

Routing Options Feature Guide for EX9200 Switches

Release

15.1



Modified: 2016-06-28

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

Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, and JunosE are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Routing Options Feature Guide for EX9200 Switches

15.1

Copyright © 2016, 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 <http://www.juniper.net/support/eula.html>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

| | | |
|------------------|--|----------|
| | About the Documentation | ix |
| | Documentation and Release Notes | ix |
| | Supported Platforms | ix |
| | Using the Examples in This Manual | ix |
| | Merging a Full Example | x |
| | Merging a Snippet | x |
| | Documentation Conventions | xi |
| | Documentation Feedback | xiii |
| | Requesting Technical Support | xiii |
| | Self-Help Online Tools and Resources | xiii |
| | Opening a Case with JTAC | xiv |
| Part 1 | Overview | |
| Chapter 1 | Understanding Routing Properties | 3 |
| | Protocol-Independent Routing Properties Overview | 3 |
| Part 2 | Configuring Routing Properties | |
| Chapter 2 | Routing Properties Examples | 7 |
| | Examples: Configuring BFD for Static Routes | 7 |
| | Understanding BFD for Static Routes for Faster Network Failure Detection | 7 |
| | Example: Configuring BFD for Static Routes | 11 |
| | Example: Enabling BFD on Qualified Next Hops in Static Routes for Route Selection | 16 |
| | Example: Configuring BFD Authentication for Static Routes | 22 |
| | Understanding BFD Authentication for Static Route Security | 22 |
| | BFD Authentication Algorithms | 23 |
| | Security Authentication Keychains | 24 |
| | Strict Versus Loose Authentication | 24 |
| | Example: Configuring BFD Authentication for Securing Static Routes | 24 |

| | | |
|------------------|--|-----------|
| Part 3 | Troubleshooting | |
| Chapter 3 | Configuration Statements and Operational Commands | 33 |
| | Configuration Statements | 33 |
| | [edit routing-options] Hierarchy Level | 33 |
| | Common Routing Options | 33 |
| | Complete [edit routing-options] Hierarchy | 35 |
| | bfd | 45 |
| | bfd-liveness-detection (Routing Options Static Route) | 47 |
| | Operational Commands | 50 |
| | Operational-Mode Commands | 50 |
| | Overview of Junos OS CLI Operational Mode Commands | 50 |
| | Example: Running Operational Mode Commands on Logical Systems | 53 |
| | Example: Viewing BGP Trace Files on Logical Systems | 55 |
| | Example: Configuring System Logging on Logical Systems | 60 |

List of Figures

| | | |
|-----------|---|----|
| Part 2 | Configuring Routing Properties | |
| Chapter 2 | Routing Properties Examples | 7 |
| | Figure 1: Customer Routes Connected to a Service Provider | 12 |
| | Figure 2: BFD Enabled on Qualified Next Hops | 17 |
| | Figure 3: Customer Routes Connected to a Service Provider | 25 |

List of Tables

| | |
|------------------|---|
| | About the Documentation ix |
| | Table 1: Notice Icons xi |
| | Table 2: Text and Syntax Conventions xi |
| Part 3 | Troubleshooting |
| Chapter 3 | Configuration Statements and Operational Commands 33 |
| | Table 3: Commonly Used Operational Mode Commands 52 |

About the Documentation

- Documentation and Release Notes on page ix
- Supported Platforms on page ix
- Using the Examples in This Manual on page ix
- Documentation Conventions on page xi
- Documentation Feedback on page xiii
- Requesting Technical Support on page xiii

Documentation and Release Notes

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at <http://www.juniper.net/techpubs/>.

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

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

Supported Platforms

For the features described in this document, the following platforms are supported:

- EX Series

Using the Examples in This Manual

If you want to use the examples in this manual, you can use the **load merge** or the **load merge relative** command. These commands cause the software to merge the incoming configuration into the current candidate configuration. The example does not become active until you commit the candidate configuration.

If the example configuration contains the top level of the hierarchy (or multiple hierarchies), the example is a *full example*. In this case, use the **load merge** command.

If the example configuration does not start at the top level of the hierarchy, the example is a *snippet*. In this case, use the **load merge relative** command. These procedures are described in the following sections.

Merging a Full Example

To merge a full example, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration example into a text file, save the file with a name, and copy the file to a directory on your routing platform.

For example, copy the following configuration to a file and name the file **ex-script.conf**. Copy the **ex-script.conf** file to the **/var/tmp** directory on your routing platform.

```
system {
  scripts {
    commit {
      file ex-script.xml;
    }
  }
}
interfaces {
  fxp0 {
    disable;
    unit 0 {
      family inet {
        address 10.0.0.1/24;
      }
    }
  }
}
```

2. Merge the contents of the file into your routing platform configuration by issuing the **load merge** configuration mode command:

```
[edit]
user@host# load merge /var/tmp/ex-script.conf
load complete
```

Merging a Snippet

To merge a snippet, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration snippet into a text file, save the file with a name, and copy the file to a directory on your routing platform.

For example, copy the following snippet to a file and name the file **ex-script-snippet.conf**. Copy the **ex-script-snippet.conf** file to the **/var/tmp** directory on your routing platform.

```
commit {
  file ex-script-snippet.xml; }
```

2. Move to the hierarchy level that is relevant for this snippet by issuing the following configuration mode command:

```
[edit]
user@host# edit system scripts
[edit system scripts]
```

3. Merge the contents of the file into your routing platform configuration by issuing the **load merge relative** configuration mode command:

```
[edit system scripts]
user@host# load merge relative /var/tmp/ex-script-snippet.conf
load complete
```

For more information about the **load** command, see the *CLI User Guide*.

Documentation Conventions

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

Table 1: Notice Icons

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

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

Table 2: Text and Syntax Conventions

| Convention | Description | Examples |
|----------------------------|--------------------------------|--|
| Bold text like this | Represents text that you type. | To enter configuration mode, type the configure command: user@host> configure |

Table 2: Text and Syntax Conventions (*continued*)

| Convention | Description | Examples |
|--------------------------------|---|--|
| Fixed-width text like this | Represents output that appears on the terminal screen. | user@host> show chassis alarms No alarms currently active |
| <i>Italic text like this</i> | <ul style="list-style-type: none">Introduces or emphasizes important new terms.Identifies guide names.Identifies RFC and Internet draft titles. | <ul style="list-style-type: none">A policy <i>term</i> is a named structure that defines match conditions and actions.<i>Junos OS CLI User Guide</i>RFC 1997, <i>BGP Communities Attribute</i> |
| <i>Italic text like this</i> | Represents variables (options for which you substitute a value) in commands or configuration statements. | Configure the machine's domain name: [edit] root@# set system domain-name <i>domain-name</i> |
| Text like this | Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components. | <ul style="list-style-type: none">To configure a stub area, include the stub statement at the [edit protocols ospf area area-id] hierarchy level.The console port is labeled CONSOLE. |
| < > (angle brackets) | Encloses optional keywords or variables. | stub <default-metric <i>metric</i>>; |
| (pipe symbol) | Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity. | broadcast multicast (<i>string1</i> <i>string2</i> <i>string3</i>) |
| # (pound sign) | Indicates a comment specified on the same line as the configuration statement to which it applies. | rsvp { # Required for dynamic MPLS only |
| [] (square brackets) | Encloses a variable for which you can substitute one or more values. | community name members [<i>community-ids</i>] |
| Indentation and braces ({ }) | Identifies a level in the configuration hierarchy. | [edit] routing-options { static { route default { nexthop <i>address</i> ; retain; } } } |
| ;(semicolon) | Identifies a leaf statement at a configuration hierarchy level. | |
| GUI Conventions | | |
| Bold text like this | Represents graphical user interface (GUI) items you click or select. | <ul style="list-style-type: none">In the Logical Interfaces box, select All Interfaces.To cancel the configuration, click Cancel. |

Table 2: Text and Syntax Conventions (*continued*)

| Convention | Description | Examples |
|------------------------------|---|--|
| > (bold right angle bracket) | Separates levels in a hierarchy of menu selections. | In the configuration editor hierarchy, select Protocols>Ospf . |

Documentation Feedback

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

- Online feedback rating system—On any page of the Juniper Networks TechLibrary site at <http://www.juniper.net/techpubs/index.html>, simply click the stars to rate the content, and use the pop-up form to provide us with information about your experience. Alternately, you can use the online feedback form at <http://www.juniper.net/techpubs/feedback/>.
- E-mail—Send your comments to techpubs-comments@juniper.net. Include the document or topic name, URL or page number, and software version (if applicable).

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or Partner Support Service support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at <http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <http://www.juniper.net/support/warranty/>.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: <http://www.juniper.net/customers/support/>
- Search for known bugs: <http://www2.juniper.net/kb/>
- Find product documentation: <http://www.juniper.net/techpubs/>
- Find solutions and answer questions using our Knowledge Base: <http://kb.juniper.net/>

- Download the latest versions of software and review release notes:
<http://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications:
<http://kb.juniper.net/InfoCenter/>
- Join and participate in the Juniper Networks Community Forum:
<http://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Management tool: <http://www.juniper.net/cm/>

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

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at <http://www.juniper.net/cm/>.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see <http://www.juniper.net/support/requesting-support.html>.

PART 1

Overview

- [Understanding Routing Properties on page 3](#)

CHAPTER 1

Understanding Routing Properties

- [Protocol-Independent Routing Properties Overview on page 3](#)

Protocol-Independent Routing Properties Overview

In Junos OS, routing capabilities and features that are not specific to any particular routing protocol are collectively called protocol-independent routing properties. These features often interact with routing protocols. In many cases, you combine protocol-independent properties and routing policy to achieve a goal. For example, you define a static route using protocol-independent properties, and then, using a routing policy, you can redistribute the static route into a routing protocol, such as BGP, OSPF, or IS-IS.

Protocol-independent routing properties include:

- Static, aggregate, and generated routes
- Bidirectional Forwarding Detection on static routes
- Global preference
- Martian routes
- Routing tables and routing information base (RIB) groups

Related Documentation

- *Examples: Configuring Static Routes*
- *Examples: Creating a Routing Table and Populating It with Routes*

PART 2

Configuring Routing Properties

- [Routing Properties Examples on page 7](#)

CHAPTER 2

Routing Properties Examples

- [Examples: Configuring BFD for Static Routes on page 7](#)
- [Example: Configuring BFD Authentication for Static Routes on page 22](#)

Examples: Configuring BFD for Static Routes

- [Understanding BFD for Static Routes for Faster Network Failure Detection on page 7](#)
- [Example: Configuring BFD for Static Routes on page 11](#)
- [Example: Enabling BFD on Qualified Next Hops in Static Routes for Route Selection on page 16](#)

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.



NOTE: EX3300 supports BFD over static routes only.

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.

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

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

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.



NOTE:

Inline BFD is supported on PTX routers with Third generation FPCs starting in Junos OS Release 15.1F3.

There are three types of BFD sessions based on the source from which BFD packets are sent to the neighbors. Different types of BFD sessions and their descriptions are given in the table below:

| Type of BFD session | Description |
|---------------------|--|
| Non-distributed BFD | BFD sessions running completely on the Routing Engine. |
| Distributed BFD | BFD sessions running on the Packet Forwarding Engine. |
| Inline BFD | BFD sessions running on the FPC hardware. |

NOTE: Supported only on static routers starting from Junos OS Release 13.3 and supported on PTX Series routers starting from Junos OS Release 15.1F3.

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: 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.



NOTE: SRX Series devices do not support distributed BFD.

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.

Example: Configuring BFD for Static Routes

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

- [Requirements on page 11](#)
- [Overview on page 11](#)
- [Configuration on page 12](#)
- [Verification on page 15](#)

Requirements

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

Overview

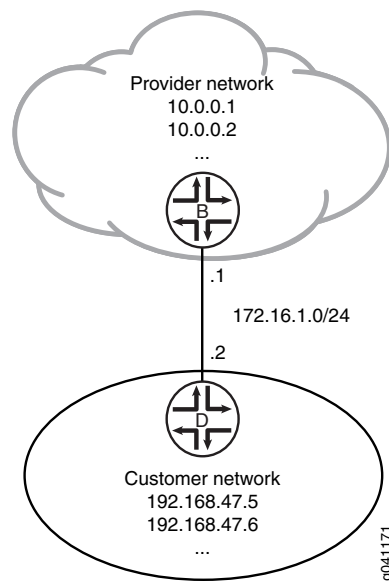
There are many practical applications for static routes. Static routing is often used at the network edge to support attachment to stub networks, which, given their single point of entry and egress, are well suited to the simplicity of a static route. In Junos OS, static routes have a global preference 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 12](#) shows the sample network.

Figure 1: Customer Routes Connected to a Service Provider



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, 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 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
```

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 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
```
  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 {
 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 {
 minimum-interval 1000;
 }
}

```

## Verification

Confirm that the configuration is working properly.

- [Verifying That BFD Sessions Are Up on page 15](#)
- [Viewing Detailed BFD Events on page 16](#)

### 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, 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

```
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: ppm_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: Enabling BFD on Qualified Next Hops in Static Routes for Route Selection

This example shows how to configure a static route with multiple possible next hops. Each next hop has Bidirectional Forwarding Detection (BFD) enabled.

- [Requirements on page 16](#)
- [Overview on page 16](#)
- [Configuration on page 17](#)
- [Verification on page 20](#)

---

#### Requirements

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

---

#### Overview

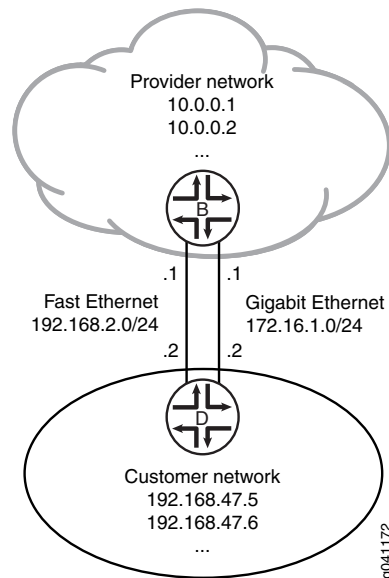
In this example, Device B has the static route **192.168.47.0/24** with two possible next hops. The two next hops are defined using two **qualified-next-hop** statements. Each next hop has BFD enabled.

BFD is also enabled on Device D because BFD must be enabled on both ends of the connection.

A next hop is included in the routing table if the BFD session is up. The next hop is removed from the routing table if the BFD session is down.

See [Figure 2 on page 17](#).

**Figure 2: BFD Enabled on Qualified Next Hops**



### 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, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

**Device B**

```

set interfaces fe-0/1/0 unit 2 description secondary-B->D
set interfaces fe-0/1/0 unit 2 family inet address 192.168.2.1/24
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 routing-options static route 192.168.47.0/24 qualified-next-hop 192.168.2.2
 bfd-liveness-detection minimum-interval 60
set routing-options static route 192.168.47.0/24 qualified-next-hop 172.16.1.2
 bfd-liveness-detection minimum-interval 60

```

**Device D**

```

set interfaces fe-0/1/0 unit 3 description secondary-D->B
set interfaces fe-0/1/0 unit 3 family inet address 192.168.2.2/24
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 routing-options static route 0.0.0.0/0 qualified-next-hop 192.168.2.1
set routing-options static route 0.0.0.0/0 qualified-next-hop 172.16.1.1
set routing-options static route 0.0.0.0/0 bfd-liveness-detection minimum-interval 60

```

**Step-by-Step Procedure** The following example requires that you 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*.

To configure a static route with two possible next hops, both with BFD enabled:

1. On Device B, configure the interfaces.

```
[edit interfaces fe-0/1/0]
user@B# set unit 2 description secondary-B->D
user@B# set unit 2 family inet address 192.168.2.1/24
```

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

2. On Device B, configure the static route with two next hops, both with BFD enabled.

```
[edit routing-options static route 192.168.47.0/24]
user@B# set qualified-next-hop 192.168.2.2 bfd-liveness-detection minimum-interval
60
user@B# set qualified-next-hop 172.16.1.2 bfd-liveness-detection minimum-interval
60
```

3. On Device D, configure the interfaces.

```
[edit interfaces fe-0/1/0]
user@D# set unit 3 description secondary-D->B
user@D# set unit 3 family inet address 192.168.2.2/24
```

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

4. On Device D, configure a BFD-enabled default static route with two next hops to the provider network.

In this case, BFD is enabled on the route, not on the next hops.

```
[edit routing-options static route 0.0.0.0/0]
user@D# set qualified-next-hop 192.168.2.1
user@D# set qualified-next-hop 172.16.1.1
user@D# set bfd-liveness-detection minimum-interval 60
```

**Results** Confirm your configuration by issuing 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.

```
user@B# show interfaces
fe-0/1/0 {
 unit 2 {
 description secondary-B->D;
 family inet {
 address 192.168.2.1/24;
 }
 }
}
```



```

ge-1/2/0 {
 unit 0 {
 description B->D;
 family inet {
 address 172.16.1.1/24;
 }
 }
}

user@B# show routing-options
static {
 route 192.168.47.0/24 {
 qualified-next-hop 192.168.2.2 {
 bfd-liveness-detection {
 minimum-interval 60;
 }
 }
 qualified-next-hop 172.16.1.2 {
 bfd-liveness-detection {
 minimum-interval 60;
 }
 }
 }
}

user@D# show interfaces
fe-0/1/0 {
 unit 3 {
 description secondary-D->B;
 family inet {
 address 192.168.2.2/24;
 }
 }
}
ge-1/2/0 {
 unit 1 {
 description D->B;
 family inet {
 address 172.16.1.2/24;
 }
 }
}

user@D# show routing-options
static {
 route 0.0.0.0/0 {
 qualified-next-hop 192.168.2.1;
 qualified-next-hop 172.16.1.1;
 bfd-liveness-detection {
 minimum-interval 60;
 }
 }
}

```

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

## Verification

Confirm that the configuration is working properly.

- [Checking the Routing Tables on page 20](#)
- [Verifying the BFD Sessions on page 20](#)
- [Removing BFD from Device D on page 20](#)
- [Removing BFD from One Next Hop on page 21](#)

### Checking the Routing Tables

**Purpose** Make sure that the static route appears in the routing table on Device B with two possible next hops.

**Action** user@B> show route 192.168.47.0 extensive  
 inet.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)  
 192.168.47.0/24 (1 entry, 1 announced)  
 TSI:  
 KRT in-kernel 192.168.47.0/24 -> {192.168.2.2}  
     \*Static Preference: 5  
         Next hop type: Router  
         Address: 0x9334010  
         Next-hop reference count: 1  
         Next hop: 172.16.1.2 via ge-1/2/0.0  
         Next hop: 192.168.2.2 via fe-0/1/0.2, selected  
         State: <Active Int Ext>  
         Age: 9  
         Task: RT  
         Announcement bits (1): 3-KRT  
         AS path: I

**Meaning** Both next hops are listed. The next hop 192.168.2.2 is the selected route.

### Verifying the BFD Sessions

**Purpose** Make sure that the BFD sessions are up.

**Action** user@B> show bfd session

| Address     | State | Interface  | Detect Time | Transmit Interval | Multiplier |
|-------------|-------|------------|-------------|-------------------|------------|
| 172.16.1.2  | Up    | ge-1/2/0.0 | 0.720       | 0.240             | 3          |
| 192.168.2.2 | Up    | fe-0/1/0.2 | 0.720       | 0.240             | 3          |

2 sessions, 2 clients  
 Cumulative transmit rate 8.3 pps, cumulative receive rate 8.3 pps

**Meaning** The output shows that the BFD sessions are up.

### Removing BFD from Device D

**Purpose** Demonstrate what happens when the BFD session is down for both next hops.

- Action** 1. Deactivate BFD on Device D.

```
[edit routing-options static route 0.0.0.0/0]
user@D# deactivate bfd-liveness-detection
user@D# commit
```

2. Rerun the **show bfd session** command on Device B.

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

| Address     | State | Interface  | Detect Time | Transmit Interval | Multiplier |
|-------------|-------|------------|-------------|-------------------|------------|
| 172.16.1.2  | Down  | ge-1/2/0.0 | 3.000       | 1.000             | 3          |
| 192.168.2.2 | Down  | fe-0/1/0.2 | 3.000       | 1.000             | 3          |

```
2 sessions, 2 clients
```

```
Cumulative transmit rate 2.0 pps, cumulative receive rate 2.0 pps
```

3. Rerun the **show route 192.168.47.0** command on Device B.

```
user@B> show route 192.168.47.0
```

**Meaning** As expected, when the BFD sessions are down, the static route is removed from the routing table.

### *Removing BFD from One Next Hop*

**Purpose** Demonstrate what happens when only one next hop has BFD enabled.

- Action** 1. If it is not already deactivated, deactivate BFD on Device D.

```
[edit routing-options static route 0.0.0.0/0]
user@D# deactivate bfd-liveness-detection
user@D# commit
```

2. Deactivate BFD on one of the next hops on Device B.

```
[edit routing-options static route 192.168.47.0/24 qualified-next-hop 172.16.1.2]
user@B# deactivate bfd-liveness-detection
user@B# commit
```

3. Rerun the **show bfd session** command on Device B.

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

| Address     | State | Interface  | Detect Time | Transmit Interval | Multiplier |
|-------------|-------|------------|-------------|-------------------|------------|
| 192.168.2.2 | Down  | fe-0/1/0.2 | 3.000       | 1.000             | 3          |

4. Rerun the **show route 192.168.47.0 extensive** command on Device B.

```
user@B> show route 192.168.47.0 extensive
```

```
inet.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)
```

```
192.168.47.0/24 (1 entry, 1 announced)
```

```
TSI:
```

```
KRT in-kernel 192.168.47.0/24 -> {172.16.1.2}
```

```
*Static Preference: 5
```

```
Next hop type: Router, Next hop index: 624
```

```
Address: 0x92f0178
```

```
Next-hop reference count: 3
```

```
Next hop: 172.16.1.2 via ge-1/2/0.0, selected
State: <Active Int Ext>
Age: 2:36
Task: RT
Announcement bits (1): 3-KRT
AS path: I
```

**Meaning** As expected, the BFD session is down for the 192.168.2.2 next hop. The 172.16.1.2 next hop remains in the routing table, and the route remains active, because BFD is not a condition for this next hop to remain valid.

- Related Documentation**
- [Example: Configuring BFD Authentication for Static Routes on page 22](#)
  - [Example: Configuring BFD for OSPF](#)
  - [Example: Configuring BFD for BGP](#)
  - [Example: Configuring BFD for IS-IS](#)
  - [Configuring PIM and the Bidirectional Forwarding Detection \(BFD\) Protocol](#)

---

## Example: Configuring BFD Authentication for Static Routes

- [Understanding BFD Authentication for Static Route Security on page 22](#)
- [Example: Configuring BFD Authentication for Securing Static Routes on page 24](#)

### Understanding BFD Authentication for Static Route Security

Bidirectional Forwarding Detection (BFD) enables rapid detection of communication failures between adjacent systems. By default, authentication for BFD sessions is disabled. However, when you run BFD over Network Layer protocols, the risk of service attacks can be significant.



**NOTE:** We strongly recommend using authentication if you are running BFD over multiple hops or through insecure tunnels.

Beginning with Junos OS Release 9.6, Junos OS supports authentication for BFD sessions running over IPv4 and IPv6 static routes. BFD authentication is not supported on MPLS OAM sessions. BFD authentication is only supported in the Canada and United States version of the Junos OS image and is not available in the export version.



**NOTE:** EX3300 supports BFD over static routes only.

You authenticate BFD sessions by specifying an authentication algorithm and keychain, and then associating that configuration information with a security authentication keychain using the keychain name.

The following sections describe the supported authentication algorithms, security keychains, and level of authentication that can be configured:

- [BFD Authentication Algorithms on page 23](#)
- [Security Authentication Keychains on page 24](#)
- [Strict Versus Loose Authentication on page 24](#)

### BFD Authentication Algorithms

---

Junos OS supports the following algorithms for BFD authentication:

- **simple-password**—Plain-text password. One to 16 bytes of plain text are used to authenticate the BFD session. One or more passwords can be configured. This method is the least secure and should be used only when BFD sessions are not subject to packet interception.
- **keyed-md5**—Keyed Message Digest 5 hash algorithm for sessions with transmit and receive intervals greater than 100 ms. To authenticate the BFD session, keyed MD5 uses one or more secret keys (generated by the algorithm) and a sequence number that is updated periodically. With this method, packets are accepted at the receiving end of the session if one of the keys matches and the sequence number is greater than or equal to the last sequence number received. Although more secure than a simple password, this method is vulnerable to replay attacks. Increasing the rate at which the sequence number is updated can reduce this risk.
- **meticulous-keyed-md5**—Meticulous keyed Message Digest 5 hash algorithm. This method works in the same manner as keyed MD5, but the sequence number is updated with every packet. Although more secure than keyed MD5 and simple passwords, this method might take additional time to authenticate the session.
- **keyed-sha-1**—Keyed Secure Hash Algorithm I for sessions with transmit and receive intervals greater than 100 ms. To authenticate the BFD session, keyed SHA uses one or more secret keys (generated by the algorithm) and a sequence number that is updated periodically. The key is not carried within the packets. With this method, packets are accepted at the receiving end of the session if one of the keys matches and the sequence number is greater than the last sequence number received.
- **meticulous-keyed-sha-1**—Meticulous keyed Secure Hash Algorithm I. This method works in the same manner as keyed SHA, but the sequence number is updated with every packet. Although more secure than keyed SHA and simple passwords, this method might take additional time to authenticate the session.



**NOTE:** Nonstop active routing (NSR) is not supported with meticulous-keyed-md5 and meticulous-keyed-sha-1 authentication algorithms. BFD sessions using these algorithms might go down after a switchover.

---

## Security Authentication Keychains

---

The security authentication keychain defines the authentication attributes used for authentication key updates. When the security authentication keychain is configured and associated with a protocol through the keychain name, authentication key updates can occur without interrupting routing and signaling protocols.

The authentication keychain contains one or more keychains. Each keychain contains one or more keys. Each key holds the secret data and the time at which the key becomes valid. The algorithm and keychain must be configured on both ends of the BFD session, and they must match. Any mismatch in configuration prevents the BFD session from being created.

BFD allows multiple clients per session, and each client can have its own keychain and algorithm defined. To avoid confusion, we recommend specifying only one security authentication keychain.

## Strict Versus Loose Authentication

---

By default, strict authentication is enabled, and authentication is checked at both ends of each BFD session. Optionally, to smooth migration from nonauthenticated sessions to authenticated sessions, you can configure *loose checking*. When loose checking is configured, packets are accepted without authentication being checked at each end of the session. This feature is intended for transitional periods only.

## Example: Configuring BFD Authentication for Securing Static Routes

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

- [Requirements on page 24](#)
- [Overview on page 24](#)
- [Configuration on page 25](#)
- [Verification on page 28](#)

## Requirements

---

Junos OS Release 9.6 or later (Canda and United States version).

BFD authentication is only supported in the Canada and United States version of the Junos OS image and is not available in the export version.

## Overview

---

You can configure authentication for BFD sessions running over IPv4 and IPv6 static routes. Routing instances and logical systems are also supported.

The following steps are needed to configure authentication on a BFD session:

1. Specify the BFD authentication algorithm for the static route.
2. Associate the authentication keychain with the static route.

3. Configure the related security authentication keychain. This must be configured on the main router.

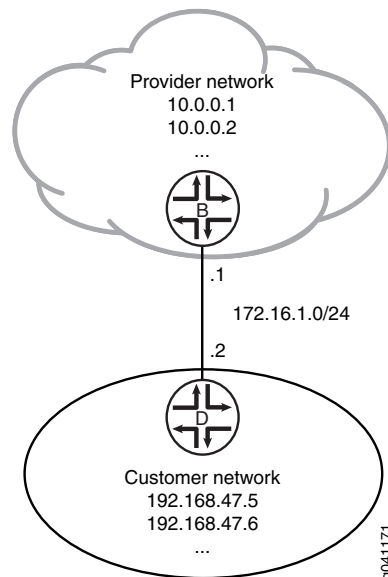


**TIP:** We recommend that you specify loose authentication checking if you are transitioning from nonauthenticated sessions to authenticated sessions.

```
[edit]
user@host> set routing-options static route ipv4 bfd-liveness-detection
authentication loose-check
```

Figure 3 on page 25 shows the sample network.

**Figure 3: Customer Routes Connected to a Service Provider**



### 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, 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 authentication
key-chain bfd-kc4
set routing-options static route 192.168.47.0/24 bfd-liveness-detection authentication
algorithm keyed-sha-1
```

```
set security authentication-key-chains key-chain bfd-kc4 key 5 secret
"$ABC123$ABC123$ABC123"
set security authentication-key-chains key-chain bfd-kc4 key 5 start-time
"2011-1-1.12:00:00 -0800"
```

**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 routing-options static route 0.0.0.0/0 bfd-liveness-detection authentication key-chain
bfd-kc4
set routing-options static route 0.0.0.0/0 bfd-liveness-detection authentication algorithm
keyed-sha-1
set security authentication-key-chains key-chain bfd-kc4 key 5 secret
"$ABC123$ABC123$ABC123"
set security authentication-key-chains key-chain bfd-kc4 key 5 start-time
"2011-1-1.12:00:00 -0800"
```

**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 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
```

4. On Device B, specify the algorithm (**keyed-md5**, **keyed-sha-1**, **meticulous-keyed-md5**, **meticulous-keyed-sha-1**, or **simple-password**) to use for BFD authentication on the static route.

```
[edit routing-options]
user@B# set static route 192.168.47.0/24 bfd-liveness-detection authentication
algorithm keyed-sha-1
```





**NOTE:** Nonstop active routing (NSR) is not supported with the meticulous-keyed-md5 and meticulous-keyed-sha-1 authentication algorithms. BFD sessions using these algorithms might go down after a switchover.

5. On Device B, specify the keychain to be used to associate BFD sessions on the specified route with the unique security authentication keychain attributes.

This should match the keychain name configured at the **[edit security authentication key-chains]** hierarchy level.

```
[edit routing-options]
user@B# set static route 192.168.47.0/24 bfd-liveness-detection authentication
key-chain bfd-kc4
```

6. On Device B, specify the unique security authentication information for BFD sessions:

- The matching keychain name as specified in Step 5.
- At least one key, a unique integer between 0 and 63. Creating multiple keys allows multiple clients to use the BFD session.
- The secret data used to allow access to the session.
- The time at which the authentication key becomes active, in the format *yyyy-mm-dd.hh:mm:ss*.

```
[edit security authentication-key-chains key-chain bfd-kc4]
user@B# set key 5 secret "$ABC123$ABC123$ABC123"
user@B# set key 5 start-time "2011-1-1.12:00:00 -0800"
```

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

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

8. Repeat the configuration on Device D.

The algorithm and keychain must be configured on both ends of the BFD session, and they must match. Any mismatch in configuration prevents the BFD session from being created.

### Results

Confirm your configuration by issuing the **show interfaces**, **show routing-options**, and **show security** 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@B# show routing-options
static {
 route 192.168.47.0/24 {
 next-hop 172.16.1.2;
 bfd-liveness-detection {
 minimum-interval 1000;
 authentication {
 key-chain bfd-kc4;
 algorithm keyed-sha-1;
 }
 }
 }
}

user@B# show security
authentication-key-chains {
 key-chain bfd-kc4 {
 key 5 {
 secret "$ABC123$ABC123$ABC123"; ## SECRET-DATA
 start-time "2011-1-1.12:00:00 -0800";
 }
 }
}

```

## Verification

Confirm that the configuration is working properly.

- [Verifying That BFD Sessions Are Up on page 28](#)
- [Viewing Details About the BFD Session on page 29](#)
- [Viewing Extensive BFD Session Information on page 29](#)

### *Verifying That BFD Sessions Are Up*

**Purpose** Verify that the BFD sessions are up.

**Action** From operational mode, enter the **show bfd session** command.

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

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

1 sessions, 1 clients

Cumulative transmit rate 1.0 pps, cumulative receive rate 1.0 pps

**Meaning** The command output shows that the BFD session is up.

#### *Viewing Details About the BFD Session*

**Purpose** View details about the BFD sessions and make sure that authentication is configured.

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

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

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

Client Static, TX interval 1.000, RX interval 1.000, **Authenticate**  
 Session up time 00:53:58  
 Local diagnostic NbrSignal, remote diagnostic None  
 Remote state Up, version 1  
 Logical system 9, routing table index 22

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

**Meaning** In the command output, **Authenticate** is displayed to indicate that BFD authentication is configured.

#### *Viewing Extensive BFD Session Information*

**Purpose** View more detailed information about the BFD sessions.

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

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

| Address    | State | Interface  | Time  | Interval | Multiplier |
|------------|-------|------------|-------|----------|------------|
| 172.16.1.2 | Up    | ge-1/2/0.0 | 3.000 | 1.000    | 3          |

Client Static, TX interval 1.000, RX interval 1.000, **Authenticate**  
 keychain bfd-kc4, algo keyed-sha-1, mode strict  
 Session up time 01:39:45  
 Local diagnostic NbrSignal, remote diagnostic None  
 Remote state Up, version 1  
 Logical system 9, routing table index 22  
 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 3, remote discriminator 4  
 Echo mode disabled/inactive  
 Authentication enabled/active, keychain bfd-kc4, algo keyed-sha-1, mode strict

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

**Meaning** In the command output, **Authenticate** is displayed to indicate that BFD authentication is configured. The output for the **extensive** command provides the keychain name, the authentication algorithm, and the mode for each client in the session.

- Related Documentation**
- [Examples: Configuring BFD for Static Routes on page 7](#)

## PART 3

# Troubleshooting

- [Configuration Statements and Operational Commands on page 33](#)



## CHAPTER 3

# Configuration Statements and Operational Commands

- [Configuration Statements on page 33](#)
- [Operational Commands on page 50](#)

## Configuration Statements

---

- [\[edit routing-options\] Hierarchy Level on page 33](#)
- [bfd on page 45](#)
- [bfd-liveness-detection \(Routing Options Static Route\) on page 47](#)

## [edit routing-options] Hierarchy Level

Several statements in the **[edit routing-options]** hierarchy are valid at numerous locations within the hierarchy. To make the complete hierarchy easier to read, the repeated statements are listed in “[Common Routing Options](#)” on page 33 and that section is referenced at the appropriate locations in “[Complete \[edit routing-options\] Hierarchy](#)” on page 35.

- [Common Routing Options on page 33](#)
- [Complete \[edit routing-options\] Hierarchy on page 35](#)

## Common Routing Options

---

This section lists statements that are valid at the following hierarchy levels, and is referenced at those levels in “[Complete \[edit routing-options\] Hierarchy](#)” on page 35 instead of the statements being repeated.

- **[edit routing-options aggregate defaults]**
- **[edit routing-options aggregate route *ip-prefix* </prefix-length>]**
- **[edit routing-options generate defaults]**
- **[edit routing-options generate route *ip-prefix* </prefix-length>]**
- **[edit routing-options static defaults]**
- **[edit routing-options static route *ip-prefix* </prefix-length>]**

The common routing options are as follows:

```
(active | passive);
as-path {
 aggregator as-number address;
 atomic-aggregate;
 origin (egp | igp | incomplete);
 path path-identifier;
}
color metric <type metric-type>;
color2 metric <type metric-type>;
community [community-id no-advertise no-export no-export-subconfed];
metric metric <type metric-type>;
metric2 metric <type metric-type>;
metric3 metric <type metric-type>;
metric4 metric <type metric-type>;
passive;
preference preference-value <type metric-type>;
preference2 preference-value <type metric-type>;
tag metric <type metric-type>;
tag2 metric <type metric-type>;
```



### Complete [edit routing-options] Hierarchy

The statement hierarchy in this section can also be included at the [edit logical-systems *logical-system-name*] hierarchy level.

```

routing-options {
 access {
 route ip-prefix</prefix-length> {
 metric metric;
 next-hop [addresses];
 preference preference-value;
 qualified-next-hop address;
 tag route-tag;
 }
 }
 access-internal {
 route ip-prefix</prefix-length> {
 next-hop [addresses];
 qualified-next-hop address;
 tag route-tag;
 }
 }
 tag route-tag;
}
aggregate {
 defaults {
 ... statements in Common Routing Options on page 33 PLUS ...
 (brief | full);
 discard;
 }
 route ip-prefix</prefix-length> {
 ... statements in Common Routing Options on page 33 PLUS ...
 (brief | full);
 discard;
 policy [policy-names];
 }
}
auto-export {
 disable;
 family inet {
 disable;
 flow {
 disable;
 rib-group rib-group;
 }
 multicast {
 disable;
 rib-group rib-group;
 }
 unicast {
 disable;
 rib-group rib-group;
 }
 }
 family inet6 {

```

```

 disable;
 multicast {
 disable;
 rib-group rib-group;
 }
 unicast {
 disable;
 rib-group rib-group;
 }
 }
 family iso {
 disable;
 unicast {
 disable;
 rib-group rib-group;
 }
 }
 traceoptions {
 file filename <files number> <size maximum-file-size> <world-readable |
 no-world-readable>;
 flag flag <flag-modifier> <disable>;
 }
}
autonomous-system autonomous-system <asdot-notation> <loops number>;
backup-selection (Protocols ISIS){
 destination prefix {
 interface (interface-name| all){
 admin-group {
 exclude [group-name];
 include-all [group-name];
 include-any [group-name];
 preference [group-name];
 }
 bandwidth-greater-equal-primary;
 dest-metric (highest | lowest);
 downstream-paths-only;
 metric-order [root dest];
 node {
 exclude [neighbor-address];
 preference [neighbor-address];
 }
 node-tag {
 exclude [route-tag];
 preference [route-tag];
 }
 protection-type (link | node | node-link);
 root-metric (highest | lowest);
 srlg (loose | strict);
 evaluation-order [admin-group srlg bandwidth protection-type neighbor neighbor-tag
 metric];
 }
 }
}
bgp-orf-cisco-mode;
bmp {
 authentication-algorithm (aes-128-cmac-96 | hmac-sha-1-96 | md5);

```

```

authentication-key key;
authentication-key-chain authentication-key-chain;
connection-mode (active | passive);
hold-down {
 seconds;
 flaps flaps;
 period seconds;
}
initiation-message text;
local-address address;
local-port port;
monitor (disable | enable);
priority (high | low | medium);
route-monitoring {
 none;
 post-policy {
 exclude-non-eligible;
 }
 pre-policy {
 exclude-non-feasible;
 }
}
}
station station-name {
 authentication-algorithm (aes-128-cmac-96 | hmac-sha-1-96 | md5);
 authentication-key key;
 authentication-key-chain authentication-key-chain;
 connection-mode (active | passive);
 hold-down {
 seconds;
 flaps flaps;
 period seconds;
 }
 initiation-message text;
 local-address address;
 local-port port;
 monitor (disable | enable);
 priority (high | low | medium);
 route-monitoring {
 none;
 post-policy {
 exclude-non-eligible;
 }
 pre-policy {
 exclude-non-feasible;
 }
 }
}
station-address (ip-address | name);
station-port port-number;
statistics-timeout seconds;
traceoptions {
 file filename <files number> <size size> <world-readable | no-world-readable>;
 flag flag <flag-modifier>;
}
}
station-address (ip-address | name);
station-port port-number;

```

```

statistics-timeout seconds;
traceoptions {
 file filename <files number> <size size> <world-readable | no-world-readable>;
 flag flag <flag-modifier>;
}
}
confederation as-number members [as-numbers];
dynamic-tunnels tunnel-name {
 destination-networks prefix;
 gre;
 rsvp-te entry-name {
 destination-networks network-prefix;
 label-switched-path-template (Multicast) {
 default-template;
 template-name;
 }
 }
 source-address address;
}
fate-sharing {
 group group-name {
 cost value;
 from {
 address <to address>;
 }
 }
}
flow {
 route name {
 match {
 destination address;
 destination-port [afs bgp biff bootpc bootps cmd cvspserver dhcp domain eklogin
 ekshell exec finger ftp ftp-data http https ident imap kerberos-sec klogin kpasswd
 krb-prop krbupdate kshell ldap ldp login mobileip-agent mobilip-mn msdp
 netbios-dgm netbios-ns netbios-ssn nfsd nntp ntalk ntp pop3 pptp printer radacct
 radius rip rkinit smtp snmp snmptrap snpp socks ssh sunrpc syslog tacacs tacacs-ds
 talk telnet tftp timed who xdmcp];
 dscp [code-points];
 fragment [don't-fragment first-fragment is-fragment last-fragment
 not-a-fragment];
 icmp-code [communication-prohibited-by-filtering destination-host-prohibited
 destination-host-unknown fragmentation-needed host-precedence-violation
 host-unreachable host-unreachable-for-tos ip-header-bad network-unreachable
 network-unreachable-for-tos port-unreachable precedence-cutoff-in-effect
 protocol-unreachable redirect-for-host redirect-for-network
 redirect-for-tos-and-host redirect-for-tos-and-net required-option-missing
 source-host-isolated source-route-failed ttl-eq-zero-during-reassembly
 ttl-eq-zero-during-transit];
 icmp-type [echo-reply echo-request info-reply info-request mask-reply mask-request
 parameter-problem redirect router-advertisement router-solicit source-quench
 time-exceeded timestamp timestamp-reply unreachable];
 packet-length [values];
 port [... same values as for the preceding destination-port statement ...];
 protocol [ah esp gre icmp igmp ipip ospf pim rsvp sctp tcp udp];
 source address;
 source-port [... same values as for the preceding destination-port statement ...];
 }
 }
}

```

```

 tcp-flags [ack fin push rst syn urgent];
 }
 then {
 (accept | discard);
 community community-name;
 next-term;
 rate-limit value;
 routing-instance routing-instance-name;
 sample;
 }
}
validation {
 traceoptions {
 file filename <files number> <size maximum-file-size> <world-readable |
 no-world-readable>;
 flag flag <flag-modifier> <disable>;
 }
}
}
forwarding-table {
 chained-composite-next-hop {
 ingress {
 l3vpn {
 extended-space;
 }
 }
 }
}
export [policy-name];
(indirect-next-hop | no-indirect-next-hop);
(indirect-next-hop-change-acknowledgements |
 no-indirect-next-hop-change-acknowledgements);
krt-nexthop-ack-timeout interval;
unicast-reverse-path (active-paths | feasible-paths);
}
generate {
 defaults {
 ... statements in Common Routing Options on page 33 PLUS ...
 (brief | full);
 discard;
 }
 route ip-prefix </prefix-length> {
 ... statements in Common Routing Options on page 33 PLUS ...
 (brief | full);
 discard;
 policy [policy-names];
 }
}
graceful-restart {
 disable;
 restart-duration seconds;
}
host-fast-reroute {
 global-arp-prefix-limit number;
 global-supplementary-blackout-timer minutes;
}
instance-export [policy-names];

```

```

instance-import [policy-names];
interface interface-name { # In the routing-instance only
 arp-prefix-limit number;
 link-protection;
 supplementary-blackout-timer minutes;
}
interface-routes {
 family (inet | inet6) {
 export {
 lan;
 point-to-point;
 }
 import [policy-names];
 }
}
rib-group {
 inet group-name;
 inet6 group-name;
}
}
logical-system-mux {
 traceoptions {
 file {
 <file name>;
 files;
 no-world-readable;
 size;
 world-readable;
 }
 flag {
 all;
 debug;
 general;
 normal;
 parse;
 policy;
 route;
 state;
 task;
 timer;
 }
 }
}
martians {
 ip-prefix</prefix-length> (exact | longer | orlonger |
 prefix-length-range /minimum-prefix-length–/maximum-prefix-length |
 through ip-prefix</prefix-length> | upto /prefix-length) <allow>;
}
maximum-paths path-limit <log-only | threshold value> <log-interval seconds>;
maximum-prefixes prefix-limit <log-only | threshold value> <log-interval seconds>;
med-igp-update-interval minutes;
multicast {
 ... the multicast subhierarchy appears after the main [edit routing-options] hierarchy ...
}
no-bfd-triggered-local-repair;
nonstop-routing;
options {

```

```

 mark seconds;
 syslog {
 level level;
 upto level;
 }
}
ppm {
 no-delegate-processing;
}
resolution {
 rib routing-table-name {
 import [policy-names];
 resolution-ribs [routing-table-names];
 }
 tracefilter [filter-policy-names];
 traceoptions {
 file filename <files number> <size maximum-file-size> <world-readable |
 no-world-readable>;
 flag flag <flag-modifier> <disable>;
 }
}
rib routing-table-name {
 access {
 ... same statements as at the [edit routing-options access] hierarchy level ...
 }
 access-internal {
 ... same statements as at the [edit routing-options access-internal] hierarchy level ...
 }
 aggregate {
 ... same statements as at the [edit routing-options aggregate] hierarchy level ...
 }
 generate {
 ... same statements as at the [edit routing-options generate] hierarchy level ...
 }
 martians {
 ip-prefix </prefix-length> (exact | longer | orlonger |
 prefix-length-range /minimum-prefix-length–/maximum-prefix-length |
 through ip-prefix </prefix-length> | upto /prefix-length) <allow>;
 }
 maximum-paths path-limit <log-only | threshold value> <log-interval seconds>;
 maximum-prefixes prefix-limit <log-only | threshold value> <log-interval seconds>;
 static {
 ... same statements as at the [edit routing-options static] hierarchy level ...
 }
}
rib-groups {
 group-name {
 export-rib table-name;
 import-policy [policy-names];
 import-rib [table-names];
 }
}
route-distinguisher-id address;
route-record;
router-id address;
source-routing {

```

```

 ip;
 ipv6;
}
static {
 ... the static subhierarchy appears after the main [edit routing-options] hierarchy ...
}
topologies {
 family (inet | inet6) {
 topology topology-name;
 }
}
traceoptions {
 file filename <files number> <size maximum-file-size> <world-readable |
 no-world-readable>;
 flag flag <disable>;
}
validation {
 group group-name {
 max-sessions number;
 session address {
 hold-time seconds;
 local-address local-ip-address;
 port port-number;
 preference number;
 record-lifetime seconds;
 refresh-time seconds;
 }
 }
}
static {
 record destination {
 maximum-length prefix-length {
 origin-autonomous-system as-number {
 validation-state (invalid | valid);
 }
 }
 }
}
}
traceoptions {
 file filename <files number> <size size> <world-readable | no-world-readable>;
 flag flag;
}
}
}

routing-options {
 multicast {
 asm-override-ssm;
 backup-pe-group group-name {
 backups [addresses];
 local-address address;
 }
 flow-map flow-map-name {
 bandwidth <bps> <adaptive>;
 forwarding-cache {
 timeout (never <non-discard-entry-only> | minutes);
 }
 }
 }
}

```



```

 policy [policy-names];
 redundant-sources [addresses];
}
forwarding-cache {
 allow-maximum;
 family (inet | inet6) {
 threshold {
 log-warning value;
 suppress value <reuse value>;
 }
 timeout minutes;
 }
}
interface interface-name {
 maximum-bandwidth bps;
 no-qos-adjust;
 reverse-oif-mapping {
 no-qos-adjust;
 }
 subscriber-leave-timer seconds;
}
pim-to-igmp-proxy {
 upstream-interface [interface-names];
}
pim-to-mld-proxy {
 upstream-interface [interface-names];
}
rpf-check-policy [policy-names];
scope scope-name {
 interface [interface-names];
 prefix ip-prefix </prefix-length>;
}
scope-policy [policy-names];
ssm-groups [ip-prefix </prefix-length>];
ssm-map ssm-map-name {
 policy [policy-names];
 source [addresses];
}
traceoptions {
 file filename <files number> <size maximum-file-size> <world-readable |
 no-world-readable>;
 flag flag <disable>;
}
}
}

routing-options {
 static {
 defaults {
 ... statements in Common Routing Options on page 33 PLUS ...
 (install | no-install);
 (readvertise | no-readvertise);
 (resolve | no-resolve);
 (retain | no-retain);
 }
 rib-group group-name;
 }
}

```

```

route destination-prefix {
 ... statements in Common Routing Options on page 33 PLUS ...
 backup-pe-group group-name;
 bfd-liveness-detection {
 detection-time {
 threshold milliseconds;
 }
 holddown-interval milliseconds;
 local-address ip-address;
 minimum-interval milliseconds;
 minimum-receive-interval milliseconds;
 minimum-receive-ttl milliseconds;
 multiplier number;
 neighbor address;
 no-adaptation;
 transmit-interval {
 minimum-interval milliseconds;
 threshold milliseconds;
 }
 version (1 | automatic);
 }
 (discard | next-hop [addresses] | next-table address | receive | reject);
 (install | no-install);
 lsp-next-hop {
 metric metric;
 preference preference;
 }
 p2mp-lsp-next-hop lsp-name {
 metric metric;
 preference preference;
 }
 p2mp-ldp-next-hop {
 root-address root-address;
 lsp-id id;
 }
 (readvertise | no-readvertise);
 (resolve | no-resolve);
 (retain | no-retain);
 static-lsp-next-hop lsp-name {
 metric metric;
 preference preference-value;
 }
}
}
}

```

#### Related Documentation

- [Notational Conventions Used in Junos OS Configuration Hierarchies](#)

## bfd

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>              | <pre> bfd {   traceoptions {     file <i>filename</i> &lt;files <i>number</i>&gt; &lt;match <i>regular-expression</i>&gt; &lt;size <i>size</i>&gt; &lt;world-readable         no-world-readable&gt;;     flag <i>flag</i> &lt;<i>flag-modifier</i>&gt; &lt;disable&gt;;   } } </pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Hierarchy Level</b>     | <p>[edit logical-systems <i>logical-system-name</i> protocols],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols],</p> <p>[edit protocols],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols]</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Release Information</b> | Statement introduced before Junos OS Release 7.4.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Description</b>         | Configure trace options for Bidirectional Forwarding Protocol (BFD) traffic.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Default</b>             | If you do not include this statement, no BFD tracing operations are performed.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Options</b>             | <p><b>disable</b>—(Optional) Disable the BFD tracing operation. You can use this option to disable a single operation when you have defined a broad group of tracing operations, such as <b>all</b>.</p> <p><b>file <i>filename</i></b>—Name of the file to receive the output of the tracing operation. Enclose the name in quotation marks. All files are placed in the <b>/var/log</b> directory. We recommend that you place global routing protocol tracing output in the <b>routing-log</b> file.</p> <p><b>files <i>number</i></b>—(Optional) Maximum number of trace files. When a trace file named <b>trace-file</b> reaches its maximum size, it is renamed <b>trace-file.0</b>, then <b>trace-file.1</b>, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.</p> <p>If you specify a maximum number of files, you also must specify a maximum file size with the <b>size</b> option.</p> <p><b>Range:</b> 2 through 1000 files</p> <p><b>Default:</b> 2 files</p> <p><b>flag <i>flag</i></b>—Tracing operation to perform. To specify more than one tracing operation, include multiple <b>flag</b> statements. These are the BFD protocol tracing options:</p> <ul style="list-style-type: none"> <li>• <b>adjacency</b>—Trace adjacency messages.</li> <li>• <b>all</b>—Trace all options for BFD.</li> <li>• <b>error</b>—Trace all errors.</li> <li>• <b>event</b>—Trace all events.</li> <li>• <b>issu</b>—Trace in-service software upgrade (ISSU) packet activity.</li> </ul> |

- **nsr-packet**—Trace non-stop-routing (NSR) packet activity.
- **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 (PPM).
- **state**—Trace state transitions.
- **timer**—Trace timer processing.

**match *regular-expression***—(Optional) Regular expression for lines to be logged.

**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.

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.

|                                 |                                                                                                                         |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| <b>Required Privilege Level</b> | routing and trace—To view this statement in the configuration.                                                          |
|                                 | routing-control and trace-control—To add this statement to the configuration.                                           |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Example: Configuring BFD for Static Routes on page 11</a></li></ul> |

## bfd-liveness-detection (Routing Options Static Route)

**Syntax** `bfd-liveness-detection {`  
     `authentication {`  
         `algorithm` *algorithm-name*;  
         `key-chain` *key-chain-name*;  
         `loose-check`;  
     `}`  
     `detection-time {`  
         `threshold` *milliseconds*;  
     `}`  
     `holddown-interval` *milliseconds*;  
     `local-address` *ip-address*;  
     `minimum-interval` *milliseconds*;  
     `minimum-receive-interval` *milliseconds*;  
     `minimum-receive-ttl` *number*;  
     `multiplier` *number*;  
     `neighbor` *address*;  
     `no-adaptation`;  
     `transmit-interval {`  
         `minimum-interval` *milliseconds*;  
         `threshold` *milliseconds*;  
     `}`  
     `version` (1 | automatic);  
`}`

**Hierarchy Level** [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* routing-options rib *routing-table-name* static route *destination-prefix*],  
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* routing-options rib *routing-table-name* static route *destination-prefix* qualified-next-hop (*interface-name* | *address*)],  
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* routing-options static route *destination-prefix*],  
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* routing-options static route *destination-prefix* qualified-next-hop (*interface-name* | *address*)],  
 [edit logical-systems *logical-system-name* routing-options rib *routing-table-name* static route *destination-prefix*],  
 [edit logical-systems *logical-system-name* routing-options rib *routing-table-name* static route *destination-prefix* qualified-next-hop (*interface-name* | *address*)],  
 [edit logical-systems *logical-system-name* routing-options static route *destination-prefix*],  
 [edit logical-systems *logical-system-name* routing-options static route *destination-prefix* qualified-next-hop (*interface-name* | *address*)],  
 [edit routing-instances *routing-instance-name* routing-options rib *routing-table-name* static route *destination-prefix*],  
 [edit routing-instances *routing-instance-name* routing-options rib *routing-table-name* static route *destination-prefix* qualified-next-hop (*interface-name* | *address*)],  
 [edit routing-instances *routing-instance-name* routing-options static route *destination-prefix*],  
 [edit routing-instances *routing-instance-name* routing-options static route *destination-prefix* qualified-next-hop (*interface-name* | *address*)],  
 [edit routing-options rib *routing-table-name* static route *destination-prefix*],  
 [edit routing-options rib *routing-table-name* static route *destination-prefix* qualified-next-hop (*interface-name* | *address*)],  
 [edit routing-options static route *destination-prefix*],

[edit routing-options static route *destination-prefix* qualified-next-hop (*interface-name* | *address*)]

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Release Information</b> | <p>Statement introduced before Junos OS Release 7.4.</p> <p><b>detection-time threshold</b> and <b>transmit-interval threshold</b> options introduced in Junos OS Release 8.2.</p> <p><b>local-address</b> statement introduced in Junos OS Release 8.2.</p> <p><b>minimum-receive-ttl</b> statement introduced in Junos OS Release 8.2.</p> <p>Support for logical routers introduced in Junos OS Release 8.3.</p> <p><b>holddown-interval</b> statement introduced in Junos OS Release 8.5.</p> <p><b>no-adaptation</b> statement introduced in Junos OS Release 9.0.</p> <p>Support for IPv6 static routes introduced in Junos OS Release 9.1.</p> <p><b>authentication algorithm</b>, <b>authentication key-chain</b>, and <b>authentication loose-check</b> statements introduced in Junos OS Release 9.6.</p> <p>Statement introduced in Junos OS Release 12.1 for the QFX Series.</p> <p>Statement introduced in Junos OS Release 12.3 for ACX Series routers.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p> |
| <b>Description</b>         | <p>Configure bidirectional failure detection timers and authentication criteria for static routes.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

**Options** **authentication algorithm** *algorithm-name*—Configure the algorithm used to authenticate the specified BFD session: **simple-password**, **keyed-md5**, **keyed-sha-1**, **meticulous-keyed-md5**, or **meticulous-keyed-sha-1**.

**authentication key-chain** *key-chain-name*—Associate a security key with the specified BFD session using the name of the security keychain. 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.

**authentication loose-check**—(Optional) Configure loose authentication checking on the BFD session. Use only for transitional periods when authentication may not be configured at both ends of the BFD session.

**detection-time threshold** *milliseconds*—Configure a 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.

**holddown-interval** *milliseconds*—Configure an interval specifying how long a BFD session must remain 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** *ip-address*—Enable a multihop BFD session and configure the source address for the BFD session.

**minimum-interval** *milliseconds*—Configure the minimum interval after which the local routing device transmits a hello packet and then expects to receive a reply from the neighbor with which it has established a BFD session. 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.

**Range:** 1 through 255,000

**minimum-receive-interval** *milliseconds*—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. 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.

**Range:** 1 through 255,000

**minimum-receive-ttl** *number*—Configure the time to live (TTL) for the multihop BFD session.

**Range:** 1 through 255

**Default:** 255

**multiplier** *number*—Configure number of hello packets not received by the neighbor that causes the originating interface to be declared down.

**Range:** 1 through 255

**Default:** 3

**neighbor address**—Configure a next-hop address for the BFD session for a next hop specified as an interface name.

**no-adaptation**—Specify for BFD sessions not to 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.

**transmit-interval threshold *milliseconds***—Configure 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. The interval threshold must be greater than the minimum transmit interval.

**Range:** 0 through 4,294,967,295

**transmit-interval minimum-interval *milliseconds***—Configure the minimum interval at which the routing device transmits hello packets to a neighbor with which it has established a BFD session. 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.

**Range:** 1 through 255,000

**version**—Configure the BFD version to detect: **1** (BFD version 1) or **automatic** (autodetect the BFD version).

**Default:** automatic

|                                 |                                                             |
|---------------------------------|-------------------------------------------------------------|
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.        |
|                                 | routing-control—To add this statement to the configuration. |

|                              |                                                                                                                                                                                                                                 |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Related Documentation</b> | <ul style="list-style-type: none"><li>• <a href="#">Example: Configuring BFD for Static Routes on page 11</a></li><li>• <a href="#">Example: Configuring BFD Authentication for Securing Static Routes on page 24</a></li></ul> |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

## Operational Commands

- [Operational-Mode Commands on page 50](#)

### Operational-Mode Commands

- [Overview of Junos OS CLI Operational Mode Commands on page 50](#)
- [Example: Running Operational Mode Commands on Logical Systems on page 53](#)
- [Example: Viewing BGP Trace Files on Logical Systems on page 55](#)
- [Example: Configuring System Logging on Logical Systems on page 60](#)

---

#### Overview of Junos OS CLI Operational Mode Commands

This topic provides an overview of Junos OS CLI operational mode commands and contains the following sections:

- [CLI Command Categories on page 51](#)
- [Commonly Used Operational Mode Commands on page 52](#)



### **CLI Command Categories**

When you log in to a device running Junos OS and the CLI starts, there are several broad groups of CLI commands:

- Commands for controlling the CLI environment—Some set commands in the **set** hierarchy configure the CLI display screen. For information about these commands, see *Understanding the Junos OS CLI Modes, Commands, and Statement Hierarchies*.
- Commands for monitoring and troubleshooting—The following commands display information and statistics about the software and test network connectivity. Detailed command descriptions are provided in the *Junos OS Interfaces Command Reference*.
  - **clear**—Clear statistics and protocol database information.
  - **mtrace**—Trace mtrace packets from source to receiver.
  - **monitor**—Perform real-time debugging of various software components, including the routing protocols and interfaces.
  - **ping**—Determine the reachability of a remote network host.
  - **show**—Display the current configuration and information about interfaces, routing protocols, routing tables, routing policy filters, system alarms, and the chassis.
  - **test**—Test the configuration and application of policy filters and autonomous system (AS) path regular expressions.
  - **traceroute**—Trace the route to a remote network host.
- Commands for connecting to other network systems—The **ssh** command opens Secure Shell connections, and the **telnet** command opens telnet sessions to other hosts on the network. For information about these commands, see the [CLI Explorer](#).
- Commands for copying files—The **copy** command copies files from one location on the router or switch to another, from the router or switch to a remote system, or from a remote system to the router or switch. For information about these commands, see the [CLI Explorer](#).
- Commands for restarting software processes—The commands in the **restart** hierarchy restart the various Junos OS processes, including the routing protocol, interface, and SNMP. For information about these commands, see the [CLI Explorer](#).
- A command—**request**—for performing system-level operations, including stopping and rebooting the router or switch and loading Junos OS images. For information about this command, see the [CLI Explorer](#).
- A command—**start**—to exit the CLI and start a UNIX shell. For information about this command, see the [CLI Explorer](#).
- A command—**configure**—for entering configuration mode, which provides a series of commands that configure Junos OS, including the routing protocols, interfaces, network management, and user access. For information about the CLI configuration commands, see *Understanding Junos OS CLI Configuration Mode*.

- A command—**quit**—to exit the CLI. For information about this command, see the [CLI Explorer](#).
- For more information about the CLI operational mode commands, see the [CLI Explorer](#).

### Commonly Used Operational Mode Commands

Table 3 on page 52 lists some operational commands you may find useful for monitoring router or switch operation. For a complete description of operational commands, see the Junos OS command references.



**NOTE:** The QFX3500 switch does not support the IS-IS, OSPF, BGP, MPLS, and RSVP protocols.

**Table 3: Commonly Used Operational Mode Commands**

| Items to Check               | Description                                             | Command                             |
|------------------------------|---------------------------------------------------------|-------------------------------------|
| Software version             | Versions of software running on the router or switch    | <b>show version</b>                 |
| Log files                    | Contents of the log files                               | <b>monitor</b>                      |
|                              | Log files and their contents and recent user logins     | <b>show log</b>                     |
| Remote systems               | Host reachability and network connectivity              | <b>ping</b>                         |
|                              | Route to a network system                               | <b>traceroute</b>                   |
| Configuration                | Current system configuration                            | <b>show configuration</b>           |
| Manipulate files             | List of files and directories on the router or switch   | <b>file list</b>                    |
|                              | Contents of a file                                      | <b>file show</b>                    |
| Interface information        | Detailed information about interfaces                   | <b>show interfaces</b>              |
| Chassis                      | Chassis alarm status                                    | <b>show chassis alarms</b>          |
|                              | Information currently on craft display                  | <b>show chassis craft-interface</b> |
|                              | Router or switch environment information                | <b>show chassis environment</b>     |
|                              | Hardware inventory                                      | <b>show chassis hardware</b>        |
| Routing table information    | Information about entries in the routing tables         | <b>show route</b>                   |
| Forwarding table information | Information about data in the kernel's forwarding table | <b>show route forwarding-table</b>  |

Table 3: Commonly Used Operational Mode Commands (*continued*)

| Items to Check | Description                                                                               | Command                               |
|----------------|-------------------------------------------------------------------------------------------|---------------------------------------|
| IS-IS          | Adjacent routers or switches                                                              | <b>show isis adjacency</b>            |
| OSPF           | Display standard information about OSPF neighbors                                         | <b>show ospf neighbor</b>             |
| BGP            | Display information about BGP neighbors                                                   | <b>show bgp neighbor</b>              |
| MPLS           | Status of interfaces on which MPLS is running                                             | <b>show mpls interface</b>            |
|                | Configured LSPs on the router or switch, as well as all ingress, transit, and egress LSPs | <b>show mpls lsp</b>                  |
|                | Routes that form a label-switched path                                                    | <b>show route label-switched-path</b> |
| RSVP           | Status of interfaces on which RSVP is running                                             | <b>show rsvp interface</b>            |
|                | Currently active RSVP sessions                                                            | <b>show rsvp session</b>              |
|                | RSVP packet and error counters                                                            | <b>show rsvp statistics</b>           |

#### Example: Running Operational Mode Commands on Logical Systems

This example shows how to set the CLI to a specified logical system view, run operational-mode commands for the logical system, and then return to the main router view.

- [Requirements on page 53](#)
- [Overview on page 54](#)
- [Configuration on page 54](#)

#### Requirements

You must have the **view** privilege for the logical system.

### Overview

For some operational-mode commands, you can include a **logical-system** option to narrow the output of the command or to limit the operation of the command to the specified logical system. For example, the **show route** command has a **logical-system** option. To run this command on a logical system called LS3, you can use **show route logical-system LS3**. However, some commands, such as **show interfaces**, do not have a **logical-system** option. For commands like this, you need another approach.

You can place yourself into the context of a specific logical system. To configure a logical system context, issue the **set cli logical-system logical-system-name** command.

When the CLI is in logical system context mode and you enter an operational-mode command, the output of the command displays information related to the logical system only.

### Configuration

**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 set the CLI to a specific logical system context:

1. From the main router, configure the logical system.

```
[edit]
user@host# set logical-systems LS3
```

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

```
[edit]
user@host# commit
user@host# exit
```

3. Set the CLI to view the logical system.

```
user@host> set cli logical-system LS3
Logical system: LS3
user@host:LS3>
```

4. Run an operational-mode command.

```
user@host:LS3> show interfaces terse
Interface Admin Link Proto Local Remote
1t-1/2/0
1t-1/2/0.3 up up inet 10.0.2.1/30
```

5. Enter configuration mode to edit the logical system configuration.

```
user@host:LS3> edit
Entering configuration mode
user@host:LS3#
```

6. Exit configuration mode to return to operational mode.

```
user@host:LS3# exit
Exiting configuration mode
```

7. Clear the logical system view to return to the main router view.

```
user@host:LS3> clear cli logical-system
Cleared default logical system
```

```
user@host>
```

8. To achieve the same effect when using a Junos XML protocol client application, include the `<set-logical-system>` tag.

```
<rpc>
<set-logical-system>
<logical-system>LS1</logical-system>
</set-logical-system>
</rpc>
```

---

### Example: Viewing BGP Trace Files on Logical Systems

This example shows how to list and view files that are stored on a logical system.

- [Requirements on page 55](#)
- [Overview on page 56](#)
- [Configuration on page 56](#)
- [Verification on page 60](#)

#### **Requirements**

- You must have the **view** privilege for the logical system.
- Configure a network, such as the BGP network shown in *Example: Configuring Internal BGP Peering Sessions on Logical Systems*.

### Overview

Logical systems have their individual directory structure created in the `/var/logical-systems/logical-system-name` directory. It contains the following subdirectories:

- `/config`—Contains the active configuration specific to the logical system.
- `/log`—Contains system log and tracing files specific to the logical system.

To maintain backward compatibility for the log files with previous versions of Junos OS, a symbolic link (symlink) from the `/var/logs/logical-system-name` directory to the `/var/logical-systems/logical-system-name` directory is created when a logical system is configured.

- `/tmp`—Contains temporary files specific to the logical system.

The file system for each logical system enables logical system users to view trace logs and modify logical system files. Logical system administrators have full access to view and modify all files specific to the logical system.

Logical system users and administrators can save and load configuration files at the logical-system level using the **save** and **load** configuration mode commands. In addition, they can also issue the **show log**, **monitor**, and **file** operational mode commands at the logical-system level.

This example shows how to configure and view a BGP trace file on a logical system. The steps can be adapted to apply to trace operations for any Junos OS hierarchy level that supports trace operations.



**TIP:** To view a list of hierarchy levels that support tracing operations, enter the **help apropos traceoptions** command in configuration mode.

### Configuration

- [Configuring Trace Operations on page 57](#)
- [Viewing the Trace File on page 57](#)
- [Deactivating and Reactivating Trace Logging on page 59](#)
- [Results on page 60](#)

#### 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 logical-systems A protocols bgp group internal-peers traceoptions file bgp-log
set logical-systems A protocols bgp group internal-peers traceoptions file size 10k
set logical-systems A protocols bgp group internal-peers traceoptions file files 2
set logical-systems A protocols bgp group internal-peers traceoptions flag update detail
```

### Configuring Trace Operations

**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 the trace operations:

1. Configure trace operations on the logical system.

```
[edit logical-systems A protocols bgp group internal-peers]
user@host# set traceoptions file bgp-log
user@host# set traceoptions file size 10k
user@host# set traceoptions file files 2
user@host# set traceoptions flag update detail
```

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

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

### Viewing the Trace File

**Step-by-Step Procedure** To view the trace file:

1. In operational mode on the main router, list the directories on the logical system.

```
user@host> file list /var/logical-systems/A
/var/logical-systems/A:
config/
log/
tmp/
```

2. In operational mode on the main router, list the log files on the logical system.

```
user@host> file list /var/logical-systems/A/log/
/var/logical-systems/A/log:
bgp-log
```

3. View the contents of the **bgp-log** file.

```
user@host> file show /var/logical-systems/A/log/bgp-log
Aug 10 17:12:01 trace_on: Tracing to "/var/log/A/bgp-log" started
Aug 10 17:14:22.826182 bgp_peer_mgmt_clear:5829: NOTIFICATION sent to
192.163.6.4 (Internal AS 17): code 6 (Cease) subcode 4 (Administratively
Reset), Reason: Management session cleared BGP neighbor
Aug 10 17:14:22.826445 bgp_send: sending 21 bytes to 192.163.6.4 (Internal
AS 17)
Aug 10 17:14:22.826499
Aug 10 17:14:22.826499 BGP SEND 192.168.6.5+64965 -> 192.163.6.4+179
Aug 10 17:14:22.826559 BGP SEND message type 3 (Notification) length 21
Aug 10 17:14:22.826598 BGP SEND Notification code 6 (Cease) subcode 4
(Administratively Reset)
Aug 10 17:14:22.831756 bgp_peer_mgmt_clear:5829: NOTIFICATION sent to
192.168.40.4 (Internal AS 17): code 6 (Cease) subcode 4 (Administratively
Reset), Reason: Management session cleared BGP neighbor
Aug 10 17:14:22.831851 bgp_send: sending 21 bytes to 192.168.40.4 (Internal
AS 17)
Aug 10 17:14:22.831901
Aug 10 17:14:22.831901 BGP SEND 192.168.6.5+53889 -> 192.168.40.4+179
```

```
Aug 10 17:14:22.831959 BGP SEND message type 3 (Notification) length 21
Aug 10 17:14:22.831999 BGP SEND Notification code 6 (Cease) subcode 4
(Administratively Reset)
...
```

4. Filter the output of the log file.

```
user@host> file show /var/logical-systems/A/log/bgp-log | match "flags 0x40"
Aug 10 17:14:54.867460 BGP SEND flags 0x40 code Origin(1): IGP
Aug 10 17:14:54.867595 BGP SEND flags 0x40 code ASPath(2) length 0: <null>
Aug 10 17:14:54.867650 BGP SEND flags 0x40 code NextHop(3): 192.168.6.5
Aug 10 17:14:54.867692 BGP SEND flags 0x40 code LocalPref(5): 100
Aug 10 17:14:54.884529 BGP RECV flags 0x40 code Origin(1): IGP
Aug 10 17:14:54.884581 BGP RECV flags 0x40 code ASPath(2) length 0: <null>
Aug 10 17:14:54.884628 BGP RECV flags 0x40 code NextHop(3): 192.168.6.4
Aug 10 17:14:54.884667 BGP RECV flags 0x40 code LocalPref(5): 100
Aug 10 17:14:54.911377 BGP RECV flags 0x40 code Origin(1): IGP
Aug 10 17:14:54.911422 BGP RECV flags 0x40 code ASPath(2) length 0: <null>
Aug 10 17:14:54.911466 BGP RECV flags 0x40 code NextHop(3): 192.168.40.4
Aug 10 17:14:54.911507 BGP RECV flags 0x40 code LocalPref(5): 100
Aug 10 17:14:54.916008 BGP SEND flags 0x40 code Origin(1): IGP
Aug 10 17:14:54.916054 BGP SEND flags 0x40 code ASPath(2) length 0: <null>
Aug 10 17:14:54.916100 BGP SEND flags 0x40 code NextHop(3): 192.168.6.5
Aug 10 17:14:54.916143 BGP SEND flags 0x40 code LocalPref(5): 100
Aug 10 17:14:54.920304 BGP RECV flags 0x40 code Origin(1): IGP
Aug 10 17:14:54.920348 BGP RECV flags 0x40 code ASPath(2) length 0: <null>
Aug 10 17:14:54.920393 BGP RECV flags 0x40 code NextHop(3): 10.0.0.10
Aug 10 17:14:54.920434 BGP RECV flags 0x40 code LocalPref(5): 100
```

5. View the tracing operations in real time.

```
user@host> clear bgp neighbor logical-system A
Cleared 2 connections
```



**CAUTION:** Clearing the BGP neighbor table is disruptive in a production environment.

6. Run the **monitor start** command with an optional **match** condition.

```
user@host> monitor start A/bgp-log | match 0.0.0.0/0
Aug 10 19:21:40.773467 BGP RECV 0.0.0.0/0
Aug 10 19:21:40.773685 bgp_rcv_nlr: 0.0.0.0/0
Aug 10 19:21:40.773778 bgp_rcv_nlr: 0.0.0.0/0 belongs to meshgroup
Aug 10 19:21:40.773832 bgp_rcv_nlr: 0.0.0.0/0 qualified bnp->ribact 0x0
12afcb 0x0
```

7. Pause the **monitor** command by pressing Esc-Q.  
To unpause the output, press Esc-Q again.
8. Halt the **monitor** command by pressing Enter and typing **monitor stop**.

```
[Enter]
user@host> monitor stop
```

9. When you are finished troubleshooting, consider deactivating trace logging to avoid any unnecessary impact to system resources.

```
[edit protocols bgp group internal-peers]
user@host:A# deactivate traceoptions
user@host:A# commit
```



When configuration is deactivated, it appears in the configuration with the **inactive** tag. To reactivate trace operations, use the **activate** configuration-mode statement.

```
[edit protocols bgp group internal-peers]
user@host:A# show

type internal;
inactive: traceoptions {
 file bgp-log size 10k files 2;
 flag update detail;
 flag all;
}
local-address 192.168.6.5;
export send-direct;
neighbor 192.163.6.4;
neighbor 192.168.40.4;
```

10. To reactivate trace operations, use the **activate** configuration-mode statement.

```
[edit protocols bgp group internal-peers]
user@host:A# activate traceoptions
user@host:A# commit
```

### *Deactivating and Reactivating Trace Logging*

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

To deactivate and reactivate the trace file:

1. When you are finished troubleshooting, consider deactivating trace logging to avoid an unnecessary impact to system resources.

```
[edit protocols bgp group internal-peers]
user@host:A# deactivate traceoptions
user@host:A# commit
```

When configuration is deactivated, the statement appears in the configuration with the **inactive** tag.

```
[edit protocols bgp group internal-peers]
user@host:A# show

type internal;
inactive: traceoptions {
 file bgp-log size 10k files 2;
 flag update detail;
 flag all;
}
local-address 192.168.6.5;
export send-direct;
neighbor 192.163.6.4;
neighbor 192.168.40.4;
```

2. To reactivate logging, use the **activate** configuration-mode statement.

```
[edit protocols bgp group internal-peers]
user@host:A# activate traceoptions
user@host:A# commit
```

### Results

From configuration mode, confirm your configuration by entering the **show logical-systems A protocols bgp group internal-peers** command. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@host# show logical-systems A protocols bgp group internal-peers
traceoptions {
 file bgp-log size 10k files 2;
 flag update detail;
}
```

### Verification

Confirm that the configuration is working properly.

#### *Verifying That the Trace Log File Is Operating*

**Purpose** Make sure that events are being written to the log file.

**Action** user@host:A> **show log bgp-log**  
Aug 12 11:20:57 trace\_on: Tracing to "/var/log/A/bgp-log" started

---

### Example: Configuring System Logging on Logical Systems

This example shows how to configure system logging on logical systems and how to view the logs.

- [Requirements on page 60](#)
- [Overview on page 61](#)
- [Configuration on page 61](#)
- [Verification on page 62](#)

### Requirements

This example has the following requirements:

- You must have the **view** privilege for the logical system.
- Junos OS Release 11.4 or later.

### Overview

Each logical system has its individual directory structure created in the `/var/logical-systems/logical-system-name` directory. This directory contains the following subdirectories:

- `/config`—Contains the active configuration specific to the logical system.
- `/log`—Contains system log and tracing files specific to the logical system.

To maintain backward compatibility for the log files with previous versions of Junos OS, a symbolic link (symlink) from the `/var/log/logical-system-name` directory to the `/var/logical-systems/logical-system-name` directory is created when a logical system is configured.

- `/tmp`—Contains temporary files specific to the logical system.

The file system for each logical system enables logical system users to view trace logs and modify logical system files. Logical system administrators have full access to view and modify all files specific to the logical system.

Logical system users and administrators can save and load configuration files at the logical system level using the **save** and **load** configuration mode commands. In addition, they can issue the **show log**, **monitor**, and **file** operational mode commands at the logical system level.

This example shows how to configure system logging on a logical system.

### 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, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

```
set logical-systems lsys1 system syslog host 10.209.10.69 ftp critical
set logical-systems lsys1 system syslog allow-duplicates
set logical-systems lsys1 system syslog file lsys1-file1 daemon error
set logical-systems lsys1 system syslog file lsys1-file1 firewall critical
```

#### 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 system logging:

1. Configure trace operations on the logical system.

```
[edit logical-systems lsys1 system syslog]
user@host# set host 10.209.10.69 ftp critical
user@host# set allow-duplicates
user@host# set file lsys1-file1 daemon error
user@host# set file lsys1-file1 firewall critical
```

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

```
[edit]
user@host# commit
user@host# exit
```

### Results

From configuration mode, confirm your configuration by entering the **show logical-systems** command. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@host# show logical-systems
lsys1 {
 system {
 syslog {
 host 10.209.10.69 {
 ftp critical;
 }
 allow-duplicates;
 file lsys1-file1 {
 daemon error;
 firewall critical;
 }
 }
 }
}
```

### Verification

Confirm that the configuration is working properly.

#### Verifying That the System Log File Is Operating

**Purpose** Make sure that events are being written to the log file.

#### Action



**TIP:** To make entries in the system log, you can use the **start shell** command and then use the **logger** shell command. For example: **logger -e "firewall\_crit" -p firewall.crit -l lsys1 TEST**

```
user@host> show log lsys1/lsys1-file1
Sep 7 14:15:46 host clear-log[2752]: logfile cleared
Sep 7 14:19:04 host logger: % -: firewall_crit: TEST
...
```

```
user@host> file show /var/logical-systems/lsys1/log/lsys1-file1
Sep 7 14:19:04 host logger: % -: firewall_crit: TEST
...
```

**Related Documentation**

- *Introduction to Logical Systems*