protocols ripng redistribute ospfv3 ................................................................. 43
protocols ripng redistribute static ................................................................. 44

Route Filtering Commands ................................................................................... 45
protocols ripng distribute-list access-list ......................................................... 46
protocols ripng distribute-list interface <interface-name> access-list .......... 47
protocols ripng distribute-list interface <interface-name> prefix-list .......... 48
protocols ripng distribute-list prefix-list ......................................................... 49

RIPng Interface Commands ................................................................................ 51
interfaces <interface> ipv6 ripng enable ......................................................... 52
interfaces <interface> ipv6 ripng metric-offset .............................................. 53
interfaces <interface> ipv6 ripng split-horizon ............................................ 54
interfaces <interface> ipv6 ripng neighbor <ip-address> ............................... 55

Supported Interface Types .................................................................................. 57

List of Acronyms ................................................................................................. 59
Document conventions

The document conventions describe text formatting conventions, command syntax conventions, and important notice formats used in Brocade technical documentation.

Text formatting conventions

Text formatting conventions such as boldface, italic, or Courier font may be used in the flow of the text to highlight specific words or phrases.

<table>
<thead>
<tr>
<th>Format</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bold text</td>
<td>Identifies command names</td>
</tr>
<tr>
<td></td>
<td>Identifies keywords and operands</td>
</tr>
<tr>
<td></td>
<td>Identifies the names of user-manipulated GUI elements</td>
</tr>
<tr>
<td></td>
<td>Identifies text to enter at the GUI</td>
</tr>
<tr>
<td>italic text</td>
<td>Identifies emphasis</td>
</tr>
<tr>
<td></td>
<td>Identifies variables</td>
</tr>
<tr>
<td></td>
<td>Identifies document titles</td>
</tr>
<tr>
<td>Courier font</td>
<td>Identifies CLI output</td>
</tr>
<tr>
<td></td>
<td>Identifies command syntax examples</td>
</tr>
</tbody>
</table>

Command syntax conventions

Bold and italic text identify command syntax components. Delimiters and operators define groupings of parameters and their logical relationships.

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bold text</td>
<td>Identifies command names, keywords, and command options.</td>
</tr>
<tr>
<td>italic text</td>
<td>Identifies a variable.</td>
</tr>
<tr>
<td>value</td>
<td>In Fibre Channel products, a fixed value provided as input to a command option is printed in plain text, for example, --show WWN.</td>
</tr>
</tbody>
</table>
### Notes, cautions, and warnings

Notes, cautions, and warning statements may be used in this document. They are listed in the order of increasing severity of potential hazards.

---

**NOTE**
A Note provides a tip, guidance, or advice, emphasizes important information, or provides a reference to related information.

---

**ATTENTION**
An Attention statement indicates a stronger note, for example, to alert you when traffic might be interrupted or the device might reboot.

---

**CAUTION**
A Caution statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.

---

**DANGER**
A Danger statement indicates conditions or situations that can be potentially lethal or extremely hazardous to you. Safety labels are also attached directly to products to warn of these conditions or situations.
Brocade resources

Visit the Brocade website to locate related documentation for your product and additional Brocade resources.

You can download additional publications supporting your product at www.brocade.com. Select the Brocade Products tab to locate your product, then click the Brocade product name or image to open the individual product page. The user manuals are available in the resources module at the bottom of the page under the Documentation category.

To get up-to-the-minute information on Brocade products and resources, go to MyBrocade. You can register at no cost to obtain a user ID and password.

Release notes are available on MyBrocade under Product Downloads.

White papers, online demonstrations, and data sheets are available through the Brocade website.

Contacting Brocade Technical Support

As a Brocade customer, you can contact Brocade Technical Support 24x7 online, by telephone, or by e-mail. Brocade OEM customers contact their OEM/Solutions provider.

Brocade customers

For product support information and the latest information on contacting the Technical Assistance Center, go to http://www.brocade.com/services-support/index.html.

If you have purchased Brocade product support directly from Brocade, use one of the following methods to contact the Brocade Technical Assistance Center 24x7.

<table>
<thead>
<tr>
<th>Online</th>
<th>Telephone</th>
<th>E-mail</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preferred method of contact for non-urgent issues:</td>
<td>Required for Sev 1-Critical and Sev 2-High issues:</td>
<td><a href="mailto:support@brocade.com">support@brocade.com</a></td>
</tr>
<tr>
<td>• My Cases through MyBrocade</td>
<td>• Continental US: 1-800-752-8061</td>
<td>Please include:</td>
</tr>
<tr>
<td>• Software downloads and licensing tools</td>
<td>• Europe, Middle East, Africa, and Asia Pacific: +800-AT FIBREE (+800 28 34 27 33)</td>
<td>• Problem summary</td>
</tr>
<tr>
<td>• Knowledge Base</td>
<td>• For areas unable to access toll free number: +1-408-333-6061</td>
<td>• Serial number</td>
</tr>
<tr>
<td></td>
<td>• Toll-free numbers are available in many countries.</td>
<td>• Installation details</td>
</tr>
</tbody>
</table>

Brocade OEM customers

If you have purchased Brocade product support from a Brocade OEM/Solution Provider, contact your OEM/Solution Provider for all of your product support needs.

• OEM/Solution Providers are trained and certified by Brocade to support Brocade® products.
• Brocade provides backline support for issues that cannot be resolved by the OEM/Solution Provider.
• Brocade Supplemental Support augments your existing OEM support contract, providing direct access to Brocade expertise. For more information, contact Brocade or your OEM.
• For questions regarding service levels and response times, contact your OEM/Solution Provider.

Document feedback

To send feedback and report errors in the documentation you can use the feedback form posted with the document or you can e-mail the documentation team.

Quality is our first concern at Brocade and we have made every effort to ensure the accuracy and completeness of this document. However, if you find an error or an omission, or you think that a topic needs further development, we want to hear from you. You can provide feedback in two ways:

• Through the online feedback form in the HTML documents posted on www.brocade.com.
• By sending your feedback to documentation@brocade.com.

Provide the publication title, part number, and as much detail as possible, including the topic heading and page number if applicable, as well as your suggestions for improvement.
About This Guide

This guide describes how to configure Routing Information Protocol next generation (RIPng) on the Brocade 5600 vRouter (referred to as a virtual router, vRouter, or router in the guide).
RIPng Configuration

- RIPng overview
- Supported standards
- Configuring RIPng

RIPng overview

RIPng is a dynamic routing protocol that is suitable for small, homogenous IPv6 networks. It is classified as an interior gateway protocol (IGP) and employs the distance-vector routing algorithm. RIPng determines the best path by counting the hops to the destination. The maximum hop count is 15 (16 is considered an infinite distance), making RIPng less suitable for large networks. RIPng is an extension of RIP version 2 for IPv6.

Supported standards

The Brocade vRouter implementation of RIPng complies with the following standards:
- RFC 2080: RIPng for IPv6
- RFC 2081: RIPng Protocol Applicability Statement

Configuring RIPng

This section presents the following topics:
- Enable forwarding on R1 and R2
- Enable RIPng on an interface
- Advertise connected networks
- Confirm visibility of remote networks

This section presents an example configuration of RIPng. The configuration example is based on the reference diagram in the following figure. This example shows the configuration of the nodes by using dynamic IPv6 routing with RIPng to enable R3 and R4 to communicate through R1 and R2.
Enabling forwarding on R1 and R2

For R1 to pass data between the dp0p1p1 and dp0p1p3 interfaces and R2 to pass data between the dp0p1p1 and dp0p1p2 interfaces, R1 and R2 must be configured to enable forwarding. To enable forwarding on R1, perform the following step in configuration mode.

**TABLE 1  Enabling forwarding on R1**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable forwarding on R1.</td>
<td>vyatta@R1# delete system ipv6 disable-forwarding</td>
</tr>
<tr>
<td>Commit the change.</td>
<td>vyatta@R1# commit</td>
</tr>
</tbody>
</table>

To enable forwarding on R2, perform the following steps in configuration mode.

**TABLE 2  Enabling forwarding on R2**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable forwarding on R2.</td>
<td>vyatta@R2# delete system ipv6 disable-forwarding</td>
</tr>
<tr>
<td>Commit the change.</td>
<td>vyatta@R2# commit</td>
</tr>
</tbody>
</table>
Enabling RIPng on an interface

To allow dynamic routing by using RIPng, RIPng must be enabled on the interfaces that are to use it. To enable RIPng on R1, perform the following steps in configuration mode.

**TABLE 3  Enable RIPng on R1**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable RIPng on dp0p1p1.</td>
<td>vyatta@R1# set interfaces dataplane dp0p1p1 ipv6 ripng enable</td>
</tr>
<tr>
<td>Enable RIPng on dp0p1p3.</td>
<td>vyatta@R1# set interfaces dataplane dp0p1p3 ipv6 ripng enable</td>
</tr>
<tr>
<td>Commit the change.</td>
<td>vyatta@R1# commit</td>
</tr>
<tr>
<td>Change to operational mode.</td>
<td>vyatta@R1# exit</td>
</tr>
<tr>
<td>Verify the status of RIPng.</td>
<td>vyatta@R1:~$ show ipv6 ripng status</td>
</tr>
<tr>
<td></td>
<td>Sending updates every 30 seconds with +/-50%, next due in 4 seconds</td>
</tr>
<tr>
<td></td>
<td>Timeout after 180 seconds, garbage collect after 120 seconds</td>
</tr>
<tr>
<td></td>
<td>Outgoing update filter list for all interface is not set</td>
</tr>
<tr>
<td></td>
<td>Incoming update filter list for all interface is not set</td>
</tr>
<tr>
<td></td>
<td>Default redistribution metric is 1</td>
</tr>
<tr>
<td></td>
<td>Distributing:</td>
</tr>
<tr>
<td></td>
<td>Interface</td>
</tr>
<tr>
<td></td>
<td>dp0p1p1</td>
</tr>
<tr>
<td></td>
<td>dp0p1p2</td>
</tr>
<tr>
<td>Display information for RIPng interfaces.</td>
<td>vyatta@R1:~$ show ipv6 ripng interface</td>
</tr>
<tr>
<td></td>
<td>dp0p1p1 is up, line protocol is up</td>
</tr>
<tr>
<td></td>
<td>Routing Protocol: RIPng</td>
</tr>
<tr>
<td></td>
<td>Passive interface: Disabled</td>
</tr>
<tr>
<td></td>
<td>Split horizon: Enabled with Poisoned</td>
</tr>
<tr>
<td></td>
<td>Reversed</td>
</tr>
<tr>
<td></td>
<td>IPv6 interface address:</td>
</tr>
<tr>
<td></td>
<td>fe80::5054:ff:fe8b:1/64</td>
</tr>
<tr>
<td></td>
<td>dp0p1p2 is up, line protocol is up</td>
</tr>
<tr>
<td></td>
<td>Routing Protocol: RIPng</td>
</tr>
<tr>
<td></td>
<td>Passive interface: Disabled</td>
</tr>
<tr>
<td></td>
<td>Split horizon: Enabled with Poisoned</td>
</tr>
<tr>
<td></td>
<td>Reversed</td>
</tr>
<tr>
<td></td>
<td>IPv6 interface address:</td>
</tr>
<tr>
<td></td>
<td>fe80::5054:ff:fe98:2/64</td>
</tr>
</tbody>
</table>

Advertising connected networks

The redistribute command is then used to advertise the connected networks. To advertise connected networks on R1, perform the following steps in configuration mode.

**TABLE 4  Advertising connected networks on R1**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
</tr>
</thead>
</table>
Confirming visibility of remote networks

After enabling RIPng on the other interfaces of R2, R3, and R4 and advertising connected networks on R2, check the routing table of R4 to verify that it has learned the network. To confirm visibility of remote networks on R4, perform the following step in operational mode.

Confirming visibility of remote networks on R4

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trace the route from R2 to R4.</td>
<td>vyatta@R4:~$ show ipv6 route IPv6 Routing Table Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF, IA - OSPF inter area, E1 - OSPF external type 1, E2 - OSPF external type 2, I - IS-IS, B - BGP &gt; - selected route, * - FIB route, p - stale info Timers: Uptime S&gt;* ::/0 [1/0] via 2001:db8:1::1, dp0s1 C&gt;* ::1/128 is directly connected, lo C&gt;* 2001:db8:1::/64 is directly connected, dp0s1 R&gt;* 2001:db8:1::/64 [120/2] via fe80::20c:29ff:fed6:816c, dp0s1, 00:43:00 R&gt;* 2001:db8:3::/64 [120/3] via fe80::20c:29ff:fed6:816c, dp0s1, 00:00:03 C&gt;* fe80::/64 is directly connected, dp0s1</td>
</tr>
</tbody>
</table>

The R in the first column indicates that two routes have been learned from RIPng. Because a route now exists for 2001:db8:3::/64, R3 can be pinged. To confirm connectivity, perform the following steps in operational mode.

Confirming connectivity between R4 and R3

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
</tr>
</thead>
</table>

TABLE 4 Advertising connected networks on R1 (Continued)

| Advertise connected networks through RIPng. | vyatta@R1# set protocols ripng redistribute connected |
| Commit the change. | vyatta@R1# commit |
| Verify the redistribution. | vyatta@R1:~$ show ipv6 ripng status Routing Protocol is "RIPng" Sending updates every 30 seconds with +/-50%, next due in 4 seconds Timeout after 180 seconds, garbage collect after 120 seconds Outgoing update filter list for all interface is not set Incoming update filter list for all interface is not set Default redistribution metric is 1 Redistributing: connected Interface dp0p1p1 dp0p1p2 |
TABLE 6  Confirming connectivity between R4 and R3 (Continued)

Ping R3 from R4.

vyatta@R4:~$ ping 2001:db8:3::3
PING 2001:db8:3::3(2001:db8:3::3) 56 data bytes
64 bytes from 2001:db8:3::3: icmp_seq=1 ttl=62 time=5.98 ms
64 bytes from 2001:db8:3::3: icmp_seq=2 ttl=62 time=0.603 ms
^C
--- 2001:db8:3::3 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1011ms
rtt min/avg/max/mdev = 0.603/3.294/5.986/2.692 ms

Display the RIPng status.

vyatta@R4:~$ show ipv6 ripng
Codes: R - RIP, Rc - RIP connected, Rs - RIP static, Ra - RIP aggregated,
       Rcx - RIP connect suppressed, Rsx - RIP static suppressed,
       K - Kernel, C - Connected, S - Static, O - OSPF, I - IS-IS, B - BGP

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
</tr>
</thead>
<tbody>
<tr>
<td>C 2001:db8:1::/64</td>
<td>dp0p1p1</td>
</tr>
<tr>
<td>R 2001:db8:2::/64</td>
<td>dp0p1p1</td>
</tr>
<tr>
<td>R 2001:db8:3::/64</td>
<td>dp0p1p1</td>
</tr>
<tr>
<td>R 2001:db8:4::/64</td>
<td>dp0p1p1</td>
</tr>
</tbody>
</table>
Confirming visibility of remote networks
Router-Level Configuration Commands

- monitor protocol ripng disable events................................................................. 18
- monitor protocol ripng disable packet................................................................. 19
- monitor protocol ripng disable rib................................................................. 20
- monitor protocol ripng enable events................................................................. 21
- monitor protocol ripng enable packet................................................................. 22
- monitor protocol ripng enable rib................................................................. 23
- show monitoring protocols ripng................................................................. 24
- protocols ripng aggregate-address <ipv6net>............................................... 25
- protocols ripng default-information originate................................................ 26
- protocols ripng default-metric <metric>.............................................................. 27
- protocols ripng log................................................................. 28
- protocols ripng log packet................................................................. 29
- protocols ripng passive-interface <interface-name>........................................ 30
- protocols ripng route <ipv6net>................................................................. 31
- protocols ripng timers garbage-collection <seconds>........................................ 32
- protocols ripng timers timeout <seconds>.................................................. 33
- protocols ripng timers update <seconds>.................................................. 34
- reset ipv6 ripng route................................................................. 35
- show ipv6 route ripng................................................................. 36
- show ipv6 ripng................................................................. 37
monitor protocol ripng disable events

Disables the generation of debug messages that are related to RIPng events.

Syntax

```
monitor protocol ripng disable events
```

Modes

Operational mode

Usage Guidelines

Use this command to disable the generation of debug (trace-level) messages that are related to RIPng events.
## monitor protocol ripng disable packet

Disables the generation of debug messages that are related to all RIPng packet types.

### Syntax

```
monitor protocol ripng disable packet [ recv | send ]
```

### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>recv</td>
<td>Disables debugging of all received packets.</td>
</tr>
<tr>
<td>send</td>
<td>Disables debugging of all sent packets.</td>
</tr>
</tbody>
</table>

### Modes

- Operational mode

### Usage Guidelines

Use this command to disable the generation of debug (trace-level) messages that are related to RIPng packet types.
**monitor protocol ripng disable rib**

Disables the generation of debug messages that are related to the RIPng RIB.

**Syntax**

`monitor protocol ripng disable rib`

**Command Default**

Debug messages are disabled for actions that are related to the RIPng RIB.

**Modes**

Operational mode

**Usage Guidelines**

Use this command to disable the generation of debug (trace-level) messages that are related to the RIPng RIB.
**monitor protocol ripng enable events**

Enables the generation of debug messages that are related to RIPng events.

**Syntax**  
`monitor protocol ripng enable events`

**Modes**  
Operational mode

**Usage Guidelines**  
Use this command to enable the generation of debug (trace-level) messages that are related to RIPng events.
**monitor protocol ripng enable packet**

Enables the generation of debug messages that are related to all RIPng packet types.

**Syntax**

```
monitor protocol ripng enable packet [ recv | send ]
```

**Parameters**

- `recv`
  
  Enables debugging of all received packets.

- `send`
  
  Enables debugging of all sent packets.

**Modes**

- Operational mode

**Usage Guidelines**

Use this command to enable the generation of debug (trace-level) messages that are related to all RIPng packet types.
**monitor protocol ripng enable rib**

Enables the generation of debug messages that are related to the RIPng RIB.

**Syntax**

```
monitor protocol ripng enable rib
```

**Command Default**

Debug messages are generated for actions that are related to the RIPng RIB.

**Modes**

Operational mode

**Usage Guidelines**

Use this command to enable the generation of debug (trace-level) messages that are related to the RIPng RIB.
show monitoring protocols ripng

Displays RIPng protocol debugging flags.

**Syntax**

show monitoring protocols ripng

**Modes**

Operational mode

**Usage Guidelines**

Use this command to display how debugging is set for RIPng.
protocols ripng aggregate-address <ipv6net>

Specifies an aggregate RIPng route announcement.

**Syntax**

- `set protocols ripng aggregate-address ipv6net`
- `delete protocols ripng aggregate-address ipv6net`
- `show protocols ripng aggregate-address [ipv6net]`

**Parameters**

- `ipv6net`
  
  An IPv6 network from which routes are to aggregate. The format is `ipv6-address/prefix`.

**Modes**

- Configuration mode

**Configuration Statement**

```
protocols {
  ripng {
    aggregate-address ipv6net
  }
}
```

**Usage Guidelines**

- Use this command for IPv6 address aggregation.
- Use the `set` form of this command to specify a contiguous block of IPv6 addresses to aggregate.
- Use the `delete` form of this command to delete an aggregate address.
- Use the `show` form of this command to display aggregate address configuration settings.
protocols ripng default-information originate

Generates a default route into the RIPng routing domain.

**Syntax**

- `set protocols ripng default-information originate`
- `delete protocols ripng default-information originate`
- `show protocols ripng default-information originate`

**Command Default**
A default route into the RIPng routing domain is not generated.

**Modes**
Configuration mode

**Configuration Statement**

```bash
protocols {
    ripng {
        default-information {
            originate
        }
    }
}
```

**Usage Guidelines**

Use the **set** form of this command to generate a default route into the RIPng routing domain.

Use the **delete** form of this command to restore the default behavior for default route generation into RIPng; that is, a default route is not generated.

Use the **show** form of this command to display the default configuration of route generation into RIPng.
protocols ripng default-metric <metric>

Sets the default metric for external routes that are redistributed into RIPv2.

Syntax

set protocols ripng default-metric metric
delete protocols ripng default-metric
show protocols ripng default-metric

Command Default

Routes that are imported into RIPv2 are assigned a metric of 1.

Parameters

metric

Mandatory. A metric assigned to external routes that are imported into RIPv2.
The metric ranges from 1 through 16. The default metric is 1.

Modes

Configuration mode

Configuration Statement

protocols {
  ripng {
    default-metric metric
  }
}

Usage Guidelines

Use the set form of this command to set the default metric for external routes that are redistributed into RIPv2.

Use the delete form of this command to restore the default RIPv2 metric for external routes that are redistributed into RIPv2; that is, routes are assigned a metric of 1.

Use the show form of this command to display the default metric for external routes that are redistributed into RIPv2.
protocols ripng log

Enables logging for RIPng.

**Syntax**

```plaintext
set protocols ripng log { all | events | nsm | packet | rib }
```

```plaintext
delete protocols ripng log { all | events | nsm | packet | rib }
```

```plaintext
show protocols ripng log { all | events | nsm | packet | rib }
```

**Command Default**
None

**Parameters**

- `all`
  Enables all RIPng logs.
- `events`
  Enables RIPng events logs.
- `nsm`
  Enables RIPng NSM logs.
- `packet`
  Enables RIPng packet logs.
- `rib`
  Enables RIPng RIB logs.

**Modes**
Configuration mode

**Configuration Statement**

```plaintext
protocols {
  ripng {
    log {
      all
      events
      nsm
      packet
      rib
    }
  }
}
```

**Usage Guidelines**

- Use the **set** form of this command to enable routing information protocol (RIP)ng logs.
- Use the **delete** form of this command to remove RIPng logs.
- Use the **show** form of this command to view RIPng logs.
protocols ripng log packet

Enables logging for RIPng packets.

Syntax

- set protocols ripng log packet { all | detail | rcv | send }
- delete protocols ripng log packet { all | detail | rcv | send }
- show protocols ripng log packet { all | detail | rcv | send }

Command Default
None

Parameters

- all
  Enables all RIPng packet logs.
- detail
  Enables only RIPng packet detail logs.
- rcv
  Enables only RIPng packet receive logs.
- send
  Enables only RIPng packet send logs.

Modes
Configuration mode

Configuration Statement

```plaintext
protocols {
  ripng {
    log {
      packet {
        all
        detail
        rcv
        send
      }
    }
  }
}
```

Usage Guidelines

Use the `set` form of this command to enable routing information protocol (RIP)ng packet logs.

Use the `delete` form of this command to remove RIPng packet logs.

Use the `show` form of this command to view RIPng packet logs.
protocols ripng passive-interface <interface-name>

Suppresses updates to RIPng routing on an interface.

**Syntax**

```
set protocols ripng passive-interface interface-name
```

```
delete protocols ripng passive-interface interface-name
```

```
show protocols ripng passive-interface
```

**Command Default**

RIPng routing updates are not suppressed.

**Parameters**

`interface-name`

The identifier of an interface. Supported interface types are:

- Dataplane
- Loopback

For more information about these interface types, refer to Supported Interface Types on page 57.

You can suppress routing updates on more than one RIPng interface by creating multiple `protocols ripng passive-interface` configuration nodes.

**Modes**

Configuration mode

**Configuration Statement**

```
protocols {
  ripng {
    passive-interface interface
  }
}
```

**Usage Guidelines**

Use the `set` form of this command to suppress updates to RIPng routing on an interface.

Use the `delete` form of this command to disable the suppression of updates to RIPng routing on an interface.

Use the `show` form of this command to display the configuration of RIPng route suppression for an interface.
protocols ripng route <ipv6net>

Sets a static route in RIPng.

**Syntax**

set protocols ripng route ipv6net

delete protocols ripng route ipv6net

show protocols ripng route

**Parameters**

ipv6net

Mandatory. The IPv6 network address defining the RIPng static route.

**Modes**

Configuration mode

**Configuration Statement**

```
protocols {
  ripng {
    route ipv6net
  }
}
```

**Usage Guidelines**

Use this command to set a static route in RIPng.

- Use the `set` form of this command to set a static route in RIPng.
- Use the `delete` form of this command to remove an RIPng static route.
- Use the `show` form of this command to display RIPng static route configuration.
protocols ripng timers garbage-collection <seconds>

Sets the timer for RIPng garbage collection.

Syntax

set protocols ripng timers garbage-collection seconds

delete protocols ripng timers garbage-collection [ seconds ]

show protocols ripng timers garbage-collection

Command Default

RIPng garbage collection occurs at 120 seconds.

Parameters

seconds

Mandatory. A timer interval in seconds. The interval ranges from 0 through 65535. The default interval is 120.

Modes

Configuration mode

Configuration Statement

protocols {
    ripng {
        timers {
            garbage-collection seconds
        }
    }
}

Usage Guidelines

Use the set form of this command to set the timer for RIPng garbage collection. When the timer expires, the system scans for stale RIPng resources and releases them for use.

Use the delete form of this command to restore the default timer interval for RIPng garbage collection, which is 120 seconds.

Use the show form of this command to display the current timer interval for RIPng garbage collection.
protocols ripng timers timeout <seconds>

Sets the interval for RIPng timeouts.

**Syntax**

```plaintext
set protocols ripng timers timeout seconds

delete protocols ripng timers timeout [ seconds ]

show protocols ripng timers timeout
```

**Command Default**

RIPng timeouts occur at 180 seconds.

**Parameters**

`seconds`

Mandatory. A timer interval in seconds. The interval ranges from 0 through 65535. The default interval is 180.

**Modes**

Configuration mode

**Configuration Statement**

```plaintext
protocols {
    ripng {
        timers {
            timeout seconds
        }
    }
}
```

**Usage Guidelines**

Use the `set` form of this command to set the interval for RIPng timeouts.

Use the `delete` form of this command to restore the default interval for RIPng time-outs, which is 180 seconds.

Use the `show` form of this command to display the current interval for RIPng time-outs.
protocols ripng timers update <seconds>

Sets the timer interval for updates to the RIPng routing table.

**Syntax**

- `set protocols ripng timers update seconds`
- `delete protocols ripng timers update [seconds]`
- `show protocols ripng timers update`

**Command Default**

The RIPng routing table is updated every 30 seconds.

**Parameters**

- `seconds`
  
  Mandatory. An interval, in seconds, at which updates to the RIPng routing table occur. The interval ranges from 0 through 65535. The default interval is 30.

**Modes**

Configuration mode

**Configuration Statement**

```plaintext
protocols {
    ripng {
        timers {
            update seconds
        }
    }
}
```

**Usage Guidelines**

Use the `set` form of this command to set the timer interval for updates to the RIPng routing table. When the interval is shorter, the routing information in the tables is more accurate; however, more protocol network traffic occurs.

Use the `delete` form of this command to restore the default interval for RIPng updates, which is 30 seconds.

Use the `show` form of this command to display the current interval for RIPng updates.
**reset ipv6 ripng route**

Resets data in the RIPng routing table.

**Syntax**

```plaintext
reset ipv6 ripng route [ all | bgp | connected | kernel | ospfv6 | ripng | static | ip-address ]
```

**Parameters**

- `all`  
  Removes all entries from the RIPng routing table.
- `bgp`  
  Removes only BGP routes from the RIPng routing table.
- `connected`  
  Removes entries for connected routes from the RIPng routing table.
- `kernel`  
  Removes kernel entries from the RIPng routing table.
- `ospfv6`  
  Removes only OSPFv6 routes from the RIPng routing table.
- `ripng`  
  Removes only RIPng routes from the RIPng routing table.
- `static`  
  Removes static entries from the RIPng routing table.
- `ip-address`  
  Removes entries that match `ip-address (x:x::x:x/M)`, a destination IPv6 address, from the RIPng routing table.

**Modes**  
Operational mode.

**Usage Guidelines**  
Use the `reset ipv6 ripng route all` command to clear the RIPng routing table.
show ipv6 route ripng

Displays all IPv6 RIPng routes.

Syntax  show ipv6 route ripng

Modes  Operational mode

Usage Guidelines  Use this command to display all RIPng routes that are contained in the RIB.

Examples  The following command is an example of the show ipv6 route ripng command:

```
vyatta@vyatta:~$ show ipv6 route ripng
R>* 2001:db8:2::/64 [120/2] via fe80::20c:29ff:fed6:816c, dp0s1, 00:43:00
R>* 2001:db8:3::/64 [120/3] via fe80::20c:29ff:fed6:816c, dp0s1, 00:00:03
```

vyatta@vyatta:~$
show ipv6 ripng

Displays information about RIPng.

Syntax

show ipv6 ripng [ interface | status ]

Command Default
Displays all information about RIPng.

Parameters

interface
Optional. Displays information for RIPng interfaces.

status
Optional. Displays only RIPng protocol status information.

Modes
Operational mode

Usage Guidelines
Use this command to display information about RIPng.

Examples
The following example lists RIPng information.

vyatta@vyatta:~$ show ipv6 ripng
Codes: R - RIPng, C - connected, S - Static, O - OSPF, B - BGP
Sub-codes:
(n) - normal, (s) - static, (d) - default, (r) - redistribute,
(i) - interface, (a/S) - aggregated/Suppressed

Network      Next Hop                      Via     Metric Tag Time
----- ------- ----------------------------- ----- ------- --------
C(i) 2001:db8:1::/64                       ::      self  1 0
R(n) 2001:db8:2::/64           fe80::20c:29ff:fed6:816c dp0s1  2 0 02:56
R(n) 2001:db8:3::/64           fe80::20c:29ff:fed6:816c dp0s1  3 0 02:56

vyatta@vyatta:~$

The following example lists RIPng protocol status information.

vyatta@vyatta:~$ show ipv6 ripng status
Routing Protocol is "RIPng"
Sending updates every 30 seconds with +/-50%, next due in 4 seconds
Timeout after 180 seconds, garbage collect after 120 seconds
Outgoing update filter list for all interface is not set
Incoming update filter list for all interface is not set
Default redistribution metric is 1
Redistributing:
  Interface
  dp0s1
show ipv6 ripng
Route Redistribution Commands

- protocols ripng redistribute bgp.................................................................40
- protocols ripng redistribute connected....................................................41
- protocols ripng redistribute kernel..........................................................42
- protocols ripng redistribute ospfv3..........................................................43
- protocols ripng redistribute static............................................................44
**protocols ripng redistribute bgp**

Redistributes BGP routes into RIPng routing tables.

**Syntax**

```
set protocols ripng redistribute bgp [ metric metric | route-map map-name ]
delete protocols ripng redistribute bgp [ metric | route-map ]
show protocols ripng redistribute bgp [ metric | route-map ]
```

**Command Default**

BGP routes that are redistributed into RIPng are assigned a routing metric of 1. By default, no route map is applied to redistributed BGP routes.

**Parameters**

- **metric**
  
  Applies a metric to BGP routes that are imported into RIPng routing tables. The metric ranges from 1 through 16. The default metric is 1.

- **route-map map-name**
  
  Applies a route map to BGP routes that are imported into RIPng routing tables.

**Modes**

Configuration mode

**Configuration Statement**

```
protocols {
    ripng {
        redistribute {
            bgp {
                metric metric
                route-map map-name
            }
        }
    }
}
```

**Usage Guidelines**

Use the **set** form of this command to redistribute BGP routes into RIPng routing tables. You can set the routing metric for or specify a route map to apply to redistributed BGP routes.

Use the **delete** form of this command to remove the current configuration of BGP route redistribution.

Use the **show** form of this command to display the current configuration of BGP route redistribution.
protocols ripng redistribute connected

Redistributes directly connected routes into RIPng routing tables.

Syntax

set protocols ripng redistribute connected [ metric metric | route-map map-name ]
delete protocols ripng redistribute connected [ metric | route-map ]
show protocols ripng redistribute connected [ metric | route-map ]

Command Default

Connected routes that are redistributed into RIPng are assigned a routing metric of 1. By default, no route map is applied to redistributed connected routes.

Parameters

metric

Optional. The routing metric to be applied to connected routes being imported into RIPng routing tables. The range is 1 to 16. The default is 1.

map-name

Optional. Applies the specified route map to connected routes being imported into RIPng routing tables.

Modes

Configuration mode

Configuration Statement

protocols {
 ripng {
 redistribute {
 connected {
 metric metric
 route-map map-name
 }
 }
 }
}

Usage Guidelines

Use the set form of this command to redistribute directly connected routes into RIPng routing tables. You can set the routing metric for or specify a route map to apply to directly connected BGP routes.

Use the delete form of this command to remove the current configuration of directly connected route redistribution.

Use the show form of this command to display the current configuration of directly connected route redistribution.
protocols ripng redistribute kernel

Redistributes kernel routes into RIPng routing tables.

**Syntax**

```plaintext
set protocols ripng redistribute kernel [ metric metric | route-map map-name ]
```

```plaintext
delete protocols ripng redistribute kernel [ metric | route-map ]
```

```plaintext
show protocols ripng redistribute kernel [ metric | route-map ]
```

**Command Default**

Kernel routes that are redistributed into RIPng are assigned a routing metric of 1. By default, no route map is applied to redistributed kernel routes.

**Parameters**

- `metric`
  Optional. The routing metric to be applied to kernel routes being imported into RIPng routing tables. The range is 1 to 16. The default is 1.

- `map-name`
  Optional. Applies the specified route map to kernel routes being imported into RIPng routing tables.

**Modes**

Configuration mode

**Configuration Statement**

```plaintext
protocols {
  ripng {
    redistribute {
      kernel {
        metric metric
        route-map map-name
      }
    }
  }
}
```

**Usage Guidelines**

Use the `set` form of this command to redistribute kernel routes into RIPng routing tables. You can set the routing metric for or specify a route map to apply to redistributed kernel routes.

Use the `delete` form of this command to remove the current configuration of kernel route redistribution.

Use the `show` form of this command to display the current configuration of kernel route redistribution.
protocols ripng redistribute ospfv3

Redistributes OSPFv3 routes into RIPng routing tables.

Syntax

set protocols ripng redistribute ospfv3 [ metric metric | route-map map-name ]
delete protocols ripng redistribute ospfv3 [ metric | route-map ]
show protocols ripng redistribute ospfv3 [ metric | route-map ]

Command Default

OSPFv3 routes that are redistributed into RIPng are assigned a routing metric of 1. By default, no route map is applied to redistributed OSPFv3 routes.

Parameters

metric

Optional. The routing metric to be applied to OSPFv3 routes being imported into RIPng routing tables. The range is 1 to 16. The default is 1.

map-name

Optional. Applies the specified route map to OSPFv3 routes being imported into RIPng routing tables.

Modes

Configuration mode

Configuration Statement

protocols {
  ripng {
    redistribute {
      ospfv3 {
        metric metric
        route-map map-name
      }
    }
  }
}

Usage Guidelines

Use the set form of this command to redistribute OSPFv3 routes into RIPng routing tables. You can set the routing metric for or specify a route map to apply to redistributed OSPFv3 routes.

Use the delete form of this command to remove the current configuration of OSPFv3 route redistribution.

Use the show form of this command to display the current configuration of OSPFv3 route redistribution.
protocols ripng redistribute static

Redistributes static routes into RIPng routing tables.

**Syntax**

```
set protocols ripng redistribute static [ metric metric | route-map map-name ]
```

```
delete protocols ripng redistribute static [ metric | route-map ]
```

```
show protocols ripng redistribute static [ metric | route-map ]
```

**Command Default**

Static routes that are redistributed into RIPng are assigned a routing metric of 1. By default, no route map is applied to redistributed static routes.

**Parameters**

`metric`

Optional. The routing metric to be applied to static routes being imported into RIPng routing tables. The range is 1 to 16. The default is 1.

`route-map map-name`

Optional. Applies the specified route map to static routes being imported into RIPng routing tables.

**Modes**

Configuration mode

**Configuration Statement**

```
protocols {
  ripng {
    redistribute {
      static {
        metric metric
        route-map map-name
      }
    }
  }
}
```

**Usage Guidelines**

Use the `set` form of this command to redistribute static routes into RIPng routing tables. You can set the routing metric for or specify a route map to apply to redistributed static routes.

Use the `delete` form of this command to remove the current configuration of static route redistribution.

Use the `show` form of this command to display the current configuration of static route redistribution.
Route Filtering Commands

- protocols ripng distribute-list access-list .................................................................46
- protocols ripng distribute-list interface <interface-name> access-list ..................47
- protocols ripng distribute-list interface <interface-name> prefix-list ....................48
- protocols ripng distribute-list prefix-list ..................................................................49
protocols ripng distribute-list access-list

Applies an access list to filter inbound or outbound RIPng packets.

**Syntax**
```
set protocols ripng distribute-list access-list { in in-list | out out-list }
delete protocols ripng distribute-list access-list { in | out }
show protocols ripng distribute-list access-list { in | out }
```

**Parameters**
- **in-list**
  Specifies the identifier of a defined access list. The access list filters inbound RIPng packets.
- **out-list**
  Specifies the identifier of a defined access list. The access list filters outbound RIPng packets.

**Modes**
- Configuration mode

**Configuration Statement**
```
protocols {
  ripng {
    distribute-list {
      access-list {
        in in-list
        out out-list
      }
    }
  }
}
```

**Usage Guidelines**
Use the **set** form of this command to apply an access list to filter inbound or outbound RIPng packets.

Use the **delete** form of this command to remove the filtering of RIPng inbound or outbound packets by an access list.

Use the **show** form of this command to display RIPng access list filtering configuration.
protocols ripng distribute-list interface <interface-name> access-list

Applies an access list to an interface to filter inbound or outbound RIPng packets.

**Syntax**

- `set protocols ripng distribute-list interface interface-name access-list { in in-list | out out-list }
- `delete protocols ripng distribute-list interface interface-name access-list { in | out }
- `show protocols ripng distribute-list interface interface-name access-list { in | out }

**Parameters**

- `interface-name`
  - The identifier of an interface. Supported interface types are:
    - Dataplane
    - Loopback
  - For more information about these interface types, refer to [Supported Interface Types](#) on page 57.

- `in in-list`
  - Specifies the identifier of a defined access list. The access list applies to the specified interface to filter inbound RIPng packets.

- `out out-list`
  - Specifies the identifier of a defined access list. The access list applies to the specified interface to filter outbound RIPng packets.

**Modes**

- Configuration mode

**Configuration Statement**

```plaintext
protocols {
  ripng {
    distribute-list {
      interface interface-name {
        access-list {
          in in-list
          out out-list
        }
      }
    }
  }
}
```

**Usage Guidelines**

- Use the `set` form of this command to apply an access list to a specific interface to filter inbound or outbound RIPng packets.
- Use the `delete` form of this command to remove the filtering of RIPng inbound or outbound packets on an interface by an access list.
- Use the `show` form of this command to display RIPng access list filtering configuration for an interface.
protocols ripng distribute-list interface <interface-name> prefix-list

Applies a prefix list to an interface to filter inbound or outbound RIPng packets.

**Syntax**

```plaintext
set protocols ripng distribute-list interface interface-name prefix-list { in in-list | out out-list }
delete protocols ripng distribute-list interface interface-name prefix-list { in | out }
show protocols ripng distribute-list interface interface-name prefix-list { in | out }
```

**Parameters**

- `interface-name` The identifier of an interface. Supported interface types are:
  - Dataplane
  - Loopback
  
  For more information about these interface types, refer to Supported Interface Types on page 57.

- `in in-list` Specifies the identifier of a defined prefix list. The prefix list applies to the specified interface to filter inbound RIPng packets.

- `out out-list` Specifies the identifier of a defined prefix list. The prefix list applies to the specified interface to filter outbound RIPng packets.

**Modes**

Configuration mode

```plaintext
protocols {
  ripng {
    distribute-list {
      interface interface-name {
        prefix-list {
          in in-list
            out out-list
        }
      }
    }
  }
}
```

**Usage Guidelines**

Use the `set` form of this command to apply a prefix list to an interface to filter inbound or outbound RIPng packets.

Use the `delete` form of this command to remove the filtering of RIPng inbound or outbound packets on an interface by a prefix list.

Use the `show` form of this command to display RIPng prefix list filtering configuration for an interface.
protocols ripng distribute-list prefix-list

Applies a prefix list to filter inbound or outbound RIPng packets.

Syntax

set protocols ripng distribute-list prefix-list { in in-list | out out-list }
delete protocols ripng distribute-list prefix-list { in | out }
show protocols ripng distribute-list prefix-list { in | out }

Parameters

in in-list
- Specifies the identifier of a defined prefix list. The prefix list filters inbound RIPng packets.

out out-list
- Specifies the identifier of a defined prefix list. The prefix list filters outbound RIPng packets.

Modes

Configuration mode

Configuration Statement

protocols {  ripng {   distribute-list {     prefix-list {      in in-list     out out-list   }  }  }
}

Usage Guidelines

Use the set form of this command to apply a prefix list to filter inbound or outbound RIPng packets.

Use the delete form of this command to remove the filtering of RIPng inbound or outbound packets by a prefix list.

Use the show form of this command to display RIPng prefix list filtering configuration.
protocols ripng distribute-list prefix-list
RIPng Interface Commands

- `interfaces <interface> ipv6 ripng enable` ................................................................. 52
- `interfaces <interface> ipv6 ripng metric-offset` ..................................................... 53
- `interfaces <interface> ipv6 ripng split-horizon` .................................................... 54
- `interfaces <interface> ipv6 ripng neighbor <ip-address>` ....................................... 55
interfaces <interface> ipv6 ripng enable

Enables RIPng on an interface.

**Syntax**

```plaintext
set interfaces interface ipv6 ripng enable
delete interfaces interface ipv6 ripng enable
show interfaces interface ipv6 ripng
```

**Parameters**

`interface`

Mandatory. A type of interface. For detailed keywords and arguments that can be specified as interface types, refer to Supported Interface Types on page 57.

**Modes**

Configuration mode

**Configuration Statement**

```plaintext
interfaces interface {
  ipv6 {
    ripng
  }
}
```

**Usage Guidelines**

Use this command to enable RIPng.

Use the `set` form of this command to enable RIPng on an interface.

Use the `delete` form of this command to remove all RIPng configuration and disable RIPng on the interface.

Use the `show` form of this command to display the current RIPng configuration on an interface.
interfaces <interface> ipv6 ripng metric-offset

Sets a metric to add to routes that are received from RIPng on an interface.

**Syntax**

```
set interfaces interface ipv6 ripng metric-offset metric
show interfaces interface ipv6 ripng metric-offset
```

**Parameters**

- **interface**
  - Mandatory. A type of interface. For detailed keywords and arguments that can be specified as interface types, refer to Supported Interface Types on page 57.

- **metric**
  - Mandatory. A metric to be added to the routes over the interface. The metric ranges from 1 through 16.

**Modes**

Configuration mode

**Configuration Statement**

```
interfaces interface {
  ipv6 {
    ripng {
      metric-offset metric
    }
  }
}
```

**Usage Guidelines**

Use this command to set the metric for inbound and outbound routes on an interface that are beyond the normal operation of RIPng.

Use the **set** form of this command to set a metric to add to routes that are received from RIPng on an interface.

Use the **show** form of this command to display the current metric that is added to routes that are received from RIPng on an interface.
interfaces <interface> ipv6 ripng split-horizon

Configures split-horizon and split-horizon poison-reverse on an interface that is running RIPng.

Syntax
set interfaces interface ipv6 ripng split-horizon [ disable | poison-reverse ]
show interfaces interface ipv6 ripng split-horizon

Command Default
Split-horizon is enabled.

Parameters
interface
Mandatory. A type of interface. For detailed keywords and arguments that can be specified as interface types, refer to Supported Interface Types on page 57.

disable
Disables split-horizon on the specified interface.

poison-reverse
Enables poison-reverse on the specified interface.

Modes
Configuration mode

Configuration Statement
interfaces interface {
  ipv6 {
    ripng {
      split-horizon {
        disable {
          disable
          poison-reverse
        }"n
      }"n
    }"n
  }"n
}

Usage Guidelines
Use this command to disable split-horizon or enable split-horizon poison-reverse on an interface that is running RIPng.

Split-horizon is a stability feature that reduces the possibility of network loops, particularly when links become disconnected. It stops an interface from including in its network updates to any routes that it learned from that interface. Split-horizon is effective at preventing loops between routers that are directly connected to each other, and it speeds convergence when network conditions change. Split-horizon is the default setting in RIPng.

Poison-reverse is a variation of split-horizon. When an interface that has poison-reverse enabled detects a link that is down, it increases the metric for that route to 16 and propagates that information in its next update. Because 15 is the largest number of hops that can be reached on a RIPng network, increasing the metric to 16 renders the route unreachable as far as downstream RIPng routers are concerned. This is called “poisoning” the route. Poison-reverse is useful for propagating information about bad routes to routers that are downstream but not immediate neighbors, where split-horizon is ineffective.

When this option is enabled, the router includes the route in announcements to the neighbor from which it was learned. When this option is disabled, the router omits the route from announcements to the neighbor from which it was learned.

Use the set form of this command to configure split-horizon and split-horizon poison-reverse on an interface that is running RIPng.

Use the show form of this command to display the current configuration of split-horizon.
interfaces <interface> ipv6 ripng neighbor <ip-address>

Configures the IPv6 link-local address of a neighbor for RIPng.

**Syntax**

```
set interfaces interface ipv6 ripng neighbor ip-address
```

```
show interface interface ipv6 ripng neighbor
```

**Parameters**

- **interface**
  A type of interface. For detailed keywords and arguments that can be specified as interface types, refer to Supported Interface Types on page 57.

- **ip-address**
  The IPv6 link-local address of a neighbor.

**Modes**

Configuration mode.

**Configuration Statement**

```
interfaces interface {
  address address {
    ipv6 {
      ripng {
        neighbor ip-address
      }
    }
  }
}
```

**Usage Guidelines**

- Use the **set** form of this command to configure the IPv6 link-local address of a neighbor for RIPng.
- Use the **show** form of this command to display the IPv6 link-local address of the neighbor.
interfaces <interface> ipv6 ripng neighbor <ip-address>
## Supported Interface Types

The following table shows the syntax and parameters of supported interface types. Depending on the command, some of these types may not apply.

<table>
<thead>
<tr>
<th>Interface Type</th>
<th>Syntax</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bridge</td>
<td><code>bridge brx</code></td>
<td><code>brx</code>: The name of a bridge group. The name ranges from br0 through br999.</td>
</tr>
<tr>
<td>Dataplane</td>
<td><code>dataplane interface-name</code></td>
<td><code>interface-name</code>: The name of a dataplane interface. Following are the supported formats of the interface name:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <code>dp&lt;py pz</code> — The name of a dataplane interface, where</td>
</tr>
<tr>
<td></td>
<td></td>
<td>— <code>px</code> specifies the dataplane identifier (ID). Currently, only dp0 is supported.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>— <code>py</code> specifies a physical or virtual PCI slot index (for example, p129).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>— <code>pz</code> specifies a port index (for example, p1). For example, dp0p1p2, dp0p160p1, and dp0p192p1.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <code>dp&lt;em y</code> — The name of a dataplane interface on a LAN-on-motherboard (LOM) device that does not have a PCI slot, where <code>em y</code> specifies an embedded network interface number (typically, a small number). For example, dp0em3.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <code>dp&lt;x y</code> — The name of a dataplane interface on a device that is installed on a virtual PCI slot, where <code>x y</code> specifies an embedded network interface number (typically, a small number). For example, dp0s2. Currently, this format applies only when using the KVM or Hyper-V platforms.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <code>dp&lt;P n p y p z</code> — The name of a dataplane interface on a device that is installed on a secondary PCI bus, where <code>P n</code> specifies the bus number. You can use this format to name dataplane interfaces on large physical devices with multiple PCI buses. For these devices, it is possible to have network interface cards installed on different buses with these cards having the same slot ID. The value of <code>n</code> must be an integer greater than 0. For example, dp0P1p162p1 and dp0P2p162p1.</td>
</tr>
<tr>
<td>Dataplane vif</td>
<td><code>dataplane interface-name vif vif-id [vlan vlan-id]</code></td>
<td><code>interface-name</code>: Refer to the preceding description.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>vif-id</code>: A virtual interface ID. The ID ranges from 1 through 4094.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>vlan-id</code>: The VLAN ID of a virtual interface. The ID ranges from 1 through 4094.</td>
</tr>
<tr>
<td>Loopback</td>
<td><code>loopback lo</code> or <code>loopback l&lt;o n</code></td>
<td><code>n</code>: The name of a loopback interface, where <code>n</code> ranges from 1 through 99999.</td>
</tr>
<tr>
<td>OpenVPN</td>
<td><code>openvpn vtun x</code></td>
<td><code>vtun x</code>: The identifier of an OpenVPN interface. The identifier ranges from vtun0 through vtunx, where <code>x</code> is a nonnegative integer.</td>
</tr>
</tbody>
</table>
### Supported Interface Types

<table>
<thead>
<tr>
<th>Interface Type</th>
<th>Syntax</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tunnel</td>
<td><code>tunnel tunx</code></td>
<td><code>tunx</code>: The identifier of a tunnel interface you are defining. The identifier ranges from tun0 through tunx, where x is a nonnegative integer.</td>
</tr>
<tr>
<td></td>
<td>or</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>tunnel tunx</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>parameters</td>
<td></td>
</tr>
<tr>
<td>Virtual tunnel</td>
<td><code>vti vtix</code></td>
<td><code>vtix</code>: The identifier of a virtual tunnel interface you are defining. The identifier ranges from vti0 through vtix, where x is a nonnegative integer.</td>
</tr>
</tbody>
</table>
| VRRP           | `parent-interface vrrp vrrp-group group` | `parent-interface`: The type and identifier of a parent interface; for example, dataplane dp0p1p2 or bridge br999.  
`group`: A VRRP group identifier.  
The name of a VRRP interface is not specified. The system internally constructs the interface name from the parent interface identifier plus the VRRP group number; for example, dp0p1p2v99. Note that VRRP interfaces support the same feature set as does the parent interface. |

**Note:** This interface does not support IPv6.
# List of Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACL</td>
<td>access control list</td>
</tr>
<tr>
<td>ADSL</td>
<td>Asymmetric Digital Subscriber Line</td>
</tr>
<tr>
<td>AH</td>
<td>Authentication Header</td>
</tr>
<tr>
<td>AMI</td>
<td>Amazon Machine Image</td>
</tr>
<tr>
<td>API</td>
<td>Application Programming Interface</td>
</tr>
<tr>
<td>AS</td>
<td>autonomous system</td>
</tr>
<tr>
<td>ARP</td>
<td>Address Resolution Protocol</td>
</tr>
<tr>
<td>AWS</td>
<td>Amazon Web Services</td>
</tr>
<tr>
<td>BGP</td>
<td>Border Gateway Protocol</td>
</tr>
<tr>
<td>BIOS</td>
<td>Basic Input Output System</td>
</tr>
<tr>
<td>BPDU</td>
<td>Bridge Protocol Data Unit</td>
</tr>
<tr>
<td>CA</td>
<td>certificate authority</td>
</tr>
<tr>
<td>CCMP</td>
<td>AES in counter mode with CBC-MAC</td>
</tr>
<tr>
<td>CHAP</td>
<td>Challenge Handshake Authentication Protocol</td>
</tr>
<tr>
<td>CLI</td>
<td>command-line interface</td>
</tr>
<tr>
<td>DDNS</td>
<td>dynamic DNS</td>
</tr>
<tr>
<td>DHCP</td>
<td>Dynamic Host Configuration Protocol</td>
</tr>
<tr>
<td>DHCPv6</td>
<td>Dynamic Host Configuration Protocol version 6</td>
</tr>
<tr>
<td>DLCI</td>
<td>data-link connection identifier</td>
</tr>
<tr>
<td>DMI</td>
<td>desktop management interface</td>
</tr>
<tr>
<td>DMVPN</td>
<td>dynamic multipoint VPN</td>
</tr>
<tr>
<td>DMZ</td>
<td>demilitarized zone</td>
</tr>
<tr>
<td>DN</td>
<td>distinguished name</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Name System</td>
</tr>
<tr>
<td>DSCP</td>
<td>Differentiated Services Code Point</td>
</tr>
<tr>
<td>DSL</td>
<td>Digital Subscriber Line</td>
</tr>
<tr>
<td>eBGP</td>
<td>external BGP</td>
</tr>
<tr>
<td>EBS</td>
<td>Amazon Elastic Block Storage</td>
</tr>
<tr>
<td>EC2</td>
<td>Amazon Elastic Compute Cloud</td>
</tr>
<tr>
<td>EGP</td>
<td>Exterior Gateway Protocol</td>
</tr>
<tr>
<td>ECMP</td>
<td>equal-cost multipath</td>
</tr>
<tr>
<td>ESP</td>
<td>Encapsulating Security Payload</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>FIB</td>
<td>Forwarding Information Base</td>
</tr>
<tr>
<td>FTP</td>
<td>File Transfer Protocol</td>
</tr>
<tr>
<td>GRE</td>
<td>Generic Routing Encapsulation</td>
</tr>
<tr>
<td>HDLC</td>
<td>High-Level Data Link Control</td>
</tr>
<tr>
<td>I/O</td>
<td>Input/Output</td>
</tr>
<tr>
<td>ICMP</td>
<td>Internet Control Message Protocol</td>
</tr>
<tr>
<td>IDS</td>
<td>Intrusion Detection System</td>
</tr>
<tr>
<td>IEEE</td>
<td>Institute of Electrical and Electronics Engineers</td>
</tr>
<tr>
<td>IGMP</td>
<td>Internet Group Management Protocol</td>
</tr>
<tr>
<td>IGP</td>
<td>Interior Gateway Protocol</td>
</tr>
<tr>
<td>IPS</td>
<td>Intrusion Protection System</td>
</tr>
<tr>
<td>IKE</td>
<td>Internet Key Exchange</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>IPOA</td>
<td>IP over ATM</td>
</tr>
<tr>
<td>IPsec</td>
<td>IP Security</td>
</tr>
<tr>
<td>IPv4</td>
<td>IP Version 4</td>
</tr>
<tr>
<td>IPv6</td>
<td>IP Version 6</td>
</tr>
<tr>
<td>ISAKMP</td>
<td>Internet Security Association and Key Management Protocol</td>
</tr>
<tr>
<td>ISM</td>
<td>Internet Standard Multicast</td>
</tr>
<tr>
<td>ISP</td>
<td>Internet Service Provider</td>
</tr>
<tr>
<td>KVM</td>
<td>Kernel-Based Virtual Machine</td>
</tr>
<tr>
<td>L2TP</td>
<td>Layer 2 Tunneling Protocol</td>
</tr>
<tr>
<td>LACP</td>
<td>Link Aggregation Control Protocol</td>
</tr>
<tr>
<td>LAN</td>
<td>local area network</td>
</tr>
<tr>
<td>LDAP</td>
<td>Lightweight Directory Access Protocol</td>
</tr>
<tr>
<td>LLDP</td>
<td>Link Layer Discovery Protocol</td>
</tr>
<tr>
<td>MAC</td>
<td>medium access control</td>
</tr>
<tr>
<td>mGRE</td>
<td>multipoint GRE</td>
</tr>
<tr>
<td>MIB</td>
<td>Management Information Base</td>
</tr>
<tr>
<td>MLD</td>
<td>Multicast Listener Discovery</td>
</tr>
<tr>
<td>MLPPP</td>
<td>multilink PPP</td>
</tr>
<tr>
<td>MRRU</td>
<td>maximum received reconstructed unit</td>
</tr>
<tr>
<td>MTU</td>
<td>maximum transmission unit</td>
</tr>
<tr>
<td>NAT</td>
<td>Network Address Translation</td>
</tr>
<tr>
<td>NBMA</td>
<td>Non-Broadcast Multi-Access</td>
</tr>
<tr>
<td>ND</td>
<td>Neighbor Discovery</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>NHRP</td>
<td>Next Hop Resolution Protocol</td>
</tr>
<tr>
<td>NIC</td>
<td>network interface card</td>
</tr>
<tr>
<td>NTP</td>
<td>Network Time Protocol</td>
</tr>
<tr>
<td>OSPF</td>
<td>Open Shortest Path First</td>
</tr>
<tr>
<td>OSPFv2</td>
<td>OSPF Version 2</td>
</tr>
<tr>
<td>OSPFv3</td>
<td>OSPF Version 3</td>
</tr>
<tr>
<td>PAM</td>
<td>Pluggable Authentication Module</td>
</tr>
<tr>
<td>PAP</td>
<td>Password Authentication Protocol</td>
</tr>
<tr>
<td>PAT</td>
<td>Port Address Translation</td>
</tr>
<tr>
<td>PCI</td>
<td>peripheral component interconnect</td>
</tr>
<tr>
<td>PIM</td>
<td>Protocol Independent Multicast</td>
</tr>
<tr>
<td>PIM-DM</td>
<td>PIM Dense Mode</td>
</tr>
<tr>
<td>PIM-SM</td>
<td>PIM Sparse Mode</td>
</tr>
<tr>
<td>PKI</td>
<td>Public Key Infrastructure</td>
</tr>
<tr>
<td>PPP</td>
<td>Point-to-Point Protocol</td>
</tr>
<tr>
<td>PPPoA</td>
<td>PPP over ATM</td>
</tr>
<tr>
<td>PPPoE</td>
<td>PPP over Ethernet</td>
</tr>
<tr>
<td>PPTP</td>
<td>Point-to-Point Tunneling Protocol</td>
</tr>
<tr>
<td>PTMU</td>
<td>Path Maximum Transfer Unit</td>
</tr>
<tr>
<td>PVC</td>
<td>permanent virtual circuit</td>
</tr>
<tr>
<td>QoS</td>
<td>quality of service</td>
</tr>
<tr>
<td>RADIUS</td>
<td>Remote Authentication Dial-In User Service</td>
</tr>
<tr>
<td>RHEL</td>
<td>Red Hat Enterprise Linux</td>
</tr>
<tr>
<td>RIB</td>
<td>Routing Information Base</td>
</tr>
<tr>
<td>RIP</td>
<td>Routing Information Protocol</td>
</tr>
<tr>
<td>RIPng</td>
<td>RIP next generation</td>
</tr>
<tr>
<td>RP</td>
<td>Rendezvous Point</td>
</tr>
<tr>
<td>RPF</td>
<td>Reverse Path Forwarding</td>
</tr>
<tr>
<td>RSA</td>
<td>Rivest, Shamir, and Adleman</td>
</tr>
<tr>
<td>Rx</td>
<td>receive</td>
</tr>
<tr>
<td>S3</td>
<td>Amazon Simple Storage Service</td>
</tr>
<tr>
<td>SLAAC</td>
<td>Stateless Address Auto-Configuration</td>
</tr>
<tr>
<td>SNMP</td>
<td>Simple Network Management Protocol</td>
</tr>
<tr>
<td>SMTP</td>
<td>Simple Mail Transfer Protocol</td>
</tr>
<tr>
<td>SONET</td>
<td>Synchronous Optical Network</td>
</tr>
<tr>
<td>SPT</td>
<td>Shortest Path Tree</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>------------------------------------</td>
</tr>
<tr>
<td>SSH</td>
<td>Secure Shell</td>
</tr>
<tr>
<td>SSID</td>
<td>Service Set Identifier</td>
</tr>
<tr>
<td>SSM</td>
<td>Source-Specific Multicast</td>
</tr>
<tr>
<td>STP</td>
<td>Spanning Tree Protocol</td>
</tr>
<tr>
<td>TACACS+</td>
<td>Terminal Access Controller Access Control System Plus</td>
</tr>
<tr>
<td>TBF</td>
<td>Token Bucket Filter</td>
</tr>
<tr>
<td>TCP</td>
<td>Transmission Control Protocol</td>
</tr>
<tr>
<td>TKIP</td>
<td>Temporal Key Integrity Protocol</td>
</tr>
<tr>
<td>ToS</td>
<td>Type of Service</td>
</tr>
<tr>
<td>TSS</td>
<td>TCP Maximum Segment Size</td>
</tr>
<tr>
<td>Tx</td>
<td>transmit</td>
</tr>
<tr>
<td>UDP</td>
<td>User Datagram Protocol</td>
</tr>
<tr>
<td>VHD</td>
<td>virtual hard disk</td>
</tr>
<tr>
<td>vif</td>
<td>virtual interface</td>
</tr>
<tr>
<td>VLAN</td>
<td>virtual LAN</td>
</tr>
<tr>
<td>VPC</td>
<td>Amazon virtual private cloud</td>
</tr>
<tr>
<td>VPN</td>
<td>virtual private network</td>
</tr>
<tr>
<td>VRRP</td>
<td>Virtual Router Redundancy Protocol</td>
</tr>
<tr>
<td>WAN</td>
<td>wide area network</td>
</tr>
<tr>
<td>WAP</td>
<td>wireless access point</td>
</tr>
<tr>
<td>WPA</td>
<td>Wired Protected Access</td>
</tr>
</tbody>
</table>