

- [Sample Output | 1384](#)
- [Release Information | 1387](#)

## Syntax

```
show (ospf | ospf3) overview
<brief | extensive>
<instance instance-name>
<logical-system (all | logical-system-name)>
<realm (ipv4-multicast | ipv4-unicast | ipv6-multicast)>
```

## Syntax (EX Series Switch and QFX Series)

```
show (ospf | ospf3) overview
<brief | extensive>
<instance instance-name>
```

## Description

Display Open Shortest Path First (OSPF) overview information.

## Options

<b>none</b>	Display standard information about all OSPF neighbors for all routing instances.
<b>brief   extensive</b>	(Optional) Display the specified level of output.
<b>instance <i>instance-name</i></b>	(Optional) Display all OSPF interfaces under the named routing instance.
<b>logical-system (all   <i>logical-system-name</i>)</b>	(Optional) Perform this operation on all logical systems or on a particular logical system.

**realm (ipv4-multicast | ipv4-unicast | ipv6-multicast)** (Optional) (OSPFv3 only) Display information about the specified OSPFv3 realm, or address family. Use the `realm` option to specify an address family for OSPFv3 other than IPv6 unicast, which is the default.

### Required Privilege Level

view

### Output Fields

[Table 51 on page 1381](#) lists the output fields for the `show ospf overview` command. Output fields are listed in the approximate order in which they appear.

**Table 51: show ospf overview Output Fields**

Field name	Field Description	Level of Output
Instance	OSPF routing instance.	All levels
Router ID	Router ID of the routing device.	All levels
Route table index	Route table index.	All levels
Configured overload	Overload capability is enabled. If the overload timer is also configured, display the time that remains before it is set to expire. This field is not displayed after the timer expires.	All levels
Topology	Topology identifier.	All levels
Prefix export count	Number of prefixes exported into OSPF.	All levels
Full SPF runs	Number of complete Shortest Path First calculations.	All levels
SPF delay	Delay before performing consecutive Shortest Path First calculations.	All levels

Table 51: show ospf overview Output Fields *(Continued)*

Field name	Field Description	Level of Output
SPF holddown	Delay before performing additional Shortest Path First (SPF) calculations after the maximum number of consecutive SPF calculations is reached.	All levels
SPF rapid runs	Maximum number of Shortest Path First calculations that can be performed in succession before the hold-down timer begins.	All levels
LSA refresh time	Refresh period for link-state advertisement (in minutes).	All levels
SPRING	Source protocol routing in networking: enable or disable.	All levels
Node Segments	Nodes of source protocol routing in networking:enable or disable.	All levels
Ipv4 Index	Ipv4 Index.	All levels
Index Range	Ipv4 Index range.	All levels
Node Segment Blocks Allocated	Details about node segment blocks.	All levels
Database protection state	Current state of database protection.	All levels
Warning threshold	Threshold at which a warning message is logged (percentage of maximum LSA count).	All levels
Non self-generated LSAs	Number of LSAs whose router ID is not equal to the local router ID: Current, Warning (threshold), and Allowed.	All levels
Ignore time	How long the database has been in the ignore state.	All levels
Reset time	How long the database must stay out of the ignore or isolated state before it returns to normal operations.	All levels



Table 51: show ospf overview Output Fields (*Continued*)

Field name	Field Description	Level of Output
Ignore count	Number of times the database has been in the ignore state: Current and Allowed.	All levels
Restart	Graceful restart capability: enabled or disabled.	All levels
Restart duration	Time period for complete reacquisition of OSPF neighbors.	All levels
Restart grace period	Time period for which the neighbors should consider the restarting routing device as part of the topology.	All levels
Graceful restart helper mode	(OSPFv2) Standard graceful restart helper capability (based on RFC 3623): enabled or disabled.	All levels
Restart-signaling helper mode	(OSPFv2) Restart signaling-based graceful restart helper capability (based on RFC 4811, RFC 4812, and RFC 4813): enabled or disabled.	All levels
Helper mode	(OSPFv3) Graceful restart helper capability: enabled or disabled.	All levels
Trace options	OSPF-specific trace options.	extensive
Trace file	Name of the file to receive the output of the tracing operation.	extensive
Area	Area number. Area 0.0.0.0 is the backbone area.	All levels
Stub type	Stub type of area: Normal Stub, Not Stub, or Not so Stubby Stub.	All levels
Authentication Type	Type of authentication: None, Password, or MD5.  <b>NOTE:</b> The Authentication Type field refers to the authentication configured at the <code>[edit protocols ospf area <i>area-id</i>]</code> level. Any authentication configured for an interface in this area will not affect the value of this field.	All levels

**Table 51: show ospf overview Output Fields (Continued)**

Field name	Field Description	Level of Output
Area border routers	Number of area border routers.	All levels
Neighbors	Number of autonomous system boundary routers.	All levels

## Sample Output

### show ospf overview (without SRGB)

```

user@host> show ospf overview
Instance: master
  Router ID: 10.255.245.6
  Route table index: 0
    Configured overload, expires in 118 seconds
  LSA refresh time: 50 minutes
  SPRING: Enabled
  Node Segments: Enabled
  Ipv4 Index : 10, Index Range: 2048
  Node Segment Blocks Allocated:
    Start Index : 0, Size : 256, Label-Range: [ 802048, 802303 ]
    Start Index : 256, Size : 256, Label-Range: [ 802304, 802559 ]
    Start Index : 512, Size : 256, Label-Range: [ 802560, 802815 ]
    Start Index : 768, Size : 256, Label-Range: [ 802816, 803071 ]
    Start Index : 1024, Size : 256, Label-Range: [ 803072, 803327 ]
    Start Index : 1280, Size : 256, Label-Range: [ 803328, 803583 ]
    Start Index : 1536, Size : 256, Label-Range: [ 803584, 803839 ]
    Start Index : 1792, Size : 256, Label-Range: [ 803840, 804095 ]
  Restart: Enabled
    Restart duration: 20 sec
    Restart grace period: 40 sec
    Helper mode: enabled
  Area: 0.0.0.0
    Stub type: Not Stub
    Authentication Type: None
    Area border routers: 0, AS boundary routers: 0
  Neighbors

```

```

    Up (in full state): 0
Topology: default (ID 0)
Prefix export count: 0
Full SPF runs: 1
SPF delay: 0.200000 sec, SPF holddown: 5 sec, SPF rapid runs: 3

```

### **show ospf overview (with SRGB)**

```

user@host> show ospf overview
Instance: master
Router ID: 10.10.10.10
Route table index: 0
LSA refresh time: 50 minutes
Traffic engineering
SPRING: Enabled
SRGB Config Range :
  SRGB Start-Label : 1000, SRGB Index-Range : 2000
SRGB Block Allocation: Success
  SRGB Start Index : 1000, SRGB Size : 2000, Label-Range: [ 1000, 2999 ]
Node Segments: Enabled
Ipv4 Index : 1000
Post Convergence Backup: Disabled
Area: 0.0.0.0
  Stub type: Not Stub
  Authentication Type: None
  Area border routers: 0, AS boundary routers: 0
Neighbors
  Up (in full state): 3
Topology: default (ID 0)
Prefix export count: 0
Full SPF runs: 5
SPF delay: 0.200000 sec, SPF holddown: 5 sec, SPF rapid runs: 3
Backup SPF: Enabled, Remote Backup calculation enabled

```

### **show ospf overview (With Database Protection)**

```

user@host> show ospf overview
Instance: master
Router ID: 10.255.112.218

```

```

Route table index: 0
LSA refresh time: 50 minutes
Traffic engineering
Restart: Enabled
  Restart duration: 180 sec
  Restart grace period: 210 sec
  Graceful restart helper mode: Enabled
  Restart-signaling helper mode: Enabled
Database protection state: Normal
  Warning threshold: 70 percent
  Non self-generated LSAs: Current 582, Warning 700, Allowed 1000
  Ignore time: 30, Reset time: 60
  Ignore count: Current 0, Allowed 1
Area: 0.0.0.0
  Stub type: Not Stub
  Authentication Type: None
  Area border routers: 0, AS boundary routers: 0
  Neighbors
    Up (in full state): 160
Topology: default (ID 0)
  Prefix export count: 0
  Full SPF runs: 70
  SPF delay: 0.200000 sec, SPF holddown: 5 sec, SPF rapid runs: 3
  Backup SPF: Not Needed

```

### **show ospf3 overview (With Database Protection)**

```

user@host> show ospf3 overview
Instance: master
  Router ID: 10.255.112.128
  Route table index: 0
  LSA refresh time: 50 minutes
  Database protection state: Normal
    Warning threshold: 80 percent
    Non self-generated LSAs: Current 3, Warning 8, Allowed 10
    Ignore time: 30, Reset time: 60
    Ignore count: Current 0, Allowed 2
Area: 0.0.0.0
  Stub type: Not Stub
  Area border routers: 0, AS boundary routers: 0
  Neighbors

```

```

    Up (in full state): 1
Topology: default (ID 0)
Prefix export count: 0
Full SPF runs: 7
SPF delay: 0.200000 sec, SPF holddown: 5 sec, SPF rapid runs: 3
Backup SPF: Not Needed

```

## show ospf overview extensive

```

user@host> show ospf overview extensive
Instance: master
Router ID: 1.1.1.103
Route table index: 0
Full SPF runs: 13, SPF delay: 0.200000 sec
LSA refresh time: 50 minutes
Restart: Disabled
Trace options: lsa
Trace file: /var/log/ospf size 131072 files 10
Area: 0.0.0.0
Stub type: Not Stub
Authentication Type: None
Area border routers: 0, AS boundary routers: 0
Neighbors
Up (in full state): 1

```

## Release Information

Command introduced in Junos OS Release 7.4.

realm option introduced in Junos OS Release 9.2.

Database protection introduced in Junos 10.2.

## show chassis dedicated-ukern-cpu

### IN THIS SECTION

- [Syntax | 1388](#)
- [Description | 1388](#)
- [Options | 1388](#)
- [Required Privilege Level | 1388](#)
- [Output Fields | 1388](#)
- [Sample Output | 1389](#)
- [Release Information | 1389](#)

### Syntax

```
show chassis dedicated-ukern-cpu
```

### Description

Display whether dedicated Bidirectional Forwarding Detection (BFD) is enabled or disabled. If dedicated BFD is enabled, the output of the show command displays the value of the Dedicated Ukern CPU Status field as Enabled.

### Options

This command has no options.

### Required Privilege Level

view

### Output Fields

When you enter this command, you are provided feedback on the status of your request.

## Sample Output

### show chassis dedicated-ukern-cpu

```
user@host> show chassis dedicated-ukern-cpu
Dedicated Ukern CPU Status: Enabled
```

## Release Information

Command introduced in Junos OS Release 15.1X49-D100.

## RELATED DOCUMENTATION

Enabling Dedicated and Real-Time BFD on SRX Devices

[dedicated-ukern-cpu \(BFD\) | 940](#)

Understanding BFD for BGP

## show chassis in-service-upgrade

### IN THIS SECTION

- [Syntax | 1390](#)
- [Description | 1390](#)
- [Options | 1390](#)
- [Required Privilege Level | 1390](#)
- [Output Fields | 1390](#)
- [Sample Output | 1391](#)
- [Release Information | 1394](#)

Syntax

```
show chassis in-service-upgrade
```

Description

Display the status of Flexible PIC Concentrators (FPCs) and their corresponding PICs after the most recent unified in-service software upgrade (ISSU). This command must be issued on the primary Routing Engine.

**NOTE:** Only Intelligent Queuing (IQ) PICs are displayed by this command output. Unified ISSU status for other PIC types is controlled internally by the FPC.

Options

This command has no options.

Required Privilege Level

view

Output Fields

Table 52 on page 1390 lists the output fields for the show chassis in-service-upgrade command. Output fields are listed in the approximate order in which they appear.

Table 52: show chassis in-service-upgrade Output Fields

Field Name	Field Description
Item	Flexible PIC Concentrator (FPC) slot number.
Status	FPC and corresponding PIC state. State can be either of the following: <ul style="list-style-type: none"><li>• Online—FPC is online and running.</li><li>• Offline—FPC is powered down.</li></ul>



**Table 52: show chassis in-service-upgrade Output Fields *(Continued)***

Field Name	Field Description
Reason	Reason for the state (if offline).

## Sample Output

### show chassis in-service-upgrade

```

user@host> show chassis in-service-upgrade
  Item           Status           Reason
  FPC 0          Online
  FPC 1          Online
  FPC 2          Online
  PIC 0          Online
  PIC 1          Online
  FPC 3          Offline          Offlined by CLI command
  FPC 4          Online
  PIC 1          Online
  FPC 5          Online
  PIC 0          Online
  FPC 6          Online
  PIC 3          Online
  FPC 7          Online

```

### show chassis in-service-upgrade (MX2010 Router)

```

user@host> show chassis in-service-upgrade
  Item           Status           Reason
  FPC 0          Online
  FPC 1          Online
  FPC 8          Online
  FPC 9          Online

```

**show chassis in-service-upgrade (MX2020 Router)**

```
user@host> show chassis in-service-upgrade
```

Item	Status	Reason
FPC 0	Online	
FPC 1	Online	
FPC 2	Online	
FPC 3	Online	
FPC 4	Online	
FPC 5	Online	
FPC 6	Online	
FPC 7	Online	
FPC 8	Online	
FPC 9	Online	
FPC 10	Online	
FPC 11	Online	
FPC 12	Online	
FPC 13	Online	
FPC 14	Online	
FPC 15	Online	
FPC 16	Online	
FPC 17	Online	
FPC 18	Online	
FPC 19	Online	

**show chassis in-service-upgrade (MX2008 Router)**

```
user@host> show chassis in-service-upgrade
```

Item	Status	Reason
FPC 0	Online	
FPC 3	Online	
FPC 5	Online	
FPC 7	Online	
FPC 9	Online	

**show chassis in-service-upgrade (TX Matrix Plus Router)**

```
user@host> show chassis in-service-upgrade
```

```
lcc0-re0:
```

-----		
Item	Status	Reason
FPC 1	Online	
PIC 0	Online	
FPC 2	Online	
FPC 3	Online	
PIC 1	Online	
FPC 4	Online	
FPC 6	Online	
FPC 7	Online	
lcc1-re0:		
-----		
Item	Status	Reason
FPC 0	Online	
PIC 3	Online	
FPC 1	Online	
FPC 2	Online	
FPC 4	Online	
FPC 6	Online	
FPC 7	Online	
lcc2-re0:		
-----		
Item	Status	Reason
FPC 0	Online	
FPC 2	Online	
FPC 3	Online	
PIC 0	Online	
FPC 4	Online	
FPC 6	Online	
FPC 7	Online	
PIC 1	Online	
lcc3-re0:		
-----		
Item	Status	Reason
FPC 0	Online	
PIC 0	Online	
FPC 1	Online	
FPC 2	Online	
FPC 3	Online	
PIC 2	Online	

FPC 4	Online
FPC 5	Online
FPC 6	Online
FPC 7	Online
PIC 1	Online

**show chassis in-service-upgrade (QFX5100 Switch)**

```
user@switch> show chassis in-service-upgrade
```

Item	Status	Reason
FPC 0	Online (ISSU)	

**show chassis in-service-upgrade (EX9253 Switch)**

```
user@switch> show chassis in-service-upgrade
```

Item	Status	Reason
FPC 0	Online	
FPC 1	Online	

**Release Information**

Command introduced in Junos OS Release 9.0.

**RELATED DOCUMENTATION**

<i>request system software abort</i>
<a href="#">request system software in-service-upgrade   1270</a>
Getting Started with Unified In-Service Software Upgrade
Example: Performing a Unified ISSU

## show chassis realtime-ukern-thread

### IN THIS SECTION

- [Syntax | 1395](#)
- [Description | 1395](#)
- [Options | 1395](#)
- [Required Privilege Level | 1395](#)
- [Output Fields | 1395](#)
- [Sample Output | 1396](#)
- [Release Information | 1396](#)

### Syntax

```
show chassis realtime-ukern-thread
```

### Description

Display whether real-time Bidirectional Forwarding Detection (BFD) is enabled or disabled. If real-time BFD is enabled, the output of the show command displays the value of the realtime Ukern thread Status field as Enabled.

### Options

This command has no options.

### Required Privilege Level

view

### Output Fields

When you enter this command, you are provided feedback on the status of your request.

## Sample Output

### show chassis realtime-ukern-thread

```
user@host> show chassis realtime-ukern-thread
realtime Ukern thread Status: Enabled
```

## Release Information

Command introduced in Junos OS Release 15.1X49-D100.

## RELATED DOCUMENTATION

Enabling Dedicated and Real-Time BFD on SRX Devices

[realtime-ukern-thread \(BFD\) | 941](#)

Understanding BFD for BGP

## show chassis redundancy feb

### IN THIS SECTION

- [Syntax | 1397](#)
- [Description | 1397](#)
- [Options | 1397](#)
- [Required Privilege Level | 1397](#)
- [Output Fields | 1397](#)
- [Sample Output | 1399](#)
- [Release Information | 1400](#)

## Syntax

```
show chassis redundancy feb
<errors>
<redundancy-group group-name>
```

## Description

(M120 routers only) Display information about the status of configured Forwarding Engine Board (FEB) redundancy groups.

## Options

- none** Display information about the status of all configured FEB redundancy groups.
- redundancy-group *group-name*** (Optional) Display information about the specified configured redundancy group.
- errors** (Optional) Display information about any errors encountered on the components in configured redundancy groups or on links between a FEB and a Flexible PIC Concentrator (FPC).

## Required Privilege Level

view

## Output Fields

[Table 53 on page 1397](#) lists the output fields for the `show chassis redundancy feb` command. Output fields are listed in the approximate order in which they appear.

**Table 53: show chassis redundancy feb Output Fields**

Field name	Field Description
<b>Group</b>	Name of configured redundancy group.
<b>FEB</b>	Slot number of each FEB included in redundancy groups.

Table 53: show chassis redundancy feb Output Fields *(Continued)*

Field name	Field Description
<b>State</b>	State of each FEB: <ul style="list-style-type: none"> <li>• <b>Online</b>—FEB is online and running.</li> <li>• <b>Offline</b>—FEB is powered down.</li> </ul>
<b>Priority</b>	(Standard and <b>redundancy-group</b> option) Status of FEB in the redundancy group: <b>Backup</b> , <b>Primary</b> , <b>Other</b> , or null.
<b>Connected FPCs</b>	(Standard and <b>redundancy-group</b> option) Slot number of each FPC connected to the FEB. The status <b>Check</b> is displayed when an error might have occurred.
<b>Redundancy State</b>	(Standard and <b>redundancy-group</b> option) Status of the FEB: <ul style="list-style-type: none"> <li>• <b>Active</b>—FEB is currently active.</li> <li>• <b>Ready</b>—Backup FEB is ready for a switchover</li> <li>• <b>Not Ready</b>—Backup FEB is not ready for a switchover.</li> </ul>
<b>Auto-failover</b>	(Standard and <b>redundancy-group</b> option) Automatic failover status of redundancy group: <b>Enabled</b> or <b>Disabled</b> .
<b>Switch-reason</b>	(Standard and <b>redundancy-group</b> option) Reason a switchover occurred to the backup FEB in the redundancy group.
<b>Hard error: Yes</b>	( <b>errors</b> option only) Displayed when a hard error occurs on a FEB.
<b>FPC</b>	( <b>errors</b> option only) Slot number and status of FPC: <b>link ok</b> or <b>link error</b> .
<b>Fabric plane</b>	( <b>errors</b> option only) Slot number and status of fabric plane.



## Sample Output

### show chassis redundancy feb

```
user@host> show chassis redundancy feb
Group:      cfpc
  FEB  State          Priority  Connected FPCs  Redundancy state
  0    Offline         Backup           5              Active
  1    Online           Primary          0              Active
Auto-failover: Enabled
Group:      grp0
  FEB  State          Priority  Connected FPCs  Redundancy state
  3    Offline         Backup           0              Active
  5    Online           Primary          0              Active
Auto-failover: Enabled
```

### show chassis redundancy feb redundancy-group grp1

```
user@host> show chassis redundancy feb redundancy-group grp1
Group:      grp1
  FEB  State          Priority  Connected FPCs  Redundancy state
  0    Online          Other      0              Active
  1    Online          Other      1              Active
  4    Online          Primary   4              Active
  5    Online          Backup    0              Ready
Autofailover: Enabled
Switch-reason: Switchover from CLI
```

### show chassis redundancy feb redundancy-group grp0 errors

```
user@host> show chassis redundancy feb redundancy-group grp0 errors
Group: grp0
  FEB: 0    State: Online
        FPC 0 link OK
        Fabric plane 0 OK
        Fabric plane 1 OK
        Fabric plane 2 OK
        Fabric plane 3 OK
```

```

FEB: 1    State: Online
  FPC 0 link OK
  Fabric plane 0 OK
  Fabric plane 1 OK
  Fabric plane 2 OK
  Fabric plane 3 OK
FEB: 2    State: Online
  FPC 2 link OK
  Fabric plane 0 OK
  Fabric plane 1 OK
  Fabric plane 2 OK
  Fabric plane 3 OK
FEB: 3    State: Online
  FPC 3 link OK
  Fabric plane 0 OK
  Fabric plane 1 OK
  Fabric plane 2 OK
  Fabric plane 3 OK
FEB: 4    State: Online
  FPC 4 link OK
  Fabric plane 0 OK
  Fabric plane 1 OK
  Fabric plane 2 OK
  Fabric plane 3 OK
FEB: 5    State: Online
  FPC 5 link OK
  Fabric plane 0 OK
  Fabric plane 1 OK
  Fabric plane 2 OK
  Fabric plane 3 OK

```

## Release Information

Command introduced in Junos OS Release 8.2.

## RELATED DOCUMENTATION

[request chassis redundancy feb slot | 1236](#)

Configuring FEB Redundancy on the M120 Router

[Understanding Switching Control Board Redundancy | 15](#)

## show chassis high-availability data-plane statistics

### IN THIS SECTION

- [Syntax | 1401](#)
- [Description | 1401](#)
- [Required Privilege Level | 1401](#)
- [Output Fields | 1401](#)
- [Sample Output | 1404](#)
- [Release Information | 1406](#)

### Syntax

```
show chassis high-availability data-plane statistics
```

### Description

Display Multinode High Availability data plane statistics.

### Required Privilege Level

view

### Output Fields

**Table 54: show chassis cluster data-plane statistics Output Fields**

Field Name	Field Description
Services Synchronized	<ul style="list-style-type: none"> <li>• Service name—Name of the service.</li> <li>• Translation context—Messages synchronizing Network Address Translation (NAT) translation context.</li> <li>• Incoming NAT—Messages synchronizing incoming Network Address Translation (NAT) service.</li> <li>• Resource manager—Messages synchronizing resource manager groups and resources.</li> <li>• DS-LITE create—Messages synchronizing DS-LITE create sessions.</li> <li>• Session create—Messages synchronizing session creation.</li> <li>• IPv6 session create—Messages synchronizing IPv6 session create sessions.</li> <li>• IPv4/6 session RT0 ACK—Messages synchronizing IPv4/6 session RTO ACK sessions.</li> <li>• Session close—Messages synchronizing session close.</li> <li>• IPv6 session close—Messages synchronizing IPv6 session close sessions.</li> <li>• Session change—Messages synchronizing session change.</li> <li>• IPv6 session change—Messages synchronizing IPv6 session change sessions.</li> <li>• ALG Support Library—Messages synchronizing ALG Support Library sessions.</li> <li>• Gate create—Messages synchronizing creation of pinholes (temporary openings in the firewall).</li> <li>• Session ageout refresh request—Messages synchronizing request session after age-out.</li> <li>• IPv6 session ageout refresh requests—Messages synchronizing IPv6 session ageout refresh requests.</li> <li>• Session ageout refresh replies—Messages synchronizing reply session after age-out.</li> </ul>

Table 54: show chassis cluster data-plane statistics Output Fields (Continued)

Field Name	Field Description
	<ul style="list-style-type: none"> <li>• IPv6 session ageout refresh replies—Messages synchronizing IPv6 session ageout refresh replies sessions.</li> <li>• IPsec VPN—Messages synchronizing VPN session.</li> <li>• Firewall user authentication—Messages synchronizing firewall user authentication session.</li> <li>• MGCP ALG—Messages synchronizing MGCP ALG sessions.</li> <li>• H323 ALG—Messages synchronizing H.323 ALG sessions.</li> <li>• SIP ALG—Messages synchronizing SIP ALG sessions.</li> <li>• SCCP ALG—Messages synchronizing SCCP ALG sessions.</li> <li>• PPTP ALG—Messages synchronizing PPTP ALG sessions.</li> <li>• JSF PPTP ALG—Messages synchronizing JSF PPTP ALG sessions.</li> <li>• RPC ALG—Messages synchronizing RPC ALG sessions.</li> <li>• RTSP ALG—Messages synchronizing RTSP ALG sessions.</li> <li>• RAS ALG—Messages synchronizing RAS ALG sessions.</li> <li>• MAC address learning—Messages synchronizing MAC address learning sessions.</li> <li>• GPRS GTP—Messages synchronizing GPRS GTP sessions.</li> <li>• GPRS SCTP—Messages synchronizing GPRS SCTP sessions.</li> <li>• GPRS FRAMEWORK—Messages synchronizing GPRS FRAMEWORK sessions.</li> <li>• JSF RTSP ALG—Messages synchronizing JSF RTSP ALG sessions.</li> <li>• JSF SUNRPC MAP—Messages synchronizing JSF SUNRPC MAP sessions.</li> <li>• JSF MSRPC MAP—Messages synchronizing JSF MSRPC MAP sessions.</li> <li>• DS-LITE delete—Messages synchronizing DS-LITE delete sessions.</li> <li>• JSF SLB—Messages synchronizing JSF SLB sessions.</li> </ul>

**Table 54: show chassis cluster data-plane statistics Output Fields (Continued)**

Field Name	Field Description
	<ul style="list-style-type: none"> <li>• APPID—Messages synchronizing APPID sessions.</li> <li>• JSF MGCP MAP—Messages synchronizing JSF MGCP MAP sessions.</li> <li>• JSF H323 ALG—Messages synchronizing JSF H323 ALG sessions.</li> <li>• JSF RAS ALG—Messages synchronizing JSF RAS ALG sessions.</li> <li>• JSF SCCP MAP—Messages synchronizing JSF SCCP MAP sessions.</li> <li>• JSF SIP MAP—Messages synchronizing JSF SIP MAP sessions.</li> <li>• PST_NAT_CREATE—Messages synchronizing PST NAT CREATE sessions.</li> <li>• PST_NAT_CLOSE—Messages synchronizing PST NAT CLOSE sessions.</li> <li>• PST_NAT_UPDATE—Messages synchronizing PST NAT UPDATE sessions.</li> <li>• JSF TCP STACK—Messages synchronizing JSF TCP STACK sessions.</li> <li>• JSF IKE ALG—Messages synchronizing JSF IKE ALG sessions.</li> </ul>

## Sample Output

### show chassis high-availability data-plane statistics

```

user@host> show chassis high-availability data-plane
statistics
Services Synchronized:
  Service name           RT0s sent  RT0s received
  Translation context    0          0
  Incoming NAT           0          0
  Resource manager       0          0
  DS-LITE create         0          0
  Session create         0          0
  IPv6 session create    0          0
  IPv4/6 session RT0 ACK 0          0
  Session close          0          0
  IPv6 session close     0          0

```

Session change	0	0
IPv6 session change	0	0
ALG Support Library	0	0
Gate create	0	0
Session ageout refresh requests	0	0
IPv6 session ageout refresh requests	0	0
Session ageout refresh replies	0	0
IPv6 session ageout refresh replies	0	0
IPSec VPN	0	0
Firewall user authentication	0	0
MGCP ALG	0	0
H323 ALG	0	0
SIP ALG	0	0
SCCP ALG	0	0
PPTP ALG	0	0
JSF PPTP ALG	0	0
RPC ALG	0	0
RTSP ALG	0	0
RAS ALG	0	0
MAC address learning	0	0
GPRS GTP	0	0
GPRS SCTP	0	0
GPRS FRAMEWORK	0	0
JSF RTSP ALG	0	0
JSF SUNRPC MAP	0	0
JSF MSRPC MAP	0	0
DS-LITE delete	0	0
JSF SLB	0	0
APPID	0	0
JSF MGCP MAP	0	0
JSF H323 ALG	0	0
JSF RAS ALG	0	0
JSF SCCP MAP	0	0
JSF SIP MAP	0	0
PST_NAT_CREATE	0	0
PST_NAT_CLOSE	0	0
PST_NAT_UPDATE	0	0
JSF TCP STACK	0	0
JSF IKE ALG	0	0

## Release Information

Command introduced in Junos OS Release 20.4R1.

## RELATED DOCUMENTATION

| [clear chassis high-availability data-plane statistics](#) | [1226](#)

# show chassis high-availability information

## IN THIS SECTION

- [Syntax](#) | [1406](#)
- [Description](#) | [1406](#)
- [Required Privilege Level](#) | [1406](#)
- [Output Fields](#) | [1407](#)
- [Sample Output](#) | [1410](#)
- [Release Information](#) | [1415](#)

## Syntax

```
show chassis high-availability information
```

## Description

Display details of the Multinode High Availability status on your security device including health status of the peer node.

## Required Privilege Level

view



## Output Fields

Table 55 on page 1407 lists the output fields for the `show chassis high-availability information` command. Output fields are listed in the approximate order in which they appear.

**Table 55: show chassis high-availability information**

Field Name	Field Description
Node failure codes	<p>Node failure codes are:</p> <ul style="list-style-type: none"> <li>• HW Hardware monitoring</li> <li>• MB Mbuf monitoring</li> <li>• CS Cold Sync monitoring</li> <li>• LB Loopback monitoring</li> <li>• SP SPU monitoring</li> </ul>
Node Status	<ul style="list-style-type: none"> <li>• status of the node</li> <li>• Local-id—local identifier</li> <li>• Local-IP—local IP address of the node</li> </ul>
HA Peer Information	<ul style="list-style-type: none"> <li>• Description—peer information</li> <li>• Peer Id—peer identifier</li> <li>• IP address—peer IP address</li> <li>• Interface—interface name</li> <li>• Routing Instance—routing instance name</li> <li>• Encrypted—data encrypted status</li> <li>• Cold Sync Status—cold sync status of the node.</li> </ul>
HA Hardware Upgrade Events	Message on additional SPC3 installation status.

**Table 55: show chassis high-availability information *(Continued)***

Field Name	Field Description
Services Redundancy Group	<ul style="list-style-type: none"><li>• Current State—current state of the node</li><li>• Peer Information—peer information</li><li>• Peer Id—peer identifier</li></ul>
SRG failure event codes	<ul style="list-style-type: none"><li>• BF BFD monitoring—monitor Bidirectional Forwarding Detection.</li><li>• IP IP monitoring—monitor IP address</li><li>• CP Control Plane monitoring—monitor control plane state</li></ul>

Table 55: show chassis high-availability information (Continued)

Field Name	Field Description
Services Redundancy Group	<ul style="list-style-type: none"> <li>• Status—node status</li> <li>• Activeness Priority—the node with the higher activeness priority become active for the service redundancy group.</li> <li>• Services—Associated services for the SRG. <ul style="list-style-type: none"> <li>• IPsec.</li> </ul> </li> <li>• Process Packet In Backup State—packet processing in Backup state.</li> <li>• Control Plane State—Displays the Control plane cold sync readiness after taking over the backup role. Means the control plane finished syncing all the control plane data from the new active node. The options are: <ul style="list-style-type: none"> <li>• READY—Active mode</li> <li>• READY/NOT READY—Backup node based on the actual state</li> <li>• N/A—in other states</li> </ul> </li> <li>• System Integrity Check—Displays if the hold timer is running and system integrity check is under progress. Applicable only in BACKUP and INELIGIBLE state.</li> <li>• Failure Events—Displays local service redundancy group related attribute failure events.</li> <li>• Peer Information—Displays peer node information. <ul style="list-style-type: none"> <li>• Peer Id— Peer node identification number.</li> <li>• Status—Displays status of the peer node. The options are Active/Backup/Ineligible/Unknown.</li> <li>• Health Status—Displays health status of the peer node as advertised last <ul style="list-style-type: none"> <li>• HEALTHY—Peer node SRG state is healthy</li> <li>• UNHEALTHY—Peer node SRG state is unhealthy</li> </ul> </li> </ul> </li> </ul>

Table 55: show chassis high-availability information (*Continued*)

Field Name	Field Description
	<ul style="list-style-type: none"> <li>UNKNOWN—Peer link is down</li> <li>SRG NOT CONFIGURED—SRG not configured at peer node.</li> <li>Failover Readiness—Displays Failover readiness of the peer node and applicable only in Active state.</li> </ul> <p>The options are:</p> <ul style="list-style-type: none"> <li>READY—Peer's healthy, control and data plane cold sync is complete and hence peer is ready for a failover. A manual failover can be done</li> <li>NOT READY—Peer is either unhealthy, or data/control plane cold sync is pending</li> <li>UNKNOWN—Peer's failover readiness is awaited or if peer link is down</li> <li>N/A—In all states other than Active.</li> </ul>

## Sample Output

### show chassis high-availability information

```

user@host> show chassis high-availability information
Node failure codes:
  HW  Hardware monitoring   LB  Loopback monitoring
  MB  Mbuf monitoring       SP  SPU monitoring
  CS  Cold Sync monitoring  SU  Software Upgrade

Node Status: ONLINE
Local-id: 2
Local-IP: 10.22.0.2
HA Peer Information:

Peer Id: 1      IP address: 10.22.0.1    Interface: ge-0/0/2.0
Routing Instance: default
Encrypted: YES  Conn State: DOWN
Cold Sync Status: IN PROGRESS

```

Services Redundancy Group: 0

Current State: ONLINE

Peer Information:

Peer Id: 1

SRG failure event codes:

BF BFD monitoring

IP IP monitoring

IF Interface monitoring

CP Control Plane monitoring

Services Redundancy Group: 1

Deployment Type: ROUTING

Status: ACTIVE

Activeness Priority: 1

Preemption: DISABLED

Process Packet In Backup State: NO

Control Plane State: READY

System Integrity Check: N/A

Failure Events: NONE

Peer Information:

Peer Id: 1

Status : BACKUP

Health Status: HEALTHY

Failover Readiness: READY

## show chassis high-availability information detail

```
user@host> show chassis high-availability information detail
```

Node level Information:

Node Status: ONLINE

Local-id: 2

Local-IP: 10.22.0.2

HA Peer Information:

Peer-ID: 1      IP address: 10.22.0.1      Interface: ge-0/0/2.0

Routing Instance: default

Encrypted: YES      Conn State: UP

Cold Sync Status: COMPLETE

Internal Interface: st0.16000

Internal Local-IP: 180.100.1.2

Internal Peer-IP: 180.100.1.1

Internal Routing-instance: \_\_juniper\_private1\_\_

Packet Statistics:

Receive Error : 0

Send Error : 0

Packet-type	Sent	Received
SRG Status Msg	9	8
SRG Status Ack	8	7
Attribute Msg	3	2
Attribute Ack	2	2

HA Peer Conn events:

Dec 11 22:22:18.696 : HA Peer 180.100.1.1 BFD conn came up

Dec 11 22:22:25.269 : HA Peer 180.100.1.1 BFD conn went down

Dec 11 22:22:31.619 : HA Peer 180.100.1.1 BFD conn came up

Cold Synchronization:

Status:

Cold synchronization completed for: N/A

Cold synchronization failed for: N/A

Cold synchronization not known for: N/A

Current Monitoring Weight: 0

Progress:

CS Prereq	1 of 1 SPU's completed
1. if_state sync	1 SPU's completed
2. ha peer conn	1 SPU's completed
3. policy data sync	1 SPU's completed
4. cp ready	1 SPU's completed
5. VPN data sync	1 SPU's completed
6. IPID data sync	1 SPU's completed
7. All SPU ready	1 SPU's completed
8. AppID ready	1 SPU's completed
9. Tunnel Sess ready	1 SPU's completed
CS RTO sync	1 of 1 SPU's completed
CS Postreq	1 of 1 SPU's completed

Statistics:

Number of cold synchronization completed: 0

Number of cold synchronization failed: 0

Events:

Dec 11 22:22:23.870 : Cold sync for PFE is Post-req check in process

```

Dec 11 22:22:24.872 : Cold sync for PFE is Completed
Dec 11 22:22:37.293 : Cold sync for PFE is Post-req check in process
Dec 11 22:22:38.291 : Cold sync for PFE is Completed

```

#### SPU monitoring:

Status: Enabled

Current monitoring weight: 0

#### Statistics:

SPU up count: 1

NPC up count: 0

SPU down count: 0

NPC down count: 0

Chassis info processing error count: 0

#### Loopback Information:

PIC Name	Loopback	Nexthop	Mbuf
-----			
	Success	Success	Success

#### Hardware monitoring:

Status:

Activation status: Enabled

Ctrl Plane Hardware errors: 0

Data Plane Hardware errors: 0

#### SRGS Information:

##### Services Redundancy Group: 1

Deployment Type: ROUTING

Status: BACKUP

Activeness Priority: 1

Hold Timer: 1

Services: [ IPSEC ]

Process Packet In Backup State: NO

Control Plane State: READY

System Integrity Check: COMPLETE

Peer Information:

Failure Events: NONE

Peer Id: 1

Last Advertised HA Status: ACTIVE

Last Advertised Health Status: HEALTHY  
Failover Readiness: N/A

Signal Route Info:

Active Signal Route:  
IP: 10.39.1.1  
Routing Instance: default  
Status: NOT INSTALLED

Backup Signal Route:  
IP: 10.39.1.2  
Routing Instance: default  
Status: INSTALLED

Split-brain Prevention Probe Info:

DST-IP: 10.111.0.1  
SRC-IP: 10.11.0.1  
Routing Instance: default  
Status: NOT RUNNING  
Result: N/A                      Reason: N/A

SRG State Change Events:

Dec 11 22:21:36.379 : SRG[1] state UNKNOWN -> HOLD, Reason: State machine start  
Dec 11 22:23:28.889 : SRG[1] state HOLD -> ACTIVE, Reason: Peer state Backup adv received  
Dec 11 22:23:31.152 : SRG[1] state ACTIVE -> BACKUP, Reason: HA state preemption

BFD Monitoring:

Status: UNKNOWN

SRC-IP: 10.5.0.1      DST-IP: 10.5.0.2  
Routing Instance: default  
Type: SINGLE-HOP  
IFL Name: ge-0/0/3.0  
State: INSTALLED

Interface Monitoring:

Status: UP

IF Name: ge-0/0/4      State: Up



IF Name: ge-0/0/3      State: Up

## Release Information

Command introduced in Junos OS Release 20.4R1.

## RELATED DOCUMENTATION

[Multinode High Availability Monitoring | 645](#)

[Example: Configure Multinode High Availability in a Layer 3 Network | 672](#)

## show chassis high-availability peer-info

### IN THIS SECTION

- [Syntax | 1415](#)
- [Description | 1415](#)
- [Required Privilege Level | 1416](#)
- [Output Fields | 1416](#)
- [Sample Output | 1416](#)
- [Release Information | 1417](#)

## Syntax

```
show chassis high-availability peer-info
```

## Description

Display details of the peer node in a Multinode High Availability setup. Use this command to gather details of peer node, connection details, and packet statistics.

# Required Privilege Level

view

# Output Fields

Table 56 on page 1416 lists the output fields for the show chassis high-availability information command. Output fields are listed in the approximate order in which they appear.

**Table 56: show chassis high-availability peer-info**

Field Name	Field Description
HA Peer Information	<ul style="list-style-type: none"> <li>• Description—peer information</li> <li>• Peer Id—peer identifier</li> <li>• IP address—peer IP address</li> <li>• Interface—interface name</li> <li>• Routing Instance—routing instance name</li> </ul>
Internal connection details	Details related to internal traffic including internal interface, internal local IP address, internal peer IP address, and internal routing instance)
Packet Statistics	Details of packets sent and received. The detail includes: number of inbound/outbound errors and number of packets sent and received (SRG messages and attribute messages).

# Sample Output

## show chassis high-availability peer-info

```

user@host> show chassis high-availability peer-info
HA Peer Information:

Peer-ID: 2      IP address: 10.22.0.2      Interface: ge-0/0/2.0
Routing Instance: default
Encrypted: YES  Conn State: UP
Cold Sync Status: COMPLETE

```

```
Internal Interface: st0.16000
Internal Local-IP: 180.100.1.1
Internal Peer-IP: 180.100.1.2
Internal Routing-instance: __juniper_private1__
Packet Statistics:
    Receive Error : 0          Send Error : 0

    Packet-type      Sent      Received

    SRG Status Msg   4        3

    SRG Status Ack    3        4

    Attribute Msg     1        1

    Attribute Ack     1        1
```

Release Information

Command introduced in Junos OS Release 22.3R1.

RELATED DOCUMENTATION

- [Multinode High Availability Monitoring | 645](#)
- [Example: Configure Multinode High Availability in a Layer 3 Network | 672](#)

show chassis high-availability prefix-srgid-table

IN THIS SECTION

- Syntax | 1418
- Description | 1418
- Required Privilege Level | 1418
- Output Fields | 1418
- Sample Output | 1418

Syntax

```
show chassis high-availability prefix-srgid-table
```

Description

Display mapping of prefix list with SRGs.

Required Privilege Level

view

Output Fields

[Table 57 on page 1418](#) lists the output fields for the `show chassis high-availability information` command. Output fields are listed in the approximate order in which they appear.

**Table 57: show chassis high-availability prefix-srgid-table**

Field Name	Field Description
SRGID	SRG identification number.
IP Prefix	Listing of IP prefixes that represent a set of routes used as local address of IKE gateway.
Routing Table	Name of the routing table.

Sample Output

**show chassis high-availability peer-info**

```
user@host> show chassis high-availability prefix-srgid-table
IP SRGID Table:
```

SRGID	IP Prefix	Routing Table
1	10.11.0.1/32	default
1	10.19.0.1/32	default
1	10.20.0.1/32	default
2	10.11.1.1/32	default
2	10.19.1.1/32	default
2	10.20.1.1/32	default

Release Information

Command introduced in Junos OS Release 22.4R1.

RELATED DOCUMENTATION

| [Multinode High Availability Monitoring](#) | 645

show chassis high-availability services-redundancy-group

IN THIS SECTION

- [Syntax](#) | 1420
- [Description](#) | 1420
- [Required Privilege Level](#) | 1420
- [Output Fields](#) | 1420
- [Sample Output](#) | 1424
- [Release Information](#) | 1425

Syntax

```
show chassis high-availability services-redundancy-group <services-redundancy-group-id>
```

Description

Display the service redundancy group information in a Multinode High Availability setup.

Required Privilege Level

view

Output Fields

[Table 58 on page 1420](#) lists the output fields for the `show chassis high-availability services-redundancy-group` command. Output fields are listed in the approximate order in which they appear.

**Table 58: show chassis high-availability services-redundancy-group**

Field Name	Field Description
SRG failure event codes	SRG failure event codes are: <ul style="list-style-type: none"><li>• BF BFD monitoring</li><li>• IP IP monitoring</li><li>• CP Control Plane monitoring</li></ul>

Table 58: show chassis high-availability services-redundancy-group (*Continued*)

Field Name	Field Description
Services Redundancy Group	<ul style="list-style-type: none"> <li>• Deployment Type—Multinode High Availability deployment type - Routing, switching, hybrid, or cloud</li> <li>• Status—node status</li> <li>• Activeness Priority—the node with the higher activeness priority become active for the service redundancy group.</li> <li>• Process Packet In Backup State—packet processing in Backup state.</li> <li>• Control Plane State—Displays the Control plane cold sync readiness after taking over the backup role. Means the control plane finished syncing all the control plane data from the new active node.  The options are: <ul style="list-style-type: none"> <li>• READY—Active mode</li> <li>• READY/NOT READY—Backup node based on the actual state</li> <li>• N/A—in other states</li> </ul> </li> <li>• System Integrity Check—Displays if the hold timer is running and system integrity check is under progress. Applicable only in BACKUP and INELIGIBLE state.</li> <li>• Failure Events—Displays local service redundancy group related attribute failure events.</li> <li>• Peer Information—Displays peer node information. <ul style="list-style-type: none"> <li>• Peer Id— Peer node identification number.</li> <li>• Status—Displays status of the peer node. The options are Active/Backup/Ineligible/Unknown.</li> </ul> </li> </ul>

Table 58: show chassis high-availability services-redundancy-group (*Continued*)

Field Name	Field Description
	<ul style="list-style-type: none"> <li>• Health Status—Displays health status of the peer node as advertised last</li> <li>• HEALTHY—Peer node SRG state is healthy</li> <li>• UNHEALTHY—Peer node SRG state is unhealthy</li> <li>• UNKNOWN—Peer link is down</li> <li>• SRG NOT CONFIGURED—SRG not configured at peer node.</li> <li>• Failover Readiness—Displays Failover readiness of the peer node and applicable only in Active state.  The options are: <ul style="list-style-type: none"> <li>• READY—Peer's healthy, control and data plane cold sync is complete and hence peer is ready for a failover. A manual failover can be done</li> <li>• NOT READY—Peer is either unhealthy, or data/control plane cold sync is pending</li> <li>• UNKNOWN—Peer's failover readiness is awaited or if peer link is down</li> <li>• N/A—In all states other than Active.</li> </ul> </li> <li>• Signal Route Info <ul style="list-style-type: none"> <li>• Active Signal Route—Active signal route required for activeness enforcement</li> <li>• Backup Signal Route—Backup signal route required for activeness enforcement</li> </ul> </li> </ul>



Table 58: show chassis high-availability services-redundancy-group (Continued)

Field Name	Field Description
	<ul style="list-style-type: none"> <li>• Routing Instance—Routing instance of routes</li> <li>• Status—Status of the routes - <b>INSTALLED</b> or <b>NOT INSTALLED</b></li> <li>• Split-brain Prevention Probe Info <ul style="list-style-type: none"> <li>• DST-IP—IP addresses of the upstream routers as the destination IP address for the activeness determination probe.</li> <li>• SRC-IP—floating IP address as source IP address for activeness determination probe.</li> </ul> </li> <li>• Routing Instance—Routing instance of routes</li> <li>• Status—Status of the probes - <b>RUNNING</b> or <b>NOT RUNNING</b></li> <li>• BFD Monitoring <ul style="list-style-type: none"> <li>• Status—State of the BFD session: Up, Down, Init or failing</li> <li>• SRC-IP—Source IP address for outgoing BFD packets</li> <li>• DST-IP—Destination IP address for outgoing BFD packets</li> <li>• Routing Instance—Routing instance of routes on which BFD monitoring is configured.</li> <li>• Type—Session type (single hop or multihop)</li> <li>• IFL Name— Interface on which the BFD session is active</li> <li>• Status—Status of the probes - <b>RUNNING</b> or <b>NOT RUNNING</b></li> </ul> </li> </ul>

## Sample Output

### show chassis high-availability services-redundancy-group

For SRG0:

```
user@host> show chassis high-availability services-redundancy-group 0
Services Redundancy Group: 0
    Current State: ONLINE
    Peer Information:
        Peer Id: 2
```

For SRG1:

```
user@host> show chassis high-availability services-redundancy-group 1
SRG failure event codes:
    BF  BFD monitoring
    IP  IP monitoring
    IF  Interface monitoring
    CP  Control Plane monitoring

Services Redundancy Group: 1
    Deployment Type: ROUTING
    Status: ACTIVE
    Activeness Priority: 200
    Preemption: ENABLED
    Process Packet In Backup State: NO
    Control Plane State: READY
    System Integrity Check: N/A
    Failure Events: NONE
    Peer Information:
        Peer Id: 2
        Status : BACKUP
        Health Status: HEALTHY
        Failover Readiness: READY

Signal Route Info:
    Active Signal Route:
        IP: 10.39.1.1
        Routing Instance: default
        Status: INSTALLED
```

```
Backup Signal Route:  
IP: 10.39.1.2  
Routing Instance: default  
Status: NOT INSTALLED
```

```
Split-brain Prevention Probe Info:  
DST-IP: 10.111.0.1  
SRC-IP: 10.11.0.1  
Routing Instance: default  
Status: NOT RUNNING  
Result: N/A          Reason: N/A
```

```
BFD Monitoring:  
Status: UP  
  
SRC-IP: 10.4.0.1    DST-IP: 10.4.0.2  
Routing Instance: default  
Type: SINGLE-HOP  
    IFL Name: ge-0/0/4.0  
State: UP
```

## Release Information

Command introduced in Junos OS Release 20.4R1.

## RELATED DOCUMENTATION

[Multinode High Availability Monitoring | 645](#)

[Example: Configure Multinode High Availability in a Layer 3 Network | 672](#)

## show chassis nonstop-upgrade

### IN THIS SECTION

- [Syntax | 1426](#)
- [Description | 1426](#)
- [Required Privilege Level | 1426](#)
- [Output Fields | 1426](#)
- [Sample Output | 1427](#)
- [Release Information | 1428](#)

### Syntax

```
show chassis nonstop-upgrade
```

### Description

(EX6200 switches, EX8200 switches, EX8200 Virtual Chassis, QFX3500 and QFX3600 Virtual Chassis, and Virtual Chassis Fabric only) Display the status of the line cards or Virtual Chassis members in the linecard role after the most recent nonstop software upgrade (NSSU). You must issue this command on the primary Routing Engine.

### Required Privilege Level

view

### Output Fields

[Table 59 on page 1427](#) lists the output fields for the `show chassis nonstop-upgrade` command. Output fields are listed in the approximate order in which they appear.

Table 59: show chassis nonstop-upgrade Output Fields

Field Name	Field Description
<b>Item</b>	Line card slot number.
<b>Status</b>	State of line card: <ul style="list-style-type: none"> <li>• <b>Error</b>—Line card is in an error state.</li> <li>• <b>Offline</b>—Line card is powered down.</li> <li>• <b>Online</b>—Line card is online and running.</li> </ul>
<b>Reason</b>	Reason for the state (if the line card is offline).

## Sample Output

### show chassis nonstop-upgrade (EX8200 Switch)

```

user@switch> show chassis nonstop-upgrade
  Item      Status      Reason
  FPC 0     Online
  FPC 1     Online
  FPC 2     Online
  FPC 3     Offline      Offlined by CLI command
  FPC 4     Online
  FPC 5     Online
  FPC 6     Online
  FPC 7     Online

```

### show chassis nonstop-upgrade (EX8200 Virtual Chassis)

```

user@external-routing-engine> show chassis nonstop-upgrade
member0:
-----
  Item      Status      Reason
  FPC 0     Online

```

FPC 1	Online	
FPC 2	Online	
FPC 5	Online	
member1:		
-----		
Item	Status	Reason
FPC 0	Online	
FPC 1	Offline	Offlined due to config
FPC 2	Online	
FPC 3	Online	
FPC 4	Online	
FPC 5	Online	
FPC 7	Online	

**show chassis nonstop-upgrade (Virtual Chassis Fabric)**

Item	Status	Reason
FPC 0	Online	
FPC 1	Online	
FPC 2	Online	
FPC 3	Online	
FPC 4	Online	
FPC 5	Online	

**Release Information**

Command introduced in Junos OS Release 10.4.

**RELATED DOCUMENTATION**

<a href="#">request system software nonstop-upgrade   1314</a>
<a href="#">Upgrading Software on an EX6200 or EX8200 Standalone Switch Using Nonstop Software Upgrade (CLI Procedure)</a>
<a href="#">Upgrading Software on a Virtual Chassis and Mixed Virtual Chassis Using Nonstop Software Upgrade</a>
<a href="#">Upgrading Software on a Virtual Chassis Fabric Using Nonstop Software Upgrade</a>
<a href="#">Upgrading Software on an EX8200 Virtual Chassis Using Nonstop Software Upgrade (CLI Procedure)</a>

# show chassis nonstop-upgrade node-group

IN THIS SECTION

- [Syntax | 1429](#)
- [Description | 1429](#)
- [Required Privilege Level | 1429](#)
- [Output Fields | 1429](#)
- [Sample Output | 1430](#)
- [Release Information | 1430](#)

## Syntax

```
show chassis nonstop-upgrade node-group node-group-name
```

## Description

Display the status of the Node group after the most recent nonstop software upgrade (NSSU).

## Required Privilege Level

view

## Output Fields

[Table 60 on page 1429](#) lists the output fields for the `show chassis nonstop-upgrade node-group` command. Output fields are listed in the approximate order in which they appear.

**Table 60: show chassis nonstop-upgrade node-group Output Fields**

Field Name	Field Description
Item	Node device slot number.

**Table 60: show chassis nonstop-upgrade node-group Output Fields *(Continued)***

Field Name	Field Description
Status	<p>State of Node device:</p> <ul style="list-style-type: none"> <li>• Error—Node device is in an error state.</li> <li>• Offline—Node device is powered down.</li> <li>• Online—Node device is online and running.</li> </ul>
Reason	Reason for the state (if the line card is offline).

### Sample Output

**show chassis nonstop-upgrade node-group**

```

user@qfabric> show chassis nonstop-upgrade node-group NW-NG-0
  Item           Status           Reason
  P1550-C        Online

```

### Release Information

Command introduced in Junos OS Release 12.2.

### RELATED DOCUMENTATION

<i>Performing a Nonstop Software Upgrade on the QFabric System</i> <i>request system software nonstop-upgrade</i>
--



## show chassis power-budget-statistics

### IN THIS SECTION

- [Syntax | 1431](#)
- [Description | 1431](#)
- [Required Privilege Level | 1431](#)
- [Output Fields | 1431](#)
- [Sample Output | 1434](#)
- [Release Information | 1436](#)

### Syntax

```
show chassis power-budget-statistics
```

### Description

Display the power budget of the device.

### Required Privilege Level

view

### Output Fields

[Table 61 on page 1432](#) lists the output fields for the `show chassis power-budget-statistics` command. Output fields are listed in the approximate order in which they appear.

**Table 61: show chassis power-budget-statistics Output Fields**

Field Name	Field Description
PSU <i>n</i> ( <i>supply type</i> )	Capacity rating of the power supply and whether the power supply is currently operating (Online) or not (Offline). If a power supply is offline, the capacity is shown as 0 W.
Total Power supplied by all Online PSUs	Total number of watts supplied by all currently operating power supplies.
Power Redundancy Configuration	Configured power redundancy setting, either $N+1$ or $N+N$ .
Base power reserved	Total number of watts reserved for the device.
Non-PoE power being consumed	The amount of power, in W, currently being consumed for PoE.
Power Reserved for the Chassis	<p>Power reserved for the chassis:</p> <ul style="list-style-type: none"> <li>• For an EX6200 switch, 500 W.</li> <li>• For an EX8208 switch: 1600 W in an <math>N+1</math> configuration; 1200 W in an <math>N+N</math> configuration</li> <li>• For an EX8216 switch: 2400 W in an <math>N+1</math> configuration; 1800 W in an <math>N+N</math> configuration</li> </ul> <p>The power reserved for the chassis includes the maximum power requirements for the fan tray and Switch Fabric and Routing Engine (SRE), Routing Engine (RE), and Switch Fabric (SF) modules in both base and redundant configurations.</p>

Table 61: show chassis power-budget-statistics Output Fields (*Continued*)

Field Name	Field Description
Fan Tray Statistics	<p>(EX6200 switch only) Information about the fan tray:</p> <ul style="list-style-type: none"> <li>Base power—Power allocated to the fan tray in the power budget. This allocation is included in Power Reserved for the Chassis.</li> <li>Power Used—Actual power being used by the fan tray. This value is for informational purposes only: the power budget for the switch is based on allocated power (the theoretical maximum the fan tray might use) rather than used power.</li> </ul>
FPC <i>n</i> ( <i>card type</i> )	<p>Information about the line card installed in slot <i>n</i>. For EX6200 switches, information about the SRE modules in slot 4 and slot 5 is also shown.</p> <ul style="list-style-type: none"> <li>Base power—For line cards without PoE ports, the total power allocated to the line card.  For line cards with PoE ports, the power allocated to the line card before the PoE power budget is allocated. The base power includes 37 W of PoE power that is always allocated to line cards that support PoE.</li> <li>Power Used—(EX6200 switch only) The actual power being consumed by the line card or SRE module, including PoE power. This value is for informational purposes only: the power budget for the switch is based on allocated power (the theoretical maximum the line card might use) rather than used power.</li> <li>PoE power—For line cards with PoE ports, the PoE power budget allocated to the line card. This value includes the 37 W of PoE power that is always part of the base power allocation for line cards that support PoE.  For line cards without PoE ports, the value is always 0 W.</li> <li>The power priority assigned to the line card slot.</li> </ul>

**Table 61: show chassis power-budget-statistics Output Fields (Continued)**

Field Name	Field Description
Total (non-PoE) Power allocated	Power budgeted for all the components in the switch, excluding the PoE power budget allocated to line cards. This value is equal to the power reserved for the chassis plus the base power allocations of all online line cards.
Total Power allocated for PoE	The total of the PoE power budgets allocated to the line cards in the switch. This figure includes the 37 W of PoE power always included in the base allocation for each line card that supports PoE.
Total PoE power consumed	The amount of power that has been consumed by PoE.
Total PoE power remaining	The amount of available power remaining that can be used for PoE.
Power Available (Redundant case)	Unused power available to the switch in the power budget, not including the power reserved for redundancy. If power is insufficient to meet the $N+1$ or $N+N$ redundancy requirements, this value is 0. PoE power allocations are not included in the calculation of this value.
Total Power Available	Unused power available to the switch in the power budget. This value is derived by subtracting all power allocations, including PoE power allocations, from the total power available on the switch (the Total Power supplied by all Online PSUs value).

## Sample Output

### show chassis power-budget-statistics (EX6200 Switch)

```

user@switch> show chassis power-budget-statistics
PSU 0      (EX6200-PWR-AC2500)      : 2500 W   Online

```

```

PSU 1    (EX6200-PWR-AC2500)      :    2500 W  Online
PSU 2    (EX6200-PWR-AC2500)      :    2500 W  Online
PSU 3    (EX6200-PWR-AC2500)      :    2500 W  Online
Total Power supplied by all Online PSUs :   10000 W
Power Redundancy Configuration      :      N+1
Power Reserved for the Chassis      :      500 W

Fan Tray Statistics      Base power  Power Used
FTC  0                   :    300 W   43.04 W

FPC Statistics          Base power  Power Used  PoE power  Priority
FPC  1  (EX6200-48P)    :    220 W   49.47 W   1440 W     1
FPC  2  (EX6200-48P)    :    220 W   47.20 W    800 W     2
FPC  3  (EX6200-48P)    :    220 W  1493.57 W   1440 W     0
FPC  4  (EX6200-SRE64-4XS) :   100 W   51.38 W     0 W     0
FPC  5  (EX6200-SRE64-4XS) :   100 W   50.28 W     0 W     0
FPC  6  (EX6200-48P)    :    220 W   49.38 W    800 W     6
FPC  8  (EX6200-48P)    :    220 W   61.41 W   1440 W     9
FPC  9  (EX6200-48T)    :    150 W   12.49 W     0 W     9

Total (non-PoE) Power allocated      :    1750 W
Total Power allocated for PoE        :    5920 W
Power Available (Redundant case)     :    5750 W
Total Power Available                :    2515 W

```

### show chassis power-budget-statistics (EX8200 Switch)

```

user@switch> show chassis power-budget-statistics

PSU 0    (EX8200-AC2K)      :    2000 W  Online
PSU 1    (EX8200-AC2K)      :    2000 W  Online
PSU 2    (EX8200-AC2K)      :    2000 W  Online
PSU 3    (EX8200-AC2K)      :    2000 W  online
PSU 4    (EX8200-AC2K)      :    2000 W  Online
Total Power supplied by all Online PSUs :   10000 W
Power Redundancy Configuration      :      N+1
Power Reserved for the Chassis      :    2400 W

FPC Statistics          Base power  PoE power  Priority
FPC  1  (EX8200-48T)    :    350 W     0 W     15
FPC  5  (EX8200-2XS-40P) :    387 W   792 W     0
FPC  9  (EX8200-48PL)   :    267 W   915 W    15
FPC 10  (EX8200-2XS-40T) :    350 W     0 W     1
FPC 12  (EX8200-48T)    :    350 W     0 W    15

```

```

Total (non-PoE) Power allocated      :    4104 W
Total Power allocated for PoE        :    1707 W
Power Available (Redundant case)     :    3896 W
Total Power Available                :    4263 W

```

### show chassis power-budget-statistics (SRX380 device)

```

user@host> show chassis power-budget-statistics
      PSU 0   (JPSU-600W-AC-AFO   )      :    600 W   Online
      PSU 1   (JPSU-600W-AC-AFO   )      :    600 W   Online
      Power redundancy configuration      :    N+N
      Total power supplied by all online PSUs :    600 W
      Base power reserved                  :    300 W
      Non-PoE power being consumed         :    300 W
      Total power allocated for PoE        :    300 W
      Total PoE power consumed             :    289 W
      Total PoE power remaining            :     11 W

```

## Release Information

Command introduced in Junos OS Release 10.2.

## RELATED DOCUMENTATION

[Understanding Power Management on EX Series Switches | 373](#)

[Configuring the Power Priority of Line Cards \(CLI Procedure\)](#)

[Configuring Power Supply Redundancy \(CLI Procedure\)](#)

## show chassis redundant-power-system

### IN THIS SECTION

- [Syntax | 1437](#)
- [Description | 1437](#)

- [Required Privilege Level | 1437](#)
- [Output Fields | 1437](#)
- [Sample Output | 1438](#)
- [Release Information | 1439](#)

Syntax

```
show chassis redundant-power-system
```

Description

Display information about the Redundant Power Systems (RPS) connected to the switch.

Required Privilege Level

view

Output Fields

[Table 62 on page 1437](#) lists the output fields for the `show chassis redundant-power-system` command. Output fields are listed in the approximate order in which they appear.

Table 62: show chassis redundant-power-system Output Fields

Field Name	Field Description	Level of Output
Member	Member number of the switch connected to the RPS—For a switch that has never been configured in a Virtual Chassis, the value is always zero. For a Virtual Chassis member, the range is zero through the maximum number of members in the Virtual Chassis.	All levels

Table 62: show chassis redundant-power-system Output Fields (*Continued*)

Field Name	Field Description	Level of Output
<b>Status</b>	Status of the RPS: <ul style="list-style-type: none"> <li>• ARMED—The switch is ready to get backup power from the RPS if power supply fails on the switch.</li> <li>• OFF—The switch has zero and is not configured to receive backup power from the RPS.</li> <li>• BACKED-UP—The switch is receiving power backup from the RPS.</li> <li>• OVER-SUBSCRIBED—The switch cannot receive backup power from the RPS even if you set the .</li> </ul>	All levels
<b>RPS</b>	Serial number of the RPS.	
<b>Port</b>	Number of the switch connector on the RPS that is connected to a switch.	All levels

## Sample Output

### show chassis redundant-power-system (Standalone Switch)

```
user@switch> show chassis redundant-power-system
```

```
Member Status    RPS          Port
  0    Armed    CG0209121807  0
```

### show chassis redundant-power-system (Virtual Chassis member)

```
user@switch> show chassis redundant-power-system
```

```
Member Status    RPS          Port
```



0	Armed	CG0209121814	5
2	Armed	CG0209121815	4

## Release Information

Command introduced in Junos OS Release 12.1.

## RELATED DOCUMENTATION

Determining and Setting Priority for Switches Connected to an EX Series RPS

## show protection-group ethernet-ring aps

### IN THIS SECTION

- [Syntax | 1439](#)
- [Description | 1440](#)
- [Options | 1440](#)
- [Required Privilege Level | 1440](#)
- [Output Fields | 1440](#)
- [Sample Output | 1441](#)
- [Sample Output | 1441](#)
- [Sample Output | 1442](#)
- [Release Information | 1444](#)

## Syntax

```
show protection-group ethernet-ring aps
```

## Description

Display the status of the Automatic Protection Switching (APS) and Ring APS (RAPS) messages on an Ethernet ring.

## Options

This command has no options.

## Required Privilege Level

view

## Output Fields

[Table 63 on page 1440](#) lists the output fields for the `show protection-group ethernet-ring aps` command. Output fields are listed in the approximate order in which they appear.

**Table 63: show protection-group ethernet-ring aps Output Fields**

Field Name	Field Description
<b>Ethernet Ring</b>	Name configured for the Ethernet ring.
<b>Request/State</b>	<p>Status of the Ethernet ring RAPS messages.</p> <ul style="list-style-type: none"> <li>• <b>NR</b>—Indicates that there is no request for APS on the ring.</li> <li>• <b>SF</b>—Indicates that there is a signal failure on the ring.</li> <li>• <b>FS</b>—Indicates that there are active forced-switch requests in the ring.</li> <li>• <b>MS</b>—Indicates that there are active manual-switch requests in the ring.</li> </ul> <p><b>NOTE:</b> Both FS and MS values are valid only when G.8032v2 is supported.</p>
<b>Ring Protection Link Blocked</b>	Blocking on the ring protection link: <b>Yes</b> or <b>No</b> .
<b>No Flush</b>	Indicates the value of the Do Not Flush (DNF) flag in the received RAPS PDU. If the value is Yes, then FDB flush is not triggered as part of processing of the received RAPS PDU.

**Table 63: show protection-group ethernet-ring aps Output Fields (Continued)**

Field Name	Field Description
Blocked Port Reference	This parameter is the reference to the blocked ring port. If the east ring port is blocked, the Blocked Port Reference (BPR) value is 0. If the west ring port is blocked, the BPR value is 1. If both ring ports are blocked, this parameter can take any value. If both east and west ports are blocked or not blocked, the value would be 0. This field is valid only when G.8032v2 is supported.
<b>Blocked Port Reference</b>	Reference of the ring port on which traffic is blocked.
<b>Originator</b>	Indicates whether the node is the originator of the RAPS messages.
<b>Remote Node ID</b>	Identifier (in MAC address format) of the remote node.

## Sample Output

### show protection-group ethernet-ring aps (EX Switches)

```

user@switch>show protection-group ethernet-ring aps
Ring Name    Request/state No Flush  RPL Blocked  Originator  Remote Node ID erp1
NR           No           Yes       No           00:1F:12:30:B8:81

```

## Sample Output

### show protection-group ethernet-ring aps (Owner Node, Normal Operation on ACX and MX Routers)

```

user@host> show protection-group ethernet-ring aps
Ethernet Ring Request/state RPL Blocked No Flush BPR Originator Remote Node ID
Erp_1         NR           Yes       No         1      No         00:00:00:02:00:01

```

## Sample Output

**show protection-group ethernet-ring aps detail (Owner Node, Normal Operation on ACX and MX Routers)**

```
user@host> show protection-group ethernet-ring aps detail
Ethernet-Ring name      : Erp_1
Request/State           : NR
Ring Protection Link blocked : Yes
No Flush Flag           : No
Blocked Port Reference   : 1
Originator              : No
Remote Node ID          : 00:00:00:02:00:01
```

**show protection-group ethernet-ring aps (MX RPL Owner Ring Node, Failure condition on non-RPL link of the ring)**

```
user@host>show protection-group ethernet-ring aps
Ethernet Ring   Request/state   RPL Blocked   No Flush
pg101           SF              No             No

Originator      Remote Node ID
No              00:01:02:00:00:01
```

**show protection-group ethernet-ring aps (MX Interconnection Ring Node, Failure condition in major ring on non-RPL link of the ring)**

```
user@host>show protection-group ethernet-ring aps
Ethernet Ring   Request/state   RPL Blocked   No Flush   BPR
pg_major        SF              No             No          0
pg_subring       NR              Yes            Yes          0

Originator      Remote Node ID
No              00:01:00:00:00:01
No              00:02:00:00:00:02
```

**show protection-group ethernet-ring aps (MX Series router)**

```

user@host>show protection-group ethernet-ring aps
Ethernet Ring   Request/state  RPL Blocked  No Flush  BPR  Originator  Remote Node ID
Inst_Vlans_1-15 NR           Yes          Yes       1     Yes        NA
Inst_Vlans_16-30 NR           Yes          Yes       0     No         00:00:00:03:00:02

```

**show protection-group ethernet-ring aps detail (MX Series router)**

```

user@host>show protection-group ethernet-ring aps
Ethernet-Ring name      : Inst_Vlans_1-15
Request/State          : NR
Ring Protection Link blocked : Yes
No Flush Flag          : Yes
Blocked Port Reference  : 1
Originator              : Yes
Remote Node ID          : NA

Ethernet-Ring name      : Inst_Vlans_16-30
Request/State          : NR
Ring Protection Link blocked : Yes
No Flush Flag          : Yes
Blocked Port Reference  : 0
Originator              : No
Remote Node ID          : 00:00:00:03:00:02

```

**show protection-group ethernet-ring aps (MX Interconnection Ring Node as RPL owner of major ring, rings in IDLE state)**

```

user@host>show protection-group ethernet-ring aps detail

Ethernet-Ring name      : pg_major
Request/State          : NR
Ring Protection Link blocked : Yes
No Flush Flag          : Yes
Blocked Port Reference  : 0
Originator              : Yes
Remote Node ID          : NA

```

```

Ethernet-Ring name      : pg_subring
Request/State           : NR
Ring Protection Link blocked : Yes
No Flush Flag           : Yes
Blocked Port Reference   : 0
Originator              : No
Remote Node ID          : 00:00:03:00:00:03

```

### show protection-group ethernet-ring aps detail (EX2300 and EX3400 Switches)

```

user@switch>show protection-group ethernet-ring aps detail
Ethernet-Ring name      : pg1001
Request/State           : NR
Ring Protection Link blocked : Yes
No Flush Flag           : Yes
Blocked Port Reference   : 0
Originator              : Yes
Remote Node ID          : NA

```

## Release Information

Command introduced in Junos OS Release 9.4.

Command introduced in Junos OS Release 18.1 for EX2300 and EX3400 switches.

## RELATED DOCUMENTATION

---

*show protection-group ethernet-ring data-channel*

---

*show protection-group ethernet-ring interface*

---

*show protection-group ethernet-ring node-state*

---

*show protection-group ethernet-ring statistics*

---

*show protection-group ethernet-ring vlan*

# show protection-group ethernet-ring configuration

IN THIS SECTION

- [Syntax | 1445](#)
- [Description | 1445](#)
- [Required Privilege Level | 1445](#)
- [Output Fields | 1445](#)
- [Sample Output | 1448](#)
- [Release Information | 1453](#)

## Syntax

```
show protection-group ethernet-ring configuration
```

## Description

Display the configuration of Ethernet ring protection group on EX Switches and MX Series routers.

## Required Privilege Level

view

## Output Fields

[Table 64 on page 1445](#) lists the output fields for the show protection-group ethernet-ring configuration command. Output fields are listed in the approximate order in which they appear.

**Table 64: show protection-group ethernet-ring configuration Output Fields**

Output Fields	Field Description
G8032 Compatability Version	This is the compatibility version mode of ERP. This parameter always takes the value 1 in the case of G8032v1. This parameter is valid only for MX Series routers.

Table 64: show protection-group ethernet-ring configuration Output Fields *(Continued)*

Output Fields	Field Description
<b>East Interface</b>	One of the two switch interfaces that participates in a ring link. When Junos supports G8032v2, this interface is treated as interface 0.
<b>West Interface</b>	One of the two interfaces in a switch that participates in a ring link. When Junos supports G8032v2, this interface is treated as interface 1.
<b>Restore Interval</b>	<p>Configured interval of wait time after a link is restored. When a link goes down, the RPL link is activated. When the down link becomes active again, the RPL owner receives a notification. The RPL owner waits for the restore interval before issuing a block on the RPL link. The configured restore interval can be 5 through 12 minutes for ER Pv1 and 1 through 12 minutes for ER Pv2. This configuration is a global configuration and applies to all Ethernet rings if the Ethernet ring does not have a more specific configuration for this value. If no parameter is configured at the protection group level, the global configuration of this parameter uses the default value.</p> <p><b>NOTE:</b> Wait to Restore (WTR) configuration values on EX2300 and EX3400 switches must be 5-12 minutes.</p>
Wait to Block Interval	<p>Configured interval of wait time for link restoration when a manual command (manual switch or force switch) is cleared. On clearing the manual command, the RPL owner receives NR messages, which starts a timer with interval 'Wait to Block' to restore the RPL link after its expiration. This delay timer is set to be 5 seconds longer than the guard timer. The configured number can be from 5 seconds through 10 seconds. The parameter is valid only for G.8032v2.</p> <p><b>NOTE:</b> The Wait To Block Timer (WTB) is always disabled on EX2300 and EX3400 switches because it is not supported in ERPSv1. Any configuration you make to the WTB setting has no effect. The output from the CLI command 'show protection-group ethernet-ring node-state detail' lists a WTB setting but that setting has no effect.</p>
<b>Guard Interval</b>	Configured number of milliseconds (in 10 millisecond intervals, 10 milliseconds through 2000 milliseconds) that the node does not process any Ethernet ring protection protocol data units (PDUs). This configuration is a global configuration and applies to all Ethernet rings if the Ethernet ring does not have a more specific configuration for this value. If no parameter is configured at the protection group level, the global configuration of this parameter uses the default value.



**Table 64: show protection-group ethernet-ring configuration Output Fields (Continued)**

Output Fields	Field Description
Hold off interval	This is the interval at which the link is held down even before declaring that the link is down. Because the parameter is not supported at present, its value is always considered 0. This parameter is valid only for MX Series routers.
<b>Node ID</b>	Node ID for the switch or router. If the node ID is not configured, it is assigned by default. For EX Series switches, the Node ID value cannot be configured, whereas for MX Series routers, it can be configured.
Ring ID	In G8032v2, the ring ID can be within the range 1–239. All the nodes in a ring should have the same ring ID. In the case of G8032v1, the value of the ring ID is always 1. This parameter is valid only for MX Series routers.
Node Role	Indicates whether the ring node is operating as a normal ring-node or RPL-owner or RPL-neighbor. For G8032v1 RPL-neighbor role is not supported. This parameter is valid only for MX Series routers.
Revertive Mode of Operation	This parameter indicates whether the ring is operating in revertive mode or nonrevertive mode. In nonrevertive mode of operation, when all links in the ring and Ethernet Ring Nodes have recovered and no external requests are active, the Ethernet Ring does not automatically revert. G8032v1 supports only revertive mode of operation. This parameter is valid only for MX Series routers.
RAPS Tx Dot1p priority	The RAPS Tx Dot1p priority is a parameter with which the RAPS is transmitted from the ring node. For G8032v1, the value of this parameter is always 0. For G8032v2, the value of this parameter can be within the range 0–7. This parameter is valid only for MX Series routers.
Node type	Indicates whether ring node is a normal ring node having two ring-links or a open ring-node having only a single ring-link or a interconnection ring-node. An interconnection ring node can be connected to major ring in non virtual-channel mode or in virtual channel mode. Ring interconnection is not supported for G8032v1. This parameter is valid only for MX Series routers.
Major ring name	If the node type is interconnection in the ring, this parameter takes the name of the major ring to which the sub-ring node is connected. This parameter is valid only for MX Series routers.

**Table 64: show protection-group ethernet-ring configuration Output Fields (Continued)**

Output Fields	Field Description
Interconnection mode	Indicates the interconnection mode if the type of the node is interconnection. An interconnection ring node can be connected to major ring in non-virtual channel mode or in virtual channel mode. This parameter is valid only for MX Series routers.
Propagate Topology Change event	When Propagate Topology Change event is set to 1, the change in the topology of sub-ring is propagated to the major ring, enabling the transmission of EVENT FLUSH RAPS PDU in the major ring. When the parameter is set to 0, the topology change in the sub-ring is not propagated to the major ring blocking EVENT FLUSH RAPS PDU transmission in the major ring. This parameter is valid only for MX Series routers.
<b>Control Vlan</b>	The VLAN that transfers ERP PDUs from one node to another.
<b>Physical Ring</b>	Physical ring if the east and west interfaces are nontrunk ports. For MX Series routers, the ring is termed a physical ring if no data channels are defined for the ring and the entire physical port forwarding is controlled by ERP.
Data Channel VLAN(s)	Data VLANs for which forwarding behavior is controlled by the ring instance.

## Sample Output

### show protection-group ethernet-ring configuration (EX Switch)

```

user@switch>show protection-group ethernet-ring configuration
Ethernet ring configuration parameters for protection group erp1
East Interface   : ge-0/0/3.0
West Interface  : ge-0/0/9.0
Restore Interval : 5 minutes
Guard Interval   : 500 ms
Node Id         : 00:1F:12:30:B8:81
Control Vlan    : 101
Physical Ring    : yes

```

**show protection-group ethernet-ring configuration detail (MX Series Router)**

```

user@switch>show protection-group ethernet-ring configuration detail
Ethernet Ring configuration information for protection group pg_101
G8032 Compatibility Version           : 2
East interface (interface 0)         : xe-2/3/0.1
West interface (interface 1)         : xe-2/2/1.1
Restore interval                      : 5 minutes
Wait to Block interval               : 5 seconds
Guard interval                      : 500 ms
Hold off interval                    : 0 ms
Node ID                             : 64:87:88:65:37:D0
Ring ID (1 ... 239)                  : 1
Node role (normal/rpl-owner/rpl-neighbour) : normal
Revertive mode of operation          : 1
RAPS Tx Dot1p priority (0 .. 7)     : 0
Node type (normal/open/interconnection) : Normal
Control Vlan                         : 100
Physical Ring                        : No
Data Channel Vlan(s)                 : 200,300

```

**show protection-group ethernet-ring configuration (MX Series Router)**

```

user@switch>show protection-group ethernet-ring configuration
Ethernet Ring configuration information for protection group pg_101
G8032 Compatibility Version           : 2
East interface (interface 0)         : xe-2/3/0.1
West interface (interface 1)         : xe-2/2/1.1
Restore interval                      : 5 minutes
Wait to Block interval               : 5 seconds
Guard interval                      : 500 ms
Hold off interval                    : 0 ms
Node ID                             : 64:87:88:65:37:D0
Ring ID (1 ... 239)                  : 1
Node role (normal/rpl-owner/rpl-neighbour) : rpl-neighbour
Node RPL end                         : east-port
Revertive mode of operation          : 1
RAPS Tx Dot1p priority (0 .. 7)     : 0
Node type (normal/open/interconnection) : Normal
Control Vlan                         : 100

```

Physical Ring	: No
Data Channel Vlan(s)	: 200,300

### show protection-group ethernet-ring configuration detail (MX Series Router)

```

user@switch>show protection-group ethernet-ring configuration detail
Ethernet Ring configuration information for protection group pg_101
G8032 Compatibility Version          : 2
East interface (interface 0)        : xe-2/3/0.1
West interface (interface 1)        : xe-2/2/1.1
Restore interval                     : 5 minutes
Wait to Block interval              : 5 seconds
Guard interval                      : 500 ms
Hold off interval                   : 0 ms
Node ID                             : 64:87:88:65:37:D0
Ring ID (1 ... 239)                 : 1
Node role (normal/rpl-owner/rpl-neighbour) : rpl-owner
Node RPL end                        : east-port
Revertive mode of operation         : 1
RAPS Tx Dot1p priority (0 .. 7)    : 0
Node type (normal/open/interconnection) : Normal
Control Vlan                        : 100
Physical Ring                       : No
Data Channel Vlan(s)                : 200,300

```

### show protection-group ethernet-ring configuration detail (MX Series Router)

```

user@switch>show protection-group ethernet-ring configuration detail
Ethernet Ring configuration information for protection group pg_101
G8032 Compatibility Version          : 2
East interface (interface 0)        : xe-2/3/0.1
West interface (interface 1)        : (no erp)
Restore interval                     : 5 minutes
Wait to Block interval              : 5 seconds
Guard interval                      : 500 ms
Hold off interval                   : 0 ms
Node ID                             : 64:87:88:65:37:D0
Ring ID (1 ... 239)                 : 1
Node role (normal/rpl-owner/rpl-neighbour) : rpl-owner
Node RPL end                        : east-port

```

```

Revertive mode of operation      : 1
RAPS Tx Dot1p priority (0 .. 7) : 0
Node type (normal/open/interconnection) : Open
Control Vlan                    : 100
Physical Ring                   : No
Data Channel Vlan(s)            : 200,300

```

### show protection-group ethernet-ring configuration (MX Series Router)

```

user@switch>show protection-group ethernet-ring configuration
Ethernet Ring configuration information for protection group pg_major
G8032 Compatibility Version      : 2
East interface (interface 0)     : xe-2/3/0.1
West interface (interface 1)     : xe-2/2/1.1
Restore interval                 : 5 minutes
Wait to Block interval          : 5 seconds
Guard interval                   : 500 ms
Hold off interval                : 0 ms
Node ID                         : 64:87:88:65:37:D0
Ring ID (1 ... 239)             : 1
Node role (normal/rpl-owner/rpl-neighbour) : rpl-owner
Node RPL end                     : east-port
Revertive mode of operation      : 1
RAPS Tx Dot1p priority (0 .. 7) : 0
Node type (normal/open/interconnection) : Normal
Control Vlan                    : 100
Physical Ring                   : No
Data Channel Vlan(s)            : 200,300

Ethernet Ring configuration information for protection group pg_subring
G8032 Compatibility Version      : 2
East interface (interface 0)     : ge-2/0/0.1
West interface (interface 1)     : (no erp)
Restore interval                 : 5 minutes
Wait to Block interval          : 5 seconds
Guard interval                   : 500 ms
Hold off interval                : 0 ms
Node ID                         : 64:87:88:65:37:D0
Ring ID (1 ... 239)             : 2
Node role (normal/rpl-owner/rpl-neighbour) : normal
Revertive mode of operation      : 1

```

```

RAPS Tx Dot1p priority (0 .. 7)      : 0
Node type (normal/open/interconnection) : Non-VC-Interconnection
Major ring name                       : pg_major
Interconnection mode (VC/Non-VC)      : Non-VC mode
Propagate Topology Change event       : 0
Control Vlan                          : 101
Physical Ring                         : No
Data Channel Vlan(s)                  : 200,300

```

### show protection-group ethernet-ring configuration detail (MX Series Router)

```

user@switch>show protection-group ethernet-ring configuration detail
Ethernet Ring configuration information for protection group pg_major
G8032 Compatibility Version           : 2
East interface (interface 0)          : xe-2/3/0.1
West interface (interface 1)          : xe-2/2/1.1
Restore interval                      : 5 minutes
Wait to Block interval                : 5 seconds
Guard interval                       : 500 ms
Hold off interval                     : 0 ms
Node ID                              : 64:87:88:65:37:D0
Ring ID (1 ... 239)                  : 1
Node role (normal/rpl-owner/rpl-neighbour) : rpl-owner
Node RPL end                         : east-port
Revertive mode of operation           : 1
RAPS Tx Dot1p priority (0 .. 7)      : 0
Node type (normal/open/interconnection) : Normal
Control Vlan                         : 100
Physical Ring                        : No
Data Channel Vlan(s)                  : 200,300

Ethernet Ring configuration information for protection group pg_subring
G8032 Compatibility Version           : 2
East interface (interface 0)          : ge-2/0/0.1
West interface (interface 1)          : (no erp)
Restore interval                      : 5 minutes
Wait to Block interval                : 5 seconds
Guard interval                       : 500 ms
Hold off interval                     : 0 ms
Node ID                              : 64:87:88:65:37:D0
Ring ID (1 ... 239)                  : 2

```

```

Node role (normal/rpl-owner/rpl-neighbour) : normal
Revertive mode of operation                : 1
RAPS Tx Dot1p priority (0 .. 7)           : 0
Node type (normal/open/interconnection)    : Non-VC-Interconnection
Major ring name                            : pg_major
Interconnection mode (VC/Non-VC)           : Non-VC mode
Propagate Topology Change event            : 0
Control Vlan                              : 101
Physical Ring                             : No
Data Channel Vlan(s)                      : 200,300

```

## Release Information

Command introduced in Junos OS Release 12.1.

## RELATED DOCUMENTATION

*show protection-group ethernet-ring aps*

---

*show protection-group ethernet-ring data-channel*

---

*show protection-group ethernet-ring interface*

---

*show protection-group ethernet-ring node-state*

---

*show protection-group ethernet-ring statistics*

---

*show protection-group ethernet-ring vlan*

## show protection-group ethernet-ring data-channel

### IN THIS SECTION

- [Syntax | 1454](#)
- [Description | 1454](#)
- [Options | 1454](#)
- [Required Privilege Level | 1454](#)
- [Output Fields | 1454](#)
- [Sample Output | 1455](#)

## Syntax

```
show protection-group ethernet-ring data-channel  
<brief | detail>  
<group-name group-name>
```

## Description

Display the configuration of Ethernet ring protection group on EX Switches and MX Series routers.

## Options

**brief | detail** (Optional) Display the specified level of output.

***group-name*** (Optional) Protection group for which to display statistics. If you omit this optional field, all protection group statistics for configured groups will be displayed.

## Required Privilege Level

view

## Output Fields

[Table 65 on page 1455](#) lists the output fields for the `show protection-group ethernet-ring data-channel` command. Output fields are listed in the approximate order in which they appear.



Table 65: show protection-group ethernet-ring data-channel Output Fields

Field Name	Field Description
<b>Interface</b>	Name of the interface configured for the Ethernet ring.
<b>STP index</b>	The Spanning Tree Protocol (STP) index number used by each interface in an Ethernet ring. The STP index controls the forwarding behavior for a set of VLANs on a data channel on an Ethernet ring port. For multiple Ethernet ring instances on a physical ring port, there are multiple STP index numbers. Different ring instances will have different STP index numbers and may have different forwarding behavior.
<b>Forward State</b>	Forwarding state on the Ethernet ring. <ul style="list-style-type: none"> <li>• <b>forwarding</b>—Indicates packets are being forwarded.</li> <li>• <b>discarding</b>—Indicates packets are being discarded.</li> </ul>

## Sample Output

### show protection-group ethernet-ring data-channel

```

user@host> show protection-group ethernet-ring data-channel
Ethernet ring data channel information for protection group pg301

Interface    STP index  Forward State
xe-5/0/2     78         forwarding
xe-2/2/0     79         discarding

Ethernet ring data channel parameters for protection group pg302

Interface    STP index  Forward State
xe-5/0/2     80         forwarding
xe-2/2/0     81         forwarding

```

**show protection-group ethernet-ring data-channel detail**

```
user@host> show protection-group ethernet-ring data-channel detail
```

```
Ethernet ring data channel parameters for protection group pg301
```

```
Interface name      : xe-5/0/2
STP index           : 78
Forward State       : forwarding
```

```
Interface name      : xe-2/2/0
STP index           : 79
Forward State       : discarding
```

```
Ethernet ring data channel parameters for protection group pg302
```

```
Interface name      : xe-5/0/2
STP index           : 80
Forward State       : forwarding
```

```
Interface name      : xe-2/2/0
STP index           : 81
Forward State       : forwarding
```

**show protection-group ethernet-ring data-channel detail (EX2300 and EX3400 Switches)**

```
user@switch>show protection-group ethernet-ring data-channel detail
```

```
Ethernet ring data channel parameters for protection group pg1001
```

```
Interface name      : ge-0/0/42
STP index           : 52
Forward State       : discarding
```

```
Interface name      : ge-0/0/38
STP index           : 53
Forward State       : forwarding
```

## Release Information

Command introduced in Junos OS Release 10.2.

## RELATED DOCUMENTATION

<i>show protection-group ethernet-ring aps</i>
<i>show protection-group ethernet-ring interface</i>
<i>show protection-group ethernet-ring node-state</i>
<i>show protection-group ethernet-ring statistics</i>
<i>show protection-group ethernet-ring vlan</i>

## show protection-group ethernet-ring flush-info

### IN THIS SECTION

- [Syntax | 1457](#)
- [Description | 1457](#)
- [Options | 1458](#)
- [Required Privilege Level | 1458](#)
- [Output Fields | 1458](#)
- [Sample Output | 1458](#)
- [Release Information | 1459](#)

## Syntax

```
show protection-group ethernet-ring flush-info
```

## Description

Display information about flush ports in an Ethernet ring.

# Options

This command has no options.

# Required Privilege Level

view

# Output Fields

[Table 66 on page 1458](#) lists the output fields for the `show protection-group ethernet-ring flush-info` command. Output fields are listed in the approximate order in which they appear.

**Table 66: show protection-group ethernet-ring flush-info Output Fields**

Field Name	Field Description
Interface	Physical interface configured for the Ethernet ring. This can be an aggregated Ethernet link also.
Originating Node	Node from which RAPS protocol data units originates on the Ethernet Ring.
Blocked Port Reference	Reference of the ring port on which traffic is blocked.

# Sample Output

## show protection-group ethernet-ring flush-info (ACX and MX Series Routers)

```

user@host> show protection-group ethernet-ring flush-info
Ethernet ring flush port information for protection group pg100

Interface      Originating Node  Blocked Port Reference
xe-5/0/2.4001  00:00:00:00:00:00  0
xe-2/2/0.4001  00:00:00:00:00:00  0

```

## show protection-group ethernet-ring flush-info detail (ACX and MX Series Routers)

```
user@host> show protection-group ethernet-ring flush-info detail
```

Ethernet ring flush port information for protection group pg100

```
Interface name           : xe-5/0/2.4001
Originating Node         : 00:00:00:00:00:00
Blocked Port Reference    : 0
```

```
Interface name           : xe-2/2/0.4001
Originating Node         : 00:00:00:00:00:00
Blocked Port Reference    : 0
```

## Release Information

Command introduced in Junos OS Release 14.2.

## RELATED DOCUMENTATION

*show protection-group ethernet-ring data-channel*

*show protection-group ethernet-ring aps*

*show protection-group ethernet-ring node-state*

*show protection-group ethernet-ring statistics*

*show protection-group ethernet-ring vlan*

## show protection-group ethernet-ring interface

### IN THIS SECTION

- [Syntax | 1460](#)
- [Description | 1460](#)
- [Options | 1460](#)
- [Required Privilege Level | 1460](#)

- [Output Fields | 1460](#)
- [Sample Output | 1461](#)
- [Release Information | 1464](#)

Syntax

```
show protection-group ethernet-ring interface
```

Description

Displays the status of the Automatic Protection Switching (APS) interfaces on an Ethernet ring.

Options

This command has no options.

Required Privilege Level

view

Output Fields

[Table 67 on page 1460](#) lists the output fields for both the EX Series switch, and the ACX Series and MX Series router show protection-group ethernet-ring interface commands. Output fields are listed in the approximate order in which they appear.

**Table 67: MX Series Routers show protection-group ethernet-ring interface Output Fields**

Field Name	Field Description
Ethernet ring port parameters for protection group <i>group-name</i>	Output is organized by configured protection group.

Table 67: MX Series Routers show protection-group ethernet-ring interface Output Fields *(Continued)*

Field Name	Field Description
<b>Interface</b>	Physical interfaces configured for the Ethernet ring. This can be an aggregated Ethernet link also.
<b>Control Channel</b>	(MX Series router only) Logical unit configured on the physical interface.
<b>Direction</b>	Direction of the traffic.
<b>Forward State</b>	State of the ring forwarding on the interface: <b>discarding</b> or <b>forwarding</b> .
<b>Ring Protection Link End</b>	Whether this interface is the end of the ring: <b>Yes</b> or <b>No</b> .
<b>Signal Failure</b>	Whether there a signal failure exists on the link: <b>Clear</b> or <b>Set</b> .
<b>Admin State</b>	State of the interface: For EX switches, <b>ready</b> , <b>ifl ready</b> , or <b>waiting</b> . For MX routers, <b>IFF ready</b> or <b>IFF disabled</b> .

## Sample Output

### show protection-group ethernet-ring interface (EX Series Switch Owner Node)

```

user@host> show protection-group ethernet-ring interface
Ethernet ring port parameters for protection group pg101

Interface      Forward State  RPL End  Signal Failure  Admin State
-----
ge-0/0/3.0     discarding     Yes       Clear           ready
ge-0/0/9.0     forwarding     No        Clear           ready

```

**show protection-group ethernet-ring interface (Owner Node MX Series Router )**

```
user@host> show protection-group ethernet-ring interface
```

```
Ethernet ring port parameters for protection group pg101
```

Interface	Control Channel	Direction	Forward State	RPL End	SF	Admin State
ge-1/2/0	ge-1/2/0.100	east	forwarding	No	Clear	IFF ready
ge-1/2/2	ge-1/2/2.100	west	forwarding	No	Clear	IFF ready

**show protection-group ethernet-ring interface detail (Owner Node MX Series Router )**

```
user@host> show protection-group ethernet-ring interface detail
```

```
Ethernet ring port parameters for protection group pg101
```

```
Interface name           : ge-1/2/0
Control channel name     : ge-1/2/0.100
Interface direction      : east
Ring Protection Link End : No
Signal Failure           : Clear
Forward State            : forwarding
Interface Admin State    : IFF ready
```

```
Interface name           : ge-1/2/2
Control channel name     : ge-1/2/2.100
Interface direction      : west
Ring Protection Link End : No
Signal Failure           : Clear
Forward State            : forwarding
Interface Admin State    : IFF ready
```

**show protection-group ethernet-ring interface (EX Series Switch Ring Node)**

```
user@host> show protection-group ethernet-ring interface
```

```
Ethernet ring port parameters for protection group pg102
```

```
Ethernet ring port parameters for protection group pg101
```

Interface	Forward State	RPL End	Signal Failure	Admin State
-----------	---------------	---------	----------------	-------------



ge-0/0/3.0	discarding	Yes	Clear	ready
ge-0/0/9.0	forwarding	No	Clear	ready

### show protection-group ethernet-ring interface detail (ACX Series and MX Series)

```
user@host> show protection-group ethernet-ring interface detail
```

Ethernet ring port parameters for protection group Erp\_1

```
Interface name           : xe-0/0/0
Control channel name     : xe-0/0/0.1
Interface direction      : east
Ring Protection Link End : No
Signal Failure           : Clear
Forward State            : forwarding
Interface Admin State    : IFF ready
```

```
Interface name           : et-0/0/48
Control channel name     : et-0/0/48.1
Interface direction      : west
Ring Protection Link End : No
Signal Failure           : Clear
Forward State            : forwarding
Interface Admin State    : IFF ready
```

### show protection-group ethernet-ring interface detail (EX2300 and EX3400 Switches)

```
user@switch>show protection-group ethernet-ring interface detail
```

Ethernet ring port parameters for protection group pg1001

```
Interface name           : ge-0/0/14
Control channel name     : ge-0/0/14.0
Interface direction      : east
Ring Protection Link End : No
Signal Failure           : Clear
Forward State            : forwarding
Interface Admin State    : IFF ready
```

```
Interface name           : ge-0/0/18
Control channel name     : ge-0/0/18.0
```

```

Interface direction      : west
Ring Protection Link End : No
Signal Failure          : Clear
Forward State           : forwarding
Interface Admin State    : IFF ready

```

## show protection-group ethernet-ring interface detail (EX2300 and EX3400 Switches)

```

user@switch>show protection-group ethernet-ring interface detail
Ethernet ring port parameters for protection group pg1001

```

```

Interface name          : ge-0/0/42
Control channel name    : ge-0/0/42.0
Interface direction     : east
Ring Protection Link End : Yes
Signal Failure          : Clear
Forward State           : discarding
Interface Admin State    : IFF ready

```

```

Interface name          : ge-0/0/38
Control channel name    : ge-0/0/38.0
Interface direction     : west
Ring Protection Link End : No
Signal Failure          : Clear
Forward State           : forwarding
Interface Admin State    : IFF ready

```

## Release Information

Command introduced in Junos OS Release 9.4.

Command introduced in Junos OS Release 12.3X54 for ACX Series routers.

## RELATED DOCUMENTATION

---

*show protection-group ethernet-ring data-channel*

---

*show protection-group ethernet-ring aps*

---

*show protection-group ethernet-ring node-state*

---

*show protection-group ethernet-ring statistics*

---

| *show protection-group ethernet-ring vlan*

## show protection-group ethernet-ring node-state

### IN THIS SECTION

- [Syntax | 1465](#)
- [Description | 1465](#)
- [Options | 1465](#)
- [Required Privilege Level | 1465](#)
- [Output Fields | 1466](#)
- [Sample Output | 1468](#)
- [Release Information | 1471](#)

### Syntax

```
show protection-group ethernet-ring node-state
```

### Description

Display the status of the Automatic Protection Switching (APS) nodes on an Ethernet ring.

### Options

This command has no options.

### Required Privilege Level

view

Output Fields

Table 68 on page 1466 lists the output fields for the show protection-group ethernet-ring node-state command. Output fields are listed in the approximate order in which they appear.

Table 68: show protection-group ethernet-ring node-state Output Fields

Field Name	Field Description
Ring Name/Ethernet Ring	Name configured for the Ethernet ring.
APS State	<div>State of the Ethernet ring APS.</div> <div><ul style="list-style-type: none"><li>• <b>idle</b>—Indicates that the ring is working in normal condition and there is no active or pending protection-switching request in the ring. When the ring is in idle state, it is blocked at the RPL link.</li><li>• <b>protected</b>—Indicates that there is a protection switch on the ring because of a signal failure condition on the ring link.</li><li>• <b>MS</b>—Indicates that the manual switch command is active in the ring.</li><li>• <b>FS</b>—Indicates that the forced switch command is active in the ring.</li><li>• <b>pending</b>—Indicates that the ring is in pending state.</li></ul></div>

Table 68: show protection-group ethernet-ring node-state Output Fields (*Continued*)

Field Name	Field Description
<b>Event</b>	<p>Events on the ring.</p> <ul style="list-style-type: none"> <li>• <b>NR-RB</b>—Indicates that there is no APS request and the ring link is blocked on the ring owner node.</li> <li>• <b>NR</b>—Indicates that there is no APS request pending in the ring.</li> <li>• <b>local SF</b>—Indicates that there is signal failure on one or both of the ring links of the node.</li> <li>• <b>remote SF</b>—Indicates that there is signal failure on one or more ring links of any other node of the ring.</li> <li>• <b>local FS</b>—Indicates that there is a forced switched command active on one or both of the ring links of the node.</li> <li>• <b>remote FS</b>—Indicates that there is a forced switch command active on one or more ring links of any other node of the ring.</li> <li>• <b>local MS</b>—Indicates that there is a manual switch command active on one of the ring links of the node.</li> <li>• <b>remote MS</b>—Indicates that there is a manual switch command active on one or more ring links of any other node of the ring.</li> <li>• <b>WTR running</b>—Indicates that the wait to restore timer is running on the RPL owner.</li> <li>• <b>WTB running</b>—Indicates that the wait to block timer is running on the RPL owner.</li> </ul>
<b>RPL Owner / Ring Protection Link Owner</b>	Whether this node is the ring owner: <b>Yes</b> or <b>No</b> .
<b>WTR Timer / Restore Timer</b>	Restoration timer: <b>running</b> or <b>disabled</b> .

Table 68: show protection-group ethernet-ring node-state Output Fields *(Continued)*

Field Name	Field Description
<b>WTB Timer / Wait to block timer</b>	Wait to block timer: <b>running</b> or <b>disabled</b> .  <b>NOTE:</b> The Wait To Block Timer (WTB) is always disabled on EX2300 and EX3400 switches because it is not supported in ERPSv1. Any configuration you make to the WTB setting has no effect. The output from the CLI command 'show protection-group ethernet-ring node-state detail' lists a WTB setting but that setting has no effect.
<b>Wait to block timer (WTB Timer)</b>	Wait to block interval.  <b>NOTE:</b> The Wait To Block Timer (WTB) is always disabled on EX2300 and EX3400 switches because it is not supported in ERPSv1. Any configuration you make to the WTB setting has no effect. The output from the CLI command 'show protection-group ethernet-ring node-state detail' lists a WTB setting but that setting has no effect.
<b>Guard Timer</b>	Guard timer: <b>running</b> or <b>disabled</b> .
<b>Op State / Operational State</b>	State of the node: <b>Operational</b> or <b>any internal wait state..</b>

## Sample Output

**show protection-group ethernet-ring node-state (MX Series Router - RPL Owner Node, Normal Operation)**

```

user@host> show protection-group ethernet-ring node-state
Ethernet ring  APS State  Event      RPL Owner  WTR Timer  WTB Timer  Guard Timer  Operation
state
pg101          idle      NR-RB      Yes        disabled   disabled   disabled
operational
pg102          idle      NR-RB      No         disabled   disabled   disabled     operational

```

### show protection-group ethernet-ring node-state (MX Series Router - Normal Ring Node, Normal Operation)

```
user@host> show protection-group ethernet-ring node-state
Ethernet ring    APS State    Event        RPL Owner
pg102           idle        NR-RB        No

WTR Timer        WTB Timer    Guard Timer    Operation state
disabled disabled        disabled        operational
```

### show protection-group ethernet-ring node-state (MX Series Router - RPL Owner Node, Remote Failure Condition)

```
user@host> show protection-group ethernet-ring node-state
Ethernet ring    APS State    Event        RPL Owner
pg101           protected    remote SF        Yes

WTR Timer        WTB Timer    Guard Timer    Operation state
disabled disabled        disabled        operational
```

### show protection-group ethernet-ring node-state detail (ACX Series and MX Series Router)

```
user@host> show protection-group ethernet-ring node-state detail
Ethernet-Ring name      : Erp_1
APS State                : idle
Event                   : NR-RB
Ring Protection Link Owner : No
Wait to Restore Timer    : disabled
Wait to Block Timer      : disabled
Guard Timer             : disabled
Operation state          : operational
```

### show protection-group ethernet-ring node-state detail (MX Series Router - RPL Owner Node, Normal Operation)

```
user@host> show protection-group ethernet-ring node-state detail
Ethernet-Ring name      : pg101
```

```

APS State           : idle
Event               : NR-RB
Ring Protection Link Owner : Yes
Wait to Restore Timer : disabled
Wait to Block Timer  : disabled
Guard Timer         : disabled
Operation state      : operational

```

```

Ethernet-Ring name   : pg102
APS State            : idle
Event               : NR-RB
Ring Protection Link Owner : No
Wait to Restore Timer : disabled
Wait to Block Timer  : disabled
Guard Timer         : disabled
Operation state      : operational

```

### **show protection-group ethernet-ring node-state detail (MX Series Router with WTR Timer)**

```

user@host> show protection-group ethernet-ring node-state detail

Ethernet-Ring name   : pg_major
APS State            : pending
Event               : WTR running
Ring Protection Link Owner : Yes
Wait to Restore Timer : running (time to expire: 269 sec)
Wait to Block Timer  : disabled
Guard Timer         : disabled
Operation state      : operational

Ethernet-Ring name   : pg_subring
APS State            : pending
Event               : NR
Ring Protection Link Owner : No
Wait to Restore Timer : disabled
Wait to Block Timer  : disabled
Guard Timer         : disabled
Operation state      : operational

```



## show protection-group ethernet-ring node-state detail (MX Series Router with WTB Timer)

```
user@host> show protection-group ethernet-ring node-state detail
Ethernet-Ring name      : Pg-2
APS State               : pending
Event                  : WTB running
Ring Protection Link Owner : Yes
Wait to Restore Timer   : disabled
Wait to Block Timer     : running (time to expire: 2 sec)
Guard Timer            : disabled
Operation state         : operational
```

## show protection-group ethernet-ring node-state detail (EX2300 and EX3400 Switches)

```
user@switch>show protection-group ethernet-ring node-state detail
Ethernet-Ring name      : pg1001
APS State               : idle
Event                  : NR-RB
Ring Protection Link Owner : Yes
Wait to Restore Timer   : disabled
Wait to Block Timer     : disabled  <-field not supported. Always disabled.
Guard Timer            : disabled
Operation state         : operational
```

## Release Information

Command introduced in Junos OS Release 9.4.

Command introduced in Junos OS Release 12.3X54 for ACX Series routers.

## RELATED DOCUMENTATION

*show protection-group ethernet-ring data-channel*

*show protection-group ethernet-ring aps*

*show protection-group ethernet-ring interface*

*show protection-group ethernet-ring statistics*

*show protection-group ethernet-ring vlan*

## show protection-group ethernet-ring statistics

### IN THIS SECTION

- [Syntax | 1472](#)
- [Description | 1472](#)
- [Options | 1472](#)
- [Required Privilege Level | 1472](#)
- [Output Fields | 1473](#)
- [Sample Output | 1475](#)
- [Release Information | 1479](#)

### Syntax

```
show protection-group ethernet-ring statistics group-name group-name
```

<brief | detail>

### Description

Display statistics regarding Automatic Protection Switching (APS) protection groups on an Ethernet ring.

### Options

**group-name** Display statistics for the protection group. If you omit this option, protection group statistics for all configured groups are displayed.

**brief**—Display brief statistics for the protection group.

**detail**—Display detailed statistics for the protection group.

### Required Privilege Level

view

## Output Fields

Table 69 on page 1473 lists the output fields for the show protection-group ethernet-ring statistics command.

**Table 69: show protection-group ethernet-ring statistics Output Fields**

Field Name	Field Description
<b>Ethernet Ring Statistics for PG</b>	Name of the protection group for which statistics are displayed.
<b>RAPS event sent</b>	Number of times Ring Automatic Protection Switching (RAPS) message transmission event occurred locally. This field is applicable only to MX Series routers.
<b>RAPS event received</b>	Number of RAPS messages received and processed by ERP state-machine and which resulted in state transition. This field is applicable only to MX Series routers.
<b>Local SF</b>	Number of times a signal failure has occurred locally.
<b>Remote SF</b>	Number of times a signal failure has occurred anywhere else on the ring.
<b>NR event</b>	Number of times a No Request event has occurred on the ring. This field is applicable only to EX Series switches.
NR event sent	Number of times a No Request event has occurred locally. This field is applicable only to MX Series routers.
NR event received	Number of times a No Request event has occurred anywhere else on the ring. This field is applicable only to MX Series routers.
<b>NR-RB event</b>	Number of times a No Request, Ring Blocked event has occurred on the ring. This field is applicable only to EX Series switches.
NR-RB event sent	Number of times a No Request, Ring Blocked event has occurred locally. This field is applicable only to MX Series routers.

**Table 69: show protection-group ethernet-ring statistics Output Fields (Continued)**

Field Name	Field Description
NR-RB event received	Number of times a No Request, Ring Blocked event has occurred anywhere else on the ring. This field is applicable only to MX Series routers.
Flush event sent	Number of times flush-event RAPS message transmission event occurred locally. This field is applicable only to MX Series routers.
Flush event received	Number of flush-event RAPS messages received and processed by the ring instance control process. This field is applicable only to MX Series routers.
Local FS event sent	Number of times a forced switch event has occurred locally. This field is applicable only to MX Series routers.
Remote FS event received	Number of times a forced switch event has occurred anywhere else on the ring. This field is applicable only to MX Series routers.
Local MS event sent	Number of times a manual switch event has occurred locally. This field is applicable only to MX Series routers.
Remote MS event received	Number of times a manual switch event has occurred anywhere else on the ring. This field is applicable only to MX Series routers.

[Table 70 on page 1474](#) lists the output fields for the show protection-group ethernet-ring statistics command when the detail option is used. These fields are valid only for MX Series routers.

**Table 70: show protection-group ethernet-ring statistics detail Output Fields (for MX Series Routers)**

Field Name	Field Description
Total number of FDB flush	Number of times forwarding database (FDB) flush has happened for the ring instance.
Flush-logic triggered flush	Number of times FDB flush has happened because of flush-logic based on node ID and Blocked Port Reference (BPR).

**Table 70: show protection-group ethernet-ring statistics detail Output Fields (for MX Series Routers)**  
*(Continued)*

Field Name	Field Description
Remote RAPS PDU received	Number of valid RAPS PDU messages received. This counter counts only RAPS messages generated by other devices on the ring.
Remote RAPS dropped due to guard-timer	Number of RAPS messages dropped by the device because the guard timer is running.
Invalid remote RAPS PDU dropped	Number of RAPS messages dropped by the device because the messages are invalid.
RAPS dropped due to miscellaneous errors	Number of RAPS messages dropped because of any other reason. For example, messages dropped because of unsupported functionality.
Local received RAPS PDU dropped	Number of self-generated RAPS messages received and dropped.

## Sample Output

### show protection-group ethernet-ring statistics (EX Series Switch)

```
user@switch> show protection-group ethernet-ring statistics
Ring Name Local SF Remote SF NR Event NR-RB Event
erp1      2      1      2      3
```

### show protection-group ethernet-ring statistics (MX Series Router)

```
user@host> show protection-group ethernet-ring statistics
Ethernet Ring statistics for PG Pg-1
RAPS event sent           : 1
RAPS event received       : 1152
Local SF happened:        : 0
Remote SF happened:       : 428
```

```

NR event sent:           : 1
NR event received:       : 133
NR-RB event sent:        : 0
NR-RB event received:    : 591
Flush event sent         : 0
Flush event received:    : 0
Local FS event sent:     : 0
Remote FS event received: : 0
Local MS event sent:     : 0
Remote MS event received: : 0

```

### **show protection-group ethernet-ring statistics detail (Specific Group)(MX Series Router)**

```
user@host> show protection-group ethernet-ring statistics detail
```

```
Ethernet Ring statistics for PG Pg-1
```

```

RAPS event sent           : 1
RAPS event received       : 0
Local SF happened         : 0
Remote SF happened        : 0
NR event sent             : 1
NR event received         : 0
NR-RB event sent          : 0
NR-RB event received      : 0
Flush event sent          : 0
Flush event received      : 0
Local FS event sent       : 0
Remote FS event received  : 0
Local MS event sent       : 0
Remote MS event received  : 0
Total number of FDB flush : 0
Flush-logic triggered flush : 0
Remote raps PDU received  : 0
Remote raps dropped due to guard-timer : 0
Invalid remote raps PDU dropped : 0
Raps dropped due to miscellaneous errors : 0
Local received raps PDU dropped : 0

```

### show protection-group ethernet-ring statistics (Owner Node, Failure Condition on ACX and MX Router)

```

user@host> show protection-group ethernet-ring statistics group-name pg101
Ethernet Ring statistics for PG pg101
RAPS sent : 1
RAPS received : 0
Local SF happened: : 0
Remote SF happened: : 0
NR event happened: : 0
NR-RB event happened: : 1
NR event sent: : 0
NR event received: : 0
NR-RB event sent: : 1
NR-RB event received: : 0
Flush event sent : 0
Flush event received: : 0
Local FS event sent: : 0
Remote FS event received: : 0
Local MS event sent: : 0
Remote MS event received: : 0

```

### show protection-group ethernet-ring statistics (Ring Node, Failure Condition on ACX and MX Router)

```

user@host> show protection-group ethernet-ring statistics group-name pg102
Ethernet Ring statistics for PG pg102
RAPS sent : 1
RAPS received : 0
Local SF happened: : 0
Remote SF happened: : 0
NR event happened: : 0
NR-RB event happened: : 1
NR event sent: : 0
NR event received: : 0
NR-RB event sent: : 1
NR-RB event received: : 0
Flush event sent : 0
Flush event received: : 0
Local FS event sent: : 0

```

```

Remote FS event received:      : 0
Local MS event sent:          : 0
Remote MS event received:      : 0

```

### show protection-group ethernet-ring statistics detail (EX2300 and EX3400 Switches)

```

user@switch>show protection-group ethernet-ring statistics detail
Ethernet Ring statistics for PG pg1001
RAPS event sent                : 1
RAPS event received            : 1
Local SF happened              : 0
Remote SF happened             : 0
NR event sent                  : 1
NR event received              : 0
NR-RB event sent               : 0
NR-RB event received          : 1
Flush event sent               : 0
Flush event received           : 0
Local FS event sent            : 0
Remote FS event received       : 0
Local MS event sent            : 0
Remote MS event received       : 0
Total number of FDB flush      : 0
Flush-logic triggered flush    : 0
Remote raps PDU received       : 145
Remote raps dropped due to guard-timer : 0
Invalid remote raps PDU dropped : 0
Raps dropped due to miscellaneous errors : 0
Local received raps PDU dropped : 0

```

### show protection-group ethernet-ring statistics detail (EX2300 and EX3400 Switches)

```

user@switch>show protection-group ethernet-ring statistics detail
Ethernet Ring statistics for PG pg1001
RAPS event sent                : 2
RAPS event received            : 0
Local SF happened              : 0
Remote SF happened             : 0
NR event sent                  : 1
NR event received              : 0

```



```

NR-RB event sent           : 1
NR-RB event received       : 0
Flush event sent           : 0
Flush event received       : 0
Total number of FDB flush  : 0
Remote raps PDU received   : 211
Remote raps dropped due to guard-timer : 0
Invalid remote raps PDU dropped : 0
Raps dropped due to miscellaneous errors : 0
Local received raps PDU dropped : 91

```

## Release Information

Command introduced in Junos OS Release 9.4.

Command introduced in Junos OS Release 12.3X54 for ACX Series routers.

## RELATED DOCUMENTATION

*show protection-group ethernet-ring data-channel*

*show protection-group ethernet-ring aps*

*show protection-group ethernet-ring node-state*

*show protection-group ethernet-ring interface*

*show protection-group ethernet-ring vlan*

## show protection-group ethernet-ring vlan

### IN THIS SECTION

- [Syntax | 1480](#)
- [Description | 1480](#)
- [Options | 1480](#)
- [Required Privilege Level | 1480](#)
- [Output Fields | 1480](#)

- [Sample Output | 1481](#)
- [Release Information | 1485](#)

### Syntax

```
show protection-group ethernet-ring vlan
<brief | detail>
<group-name group-name>
```

### Description

On MX Series routers, display all data channel logical interfaces and the VLAN IDs controlled by a ring instance data channel.

### Options

- brief | detail** (Optional) Display the specified level of output.
- group-name*** (Optional) Protection group for which to display details such as data channel interfaces, vlan, and bridge-domain. If you omit this optional field, details for all configured protection groups will be displayed.

### Required Privilege Level

view

### Output Fields

[Table 71 on page 1481](#) lists the output fields for the show protection-group ethernet-ring vlan command. Output fields are listed in the approximate order in which they appear.

**Table 71: show protection-group ethernet-ring vlan Output Fields**

Field Name	Field Description
<b>Interface</b>	Name of the interface configured for the Ethernet protection ring.
<b>Vlan</b>	Name of the VLAN associated with the interface configured for the Ethernet protection ring.
<b>STP index</b>	The Spanning Tree Protocol (STP) index number used by each interface in an Ethernet ring. The STP index controls the forwarding behavior for a set of VLANs on a data channel on an Ethernet ring port. For multiple Ethernet ring instances on an physical ring port, there are multiple STP index numbers. Different ring instances will have different STP index numbers and may have different forwarding behavior.
<b>Bridge Domain</b>	Name of the bridge domain that is associated with the VLAN configured for the Ethernet protection ring.

## Sample Output

### show protection-group ethernet-ring vlan

```
user@host> show protection-group ethernet-ring vlan
Ethernet ring IFBD parameters for protection group vkm01
```

Interface	Vlan	STP Index	Bridge Domain
xe-5/0/2	1	78	default-switch/bd1
xe-2/2/0	1	79	default-switch/bd1
xe-5/0/2	2	78	default-switch/bd2
xe-2/2/0	2	79	default-switch/bd2
xe-5/0/2	3	78	default-switch/bd3
xe-2/2/0	3	79	default-switch/bd3
xe-5/0/2	4	78	default-switch/bd4
xe-2/2/0	4	79	default-switch/bd4
xe-5/0/2	5	78	default-switch/bd5
xe-2/2/0	5	79	default-switch/bd5
xe-5/0/2	6	78	default-switch/bd6
xe-2/2/0	6	79	default-switch/bd6

xe-5/0/2	7	78	default-switch/bd7
xe-2/2/0	7	79	default-switch/bd7
xe-5/0/2	8	78	default-switch/bd8
xe-2/2/0	8	79	default-switch/bd8
xe-5/0/2	9	78	default-switch/bd9
xe-2/2/0	9	79	default-switch/bd9
xe-5/0/2	10	78	default-switch/bd10
xe-2/2/0	10	79	default-switch/bd10
xe-5/0/2	11	78	default-switch/bd11
xe-2/2/0	11	79	default-switch/bd11
xe-5/0/2	12	78	default-switch/bd12
xe-2/2/0	12	79	default-switch/bd12
xe-5/0/2	13	78	default-switch/bd13
xe-2/2/0	13	79	default-switch/bd13
xe-5/0/2	14	78	default-switch/bd14
xe-2/2/0	14	79	default-switch/bd14
xe-5/0/2	15	78	default-switch/bd15
xe-2/2/0	15	79	default-switch/bd15

### show protection-group ethernet-ring vlan brief

```
user@host> show protection-group ethernet-ring vlan brief
Ethernet ring IFBD parameters for protection group vkm01
```

Interface	Vlan	STP Index	Bridge Domain
xe-5/0/2	1	78	default-switch/bd1
xe-2/2/0	1	79	default-switch/bd1
xe-5/0/2	2	78	default-switch/bd2
xe-2/2/0	2	79	default-switch/bd2
xe-5/0/2	3	78	default-switch/bd3
xe-2/2/0	3	79	default-switch/bd3
xe-5/0/2	4	78	default-switch/bd4
xe-2/2/0	4	79	default-switch/bd4
xe-5/0/2	5	78	default-switch/bd5
xe-2/2/0	5	79	default-switch/bd5
xe-5/0/2	6	78	default-switch/bd6
xe-2/2/0	6	79	default-switch/bd6
xe-5/0/2	7	78	default-switch/bd7
xe-2/2/0	7	79	default-switch/bd7
xe-5/0/2	8	78	default-switch/bd8
xe-2/2/0	8	79	default-switch/bd8

xe-5/0/2	9	78	default-switch/bd9
xe-2/2/0	9	79	default-switch/bd9
xe-5/0/2	10	78	default-switch/bd10
xe-2/2/0	10	79	default-switch/bd10
xe-5/0/2	11	78	default-switch/bd11
xe-2/2/0	11	79	default-switch/bd11
xe-5/0/2	12	78	default-switch/bd12
xe-2/2/0	12	79	default-switch/bd12
xe-5/0/2	13	78	default-switch/bd13
xe-2/2/0	13	79	default-switch/bd13
xe-5/0/2	14	78	default-switch/bd14
xe-2/2/0	14	79	default-switch/bd14
xe-5/0/2	15	78	default-switch/bd15
xe-2/2/0	15	79	default-switch/bd15

### show protection-group ethernet-ring vlan detail

```
user@host> show protection-group ethernet-ring vlan detail
```

Ethernet ring IFBD parameters for protection group vkm01

```
Interface name      : xe-5/0/2
Vlan                : 1
STP index           : 78
Bridge Domain       : default-switch/bd1
```

```
Interface name      : xe-2/2/0
Vlan                : 1
STP index           : 79
Bridge Domain       : default-switch/bd1
```

```
Interface name      : xe-5/0/2
Vlan                : 2
STP index           : 78
Bridge Domain       : default-switch/bd2
```

```
Interface name      : xe-2/2/0
Vlan                : 2
STP index           : 79
Bridge Domain       : default-switch/bd2
```

```
Interface name      : xe-5/0/2
```

```

Vlan                : 3
STP index            : 78
Bridge Domain        : default-switch/bd3

```

### show protection-group ethernet-ring vlan group-name vkm01

```
user@host> show protection-group ethernet-ring vlan vkm01
```

Ethernet ring IFBD parameters for protection group vkm01

Interface	Vlan	STP Index	Bridge Domain
xe-5/0/2	16	80	default-switch/bd16
xe-2/2/0	16	81	default-switch/bd16
xe-5/0/2	17	80	default-switch/bd17
xe-2/2/0	17	81	default-switch/bd17
xe-5/0/2	18	80	default-switch/bd18
xe-2/2/0	18	81	default-switch/bd18
xe-5/0/2	19	80	default-switch/bd19
xe-2/2/0	19	81	default-switch/bd19
xe-5/0/2	20	80	default-switch/bd20
xe-2/2/0	20	81	default-switch/bd20
xe-5/0/2	21	80	default-switch/bd21
xe-2/2/0	21	81	default-switch/bd21
xe-5/0/2	22	80	default-switch/bd22
xe-2/2/0	22	81	default-switch/bd22
xe-5/0/2	23	80	default-switch/bd23
xe-2/2/0	23	81	default-switch/bd23
xe-5/0/2	24	80	default-switch/bd24
xe-2/2/0	24	81	default-switch/bd24
xe-5/0/2	25	80	default-switch/bd25
xe-2/2/0	25	81	default-switch/bd25
xe-5/0/2	26	80	default-switch/bd26
xe-2/2/0	26	81	default-switch/bd26
xe-5/0/2	27	80	default-switch/bd27
xe-2/2/0	27	81	default-switch/bd27
xe-5/0/2	28	80	default-switch/bd28
xe-2/2/0	28	81	default-switch/bd28
xe-5/0/2	29	80	default-switch/bd29
xe-2/2/0	29	81	default-switch/bd29

xe-5/0/2	30	80	default-switch/bd30
xe-2/2/0	30	81	default-switch/bd30

### show protection-group ethernet-ring vlan detail (EX2300 and EX3400 Switches)

```
user@switch>show protection-group ethernet-ring vlan detail
Ethernet ring IFBD parameters for protection group pg1001
```

```
Interface name      : ge-0/0/42
Vlan                : 2001
STP index           : 52
Bridge Domain       : default-switch/vlan2001
```

```
Interface name      : ge-0/0/38
Vlan                : 2001
STP index           : 53
Bridge Domain       : default-switch/vlan2001
```

## Release Information

Command introduced in Junos OS Release 10.2.

Command introduced in Junos OS Release 18.1 for EX2300 and EX3400 switches.

## RELATED DOCUMENTATION

*show protection-group ethernet-ring aps*

*show protection-group ethernet-ring data-channel*

*show protection-group ethernet-ring interface*

*show protection-group ethernet-ring node-state*

*show protection-group ethernet-ring statistics*

## show redundant-power-system led

### IN THIS SECTION

- [Syntax | 1486](#)
- [Description | 1486](#)
- [Required Privilege Level | 1486](#)
- [Output Fields | 1486](#)
- [Sample Output | 1488](#)
- [Release Information | 1489](#)

### Syntax

```
show redundant-power-system led
```

### Description

Display information about fan status, Redundant Power System (RPS) status, and the switch connectors as displayed by the corresponding LEDs on the RPS.

### Required Privilege Level

view

### Output Fields

[Table 72 on page 1487](#) lists the output fields for the `show redundant-power-system led` command. Output fields are listed in the approximate order in which they appear.



Table 72: show redundant-power-system led Output Fields

Field Name	Field Description	Level of Output
<b>RPS</b>	The serial number of the RPS.	
<b>RPS Fan</b>	Status of the RPS power supply fans as displayed by the LED: <ul style="list-style-type: none"> <li>• Green—All RPS power supply fans are operating fine.</li> <li>• Amber—A fan has failed in at least one RPS power supply.</li> </ul>	All levels
<b>RPS System Status</b>	Status of the RPS system as displayed by the LED: <ul style="list-style-type: none"> <li>• Green—The RPS is active.</li> <li>• Blinking green—The RPS is booting.</li> <li>• Amber—An RPS power supply has failed.</li> <li>• Off—The RPS is off.</li> </ul>	All levels
<b>RPS Port LED Status</b>	Status of the RPS switch connectors as displayed by the LEDs. These LEDs indicate whether the redundant power source is being used. <ul style="list-style-type: none"> <li>• Green—The RPS connector is enabled and connected to a switch but the RPS is not actively backing up the switch.</li> <li>• Blinking green—The RPS is backing up the switch connected to the port.</li> <li>• Off—The RPS connector is not connected to a switch.</li> <li>• Amber—The RPS is oversubscribed and the backup power to the switch has failed.</li> </ul>	All levels
<b>Port</b>	Number of one of the six switch connectors on the RPS.	All levels
<b>Status</b>	Status of each switch connector on the RPS.	All levels

## Sample Output

### show redundant-power-system led (Standalone Switch)

```
user@switch> show redundant-power-system led
```

Gathering requested information.

RPS-CG0209121807

RPS Fan: GREEN

RPS System Status: GREEN

RPS Port LED Status

Port	Status
0	GREEN
1	OFF
2	OFF
3	OFF
4	OFF
5	OFF

### show redundant-power-system led (EX3300 Virtual Chassis)

```
user@switch> show redundant-power-system led
```

Gathering requested information.

RPS-CG0209121814

RPS Fan: GREEN

RPS System Status: GREEN

RPS Port LED Status

Port	Status
0	OFF
1	OFF
2	OFF
3	OFF
4	OFF
5	GREEN

RPS-CG0209121815

RPS Fan: GREEN

RPS System Status: GREEN

RPS Port LED Status

Port	Status
------	--------

0	OFF
1	OFF
2	OFF
3	OFF
4	GREEN
5	OFF

## Release Information

Command introduced in Junos OS Release 12.1.

## RELATED DOCUMENTATION

| [LEDs on an EX Series Redundant Power System](#)

## show redundant-power-system multi-backup

### IN THIS SECTION

- [Syntax | 1489](#)
- [Description | 1490](#)
- [Required Privilege Level | 1490](#)
- [Sample Output | 1490](#)
- [Release Information | 1490](#)

## Syntax

```
show redundant-power-system multi-backup
```

```
show redundant-power-system multi-backup member member-number
```

## Description

Display the current status of the Redundant Power System's (RPS's) ability to back up two switches per power supply when enough power to support Power over Ethernet (PoE) is not needed. This ability is referred to as the RPS's multi-backup ability.

## Required Privilege Level

view

## Sample Output

**show redundant-power-system multi-backup**

```
User@switch> show redundant-power-system multi-backup
Requesting information from redundant-power-system..    Multi-Backup: enabled
```

## Release Information

Command introduced in Junos OS Release 12.1.

## RELATED DOCUMENTATION

| [request redundant-power-system multi-backup](#) | [1250](#)

## show redundant-power-system network

### IN THIS SECTION

- [Syntax](#) | [1491](#)
- [Description](#) | [1491](#)
- [Required Privilege Level](#) | [1491](#)
- [Sample Output](#) | [1491](#)
- [Release Information](#) | [1491](#)

## Syntax

```
show redundant-power-system network
```

## Description

Display the Redundant Power Supply (RPS) IP address, netmask address, and gateway address required for firmware backup.

## Required Privilege Level

view

## Sample Output

**show redundant-power-system network**

```
user@switch> show redundant-power-system network
Requesting information from redundant-power-system..
  IP Address:   10.93.2.38
  Netmask: 255.255.254.0
  Gateway:   10.93.3.254
```

## Release Information

Command introduced in Junos OS Release 12.1.

## RELATED DOCUMENTATION

| [Upgrading Firmware on an EX Series Redundant Power System](#)

## show redundant-power-system power-supply

### IN THIS SECTION

- [Syntax | 1492](#)
- [Description | 1492](#)
- [Required Privilege Level | 1492](#)
- [Output Fields | 1492](#)
- [Sample Output | 1493](#)
- [Release Information | 1494](#)

### Syntax

```
show redundant-power-system power-supply
```

### Description

Display information about the power supplies installed in the Redundant Power System (RPS). After installing a power supply, we recommend that you use this command to be sure that the power supply installed correctly.

### Required Privilege Level

view

### Output Fields

[Table 73 on page 1493](#) lists the output fields for the `show redundant-power-system power-supply` command. Output fields are listed in the approximate order in which they appear.

**Table 73: show redundant-power-system power-supply Output Fields**

Field Name	Field Description	Level of Output
<b>RPS</b>	Serial number of the RPS.	All levels
<b>PSU Slot</b>	Number of the power supply slot. Slots are numbered 1 through 3.	All levels
<b>Status</b>	Status of the power supply slots: <ul style="list-style-type: none"> <li>• Present—The slot contains an RPS power supply.</li> <li>• Empty—The slot is empty.</li> </ul>	All levels
<b>Description</b>	Description of the RPS power supply installed in the slot.	All levels

## Sample Output

### show redundant-power-system power-supply (Standalone Switch)

```
user@switch> show redundant-power-system power-supply
```

```
Gathering requested information.
```

```
RPS-CG0209121807
```

```
PSU Slot Status    Description
```

```
1 Online    930W AC
```

```
2 offline    ---
```

```
3 Online    930W AC
```

### show redundant-power-system power-supply (EX3300 Virtual Chassis)

```
user@switch> show redundant-power-system power-supply
```

```
Gathering requested information.
```

```
RPS-CG0209121814
```

```
PSU Slot Status    Description
```

```
1 Online    930W AC
```

```

    2 offline    ---
    3 Online     930W AC
RPS-CG0209121815
PSU Slot Status  Description
    1 Online     930W AC
    2 Online     930W AC
    3 Online     930W AC

```

## Release Information

Command introduced in Junos OS Release 12.1.

## RELATED DOCUMENTATION

[Installing a Power Supply in the EX Series Redundant Power System](#)

## show redundant-power-system status

### IN THIS SECTION

- [Syntax | 1494](#)
- [Description | 1495](#)
- [Required Privilege Level | 1495](#)
- [Output Fields | 1495](#)
- [Sample Output | 1496](#)
- [Release Information | 1497](#)

## Syntax

```
show redundant-power-system status
```



# Description

Display the status information for the switch connectors on the Redundant Power System (RPS).

# Required Privilege Level

view

# Output Fields

Table 74 on page 1495 lists the output fields for the show redundant-power-system status command. Output fields are listed in the approximate order in which they appear.

Table 74: show redundant-power-system status Output Fields

Field Name	Field Description	Level of Output
<b>RPS</b>	Serial number of the RPS.	All levels
<b>Port</b>	Number of the switch connector.	All levels
<b>Status</b>	Status of the switch connector: <ul style="list-style-type: none"> <li>• ARMED—The switch is ready to get backup power from RPS if power supply fails on the switch.</li> <li>• OFF—The switch has zero and is not configured to receive backup power from RPS.</li> <li>• BACKED-UP—The switch is receiving power backup from RPS.</li> <li>• OVER-SUBSCRIBED—The switch cannot receive backup power from RPS even if you set the .</li> </ul>	All levels
<b>Priority</b>	Priority value of the switch connector.	All levels
<b>Power-Requested</b>	Power requested by the switch on the corresponding switch connector.	All levels

## Sample Output

### show redundant-power-system status (Standalone Switch)

```
user@switch> show redundant-power-system status
```

Gathering requested information.

RPS-CG0209121807

Port	Status	Power-requested
0	Armed	3 930W
1	Off	1 ---
2	Off	1 ---
3	Off	1 ---
4	Off	1 ---
5	Off	1 ---

### show redundant-power-system status (EX3300 Virtual Chassis)

```
user@switch> show redundant-power-system status
```

Gathering requested information.

RPS-CG0209121814

Port	Status	Power-requested
0	OFF	1 ---
1	OFF	1 ---
2	OFF	1 ---
3	OFF	1 ---
4	OFF	1 ---
5	Armed	5 930W

RPS-CG0209121815

Port	Status	Power-requested
0	OFF	1 ---
1	OFF	1 ---
2	OFF	1 ---
3	OFF	1 ---
4	Armed	4 930W
5	OFF	1 ---

## Release Information

Command introduced in Junos OS Release 12.1.

## RELATED DOCUMENTATION

[Determining and Setting Priority for Switches Connected to an EX Series RPS](#)

[Installing a Power Supply in the EX Series Redundant Power System](#)

## show redundant-power-system upgrade

### IN THIS SECTION

- [Syntax | 1497](#)
- [Description | 1497](#)
- [Required Privilege Level | 1497](#)
- [Output Fields | 1498](#)
- [Sample Output | 1498](#)
- [Release Information | 1498](#)

## Syntax

```
show redundant-power-system upgrade
```

## Description

Display RPS firmware upgrade status (pass or fail), previous RPS firmware version, and current RPS firmware version.

## Required Privilege Level

view

## Output Fields

[Table 75 on page 1498](#) lists the output fields for the `show redundant-power-system status` command. Output fields are listed in the approximate order in which they appear.

**Table 75: show redundant-power-system upgrade Output Fields**

Field Name	Field Description	Level of Output
<b>Firmware Upgrade Status</b>	Indicates whether the upgrade passed or failed	All levels
<b>Previous Firmware Version</b>	Firmware version before the upgrade	All levels
<b>Current Firmware Version</b>	Firmware version after the upgrade	

## Sample Output

### `show redundant-power-system upgrade`

```
user@switch> show redundant-power-system upgrade
Requesting information from redundant-power-system..
Firmware Upgrade Status:   Pass
Previous Firmware Version: 1.0
Current Firmware Version:  1.0
```

## Release Information

Command introduced in Junos OS Release 12.1.

## RELATED DOCUMENTATION

| [request redundant-power-system multi-backup](#) | [1250](#)

# show redundant-power-system version

IN THIS SECTION

- [Syntax | 1499](#)
- [Description | 1499](#)
- [Required Privilege Level | 1499](#)
- [Output Fields | 1499](#)
- [Sample Output | 1500](#)
- [Release Information | 1501](#)

## Syntax

```
show redundant-power-system version
```

## Description

Display version information about the Redundant Power System (RPS).

## Required Privilege Level

view

## Output Fields

[Table 76 on page 1499](#) lists the output fields for the `show redundant-power-system version` command. Output fields are listed in the approximate order in which they appear.

**Table 76: show redundant-power-system version Output Fields**

Field Name	Field Description	Level of Output
RPS	Serial number of the RPS.	All levels

**Table 76: show redundant-power-system version Output Fields (Continued)**

Field Name	Field Description	Level of Output
<b>Model</b>	Model name of the RPS.	All levels
<b>RPS Firmware Version</b>	Version number of the firmware installed on the RPS.	All levels
<b>RPS U-Boot Version</b>	Version of the bootup software installed on the RPS.	All levels

## Sample Output

### show redundant-power-system version (Standalone Switch)

```
user@switch> show redundant-power-system version
```

```

RPS-CG0209121807
Model: EX-PWR_RPS200
RPS Firmware Version [1.0]
RPS U-Boot   Version [1.1.6]
```

### show redundant-power-system version (EX3300 Virtual Chassis)

```
user@switch> show redundant-power-system version
```

```

RPS-CG0209121814
Model: EX-PWR_RPS200
RPS Firmware Version [1.0]
RPS U-Boot   Version [1.1.6]
RPS-CG0209121815
Model: EX-PWR_RPS200
RPS Firmware Version [1.0]
RPS U-Boot   Version [1.1.6]
```

## Release Information

Command introduced in Junos OS Release 12.1.

## RELATED DOCUMENTATION

[Installing a Power Supply in the EX Series Redundant Power System](#)

[Packing an EX Series Redundant Power System or Redundant Power System Components for Shipping](#)

## show security pki node-local local-certificate

### IN THIS SECTION

- [Syntax | 1501](#)
- [Description | 1501](#)
- [Options | 1502](#)
- [Required Privilege Level | 1502](#)
- [Output Fields | 1502](#)
- [Sample Output | 1504](#)
- [Release Information | 1506](#)

## Syntax

```
show security pki node-local local-certificate  
<brief/detail>  
<certificate-id certificate-id-name>  
<system-generated>
```

## Description

Display information about the local digital certificates, corresponding public keys, and the automatically generated self-signed certificate configured on the local device in a Multinode High Availability setup.

# Options

- none—Display basic information about all configured local digital certificates, corresponding public keys, and the automatically generated self-signed certificate.
- brief | detail—(Optional) Display the specified level of output.
- certificate-id *certificate-id-name* —(Optional) Display information about only the specified local digital certificates and corresponding public keys.
- system-generated—Display information about the automatically generated self-signed certificate.

# Required Privilege Level

view

# Output Fields

[Table 77 on page 1502](#) lists the output fields for the `show security pki node-local local-certificate` command. Output fields are listed in the approximate order in which they appear.

**Table 77: show security pki node-local local-certificate Output Fields**

Field Name	Field Description
Certificate identifier	Name of the digital certificate.
Certificate version	Revision number of the digital certificate.
Serial number	<p>Unique serial number of the digital certificate. Starting in Junos OS Release 20.1R1, PKI local certificate serial number is displayed with <b>0x</b> as prefix to indicate that the PKI local certificate is in the hexadecimal format.</p> <p>Starting in Junos OS Release 21.4R1, you can view the serial number of the digital certificate in both hexadecimal and decimal formats.</p>
Issued to	Device that was issued the digital certificate.
Issued by	Authority that issued the digital certificate.



**Table 77: show security pki node-local local-certificate Output Fields (Continued)**

Field Name	Field Description
Issuer	<p>Authority that issued the digital certificate, including details of the authority organized using the distinguished name format. Possible subfields are:</p> <ul style="list-style-type: none"> <li>• Organization—Organization of origin.</li> <li>• Organizational unit—Department within an organization.</li> <li>• Country—Country of origin.</li> <li>• Locality—Locality of origin.</li> <li>• Common name—Name of the authority.</li> </ul>
LSYS	Name of the logical systems.
Subject	<p>Details of the digital certificate holder organized using the distinguished name format. Possible subfields are:</p> <ul style="list-style-type: none"> <li>• Organization—Organization of origin.</li> <li>• Organizational unit—Department within an organization.</li> <li>• Country—Country of origin.</li> <li>• Locality—Locality of origin.</li> <li>• Common name—Name of the authority.</li> <li>• Serial number—Serial number of the device.</li> </ul> <p>If the certificate contains multiple subfield entries, all entries are displayed.</p>
Subject string	Subject field as it appears in the certificate.
Alternate subject	Domain name or IP address of the device related to the digital certificate.
Cert-Chain	Starting in Junos OS Release 21.4R1, you can view the certificate chain for a given local certificate.

**Table 77: show security pki node-local local-certificate Output Fields (Continued)**

Field Name	Field Description
Validity	Time period when the digital certificate is valid. Values are: <ul style="list-style-type: none"> <li>• Not before—Start time when the digital certificate becomes valid.</li> <li>• Not after—End time when the digital certificate becomes invalid.</li> </ul>
Public key algorithm	Encryption algorithm used with the private key, such as rsa Encryption(1024 bits).
Public key verification status	Public key verification status: Failed or Passed. The detail output also provides the verification hash.
Signature algorithm	Encryption algorithm that the CA used to sign the digital certificate, such as sha1WithRSAEncryption.
Fingerprint	Secure Hash Algorithm (SHA1) and Message Digest 5 (MD5) hashes used to identify the digital certificate.  Starting in Junos OS Release 21.4R1, you can also view the SHA-256 fingerprint for a local certificate along with SHA-1 and MD-5 fingerprints.
Distribution CRL	Distinguished name information and URL for the certificate revocation list (CRL) server.
Use for key	Use of the public key, such as Certificate signing, CRL signing, Digital signature, or Data encipherment.

## Sample Output

**show security pki node-local local-certificate certificate-id hello**

```

user@host> show security pki node-local local-certificate certificate-id cert-1234
LSYS: root-logical-system
Certificate identifier: cert-1234

```

```

Issued to: tc5-5-1, Issued by: DC = Juniper, CN = root-551-AAA
Validity:
  Not before: 10-14-2021 21:41 UTC
  Not after: 02-13-2026 14:27 UTC
Public key algorithm: rsaEncryption(1024 bits)
Keypair Location: Keypair generated locally

```

### **show security pki node-local local-certificate system-generated**

```

user@host> show security pki node-local local-certificate system-generated
LSYS: root-logical-system
Certificate identifier: system-generated
Issued to: 4a505bb373d7, Issued by: CN = 4a505bb373d7, CN = system generated, CN = self-signed
Validity:
  Not before: 07-12-2019 22:23 UTC
  Not after: 07-10-2024 22:23 UTC
Public key algorithm: rsaEncryption(2048 bits)
Keypair Location: Keypair generated locally

```

### **show security pki node-local local-certificate system-generated detail**

```

user@host> show security pki node-local local-certificate system-generated detail
LSYS: root-logical-system
Certificate identifier: system-generated
  Certificate version: 3

Serial number:
  hexadecimal: 0x23171f4f104463e2847bc792c39eb614
  decimal: 46643037698975347221422984685160412692
Issuer:
  Common name: 4a505bb373d7, Common name: system generated, Common name: self-signed
Subject:
  Common name: 4a505bb373d7, Common name: system generated, Common name: self-signed
Subject string:
  CN=4a505bb373d7, CN=system generated, CN=self-signed

Validity:
  Not before: 07-12-2019 22:23 UTC
  Not after: 07-10-2024 22:23 UTC
Public key algorithm: rsaEncryption(2048 bits)

```

```

30:82:01:0a:02:82:01:01:00:d5:7e:5e:7a:15:90:e3:23:07:8e:e3
4b:40:0e:95:33:31:8c:17:0b:d1:78:48:2e:b5:e8:cb:44:03:f1:fd
00:57:af:e9:d9:2c:78:96:04:37:3c:4a:65:d9:f1:fb:72:14:7f:b2
d3:42:d3:84:be:e8:c5:6c:e2:f5:91:8a:41:02:30:a7:8b:2f:10:5e
ab:5e:4e:d7:d6:f1:e7:ad:e3:6c:16:8d:6b:3c:0e:11:e9:26:8a:38
99:78:0a:57:67:cc:0a:ea:fa:35:2b:f3:51:4e:cc:30:ee:e9:a7:0a
26:14:42:fc:1b:22:ec:2d:0c:3b:10:d5:fb:e3:e6:ae:c6:cc:e7:de
0f:cf:4d:a7:87:11:e1:4e:7f:33:69:c0:16:4e:80:c8:57:b4:9a:f8
90:15:d8:e6:3e:06:7a:1c:a3:34:91:92:a6:88:9f:14:f5:89:39:da
0f:88:1c:b0:bd:7d:46:23:b2:42:e8:6f:d2:34:9e:f2:bd:00:34:23
99:4e:bb:39:0e:e4:bb:b2:9b:53:02:36:30:10:b7:28:e3:c4:8c:0e
4c:fd:cf:4f:58:81:72:91:b4:82:18:cf:ba:f6:76:59:f2:d5:36:e1
3a:29:20:72:02:5b:26:45:6f:92:0c:8e:dc:6c:d4:1c:78:55:db:66
3a:e9:9a:9c:81:02:03:01:00:01

```

Signature algorithm: sha256WithRSAEncryption

Fingerprint:

```

0b:08:f8:bc:c6:a3:c1:41:75:2b:48:da:5d:a7:0f:d8:99:45:cd:8a (sha1)
8a:1b:b9:79:19:c6:c3:88:05:a8:05:28:3c:f2:b0:e9 (md5)

```

```

a3:9b:c1:c4:55:a8:f8:79:6f:a9:27:fc:f8:5a:af:45:37:dd:42:5f:2f:2b:bb:85:e3:f0:d7:99:9d:93:65:b1
(sh256)

```

## Release Information

Command modified in Junos OS Release 22.3R1.

## RELATED DOCUMENTATION

[Multinode High Availability /](#)

[request security pki node-local local-certificate verify /](#)

[request security pki node-local local-certificate re-enroll /](#)

[request security pki node-local local-certificate load /](#)

[request security pki node-local local-certificate export](#)

[request security pki node-local local-certificate enroll /](#)

## show security pki node-local certificate-request

### IN THIS SECTION

- [Syntax | 1507](#)
- [Description | 1507](#)
- [Options | 1507](#)
- [Required Privilege Level | 1508](#)
- [Output Fields | 1508](#)
- [Sample Output | 1509](#)
- [Sample Output | 1509](#)
- [Release Information | 1510](#)

### Syntax

```
show security pki node-local certificate-request  
<brief|detail>  
<certificate-id certificate-id-name>
```

### Description

Display information about manually generated local digital certificate requests that are stored on the local device in your Multinode High Availability setup.

### Options

- none—Display basic information about all local digital certificate requests.
- brief / detail—(Optional) Display the specified level of output.
- certificate-id *certificate-id-name* —(Optional) Display information about only the specified local digital certificate requests.

## Required Privilege Level

view

## Output Fields

Table 78 on page 1508 lists the output fields for the `show security pki node-local certificate-request` command. Output fields are listed in the approximate order in which they appear.

**Table 78: show security pki node-local certificate-request Output Fields**

Field Name	Field Description
Certificate identifier	Name of the digital certificate.
Certificate version	Revision number of the digital certificate.
Issued to	Device that was issued the digital certificate.
Subject	<p>Details of the digital certificate holder organized using the distinguished name format. Possible subfields are:</p> <ul style="list-style-type: none"> <li>• Organization—Organization of origin.</li> <li>• Organizational unit—Department within an organization.</li> <li>• Country—Country of origin.</li> <li>• Locality—Locality of origin.</li> <li>• Common name—Name of the authority.</li> </ul>
Alternate subject	Domain name or IP address of the device related to the digital certificate.
Public key algorithm	Encryption algorithm used with the private key, such as <code>rsaEncryption(1024 bits)</code> .
Public key verification status	Public key verification status: Failed or Passed. The detail output also provides the verification hash.

**Table 78: show security pki node-local certificate-request Output Fields (Continued)**

Field Name	Field Description
Fingerprint	Secure Hash Algorithm (SHA1) and Message Digest 5 (MD5) hashes used to identify the digital certificate.
Use for key	Use of the public key, such as Certificate signing, CRL signing, Digital signature, or Data encipherment.

## Sample Output

### show security pki node-local certificate-request certificate-id user brief

```
user@host> show security pki node-local certificate-request certificate-id user-1
brief
Certificate identifier: user-1
    Issued to: user@example.net
    Public key algorithm: rsaEncryption(1024 bits)
```

## Sample Output

### show security pki node-local certificate-request certificate-id user detail

```
user@host> show security pki node-local certificate-request certificate-id user-1
detail
Certificate identifier: user
Certificate version: 3
Subject:
    Organization: example, Organizational unit: example, Country: IN,
        Common name: user1
Alternate subject: 192.168.72.124
Public key algorithm: rsaEncryption(1024 bits)
Public key verification status: Passed
    c7:a4:fb:e7:8c:4f:31:e7:eb:01:d8:32:65:21:f2:eb:6f:7d:49:1a:c3:9b
    63:47:e2:4f:f6:db:f6:c8:75:dd:e6:ec:0b:35:0a:62:32:45:6b:35:1f:65
    c9:66:b7:40:b2:f9:2a:ab:5b:60:f7:c7:73:36:da:68:25:fc:40:4b:12:3c
```

```
d5:c8:c6:66:f6:10:1e:86:67:a8:95:9b:7f:1c:ae:a7:55:b0:28:95:a7:9a
a2:24:28:e4:5a:b2:a9:06:7a:69:37:20:15:e1:b6:66:eb:22:b5:b6:77:f6
65:88:b0:94:2b:91:4b:99:78:4a:e3:56:cc:14:45:d7:97:fd
Fingerprint:
8f:22:1a:f2:9f:27:b0:21:6c:da:46:64:31:34:1f:68:42:5a:39:e0 (sha1)
09:15:11:aa:ea:f9:5a:b5:70:d7:0b:8e:be:a6:d3:cb (md5)
Use for key: Digital signature
```

## Release Information

Command modified in Junos OS Release 22.3R1

## RELATED DOCUMENTATION

[request security pki node-local generate-certificate-request /](#)  
[Multinode High Availability /](#)

## show chassis ssb

### IN THIS SECTION

- [Syntax | 1511](#)
- [Description | 1511](#)
- [Options | 1511](#)
- [Required Privilege Level | 1511](#)
- [Output Fields | 1511](#)
- [Sample Output | 1512](#)
- [Release Information | 1513](#)



Syntax

```
show chassis ssb
<slot>
```

Description

(M20 routers only) Display status information about the System and Switch Board (SSB).

Options

- none**    Display information about all SSBs.
- slot**    (Optional) Display information about the SSB in the specified slot. Replace *slot* with **0** or **1**.

Required Privilege Level

view

Output Fields

[Table 79 on page 1511](#) lists the output fields for the `show chassis ssb` command. Output fields are listed in the approximate order in which they appear.

Table 79: show chassis ssb Output Fields

Field Name	Field Description
Failover	Number of times primary role has changed.
Slot	SSB slot number.

Table 79: show chassis ssb Output Fields *(Continued)*

Field Name	Field Description
<b>State</b>	Current state of the SSB in this slot. State can be any one of the following: <ul style="list-style-type: none"> <li>• <b>Master</b>—SSB is online, operating as primary.</li> <li>• <b>Backup</b>—SSB running as backup.</li> <li>• <b>Empty</b>—No SSB is present.</li> </ul>
<b>Temperature</b>	Temperature of the air passing by the SSB, in degrees Celsius.
<b>CPU utilization</b>	Total percentage of the CPU being used by the SSB's processor.
<b>Interrupt utilization</b>	Of the total CPU being used by the SSB's processor, the percentage being used for interrupts.
<b>Heap utilization</b>	Percentage of heap space being used by the SSB's processor.
<b>Buffer utilization</b>	Percentage of buffer space being used by the SSB's processor.
<b>DRAM</b>	Total DRAM available to the SSB's processor.
<b>Start time</b>	Time when the SSB started running.
<b>Uptime</b>	How long the SSB has been up and running.

## Sample Output

### show chassis ssb

```
user@host> show chassis ssb
```

```
SSB status:
```

```
Failover: 0 time
```

```
Slot 0:
```

```

State:                Master
Temperature:          33 Centigrade
CPU utilization:       0 percent
Interrupt utilization: 0 percent
Heap utilization:      0 percent
Buffer utilization:    6 percent
DRAM:                 64 Mbytes
Start time:           1999-01-15 22:05:36 UTC
Uptime:               21 hours, 21 minutes, 22 seconds
...

```

## Release Information

Command introduced before Junos OS Release 7.4.

## show nonstop-routing

### IN THIS SECTION

- [Syntax | 1513](#)
- [Description | 1513](#)
- [Required Privilege Level | 1514](#)
- [Output Fields | 1514](#)
- [Sample Output | 1516](#)
- [Release Information | 1517](#)

## Syntax

```
show nonstop-routing
```

## Description

Display the status of nonstop active routing that includes the automerge statistics and state.

# Required Privilege Level

View

## Output Fields

Table 80 on page 1514 describes the output fields for the **show nonstop-routing** command. Output fields are listed in the approximate order in which they appear.

**Table 80: show nonstop-routing Output Fields**

Field Name	Field Description
Nonstop Routing	State of NSR.
Precision Timers state	<p>State of precision timer feature in the kernel.</p> <ul style="list-style-type: none"> <li>• <b>Enabled</b> By default, autokeepalive precision timers are enabled on the kernel after switchover.</li> <li>• <b>Disabled</b> Autokeepalive precision timers are disabled.</li> <li>• <b>Inactive</b> Precision timer is inactive if it is disabled.</li> <li>• <b>Ready</b> Kernel precision timer is ready but is never activated.</li> <li>• <b>InProcess</b> Kernel precision timer is operational and is generating keepalives on behalf of the RPD after switchover. The / count indicates the number of sessions being serviced against the total sessions.</li> <li>• <b>Completed</b> Kernel has completed keepalive generation for all the sessions after switchover, and RPD has taken over all of them successfully.</li> <li>• <b>Error</b> Error while retrieving the precision timer status of the kernel.</li> </ul>
Precision Timers max period	Maximum period, in seconds, after the switchover from standby to primary event for which the kernel autogenerates keepalives on behalf of BGP.

Table 80: show nonstop-routing Output Fields *(Continued)*

Field Name	Field Description
Automerge	<p>Status of the automerge.</p> <ul style="list-style-type: none"> <li>• <b>Active</b>     Automerge of sockets by the kernel after switchover is active.</li> <li>• <b>Inactive</b>     Automerge of sockets by the kernel after switchover is inactive.</li> </ul>
Batching	<p>Status of Batching.</p> <ul style="list-style-type: none"> <li>• <b>Yes</b>     Automerge of sockets by the kernel after a switchover.</li> <li>• <b>No</b>     Automerge of sockets by the kernel after switchover is inactive.</li> </ul>
Batch count	Number of sockets merged per batch.
Batch count adjust	<p>Speed at which the batch count is adjusted.</p> <ul style="list-style-type: none"> <li>• <b>Slow</b>     Number of sockets merged per batch is incremented additively.</li> <li>• <b>Exp</b>     Number of sockets merged per batch is incremented exponentially.</li> <li>• <b>None</b>     Number of sockets merged per batch remains constant.</li> </ul>
Batch interval	Time interval between batches of automerge operation.
Batch interval adjust	<p>Speed at which the batch interval is adjusted.</p> <ul style="list-style-type: none"> <li>• <b>Exp</b>     Time interval between automerge of batches is increased exponentially.</li> <li>• <b>None</b>     Time interval between automerge of batches is not adjusted.</li> </ul>

Table 80: show nonstop-routing Output Fields *(Continued)*

Field Name	Field Description
Automerge State	<p>State of the automerge</p> <ul style="list-style-type: none"> <li>• <b>Ready</b> Ready to automerge socket pairs from secondary to primary routing engine</li> <li>• <b>InProgress</b> Kernel is performing automerge after switchover</li> <li>• <b>Switchover Completed</b> Sessions merged after switchover</li> </ul>
Sessions Processed	Count of sessions that are automerged.

## Sample Output

### show nonstop-routing (MX Series Router)

```

user@host show nonstop-routing
Nonstop Routing : Enabled
  Precision Timers state: Enabled: Completed - 0/0
  Precision Timers max period: 200
  Automerge : Active
  Batching: No
  Batch count: 200
  Batch count adjust: Exponential
  Batch interval: 20 msec
  Batch interval adjust: None
  Automerge State: Ready
  Sessions Processed: 0

```

### show nonstop-routing (MX Series Router)

```

user@host> show nonstop-routing

Nonstop Routing : Enabled
  Automerge : Active

```

```
Batching: Yes
Batch count: 500
Batch count adjust: Slow
Batch interval: 50 msec
Batch interval adjust: None
Automerge State: Ready
Sessions Processed: 0
```

## Release Information

Command introduced in Junos OS Release 13.3.

## RELATED DOCUMENTATION

| [nonstop-routing](#) | [1064](#)

## show pfe ssb

### IN THIS SECTION

- [Syntax](#) | [1517](#)
- [Description](#) | [1518](#)
- [Options](#) | [1518](#)
- [Required Privilege Level](#) | [1518](#)
- [Output Fields](#) | [1518](#)
- [Sample Output](#) | [1522](#)
- [Release Information](#) | [1525](#)

## Syntax

```
show pfe ssb
```

# Description

(M20 routers only) Display Packet Forwarding Engine System and Switch Board (SSB) status and statistics information.

# Options

This command has no options.

# Required Privilege Level

admin

# Output Fields

[Table 81 on page 1518](#) lists the output fields for the `show pfe ssb` command. Output fields are listed in the approximate order in which they appear.

**Table 81: show pfe ssb Output Fields**

Field Name	Field Description
Uptime (total)	SSB uptime.
Failures	Number of failures .
Pending	Number of pending.
Peer message type receive qualifiers	Information about Peer message type receive qualifiers.
Message Type	Peer message type.
Receive Qualifier	Peer receive qualifier.
TTP	Peer message type TTP.



**Table 81: show pfe ssb Output Fields (Continued)**

Field Name	Field Description
IFD	Peer message type IFD.
IFL	Peer message type IFL.
Nexthop	Peer message type Nexthop.
COS	Peer message type COS.
Route	Peer message type Route.
SW Firewall	Peer message type SW Firewall.
HW Firewall	Peer message type HW Firewall.
PFE Statistics	Peer message type PFE Statistics.
PIC Statistics	Peer message type PIC Statistics.
Sampling	Peer message type Sampling .
Monitoring	Peer message type Monitoring.
ASP	Peer message type ASP.
L2TP	Peer message type L2TP.
Collector	Peer message type Collector.
PIC Configuration	Peer message type PIC Configuration.

**Table 81: show pfe ssb Output Fields (Continued)**

Field Name	Field Description
Queue Statistics	Peer message type Queue Statistics.
PFE Listener statistics	<p>Information about Packet Forwarding Engine listener statistics:</p> <ul style="list-style-type: none"> <li>• Open—Number of PFE listeners in the “open” state.</li> <li>• Close—Number of PFE listeners in the “close” state.</li> <li>• Sleep—Number of PFE listeners in the “sleep” state.</li> <li>• Wakeup—Number of PFE listeners in the “wakeup” state.</li> <li>• Resync Request—Number of PFE listeners in the “resync request” state.</li> <li>• Resync Done—Number of PFE listeners in the “resync done” state.</li> <li>• Resync Fail—Number of PFE listeners in the “resync fail” state</li> <li>• Resync Time—Number of PFE listeners in the resync time state.</li> </ul>

Table 81: show pfe ssb Output Fields *(Continued)*

Field Name	Field Description
PFE IPC statistics	<p>Information about Packet Forwarding Engine IPC statistics.</p> <ul style="list-style-type: none"> <li>• type—Type of IPC message. <ul style="list-style-type: none"> <li>• Header—IPC message type Header.</li> <li>• Test—IPC message type Test.</li> <li>• Interface—IPC message type Interface.</li> <li>• Chassis—IPC message type Chassis.</li> <li>• Boot—IPC message type Boot</li> <li>• Next-hop—IPC message type Next-hop.</li> <li>• Jtree—IPC message type Jtree.</li> <li>• Cprod—IPC message type Cprod.</li> <li>• Route—IPC message type Route.</li> <li>• Pfe—IPC message type PFE.</li> <li>• Dfw—IPC message type Dfw.</li> <li>• Mastership—IPC message type Primary Role.</li> <li>• Sampling—IPC message type Sampling.</li> <li>• GUCP—IPC message type GUCP.</li> <li>• CoS—IPC message type CoS.</li> <li>• GCCP—IPC message type GCCP.</li> <li>• GHCP—IPC message type GHCP.</li> <li>• IRSD—IPC message type IRSD.</li> <li>• Monitoring—IPC message type Monitoring.</li> </ul> </li> </ul>

Table 81: show pfe ssb Output Fields *(Continued)*

Field Name	Field Description
	<ul style="list-style-type: none"> <li>• RE—IPC message type RE.</li> <li>• PIC—IPC message type PIC.</li> <li>• ASP cfg—IPC message type ASP configuration.</li> <li>• ASP cmd—IPC message type ASP command..</li> <li>• L2TP cfg—IPC message type L2TP configuration.</li> <li>• Collector—IPC message type Collector.</li> <li>• PIC state—IPC message type PIC state.</li> <li>• Aggregator—IPC message type Aggregate.</li> <li>• Empty—IPC message type Empty.</li> <li>• PFE socket-buffer mbuf depth—Information about Packet Forwarding Engine socket-buffer depth</li> <li>• bucket—mbuf bucket value.</li> <li>• count—mbuf count value.</li> <li>•</li> </ul>
PFE socket-buffer bytes pending transmit—	<p>Information about Packet Forwarding Engine socket-buffer bytes pending for transmit.</p> <ul style="list-style-type: none"> <li>• TX Messages—Number of transmitted messages.</li> <li>• RX messages—Number of received messages.</li> </ul>

## Sample Output

### show pfe ssb

```

user@host> show pfe ssb
SSB status:
  Slot:          Present

```

State: Online  
Last State Change: 2005-03-06 03:10:28 PST  
Uptime (total): 11:23:27  
Failures: 0  
Pending: 0

Peer message type receive qualifiers:

Message Type	Receive Qualifier
-----	-----
TTP	Slot only
IFD	All
IFL	All
Nexthop	All
COS	All
Route	All
SW Firewall	All
HW Firewall	All
PFE Statistics	All
PIC Statistics	None
Sampling	All
Monitoring	None
ASP	None
L2TP	None
Collector	None
PIC Configuration	None
Queue Statistics	None
(null)	None

PFE listener statistics:

Open: 1  
Close: 0  
Sleep: 0  
Wakeup: 0  
Resync Request: 0  
Resync Done: 1  
Resync Fail: 0  
Resync Time: 0

PFE IPC statistics:

type	TX Messages	RX messages
-----	-----	-----

Header	0	0
Test	0	0
Interface	737	9911
Chassis	0	0
Boot	0	0
Next-hop	48	0
Jtree	0	0
Cprod	0	0
Route	94	0
Pfe	2034	683
Dfw	8	0
Mastership	0	0
Sampling	0	0
GUCP	0	0
CoS	73	0
GCCP	0	0
GHCP	0	0
IRSD	0	0
Monitoring	0	0
RE	0	0
PIC	0	0
ASP cfg	0	0
ASP cmd	0	0
L2TP cfg	0	0
Collector	0	0
PIC state	0	0
Aggregator	0	0
Empty	0	0

PFE socket-buffer mbuf depth:

bucket	count
-----	-----
0	0
1	0
2	0
3	0
4	0
5	0
6	0
7	0
8	0
9	0
10	0

11	0
12	0
13	0
14	0
15	0
16	0
17	0
18	0
19	0
20	0
21	0

PFE socket-buffer bytes pending transmit:

bucket	count
-----	-----
0	0
1	0
2	0
3	0
4	0
5	0
6	0
7	0
8	0
9	0
10	0
11	0
12	0
13	0
14	0
15	0
16	0
17	0
18	0
19	0
20	0
21	0

**Release Information**

Command introduced before Junos OS Release 7.4.

## show system switchover

### IN THIS SECTION

- [Syntax | 1526](#)
- [Syntax \(TX Matrix Router\) | 1526](#)
- [Syntax \(TX Matrix Plus Router\) | 1526](#)
- [Syntax \(MX Series Router\) | 1527](#)
- [Description | 1527](#)
- [Options | 1527](#)
- [Additional Information | 1529](#)
- [Required Privilege Level | 1529](#)
- [Output Fields | 1529](#)
- [Sample Output | 1531](#)
- [Release Information | 1534](#)

### Syntax

```
show system switchover
```

### Syntax (TX Matrix Router)

```
show system switchover  
<all-chassis | all-lcc | lcc number | scc>
```

### Syntax (TX Matrix Plus Router)

```
show system switchover  
<all-chassis | all-lcc | lcc number | sfc number>
```



## Syntax (MX Series Router)

```
show system switchover
<all-members>
<local>
<member member-id>
```

## Description

Display whether graceful Routing Engine switchover is configured, the state of the kernel replication (ready or synchronizing), any replication errors, and whether the primary and standby Routing Engines are using compatible versions of the kernel database.

**NOTE:** Issue the `show system switchover` command *only* on the backup Routing Engine. This command is *not* supported on the primary Routing Engine because the kernel-replication process daemon does not run on the primary Routing Engine. This process runs only on the backup Routing Engine.

Beginning Junos OS Release 9.6, the `show system switchover` command has been deprecated on the primary Routing Engine on all routers other than a TX Matrix (switch-card chassis) or a TX Matrix Plus (switch-fabric chassis) router.

However, in a routing matrix, if you issue the `show system switchover` command on the primary Routing Engine of the TX Matrix router (or switch-card chassis), the CLI displays graceful switchover information for the primary Routing Engine of the T640 routers (or line-card chassis) in the routing matrix. Likewise, if you issue the `show system switchover` command on the primary Routing Engine of a TX Matrix Plus router (or switch-fabric chassis), the CLI displays output for the primary Routing Engine of T1600 or T4000 routers in the routing matrix.

## Options

**all-chassis** (TX Matrix routers and TX Matrix Plus routers only) (Optional) On a TX Matrix router, display graceful Routing Engine switchover information for all Routing Engines on the TX Matrix router and the T640 routers configured in the routing matrix. On a TX Matrix Plus router, display graceful Routing Engine switchover information for all Routing Engines on the TX Matrix Plus router and the T1600 or T4000 routers configured in the routing matrix.

<b>all-lcc</b>	<p>(TX Matrix routers and TX Matrix Plus routers only) (Optional) On a TX Matrix router, display graceful Routing Engine switchover information for all T640 routers (or line-card chassis) connected to the TX Matrix router. On a TX Matrix Plus router, display graceful Routing Engine switchover information for all connected T1600 or T4000 LCCs.</p> <p>Note that in this instance, packets get dropped. The LCCs perform GRES on their own chassis (GRES cannot be handled by one particular chassis for the entire router) and synchronization is not possible as the LCC plane bringup time varies for each LCC. Therefore, when there is traffic on these planes, there may be a traffic drop.</p>
<b>all-members</b>	<p>(MX Series routers only) (Optional) Display graceful Routing Engine switchover information for all Routing Engines on all members of the Virtual Chassis configuration.</p>
<b>lcc <i>number</i></b>	<p>(TX Matrix routers and TX Matrix Plus routers only) (Optional) On a TX Matrix router, display graceful Routing Engine switchover information for a specific T640 router connected to the TX Matrix router. On a TX Matrix Plus router, display graceful Routing Engine switchover information for a specific router connected to the TX Matrix Plus router.</p> <p>Replace <i>number</i> with the following values depending on the LCC configuration:</p> <ul style="list-style-type: none"> <li>• 0 through 3, when T640 routers are connected to a TX Matrix router in a routing matrix.</li> <li>• 0 through 3, when T1600 routers are connected to a TX Matrix Plus router in a routing matrix.</li> <li>• 0 through 7, when T1600 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.</li> <li>• 0, 2, 4, or 6, when T4000 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.</li> </ul>
<b>local</b>	<p>(MX Series routers only) (Optional) Display graceful Routing Engines switchover information for all Routing Engines on the local Virtual Chassis member.</p>
<b>member <i>member-id</i></b>	<p>(MX Series routers only) (Optional) Display graceful Routing Engine switchover information for all Routing Engines on the specified member of the Virtual Chassis configuration. Replace <i>member-id</i> with a value of 0 or 1.</p>
<b>scc</b>	<p>(TX Matrix router only) (Optional) Display graceful Routing Engine switchover information for the TX Matrix router (or switch-card chassis).</p>
<b>sfc</b>	<p>(TX Matrix Plus routers only) (Optional) Display graceful Routing Engine switchover information for the TX Matrix Plus router.</p>

## Additional Information

If you issue the `show system switchover` command on a TX Matrix backup Routing Engine, the command is broadcast to all the T640 backup Routing Engines that are connected to it.

Likewise, if you issue the `show system switchover` command on a TX Matrix Plus backup Routing Engine, the command is broadcast to all the T1600 or T4000 backup Routing Engines that are connected to it.

If you issue the `show system switchover` command on the active Routing Engine in the primary router of an MX Series Virtual Chassis, the router displays a message that this command is not applicable on this member of the Virtual Chassis.

## Required Privilege Level

view

## Output Fields

[Table 82 on page 1529](#) describes the output fields for the `show system switchover` command. Output fields are listed in the approximate order in which they appear.

**Table 82: show system switchover Output Fields**

Field Name	Field Description
Graceful switchover	<p>Display graceful Routing Engine switchover status:</p> <ul style="list-style-type: none"> <li>On—Indicates graceful-switchover is specified for the routing-options configuration command.</li> <li>Off—Indicates graceful-switchover is not specified for the routing-options configuration command.</li> </ul>
Configuration database	<p>State of the configuration database:</p> <ul style="list-style-type: none"> <li>Ready—Configuration database has synchronized.</li> <li>Synchronizing—Configuration database is synchronizing. Displayed when there are updates within the last 5 seconds.</li> <li>Synchronize failed—Configuration database synchronize process failed.</li> </ul>

Table 82: show system switchover Output Fields (*Continued*)

Field Name	Field Description
Kernel database	<p>State of the kernel database:</p> <ul style="list-style-type: none"> <li>• Ready—Kernel database has synchronized. This message implies that the system is ready for GRES.</li> <li>• Synchronizing—Kernel database is synchronizing. Displayed when there are updates within the last 5 seconds.</li> <li>• Version incompatible—The primary and standby Routing Engines are running incompatible kernel database versions.</li> <li>• Replication error—An error occurred when the state was replicated from the primary Routing Engine. Inspect <b>Steady State</b> for possible causes, or notify Juniper Networks customer support.</li> </ul>
Peer state	<p>Routing Engine peer state:</p> <p>This field is displayed only when ksyncd is running in multichassis mode (LCC primary).</p> <ul style="list-style-type: none"> <li>• Steady State—Peer completed switchover transition.</li> <li>• Peer Connected—Peer in switchover transition.</li> </ul>
Switchover Status	<p>Switchover Status:</p> <ul style="list-style-type: none"> <li>• Ready—Message for system being switchover ready.</li> <li>• Not Ready—Message for system not being ready for switchover.</li> </ul>

**Table 82: show system switchover Output Fields (Continued)**

Field Name	Field Description
Platform Components	<p>Platform Components:</p> <p>FEB1:</p> <ul style="list-style-type: none"> <li>• Not Online—The backup FEB2 is not yet online.</li> <li>• Online—The backup FEB2 is online.</li> </ul> <p>FEB1-PFE0, FEB1- PFE1:</p> <ul style="list-style-type: none"> <li>• Ready—Message for FEB1- PFE0, or FEB1- PFE1 being switchover ready. The backup PFE is ready for switchover (does not include time for routes or nexthops for a scaled configuration).</li> <li>• Not Online—The backup PFE is not yet online.</li> <li>• Sync In Progress—Two-minute synchronization in progress when information flow data-path is programmed on the backup PFE (does not include time for routes or next-hops programming).</li> </ul>

## Sample Output

### show system switchover (Backup Routing Engine - Ready)

```

user@host> show system switchover
Graceful switchover: On
Configuration database: Ready
Kernel database: Ready
Peer state: Steady State
Switchover Status: Ready

```

Switchover Status: Ready is the way the last line of the output reads if you are running Junos OS Release 16.1R1 or later. If you are running Junos OS Release 15.x, the last line of the output reads as Switchover Ready, for example:

```

user@host> show system switchover
Graceful switchover: On
Configuration database: Ready

```

```
Kernel database: Ready
Switchover Ready
```

### **show system switchover (Backup Routing Engine - Not Ready)**

```
user@host> show system switchover
Graceful switchover: On
Configuration database: Ready
Kernel database: Ready
Peer state: Steady State
Switchover Status: Not Ready
```

Switchover Status: Not Ready is the way the last line of the output reads if you are running Junos OS Release 16.1R1 or later. If you are running Junos OS Release 15.x, the last line of the output reads as Not ready for primary role switch, try after xxx secs, for example:

```
user@host> show system switchover
Graceful switchover: On
Configuration database: Ready
Kernel database: Ready
Not ready for mastership switch, try after xxx secs.
```

### **show system switchover all-lcc (Routing Matrix and Routing Matrix Plus)**

```
user@host> show system switchover all-lcc
```

```
lcc0-re0:
```

```
-----
Multichassis replication: On
Configuration database: Ready
Kernel database: Ready
Peer state: Steady State
Switchover Status: Ready
```

```
lcc2-re0:
```

```
-----
Multichassis replication: On
Configuration database: Ready
Kernel database: Ready
```

```

Peer state: Steady State
Switchover Status: Ready

<command>user@host> <user-typing>show system switchover</user-typing>
> </command>
<output>lcc0-re1:
-
Multichassis replication: On
Configuration database: Ready
Kernel database: Ready
Peer state: Steady State
Switchover Status: Ready

lcc2-re0:
-
Multichassis replication: On
Configuration database: Ready
Kernel database: Ready
Peer state: Steady State
Switchover Status: Ready</output>
</sample>

```

### show system switchover (ACX7509)

The switchover status option for ACX7509 is only available on backup Routing Engine. The show outputs displayed system switchover status is "Ready" and "Not Ready" are as follows:

```

user@host> show system switchover
Graceful switchover: On
Configuration database: Ready
Object database: Ready
Applications' ready state: Ready
Switchover Status: Ready
Platform Components: Ready
FEB1 Online
FEB1-PFE0 Ready
FEB1-PFE1 Ready
user@host> show system switchover
Graceful switchover: On
Configuration database: Ready
Object database: Ready

```

```

Applications' ready state: Ready
Switchover Status: Not Ready
Platform Components: Not Ready
FEB1 Not Online
FEB1-PFE0 Not Online
FEB1-PFE1 Not Online

```

## show system switchover (Backup Routing Engine - Junos OS Evolved)

```

{backup}
user@host> show system switchover
Graceful switchover: On
Configuration database: Ready
Object database: Ready
Applications' ready state: Ready
Switchover Status: Not Ready

```

## Release Information

Command introduced before Junos OS Release 7.4.

sfc option introduced for the TX Matrix Plus router in Junos OS Release 9.6.

Command support added for ACX7509 in 22.1R1 for High Availability Platform Redundancy RCB and FEB switchover.

## RELATED DOCUMENTATION

[Routing Matrix with a TX Matrix Plus Router Solutions Page](#)

[request chassis routing-engine master](#) | 1238



## show task replication

### IN THIS SECTION

- [Syntax | 1535](#)
- [Description | 1535](#)
- [Options | 1536](#)
- [Required Privilege Level | 1536](#)
- [Output Fields | 1536](#)
- [Sample Output | 1536](#)
- [Release Information | 1537](#)

### Syntax

```
show task replication
```

### Description

Displays nonstop active routing (NSR) status. When you issue this command on the primary Routing Engine, the status of nonstop active routing synchronization is also displayed.



**CAUTION:** If BGP is configured, before attempting nonstop active routing switchover, check the output of `show bgp replication` to confirm that BGP routing table synchronization has completed on the backup Routing Engine. The `complete` status in the output of `show task replication` only indicates that the socket replication has completed and the BGP synchronization is in progress.

To determine whether BGP synchronization is complete, you must check the `Protocol state` and `Synchronization state` fields in the output of `show bgp replication` on the primary Routing Engine. The `Protocol state` must be `idle` and the `Synchronization state` must be `complete`. If you perform NSR switchover before the BGP synchronization has completed, the BGP session might flap.

# Options

This command has no options.

# Required Privilege Level

view

# Output Fields

[Table 83 on page 1536](#) lists the output fields for the `show task replication` command. Output fields are listed in the approximate order in which they appear.

**Table 83: show task replication Output Fields**

Field Name	Field Description
Stateful replication	Displays whether or not graceful Routing Engine switchover is configured. The status can be Enabled or Disabled.
RE mode	Displays the Routing Engine on which the command is issued: Master, Backup, or Not applicable (when the router has only one Routing Engine).
Protocol	Protocols that are supported by nonstop active routing.
Synchronization Status	<p>Nonstop active routing synchronization status for the supported protocols. States are NotStarted, InProgress, and Complete.</p> <p>Synchronization states are shown for each of the supported protocols that are running on the device at that moment.</p>

# Sample Output

## show task replication (Issued on the Primary Routing Engine)

```

user@host> show task replication
    Stateful Replication: Enabled
    RE mode: Master
  
```

Protocol	Synchronization Status
OSPF	NotStarted
BGP	Complete
IS-IS	NotStarted
LDP	Complete
PIM	Complete

### show task replication (Issued on the Backup Routing Engine)

```
user@host> show task replication
    Stateful Replication: Enabled
    RE mode: Backup
```

### show task replication (Junos OS Evolved)

In Junos OS Evolved, both the primary and backup Routings have the same CLI output. If you configured any protocol, you should see the synchronization state for the same.

```
user@host> show task replication

    Stateful Replication: Enabled
    RE mode: Master

Protocol      Synchronization Status
OSPF          NotStarted
BGP           Complete
IS-IS         NotStarted
LDP           Complete
PIM           Complete
```

## Release Information

Command introduced in Junos OS Release 8.5.

Support for logical systems introduced in Junos OS Release 13.3

## RELATED DOCUMENTATION

Example: Configuring Nonstop Active Routing on Switches

## show vrrp

### IN THIS SECTION

- [Syntax | 1538](#)
- [Description | 1538](#)
- [Options | 1538](#)
- [Required Privilege Level | 1539](#)
- [Output Fields | 1539](#)
- [Sample Output | 1549](#)
- [Release Information | 1555](#)

## Syntax

```
show vrrp
<brief | detail | extensive | summary>
<interface interface-name <group number>>
<logical-system logical-system-name >
<nsr>
```

## Description

Display status information about Virtual Router Redundancy Protocol (VRRP) groups.

## Options

<b>none</b>	(Same as brief) Display brief status information about all VRRP interfaces.
-------------	---

<code>brief   detail   extensive   summary</code>	(Optional) Display the specified level of output.
<code>interface <i>interface-name</i> &lt;group number&gt;</code>	(Optional) Display information and status about the specified VRRP interface and, optionally, the group number.
<code>logical-system <i>logical-system-name</i></code>	(Optional) Perform this operation on a particular logical system.
<code>nsr</code>	(Optional) Display state replication information when graceful Routing Engine switchover (GRES) with nonstop active routing (NSR) is configured. Use only on the backup Routing Engine.

### Required Privilege Level

view

### Output Fields

[Table 84 on page 1539](#) lists the output fields for the `show vrrp` command. Output fields are listed in the approximate order in which they appear

**Table 84: show vrrp Output Fields**

Field Name	Field Description	Level of Output
Interface	Name of the logical interface.	brief extensive none summary
Interface index	Physical interface index number, which reflects its initialization sequence.	extensive
Groups	Total number of VRRP groups configured on the interface.	extensive
Active	Total number of VRRP groups that are active (that is, whose interface state is either up or down).	extensive

Table 84: show vrrp Output Fields *(Continued)*

Field Name	Field Description	Level of Output
Interface VRRP PDU statistics	<p>Non-errored statistics for the logical interface:</p> <ul style="list-style-type: none"> <li>Advertisement sent—Number of VRRP advertisement protocol data units (PDUs) that the interface has transmitted.</li> <li>Advertisement received—Number of VRRP advertisement PDUs received by the interface.</li> <li>Packets received—Number of VRRP packets received for VRRP groups on the interface.</li> <li>No group match received—Number of VRRP packets received for VRRP groups that do not exist on the interface.</li> </ul>	extensive
Interface VRRP PDU error statistics	<p>Errored statistics for the logical interface:</p> <ul style="list-style-type: none"> <li>Invalid IPAH next type received—Number of packets received that use the IP Authentication Header protocol (IPAH) and that do not encapsulate VRRP packets.</li> <li>Invalid VRRP ttl value received—Number of packets received whose IP time- to-live (TTL) value is not 255.</li> <li>Invalid VRRP version received—Number of packets received whose VRRP version is not 2.</li> <li>Invalid VRRP pdu type received—Number of packets received whose VRRP PDU type is not 1.</li> <li>Invalid VRRP authentication type received—Number of packets received whose VRRP authentication is not none, simple, or md5.</li> <li>Invalid VRRP IP count received—Number of packets received whose VRRP IP count exceeds 8.</li> <li>Invalid VRRP checksum received—Number of packets received whose VRRP checksum does not match the calculated one.</li> </ul>	extensive

**Table 84: show vrrp Output Fields (Continued)**

Field Name	Field Description	Level of Output
Physical interface	Name of the physical interface.	detail extensive
Unit	Logical unit number.	All levels
Address	Address of the physical interface.	brief detail extensive none
Index	Physical interface index number, which reflects its initialization sequence.	detail extensive
SNMP ifIndex	SNMP index number for the physical interface.	detail extensive
VRRP-Traps	Status of VRRP traps: Enabled or Disabled.	detail extensive
VRRP-Version	VRRP version: 2 or 3.	detail extensive
Type and Address	Identifier for the address and the address itself: <ul style="list-style-type: none"> <li>• <code>lcl</code>—Configured local interface address.</li> <li>• <code>mas</code>—Address of the primary virtual router. This address is displayed only when the local interface is acting as a backup router.</li> <li>• <code>vip</code>—Configured virtual IP addresses.</li> </ul>	brief none summary

Table 84: show vrrp Output Fields *(Continued)*

Field Name	Field Description	Level of Output
Interface state/Int state/State	<p>State of the physical interface:</p> <ul style="list-style-type: none"> <li>• down—The device is present and the link is unavailable.</li> <li>• not present—The interface is configured, but no physical device is present.</li> <li>• unknown—The VRRP process has not had time to query the kernel about the state of the interface.</li> <li>• up—The device is present and the link is established.</li> </ul>	brief extensive none summary
Group	VRRP group number.	brief extensive none summary
State	<p>The state of the interface on which VRRP is running:</p> <ul style="list-style-type: none"> <li>• backup—The interface is acting as the backup router interface.</li> <li>• bringup—VRRP is just starting and the physical device is not yet present.</li> <li>• idle—VRRP is configured on the interface and is disabled. This can occur when VRRP is first enabled on an interface whose link is established.</li> <li>• init—VRRP is initializing.</li> <li>• master—The interface is acting as the primary router interface.</li> <li>• master(ISSU)—The primary router interface is going through a unified in-service software upgrade.</li> <li>• transition—The interface is changing between being the backup and being the primary router.</li> </ul>	extensive



**Table 84: show vrrp Output Fields (Continued)**

Field Name	Field Description	Level of Output
VRRP Mode	<p>If the interface inherits its state and configuration from the active VRRP group, or if it is part of the active VRRP group.</p> <ul style="list-style-type: none"> <li>• Active—Part of the active VRRP group</li> <li>• Inherit—Inherits state and configuration from the active VRRP group.</li> </ul>	detail extensive
Priority	Configured VRRP priority for the interface.	detail extensive
Advertisement interval	Configured VRRP advertisement interval.	detail extensive
Authentication type	Configured VRRP authentication type: none, simple, or md5.	detail extensive
Advertisement Threshold	<p>A value from 1 through 15, used for setting the time when a peer should be considered down.</p> <ul style="list-style-type: none"> <li>• The time a peer is considered down is equal to the advertisement-threshold multiplied by the advertisement-interval.</li> <li>• (advertisement-threshold *advertisement-interval) = Peer down.</li> </ul>	detail extensive
Computed Send Rate	<p>How many protocol data units (PDUs) are generated per second.</p> <p>Based on the number of instances and the advertisement interval.</p>	detail extensive
Preempt	Whether preemption is allowed on the interface: yes or no.	detail extensive
Accept-data mode	Whether the interface is configured to accept packets destined for the virtual IP address: yes or no.	detail extensive

**Table 84: show vrrp Output Fields (Continued)**

Field Name	Field Description	Level of Output
VIP count	Number of virtual IP addresses that have been configured on the interface.	detail extensive
VIP	List of virtual IP addresses configured on the interface.	detail extensive
Advertisement timer	How long, in seconds, until the advertisement timer expires.	detail extensive
Master router	IP address of the interface that is acting as the primary. If the VRRP interface is down, the output is N/A.	detail extensive
Virtual router uptime	How long, in seconds, that the virtual router has been up.	detail extensive
Master router uptime	How long, in seconds, that the primary route has been up.	detail extensive
Virtual MAC	MAC address associated with the virtual IP address.	detail extensive
Tracking	Whether tracking is enabled or disabled.	detail extensive
Current priority	Current operational priority for being the VRRP primary.	detail extensive
Configured priority	Configured base priority for being the VRRP primary.	detail extensive
Priority hold-time	Minimum time interval, in seconds, between successive changes to the current priority. Disabled indicates no minimum interval.	detail extensive
Remaining-time	(track option only) Displays the time remaining in the priority hold-time interval.	detail
Interface tracking	Whether interface tracking is enabled or disabled. When enabled, the output also displays the number of tracked interfaces.	detail extensive

**Table 84: show vrrp Output Fields (Continued)**

Field Name	Field Description	Level of Output
Interface/Tracked interface/Track Int	Name of the tracked interface.	detail extensive
Int state/Interface state/State	Current operational state of the tracked interface: up or down.	detail extensive
Int speed/Speed	Current operational speed, in bits per second, of the tracked interface.	detail extensive
Incurred priority cost	Operational priority cost incurred due to the state and speed of this tracked interface. This cost is applied to the configured priority to obtain the current priority.	detail extensive
Threshold	Speed below which the corresponding priority cost is incurred. In other words, when the speed of the interface drops below the threshold speed, the corresponding priority cost is incurred.  An entry of down means that the corresponding priority cost is incurred when the interface is down.	detail extensive
Route tracking	Whether route tracking is enabled or disabled. When enabled, the output also displays the number of tracked routes.	detail extensive
Route count	The number of routes being tracked.	detail extensive
Route	The IP address of the route being tracked.	detail extensive
VRF name	The VPN routing and forwarding (VRF) routing instance that the tracked route is in.	detail extensive
Route state	The state of the route being tracked: up, down, or unknown.	detail extensive

Table 84: show vrrp Output Fields *(Continued)*

Field Name	Field Description	Level of Output
Priority cost	Configured priority cost. This value is incurred when the interface speed drops below the corresponding threshold or when the tracked route goes down.	detail extensive
Active	Whether the threshold is active (*). If the threshold is active, the corresponding priority cost is incurred.	detail extensive
Group VRRP PDU statistics	Number of VRRP advertisements sent and received by the group.	extensive
Group VRRP PDU error statistics	<p>Errored statistics for the VRRP group:</p> <ul style="list-style-type: none"> <li>• Bad authentication type received—Number of VRRP PDUs received with an invalid authentication type. The received authentication can be none, simple, or md5 and must be the same for all routers in the VRRP group.</li> <li>• Bad password received—Number of VRRP PDUs received with an invalid key (password). The password for simple authentication must be the same for all routers in the VRRP group</li> <li>• Bad MD5 digest received—Number of VRRP PDUs received for which the MD5 digest computed from the VRRP PDU differs from the digest expected by the VRRP instance configured on the router.</li> <li>• Bad advertisement timer received—Number of VRRP PDUs received with an advertisement time interval that is inconsistent with the one in use among the routers in the VRRP group.</li> <li>• Bad VIP count received—Number of VRRP PDUs whose virtual IP address counts differ from the count that has been configured on the VRRP instance.</li> <li>• Bad VIPADDR received—Number of VRRP PDUs whose virtual IP addresses differ from the list of virtual IP addresses configured on the VRRP instance.</li> </ul>	extensive

**Table 84: show vrrp Output Fields (Continued)**

Field Name	Field Description	Level of Output
Group state transition statistics	<p>State transition statistics for the VRRP group:</p> <ul style="list-style-type: none"> <li>• Idle to master transitions—Number of times that the VRRP instance transitioned from the idle state to the primary state.</li> <li>• Idle to backup transitions—Number of times that the VRRP instance transitioned from the idle state to the backup state.</li> <li>• Backup to master transitions—Number of times that the VRRP instance transitioned from the backup state to the primary state.</li> <li>• Master to backup transitions—Number of times that the VRRP instance transitioned from the primary state to the backup state.</li> </ul>	extensive

Table 84: show vrrp Output Fields *(Continued)*

Field Name	Field Description	Level of Output
VR state	<p>The state of the VRRP:</p> <ul style="list-style-type: none"> <li>• backup—The interface is acting as the backup router interface.</li> <li>• bringup—VRRP is just starting, and the physical device is not yet present.</li> <li>• idle—VRRP is configured on the interface and is disabled. This can occur when VRRP is first enabled on an interface whose link is established.</li> <li>• init—VRRP is initializing.</li> <li>• master—The interface is acting as the primary router interface.</li> <li>• transition—The interface is changing between being the backup and being the primary router.</li> </ul> <p><b>NOTE:</b> When show vrrp nsr is used on the backup Routing Engine, it displays the current VRRP state on the primary Routing Engine, which is the future VRRP state for the backup Routing Engine. Do not use on the primary Routing Engine.</p>	brief none summary

### Table 84: show vrrp Output Fields *(Continued)*

Field Name	Field Description	Level of Output
NSR	<p>VRRP nonstop active routing is enabled for the configured VRRP group: yes or no.</p> <p><b>NOTE:</b> A yes value means that the new primary Routing Engine will immediately start with the VRRP State value from the original primary Routing Engine.</p> <p>A no value means that the VRRP session will:</p> <ul style="list-style-type: none"> <li>• Start afresh.</li> <li>• Go through asilent startup period.</li> <li>• Move to a backup state.</li> <li>• Wait for the D Timer to run out before becoming the primary (only if the primary has not been configured already).</li> </ul>	brief none
RPD-NSR	The routing options have been set to nonstop active routing: yes or no.	brief none
Timer	<p>VRRP timer information:</p> <ul style="list-style-type: none"> <li>• A—How long, in seconds, until the advertisement timer expires.</li> <li>• D—How long, in seconds, until the Primary is Down timer expires.</li> </ul>	brief none

## Sample Output

```
show vrrp
```

```
user@host> show vrrp
```

Interface	State	Group	VR state	Timer	Type	Address
fe-0/0/0.121	up	1	master	A 1.052	lcl	fec0::12:1:1:1
					vip	fe80::12:1:1:99
					vip	fec0::12:1:1:99

fe-0/0/2.131	up	1	master	A 0.364	lcl	fec0::13:1:1:1
					vip	fe80::13:1:1:99
					vip	fec0::13:1:1:99

## show vrrp brief

The output for the `show vrrp brief` command is identical to that for the `show vrrp` command. For sample output, see ["show vrrp" on page 1549](#).

## show vrrp detail (IPv6)

```
user@host> show vrrp detail
Physical interface: fe-0/0/0, Unit: 121, Vlan-id: 212, Address: fec0::12:1:1:1/120
  Index: 67, SNMP ifIndex: 45, VRRP-Traps: enabled
  Interface state: up, Group: 1, State: master, VRRP Mode: Active
  Priority: 200, Advertisement interval: 1, Authentication type: none
  Advertisement threshold: 3, Computed send rate: 0
  Preempt: yes, Accept-data mode: no, VIP count: 2, VIP: fe80::12:1:1:99, fec0::12:1:1:99
  Advertisement timer: 1.121s, Master router: fe80::12:1:1:1
  Virtual router uptime: 00:03:47, Master router uptime: 00:03:41
  Virtual MAC: 00:00:5e:00:02:01
  Tracking: disabled

Physical interface: fe-0/0/2, Unit: 131, Vlan-id: 213, Address: fec0::13:1:1:1/120
  Index: 69, SNMP ifIndex: 47, VRRP-Traps: enabled
  Interface state: up, Group: 1, State: master
  Priority: 200, Advertisement interval: 1, Authentication type: none
  Preempt: yes, Accept-data mode: no, VIP count: 2, VIP: fe80::13:1:1:99, fec0::13:1:1:99
  Advertisement timer: 0.327s, Master router: fe80::13:1:1:1
  Virtual router uptime: 00:03:47, Master router uptime: 00:03:41
  Virtual MAC: 00:00:5e:00:02:01
  Tracking: disabled
```

## show vrrp detail (Route Track)

```
user@host> show vrrp detail
Physical interface: ge-0/0/0, Unit: 1, Vlan-id: 1, Address: 101.1.1.1/24
  Index: 324, SNMP ifIndex: 623, VRRP-Traps: enabled, VRRP-Version: 2
  Interface state: up, Group: 1, State: master(ISSU), VRRP Mode: Active
```



```

Priority: 200, Advertisement interval: 1, Authentication type: none
Advertisement threshold: 3, Computed send rate: 0
Preempt: yes, Accept-data mode: no, VIP count: 1, VIP: 101.1.1.3
Advertisement Timer: 0.469s, Master router: 101.1.1.1
Virtual router uptime: 00:02:10, Master router uptime: 00:02:05
Virtual Mac: 00:00:5e:00:01:01
Tracking: disabled

```

### show vrrp detail (Route Track)

```

user@host> show vrrp detail
Physical interface: ge-1/2/0, Unit: 0, Address: 30.30.30.30/24
Index: 67, SNMP ifIndex: 379, VRRP-Traps: enabled, VRRP-Version: 2
Interface state: up, Group: 100, State: master
Priority: 150, Advertisement interval: 1, Authentication type: none
Preempt: yes, Accept-data mode: no, VIP count: 1, VIP: 30.30.30.100
Advertisement timer: 1.218s, Master router: 30.30.30.30
Virtual router uptime: 00:04:28, Master router uptime: 00:00:13
Virtual MAC: 00:00:5e:00:01:64
Tracking: enabled
  Current priority: 150, Configured priority: 150
  Priority hold-time: disabled
  Interface tracking: disabled
  Route tracking: enabled, Route count: 1
    Route          VRF name      Route state  Priority cost
    192.168.40.0/22 default       up           30

```

### show vrrp extensive

```

user@host> show vrrp extensive
Interface: ge-2/0/0.0, Interface index :65539, Groups: 1, Active :1
Interface VRRP PDU statistics
  Advertisement sent           :0
  Advertisement received       :0
  Packets received              :0
  No group match received      :0
Interface VRRP PDU error statistics
  Invalid IPAH next type received :0
  Invalid VRRP TTL value received :0
  Invalid VRRP version received  :0

```

```

Invalid VRRP PDU type received      :0
Invalid VRRP authentication type received:0
Invalid VRRP IP count received      :0
Invalid VRRP checksum received      :0

Physical interface: ge-2/0/0, Unit: 0, Address: 10.10.10.1/24
Index: 65539, SNMP ifIndex: 648, VRRP-Traps: enabled, VRRP-Version: 3
Interface state: up, Group: 1, State: backup, VRRP Mode: Active
Priority: 100, Advertisement interval: 1, Authentication type: none
Advertisement threshold: 3, Computed send rate: 0
Preempt: yes, Accept-data mode: no, VIP count: 1, VIP: 10.10.10.2
Dead timer: 3.078s, Master priority: 0, Master router: 10.10.10.1
Virtual router uptime: 00:00:04
Tracking: disabled
Group VRRP PDU statistics
  Advertisement sent                :0
  Advertisement received             :0
Group VRRP PDU error statistics
  Bad authentication Type received   :0
  Bad password received              :0
  Bad MD5 digest received            :0
  Bad advertisement timer received   :0
  Bad VIP count received             :0
  Bad VIPADDR received              :0
Group state transition statistics
  Idle to master transitions         :0
  Idle to backup transitions         :1
  Backup to master transitions       :0
  Master to backup transitions       :0

```

## show vrrp interface

```

user@host> show vrrp interface ge-0/0/0.1
Interface: ge-0/0/0.1, Interface index :324, Groups: 2, Active :2
Interface VRRP PDU statistics
  Advertisement sent                :39
  Advertisement received             :0
  Packets received                  :0
  No group match received           :0
Interface VRRP PDU error statistics
  Invalid IPAH next type received    :0

```

```

Invalid VRRP TTL value received      :0
Invalid VRRP version received        :0
Invalid VRRP PDU type received       :0
Invalid VRRP authentication type received:0
Invalid VRRP IP count received       :0
Invalid VRRP checksum received       :0

```

Physical interface: ge-0/0/0, Unit: 1, Vlan-id: 1, Address: 101.1.1.1/24

Index: 324, SNMP ifIndex: 623, VRRP-Traps: enabled, VRRP-Version: 2

Interface state: up, Group: 1, State: master(ISSU), VRRP Mode: Active

Advertisement threshold: 3, Computed send rate: 0

Priority: 200, Advertisement interval: 1, Authentication type: none

Advertisement threshold: 3, Computed send rate: 0

Preempt: yes, Accept-data mode: no, VIP count: 1, VIP: 101.1.1.3

Advertisement Timer: 0.619s, Master router: 101.1.1.1

Virtual router uptime: 00:00:22, Master router uptime: 00:00:17

Virtual Mac: 00:00:5e:00:01:01

Tracking: disabled

Group VRRP PDU statistics

```

Advertisement sent                    :20

```

```

Advertisement received                :0

```

Group VRRP PDU error statistics

```

Bad authentication Type received     :0

```

```

Bad password received                :0

```

```

Bad MD5 digest received              :0

```

```

Bad advertisement timer received     :0

```

```

Bad VIP count received               :0

```

```

Bad VIPADDR received                 :0

```

Group state transition statistics

```

Idle to master transitions            :0

```

```

Idle to backup transitions            :1

```

```

Backup to master transitions          :1

```

```

Master to backup transitions          :0

```

Interface: fe-0/0/0.121, Interface index: 67, Groups: 1, Active : 1

Interface VRRP PDU statistics

```

Advertisement sent                    :      205

```

```

Advertisement received                :         0

```

```

Packets received                     :         0

```

```

No group match received               :         0

```

Interface VRRP PDU error statistics

```

Invalid IPAH next type received       :         0

```

```

Invalid VRRP TTL value received       :         0

```

```

Invalid VRRP version received         :         0

```

```

Invalid VRRP PDU type received      :      0
Invalid VRRP authentication type received:      0
Invalid VRRP IP count received      :      0
Invalid VRRP checksum received      :      0

```

## show vrrp nsr

This command is similar to `show vrrp`. Here, the **VR state** column displays the current VRRP state on the primary Routing Engine, which is the future VRRP state for the backup Routing Engine. Do not use on the primary Routing Engine.

NSR is yes if VRRP nonstop active routing is enabled for the configured VRRP group.

RPD-NSR is yes if the routing options have been set to nonstop active routing.

```
user@host>show vrrp nsr
```

Interface	State	Group	VR state	VR Mode	Type	NSR	RPD-NSR	Address
ge-1/0/1.0	up	1	master	Active	lcl	yes	yes	10.0.0.1
					vip			10.0.0.3
ge-1/0/1.0	up	2	master	Active	lcl	yes	yes	20.0.0.1
					vip			20.0.0.3
ge-1/0/1.0	up	3	master	Active	lcl	yes	yes	30.0.0.1
					vip			30.0.0.3
ge-1/0/1.0	up	4	master	Active	lcl	yes	yes	40.0.0.1
					vip			40.0.0.3
ge-1/0/1.0	up	5	master	Active	lcl	yes	yes	50.0.0.1
					vip			50.0.0.3
ge-1/0/1.0	up	1	master	Active	lcl	yes	yes	1000::1
					vip			fe80::200:5eff:fe00:1
					vip			1000::3
ge-1/0/1.0	up	2	master	Active	lcl	yes	yes	2000::1
					vip			fe80::200:5eff:fe00:2
					vip			2000::3
ge-1/0/1.0	up	3	master	Active	lcl	yes	yes	3000::1
					vip			fe80::200:5eff:fe00:3
					vip			3000::3
ge-1/0/1.0	up	4	master	Active	lcl	yes	yes	4000::1
					vip			fe80::200:5eff:fe00:4
					vip			4000::3
ge-1/0/1.0	up	5	master	Active	lcl	yes	yes	5000::1

	vip	fe80::200:5eff:fe00:5
	vip	5000::3

**show vrrp summary**

user@host> show vrrp summary					
Interface	State	Group	VR state	Type	Address
ge-4/2/0.0	up	1	backup	lcl	10.57.0.2
				vip	10.57.0.100

**Release Information**

Command introduced before Junos OS Release 7.4.

nsr option added in Junos OS Release 13.2.

**RELATED DOCUMENTATION**

<a href="#">show vrrp track   1555</a>
<a href="#">clear vrrp   1233</a>

**show vrrp track**

**IN THIS SECTION**

- [Syntax | 1556](#)
- [Description | 1556](#)
- [Options | 1556](#)
- [Required Privilege Level | 1556](#)
- [Output Fields | 1556](#)
- [Sample Output | 1559](#)
- [Release Information | 1561](#)

Syntax

```
show vrrp track
<all | interfaces | routes>
<detail | summary>
<logical-system logical-system-name>
```

Description

Display status information about Virtual Router Redundancy Protocol (VRRP) tracked routes and tracked interfaces.

Options

<b>none</b>	(Same as <i>summary</i> ) Display summarized status information of tracked routes and tracked interfaces.
<b>all   interfaces   routes</b>	<p>(Optional) These options display the following information:</p> <ul style="list-style-type: none"><li>• <i>all</i>—Output is the same as for the <code>show vrrp track</code> command.</li><li>• <i>interfaces</i>—Show summary of VRRP tracked interfaces.</li><li>• <i>routes</i>—Show summary of VRRP tracked routes</li></ul>
<b>detail   summary</b>	(Optional) Display detailed or summarized information.
<b>logical-system <i>logical-system-name</i></b>	(Optional) Perform this operation on a particular logical system.

Required Privilege Level

view

Output Fields

[Table 85 on page 1557](#) lists the output fields for the `show vrrp track` command. Output fields are listed in the approximate order in which they appear.

**Table 85: show vrrp track Output Fields**

Fields	Description	Level
Tracked interface/ Track Int	Name of the tracked interface.	detail or summary
State	Current operational state of the tracked interface: up or down.	detail or summary
Speed	Current operational speed, in bits per second, of the tracked interface.	detail or summary
Incurred priority cost	Operational priority cost incurred resulting from the state and speed of this tracked interface. This cost is applied to the configured priority to obtain the current priority cost.	detail
VRRP Int/Tracking VRRP interface	Name of the VRRP interface.	detail or summary
Group	VRRP group number.	detail or summary

Table 85: show vrrp track Output Fields *(Continued)*

Fields	Description	Level
VR state	<p>The state of the VRRP:</p> <ul style="list-style-type: none"> <li>• backup—The interface is acting as the backup router interface.</li> <li>• bringup—VRRP is just starting, and the physical device is not yet present.</li> <li>• idle—VRRP is configured on the interface and is disabled. This can occur when VRRP is first enabled on an interface whose link is established.</li> <li>• init—VRRP is initializing.</li> <li>• master—The interface is acting as the primary router interface.</li> <li>• transition—The interface is changing between being the backup and being the primary router.</li> </ul> <p><b>NOTE:</b> When the <code>show vrrp nsr</code> command is used on the backup Routing Engine, it displays the current VRRP state on the primary Routing Engine, which is the future VRRP state for the backup Routing Engine. Do not use the <code>show vrrp nsr</code> command on the primary Routing Engine.</p>	detail or summary
Current priority	Current operational priority for being the VRRP primary.	detail or summary
Priority hold-time	Minimum time interval, in seconds, between successive changes to the current priority cost. Disabled indicates no minimum interval.	detail
Track route	IP address of route.	detail or summary
State	State of route. Possible values are unknown, up, and down.	detail or summary
Cost	Priority cost. When the route state is not up, the cost will be deducted from the configured priority of the VRRP session.	detail or summary



**Table 85: show vrrp track Output Fields (Continued)**

Fields	Description	Level
Interface	Name of the logical interface (for example, ge-0/0/1.0) on which the corresponding VRRP session is configured.	detail or summary
Cfg	Configured priority.	detail or summary
Run	Current (or running) priority cost.	detail or summary

## Sample Output

### show vrrp track summary

```
user@host> show vrrp track summary
```

Track Int	State	Speed	VRRP Int	Group	VR State	Current prio
ge-0/0/2.0	up	1g	ge-0/0/1.0	1	master	80
ge-0/0/8.0	up	1g	ge-0/0/1.0	1	master	80

Track route	State	Cost	Interface	Group	Cfg	Run	VR State
44.44.44.0/24	unknown	10	ge-0/0/1.0	1	100	80	master
55.55.55.0/24	unknown	10	ge-0/0/1.0	1	100	80	master

### show vrrp track detail

```
user@host> show vrrp track detail
```

```
Tracked interface: ge-0/0/2.0
State: up, Speed: 1g
Incurred priority cost: 0
Tracking VRRP interface: ge-0/0/1.0, Group: 1
VR State: master
Current priority: 80, Configured priority: 100
Priority hold-time: disabled
```

```

Tracked interface: ge-0/0/8.0
  State: up, Speed: 1g
  Incurred priority cost: 0
  Tracking VRRP interface: ge-0/0/1.0, Group: 1
    VR State: master
    Current priority: 80, Configured priority: 100
    Priority hold-time: disabled

```

Track route	State	Cost	Interface	Group	Cfg	Run	VR State
44.44.44.0/24	unknown	10	ge-0/0/1.0	1	100	80	master
55.55.55.0/24	unknown	10	ge-0/0/1.0	1	100	80	master

### show vrrp track interfaces summary

```

user@host> show vrrp track interfaces summary

```

Track Int	State	Speed	VRRP Int	Group	VR State	Current prio
ge-0/0/2.0	up	1g	ge-0/0/1.0	1	master	80
ge-0/0/8.0	up	1g	ge-0/0/1.0	1	master	80

### show vrrp track interfaces detail

```

user@host> show vrrp track interfaces detail

```

Tracked interface: ge-0/0/2.0

```

  State: up, Speed: 1g
  Incurred priority cost: 0
  Tracking VRRP interface: ge-0/0/1.0, Group: 1
    VR State: master
    Current priority: 80, Configured priority: 100
    Priority hold-time: disabled

```

Tracked interface: ge-0/0/8.0

```

  State: up, Speed: 1g
  Incurred priority cost: 0
  Tracking VRRP interface: ge-0/0/1.0, Group: 1
    VR State: master
    Current priority: 80, Configured priority: 100
    Priority hold-time: disabled

```

**show vrrp track routes summary**

```
user@host> show vrrp track routes summary
```

Track route	State	Cost	Interface	Group	Cfg	Run	VR State
44.44.44.0/24	unknown	10	ge-1/0/0.0	1	100	60	bringup
55.55.55.0/24	unknown	10	ge-1/0/0.0	1	100	60	bringup

**show vrrp track routes detail**

The output for show vrrp track routes detail is the same as that for show vrrp track routes summary.

**Release Information**

Command introduced before Junos OS Release 7.4.

all and routes options added in Junos OS Release 17.1.

**RELATED DOCUMENTATION**

Configuring a Logical Interface to Be Tracked for a VRRP Group
Configuring a Route to Be Tracked for a VRRP Group
<a href="#">show vrrp</a>   <a href="#">1538</a>

# Troubleshooting

## IN THIS CHAPTER

- [Tracing Nonstop Active Routing Synchronization Events | 1562](#)
- [Troubleshooting the EX Series Redundant Power System Power On and Power Backup Issues | 1564](#)

## Tracing Nonstop Active Routing Synchronization Events

To track the progress of nonstop active routing synchronization between Routing Engines, you can configure nonstop active routing trace options flags for each supported protocol and for BFD sessions and record these operations to a log file.

To configure nonstop active routing trace options for supported routing protocols, include the `nsr-synchronization` statement at the `[edit protocols protocol-name traceoptions flag]` hierarchy level and optionally specify one or more of the **detail**, **disable**, **receive**, and **send** options:

```
[edit protocols]
bgp {
    traceoptions {
        flag nsr-synchronization <detail> <disable> <receive> <send>;
    }
}
isis {
    traceoptions {
        flag nsr-synchronization <detail> <disable> <receive> <send>;
    }
}
ldp {
    traceoptions {
        flag nsr-synchronization <detail> <disable> <receive> <send>;
    }
}
mpls {
```

```

    traceoptions {
        flag nsr-synchronization;
        flag nsr-synchronization-detail;
    }
}
msdp {
    traceoptions {
        flag nsr-synchronization <detail> <disable> <receive> <send>;
    }
}
(ospf | ospf3) {
    traceoptions {
        flag nsr-synchronization <detail> <disable> <receive> <send>;
    }
}
rip {
    traceoptions {
        flag nsr-synchronization <detail> <disable> <receive> <send>;
    }
}
ripng {
    traceoptions {
        flag nsr-synchronization <detail> <disable> <receive> <send>;
    }
}
pim {
    traceoptions {
        flag nsr-synchronization <detail> <disable> <receive> <send>;
    }
}

```

To configure nonstop active routing trace options for BFD sessions, include the **nsr-synchronization** and **nsr-packet** statements at the [edit protocols bfd traceoptions flag] hierarchy level.

```

[edit protocols]
bfd {
    traceoptions {
        flag nsr-synchronization;
        flag nsr-packet;
    }
}

```

To trace the Layer 2 VPN signaling state replicated from routes advertised by BGP, include the `nsr-synchronization` statement at the `[edit routing-options traceoptions flag]` hierarchy level. This flag also traces the label and logical interface association that VPLS receives from the kernel replication state.

```
[edit routing-options]
traceoptions {
    flag nsr-synchronization;
}
```

## RELATED DOCUMENTATION

[Configuring Nonstop Active Routing | 281](#)

Configuring Nonstop Active Routing on Switches

Example: Configuring Nonstop Active Routing on Switches

Example: Configuring Nonstop Active Routing

## Troubleshooting the EX Series Redundant Power System Power On and Power Backup Issues

### IN THIS SECTION

- [The EX Series RPS Is Not Powering On | 1565](#)
- [A Switch Is Not Recognized by the RPS | 1566](#)
- [An Error Message Indicates That an RPS Power Supply is Not Supported | 1566](#)
- [The EX Series Redundant Power System Is Not Providing Power Backup to a Connected Switch | 1567](#)
- [The Wrong Switches Are Being Backed Up | 1568](#)
- [Six Switches That Do Not Require PoE Are Not All Being Backed Up | 1569](#)

This topic provides troubleshooting information for problems related to the EX Series Redundant Power System (RPS).

## The EX Series RPS Is Not Powering On

### IN THIS SECTION

- Problem | 1565
- Cause | 1565
- Solution | 1565

### Problem

### Description

The RPS does not power on even though it has a power supply installed and is connected to an AC power source outlet.

### Environment

The RPS with one EX-PWR3-930-AC power supply installed in it is connected to a switch.

### Symptoms

The SYS LED on the power supply side of the RPS is off, and when you check the RPS status using the CLI command **show chassis redundant-power-system**, the message **No RPS connected** is displayed.

### Cause

A power supply must be installed in the middle slot on the RPS to power on the RPS.

### Solution

Install a power supply in the middle slot on the power supply side of the RPS and verify that the AC power source outlet is properly connected to it. See [Installing a Power Supply in the EX Series Redundant Power System](#).

Verify that the **AC OK** LED and the **DC OK** LED on the power supply in the RPS are lit green.

## A Switch Is Not Recognized by the RPS

### IN THIS SECTION

- [Problem | 1566](#)
- [Cause | 1566](#)
- [Solution | 1566](#)

### Problem

### Description

I cannot set up the RPS.

### Cause

A switch must be active to be recognized by the RPS.

### Solution

Activate the switch by configuring it and issuing a commit statement.

## An Error Message Indicates That an RPS Power Supply is Not Supported

### IN THIS SECTION

- [Problem | 1566](#)
- [Cause | 1567](#)
- [Solution | 1567](#)

### Problem

### Description

An RPS error message indicates that an RPS power supply is not supported.



## Cause

RPS supports only one power supply, the EX-PWR3-930-AC. If you install another similar power supply, it may fit in the slot but it is not compatible with RPS.

## Solution

The power supply shipped with your RPS (in a separate box) is an EX-PWR3-930-AC. If you installed more power supplies, you ordered them separately. Replace any other power supply model (such as the EX-PWR2-930-AC) with an EX-PWR3-930-AC model.

## The EX Series Redundant Power System Is Not Providing Power Backup to a Connected Switch

### IN THIS SECTION

- [Problem | 1567](#)
- [Cause | 1568](#)
- [Solution | 1568](#)

## Problem

### Description

The RPS does not provide power backup to a connected switch.

### Environment

The RPS has an EX-PWR3-930-AC power supply installed in the middle power supply slot and is connected to two switches with power loss, one connected to RPS switch connector port 1 and the other on port 2.

### Symptoms

The status LED on the associated switch connector port is not blinking green—it is either solid green (connected) or not lit (off).

## Cause

The RPS provides backup power based on the power priority assigned to each switch.

## Solution

If the status LED on a switch connector port is off, ensure that the RPS cable is properly connected to both the RPS and the switch, and ensure that the priority configured for the switch is not 0. See ["show redundant-power-system status" on page 1494](#).

If the status LED on switch connector port 1 is on and is steadily green, check the backup priority configured for the switch and assign it a higher priority. See [Determining and Setting Priority for Switches Connected to an EX Series RPS](#)

If the status LED on switch connector port 1 is amber, check if the RPS has enough power supplies installed in it to provide backup power. If it does not, install a power supply in an empty power supply slot on the RPS. See [Installing a Power Supply in the EX Series Redundant Power System](#).

If the status LED on switch connector port 1 is still off, check the priority configured for the switch. Ensure that the is not set to 0, which means off. See ["show redundant-power-system status" on page 1494](#). The priority assigned must be from 1 through 6. See [Determining and Setting Priority for Switches Connected to an EX Series RPS](#).

Verify that a dedicated power supply is installed in the switch. The RPS cannot boot a switch that does not have a dedicated power supply. See [Installing a Power Supply in the EX Series Redundant Power System](#).

Also keep in mind that when the command ["request redundant-power-system multi-backup" on page 1250](#) has been set, support for switches that supply PoE is not guaranteed. To reverse this setting, use the command `request redundant-power-system no-multi-backup`.

## The Wrong Switches Are Being Backed Up

### IN THIS SECTION

- [Problem | 1569](#)
- [Cause | 1569](#)
- [Solution | 1569](#)

## Problem

## Description

Four or more switches are connected to an RPS with three power supplies. When all four switches fail, the wrong three switches have .

## Environment

Four or more switches are connected to an RPS with three power supplies. One or more switches provide PoE to other devices.

## Symptoms

When all four switches fail, the wrong three switches have .

## Cause

The RPS provides backup power based on the power priority assigned to each switch. This is derived from two configurations, one of which has precedence over the other one. Initial is derived from the location of the port used to attach a switch—the leftmost connector has lowest priority and the rightmost connector has highest priority. The second, dominant priority configuration is derived from a CLI priority setting on the switch itself. With this CLI configuration, 6 is highest priority and 1 is the lowest priority.

## Solution

Connect the three switches to the three rightmost connectors on the RPS. Then, using the CLI on each switch, set each switch's priority to 1 using the ["redundant-power-system" on page 1094](#) configuration command **redundant-power-system 1**. Now, physical connection location is determining .

If you do not want to change the cabling on the switches, you can use the configuration statement **redundant-power-system** on all four switches, assigning priority 6 (highest), 5, 4 and 3 to the appropriate switches. Priority configuration on the switch always overcomes set by connector location.

## Six Switches That Do Not Require PoE Are Not All Being Backed Up

### IN THIS SECTION

 [Problem | 1570](#)

- Cause | 1570
- Solution | 1570

## Problem

## Description

Only three switches out of six are simultaneously backed up when all switches experience power supply failure. None of these switches supply PoE power to any device.

## Environment

The RPS with three EX-PWR3-930-AC power supplies installed in it is connected to six switches, none of which is connected to a non-PoE device.

## Symptoms

Only three switches out of six are simultaneously backed up when all switches experience power supply failure. None of these switches supply PoE power to any device.

## Cause

Each power supply can support two switches that do not need enough power for PoE, as long as you configure the RPS to do so.

## Solution

From any of the attached switches, issue the "[request redundant-power-system multi-backup](#)" on page [1250](#) command from the operational mode. Now standard power will be supplied to two non-PoE switches per power supply.

## CHAPTER 54

# Knowledge Base