

Tunnel Properties



Published: 2013-08-29

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

This product includes the Envoy SNMP Engine, developed by Epilogue Technology, an Integrated Systems Company. Copyright © 1986-1997, Epilogue Technology Corporation. All rights reserved. This program and its documentation were developed at private expense, and no part of them is in the public domain.

This product includes memory allocation software developed by Mark Moraes, copyright © 1988, 1989, 1993, University of Toronto.

This product includes FreeBSD software developed by the University of California, Berkeley, and its contributors. All of the documentation and software included in the 4.4BSD and 4.4BSD-Lite Releases is copyrighted by the Regents of the University of California. Copyright © 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994. The Regents of the University of California. All rights reserved.

GateD software copyright © 1995, the Regents of the University. All rights reserved. Gate Daemon was originated and developed through release 3.0 by Cornell University and its collaborators. Gated is based on Kirton's EGP, UC Berkeley's routing daemon (routed), and DCN's HELLO routing protocol. Development of Gated has been supported in part by the National Science Foundation. Portions of the GateD software copyright © 1988, Regents of the University of California. All rights reserved. Portions of the GateD software copyright © 1991, D. L. S. Associates.

This product includes software developed by Maker Communications, Inc., copyright © 1996, 1997, Maker Communications, Inc.

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.

Products made or sold by Juniper Networks or components thereof might be covered by one or more of the following patents that are owned by or licensed to Juniper Networks: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186, and 6,590,785.

Tunnel Properties

Copyright © 2013, 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	vii
	Documentation and Release Notes	vii
	Supported Platforms	vii
	Using the Examples in This Manual	vii
	Merging a Full Example	viii
	Merging a Snippet	viii
	Documentation Conventions	ix
	Documentation Feedback	xi
	Requesting Technical Support	xi
	Self-Help Online Tools and Resources	xi
	Opening a Case with JTAC	xii
Part 1	Overview	
Chapter 1	Tunnel Services	3
	Tunnel Services Overview	3
	GRE Keepalive Time Overview	6
Part 2	Configuration	
Chapter 2	Configuration Tasks	9
	Configuring Unicast Tunnels	9
	Configuring a Key Number on GRE Tunnels	11
	Enabling Fragmentation on GRE Tunnels	12
	Specifying an MTU Setting for the Tunnel	13
	Configuring a GRE Tunnel to Copy ToS Bits to the Outer IP Header	13
	Configuring Packet Reassembly	13
	Configuring GRE Keepalive Time	14
	Configuring Keepalive Time and Hold time for a GRE Tunnel Interface	14
	Display GRE Keepalive Time Configuration	15
	Display Keepalive Time Information on a GRE Tunnel Interface	15
	Restricting Tunnels to Multicast Traffic	17
	Configuring Logical Tunnel Interfaces	17
	Connecting Logical Systems	18
	Configuring Tunnel Interfaces for Routing Table Lookup	19
	Configuring Virtual Loopback Tunnels for VRF Table Lookup	19
	Configuring PIM Tunnels	21
	Configuring IPv6-over-IPv4 Tunnels	22
	Configuring Dynamic Tunnels	22
	Configuring Tunnel Interfaces on MX Series Routers	23
	Configuring Tunnel Interfaces on T4000 Routers	24

Chapter 3	Examples	27
	Examples: Configuring Unicast Tunnels	27
	Example: Configuring a Virtual Loopback Tunnel for VRF Table Lookup	28
	Example: Configuring an IPv6-over-IPv4 Tunnel	29
	Example: Configuring Logical Tunnels	30
Chapter 4	Configuration Statements	33
	allow-fragmentation	33
	backup-destination	34
	copy-tos-to-outer-ip-header	34
	destination (Tunnel Remote End)	35
	destination (Routing Instance)	35
	destination-networks	36
	do-not-fragment	37
	dynamic-tunnels	38
	hold-time (OAM)	39
	interfaces	39
	keepalive-time	40
	key	41
	multicast-only	41
	peer-unit	42
	reassemble-packets	42
	routing-instance	43
	routing-instances	43
	routing-options	44
	source	44
	source-address	45
	ttl	45
	tunnel	46
	unit (Interfaces)	47
Part 3	Administration	
Chapter 5	Tunnel Services Interface Operational Mode Commands	51
	show interfaces (GRE)	52
	show interfaces (IP-over-IP)	59
	show interfaces (Logical Tunnel)	64
	show interfaces (Multicast Tunnel)	69
	show interfaces (PIM)	74
	show interfaces (Virtual Loopback Tunnel)	78
Part 4	Index	
	Index	85

List of Tables

	About the Documentation	vii
	Table 1: Notice Icons	ix
	Table 2: Text and Syntax Conventions	ix
Part 1	Overview	
Chapter 1	Tunnel Services	3
	Table 3: Tunnel Interface Types	3
Part 2	Configuration	
Chapter 2	Configuration Tasks	9
	Table 4: Methods for Configuring Egress Filtering	20
Part 3	Administration	
Chapter 5	Tunnel Services Interface Operational Mode Commands	51
	Table 5: GRE show interfaces Output Fields	53
	Table 6: IP-over-IP show interfaces Output Fields	59
	Table 7: Logical Tunnel show interfaces Output Fields	64
	Table 8: Multicast Tunnel show interfaces Output Fields	70
	Table 9: PIM show interfaces Output Fields	74
	Table 10: Virtual Loopback Tunnel show interfaces Output Fields	78

About the Documentation

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

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:

- M Series
- T Series
- MX 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 ix 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.

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

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the configure command: user@host> configure
Fixed-width text like this	Represents output that appears on the terminal screen.	user@host> show chassis alarms No alarms currently active

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

Convention	Description	Examples
<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)	Enclose 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)	Enclose a variable for which you can substitute one or more values.	community name members [<i>community-ids</i>]
Indentation and braces ({ })	Identify 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.
> (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 send your comments to techpubs-comments@juniper.net, or fill out the documentation feedback form at <https://www.juniper.net/cgi-bin/docbugreport/>. If you are using e-mail, be sure to include the following information with your comments:

- Document or topic name
- URL or page number
- Software release 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 JNASC 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: <https://www.juniper.net/alerts/>

- 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

- [Tunnel Services on page 3](#)

CHAPTER 1

Tunnel Services

- [Tunnel Services Overview on page 3](#)
- [GRE Keepalive Time Overview on page 6](#)

Tunnel Services Overview

By encapsulating arbitrary packets inside a transport protocol, tunneling provides a private, secure path through an otherwise public network. Tunnels connect discontinuous subnetworks and enable encryption interfaces, virtual private networks (VPNs), and MPLS. If you have a Tunnel Physical Interface Card (PIC) installed in your M Series or T Series router, you can configure unicast, multicast, and logical tunnels.

You can configure two types of tunnels for VPNs: one to facilitate routing table lookups and another to facilitate VPN routing and forwarding instance (VRF) table lookups.

For information about encryption interfaces, see *Configuring Encryption Interfaces* and the *Junos OS Administration Library for Routing Devices*. For information about VPNs, see the *Junos OS VPNs Library for Routing Devices*. For information about MPLS, see the *Junos OS MPLS Applications Library for Routing Devices*.

On SRX Series and J Series devices, Generic Routing Encapsulation (GRE) and IP-IP tunnels use internal interfaces, `gr-0/0/0` and `ip-0/0/0`, respectively. The Junos OS creates these interfaces at system bootup; they are not associated with physical interfaces.

The Juniper Networks Junos OS supports the tunnel types shown in [Table 3 on page 3](#).

Table 3: Tunnel Interface Types

Interface	Description
<code>gr-0/0/0</code>	<p>Configurable generic routing encapsulation (GRE) interface. GRE allows the encapsulation of one routing protocol over another routing protocol.</p> <p>Within a router, packets are routed to this internal interface, where they are first encapsulated with a GRE packet and then re-encapsulated with another protocol packet to complete the GRE. The GRE interface is an internal interface only and is not associated with a physical interface. You must configure the interface for it to perform GRE.</p>

Table 3: Tunnel Interface Types (*continued*)

Interface	Description
gre	<p>Internally generated GRE interface. This interface is generated by the Junos OS to handle GRE.</p> <p>NOTE: You can configure GRE interfaces (gre-x/y/z) only for GMPLS control channels. GRE interfaces are not supported or configurable for other applications. This type of interface does not require a Tunnel PIC. For more information about GMPLS, see the <i>Junos OS MPLS Applications Library for Routing Devices</i> and the <i>Junos OS Feature Guides</i>.</p>
ip-0/0/0	<p>Configurable IP-over-IP encapsulation (also called IP tunneling) interface. IP tunneling allows the encapsulation of one IP packet over another IP packet.</p> <p>Packets are routed to an internal interface where they are encapsulated with an IP packet and then forwarded to the encapsulating packet's destination address. The IP-IP interface is an internal interface only and is not associated with a physical interface. You must configure the interface for it to perform IP tunneling.</p>
ipip	Internally generated IP-over-IP interface. This interface is generated by the Junos OS to handle IP-over-IP encapsulation. It is not a configurable interface.
lt-0/0/0	<p>The lt interface on M Series and T Series routers supports configuration of logical systems—the capability to partition a single physical router into multiple logical devices that perform independent routing tasks.</p> <p>On SRX Series devices, the lt interface is a configurable logical tunnel interface that interconnects logical systems. See the <i>Junos OS Logical Systems Configuration Guide for Security Devices</i>.</p> <p>On J Series devices, the lt interface is used to provide class-of-service (CoS) support for real-time performance monitoring (RPM) probe packets. Packets are routed to this internal interface for services. The lt interface is an internal interface only; it is not associated with a physical interface. You must configure the interface for it to perform CoS for RPM services. See the <i>Junos OS Class of Service Configuration Guide for Security Devices</i>.</p>
mt-0/0/0	<p>Internally generated multicast tunnel interface. Multicast tunnels filter all unicast packets; if an incoming packet is not destined for a 224/8-or-greater prefix, the packet is dropped and a counter is incremented.</p> <p>Within a router, packets are routed to this internal interface for multicast filtering. The multicast tunnel interface is an internal interface only and is not associated with a physical interface. If your router has a Tunnel Services PIC, the Junos OS automatically configures one multicast tunnel interface (mt-) for each virtual private network (VPN) you configure. You do not need to configure multicast tunnel interfaces. However, you can configure properties on mt- interfaces, such as the multicast-only statement.</p>
mtun	Internally generated multicast tunnel interface. This interface is generated by the Junos OS to handle multicast tunnel services. It is not a configurable interface.

Table 3: Tunnel Interface Types (*continued*)

Interface	Description
pd-0/0/0	<p>Configurable Protocol Independent Multicast (PIM) de-encapsulation interface. In PIM sparse mode, the first-hop router encapsulates packets destined for the rendezvous point router. The packets are encapsulated with a unicast header and are forwarded through a unicast tunnel to the rendezvous point. The rendezvous point then de-encapsulates the packets and transmits them through its multicast tree.</p> <p>Within a router, packets are routed to this internal interface for de-encapsulation. The PIM de-encapsulation interface is an internal interface only and is not associated with a physical interface. You must configure the interface for it to perform PIM de-encapsulation.</p> <p>NOTE: On SRX Series devices, this interface type is ppd0.</p>
pe-0/0/0	<p>Configurable PIM encapsulation interface. In PIM sparse mode, the first-hop router encapsulates packets destined for the rendezvous point router. The packets are encapsulated with a unicast header and are forwarded through a unicast tunnel to the rendezvous point. The rendezvous point then de-encapsulates the packets and transmits them through its multicast tree.</p> <p>Within a router, packets are routed to this internal interface for encapsulation. The PIM encapsulation interface is an internal interface only and is not associated with a physical interface. You must configure the interface for it to perform PIM encapsulation.</p> <p>NOTE: On SRX Series devices, this interface type is ppe0.</p>
pimd	Internally generated PIM de-encapsulation interface. This interface is generated by the Junos OS to handle PIM de-encapsulation. It is not a configurable interface.
pime	Internally generated PIM encapsulation interface. This interface is generated by the Junos OS to handle PIM encapsulation. It is not a configurable interface.
vt-0/0/0	<p>Configurable virtual loopback tunnel interface. Facilitates VRF table lookup based on MPLS labels. This interface type is supported on M Series and T Series routers, but not on SRX Series or J Series devices.</p> <p>To configure a virtual loopback tunnel to facilitate VRF table lookup based on MPLS labels, you specify a virtual loopback tunnel interface name and associate it with a routing instance that belongs to a particular routing table. The packet loops back through the virtual loopback tunnel for route lookup.</p>

Related Documentation

- [GRE Keepalive Time Overview on page 6](#)
- [Configuring Unicast Tunnels on page 9](#)
- [Restricting Tunnels to Multicast Traffic on page 17](#)
- [Configuring Tunnel Interfaces on MX Series Routers on page 23](#)
- [Configuring Tunnel Interfaces on T4000 Routers on page 24](#)

GRE Keepalive Time Overview

Generic routing encapsulation (GRE) tunnel interfaces do not have a built-in mechanism for detecting when a tunnel is down. You can enable keepalive messages to serve as the detection mechanism.

Keepalives can be configured on the physical or on the logical interface. If configured on the physical interface, keepalives are sent on all logical interfaces that are part of the physical interface. If configured on a individual logical interface, keepalives are only sent to that logical interface. In addition to configuring a keepalive, you must configure the hold time.

- Related Documentation**
- [Configuring GRE Keepalive Time on page 14](#)
 - [keepalive-time on page 40](#)
 - [hold-time \(OAM\) on page 39](#)

PART 2

Configuration

- [Configuration Tasks on page 9](#)
- [Examples on page 27](#)
- [Configuration Statements on page 33](#)

CHAPTER 2

Configuration Tasks

- [Configuring Unicast Tunnels on page 9](#)
- [Configuring GRE Keepalive Time on page 14](#)
- [Restricting Tunnels to Multicast Traffic on page 17](#)
- [Configuring Logical Tunnel Interfaces on page 17](#)
- [Configuring Tunnel Interfaces for Routing Table Lookup on page 19](#)
- [Configuring Virtual Loopback Tunnels for VRF Table Lookup on page 19](#)
- [Configuring PIM Tunnels on page 21](#)
- [Configuring IPv6-over-IPv4 Tunnels on page 22](#)
- [Configuring Dynamic Tunnels on page 22](#)
- [Configuring Tunnel Interfaces on MX Series Routers on page 23](#)
- [Configuring Tunnel Interfaces on T4000 Routers on page 24](#)

Configuring Unicast Tunnels

To configure a unicast tunnel, you configure a **gr-** interface (to use GRE encapsulation) or an **ip-** interface (to use IP-IP encapsulation) and include the **tunnel** and **family** statements:

```
gr-fpc/pic/port or ip-fpc/pic/port {  
  unit logical-unit-number {  
    copy-tos-to-outer-ip-header;  
    reassemble-packets;  
    tunnel {  
      allow-fragmentation;  
      backup-destination address;  
      destination destination-address;  
      do-not-fragment;  
      key number;  
      routing-instance {  
        destination routing-instance-name;  
      }  
      source address;  
      ttl number;  
    }  
    family family {  
      address address {
```

```
        destination address;  
    }  
}  
}
```

You can configure these statements at the following hierarchy levels:

- [edit interfaces]
- [edit logical-systems *logical-system-name* interfaces]

You can configure multiple logical units for each GRE or IP-IP interface, and you can configure only one tunnel per unit.



NOTE: On M Series and T Series routers, you can configure the interface on a service PIC or a tunnel PIC. On MX Series routers, configure the interface on a Multiservices DPC.

Each tunnel interface must be a point-to-point interface. Point to point is the default interface connection type, so you do not need to include the **point-to-point** statement in the logical interface configuration.

You must specify the tunnel's destination and source addresses. The remaining statements are optional.



NOTE: For transit packets exiting the tunnel, forwarding path features, such as reverse path forwarding (RPF), forwarding table filtering, source class usage, destination class usage, and stateless firewall filtering, are not supported on the interfaces you configure as tunnel sources, but are supported on tunnel-pic interfaces.

However, class-of-service (CoS) information obtained from the GRE or IP-IP header is carried over the tunnel and is used by the re-entering packets. For more information, see the *Junos OS Class of Service Library for Routing Devices*.

To prevent an invalid configuration, the Junos OS disallows setting the address specified by the source or destination statement at the [edit interfaces *gr-fpc/pic/port* unit *logical-unit-number* tunnel] hierarchy level to be the same as the interface's own subnet address, specified by the address statement at the [edit interfaces *gr-fpc/pic/port* unit *logical-unit-number* family *family-name*] hierarchy level.

To set the time-to-live (TTL) field that is included in the encapsulating header, include the **ttl** statement. If you explicitly configure a TTL value for the tunnel, you must configure it to be one larger than the number of hops in the tunnel. For example, if the tunnel has seven hops, you must configure a TTL value of 8.

You must configure at least one family on the logical interface. To enable MPLS over GRE tunnel interfaces, you must include the **family mpls** statement in the GRE interface configuration. In addition, you must include the appropriate statements at the **[edit protocols]** hierarchy level to enable Resource Reservation Protocol (RSVP), MPLS, and label-switched paths (LSPs) over GRE tunnels. Unicast tunnels are bidirectional.

A configured tunnel cannot go through Network Address Translation (NAT) at any point along the way to the destination. For more information, see [“Examples: Configuring Unicast Tunnels” on page 27](#) and the *Junos OS MPLS Applications Library for Routing Devices*.

For a GRE tunnel, the default is to set the ToS bits in the outer IP header to all zeros. To have the Routing Engine copy the ToS bits from the inner IP header to the outer, include the **copy-tos-bits-to-outer-ip-header** statement. (This inner-to-outer ToS bits copying is already the default behavior for IP-IP tunnels.)

For GRE tunnel interfaces on Adaptive Services or Multiservices interfaces, you can configure additional tunnel attributes, as described in the following sections:

- [Configuring a Key Number on GRE Tunnels on page 11](#)
- [Enabling Fragmentation on GRE Tunnels on page 12](#)
- [Specifying an MTU Setting for the Tunnel on page 13](#)
- [Configuring a GRE Tunnel to Copy ToS Bits to the Outer IP Header on page 13](#)
- [Configuring Packet Reassembly on page 13](#)

Configuring a Key Number on GRE Tunnels

For Adaptive Services and Multiservices interfaces on M Series and T Series routers, you can assign a key value to identify an individual traffic flow within a GRE tunnel, as defined in RFC 2890, *Key and Sequence Number Extensions to GRE*. However, only one key is allowed for each tunnel source and destination pair.

Each IP version 4 (IPv4) packet entering the tunnel is encapsulated with the GRE tunnel key value. Each IPv4 packet exiting the tunnel is verified by the GRE tunnel key value and de-encapsulated. The Adaptive Services or Multiservices PIC drops packets that do not match the configured key value.

To assign a key value to a GRE tunnel interface, include the **key** statement:

```
key number;
```

You can include this statement at the following hierarchy levels:

- **[edit interfaces *interface-name* unit *logical-unit-number* tunnel]**
- **[edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number* tunnel]**

The key number can be 0 through 4,294,967,295. You must configure the same GRE tunnel key value on tunnel endpoints.

The following example illustrates the use of the `key` statement in a GRE tunnel configuration:

```
interfaces {
  gr-1/2/0 {
    unit 0 {
      tunnel {
        source 10.58.255.193;
        destination 10.58.255.195;
        key 1234;
      }
      ...
      family inet {
        mtu 1500;
        address 10.200.0.1/30;
      }
      ...
    }
  }
}
```

Enabling Fragmentation on GRE Tunnels

For GRE tunnel interfaces on Adaptive Services and Multiservices interfaces only, you can enable fragmentation of IPv4 packets in GRE tunnels.

By default, IPv4 traffic transmitted over GRE tunnels is not fragmented. To enable fragmentation of IPv4 packets in GRE tunnels, include the **clear-dont-fragment-bit** statement:

```
clear-dont-fragment-bit;
```

You can include this statement at the following hierarchy levels:

- [edit interfaces *interface-name* unit *logical-unit-number*]
- [edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number*]

When you include the **clear-dont-fragment-bit** statement in the configuration, the don't-fragment (DF) bit is cleared on all packets, even packets that do not exceed the tunnel maximum transmission unit (MTU). If the packet's size exceeds the tunnel's MTU value, the packet is fragmented before encapsulation. If the packet's size does not exceed the tunnel's MTU value, the packet is not fragmented.



NOTE: The Packet Forwarding Engine updates the IP identification field in the outer IP header of GRE-encapsulated packets, so that reassembly of the packets is possible after fragmentation. The previous CLI constraint check that required you to configure either the **clear-dont-fragment-bit** statement or a tunnel key with the **allow-fragmentation** statement is no longer enforced.

You can also clear the DF bit in packets transmitted over IP Security (IPsec) tunnels. For more information, see *Enabling IPsec Packet Fragmentation*.

Specifying an MTU Setting for the Tunnel

To enable key numbers and fragmentation on GRE tunnels (as described in “[Configuring a Key Number on GRE Tunnels](#)” on page 11 and “[Enabling Fragmentation on GRE Tunnels](#)” on page 12), you must also specify an MTU setting for the tunnel.

To specify an MTU setting for the tunnel, include the **mtu** statement:

```
mtu bytes;
```

You can include this statement at the following hierarchy levels:

- [edit interfaces *gr-fpc/pic/port* unit *logical-unit-number* family inet]
- [edit logical-system *logical-system-name* interfaces *gr-fpc/pic/port* unit *logical-unit-number* family inet]

For more information about MTU settings, see the *Junos OS Network Interfaces Library for Routing Devices*.

Configuring a GRE Tunnel to Copy ToS Bits to the Outer IP Header

Unlike IP-IP tunnels, GRE tunnels do not copy the ToS bits to the outer IP header by default. To have the Routing Engine copy the inner ToS bits to the outer IP header (which is required for some tunneled routing protocols) on packets sent by the Routing Engine, include the **copy-tos-to-outer-ip-header** statement at the logical unit hierarchy level of a GRE interface. This example copies the inner ToS bits to the outer IP header on a GRE tunnel:

```
[edit interfaces]
gr-0/0/0 {
  unit 0 {
    copy-tos-to-outer-ip-header;
    family inet;
  }
}
```

Configuring Packet Reassembly

On GRE tunnel interfaces only, you can enable reassembly of fragmented tunnel packets. To activate this capability, include the **reassemble-packets** statement:

```
reassemble-packets;
```

You can configure this statement at the following hierarchy levels:

- [edit interfaces *interface-name* unit *logical-unit-number*]
- [edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number*]

For each tunnel you configure on the interface, you can enable or disable fragmentation of GRE packets by including the **allow-fragmentation** or **do-not-fragment** statement:

```
allow-fragmentation;
```

`do-not-fragment;`

You can configure these statements at the following hierarchy levels:

- [edit interfaces *interface-name* unit *logical-unit-number* tunnel]
- [edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number* tunnel]

If you configure **allow-fragmentation** on a tunnel, it clears the DF bit in the outer IP header, enabling post fragmentation of GRE-encapsulated packets if the packet size exceeds the maximum transmission unit (MTU) value for the egress interface. By default, packets that exceed the MTU size are dropped and post fragmentation of GRE packets is disabled.



NOTE: Whenever you configure **allow-fragmentation** on a tunnel, you must also include either the tunnel key or the **clear-dont-fragment-bit** statement. This configuration enables the router to send affected packets to the PIC so that the correct IP header can be placed in the fragments. Otherwise, on the reassembly side some packets might be lost when fragments arrive in the PIC out of sequence at high speeds.

**Related
Documentation**

- [Tunnel Services Overview on page 3](#)
- [Examples: Configuring Unicast Tunnels on page 27](#)

Configuring GRE Keepalive Time

- [Configuring Keepalive Time and Hold time for a GRE Tunnel Interface on page 14](#)
- [Display GRE Keepalive Time Configuration on page 15](#)
- [Display Keepalive Time Information on a GRE Tunnel Interface on page 15](#)

Configuring Keepalive Time and Hold time for a GRE Tunnel Interface

You can configure the keepalives on a generic routing encapsulation (GRE) tunnel interface by including both the **keepalive-time** statement and the **hold-time** statement at the [edit protocols oam gre-tunnel interface *interface-name*] hierarchy level.



NOTE: For proper operation of keepalives on a GRE interface, you must also include the **family inet** statement at the [edit interfaces *interface-name* unit *unit*] hierarchy level. If you do not include this statement, the interface is marked as down.

To configure a GRE tunnel interface:

1. Configure the GRE tunnel interface at [edit interfaces *interface-name* unit *unit-number*] hierarchy level, where the interface name is gr-x/y/z, and the family is set as **inet**.
`user@host# set interfaces interface-name unit unit-number family family-name`

2. Configure the rest of the GRE tunnel interface options as explained in *Configuring a GRE Tunnel Interface Between a PE and CE Router* or *Configuring a GRE Tunnel Interface Between PE Routers* based on requirement.

To configure keepalive time for a GRE tunnel interface:

- 1.
2. Configure the Operation, Administration, and Maintenance (OAM) protocol at the **[edit protocols]** hierarchy level for the GRE tunnel interface.


```
[edit]
user@host# edit protocols oam
```
3. Configure the GRE tunnel interface option for OAM protocol.


```
[edit protocols oam]
user@host# edit gre-tunnel interface interface-name
```
4. Configure the keepalive time from 1 through 50 seconds for the GRE tunnel interface.


```
[edit protocols oam gre-tunnel interface interface-name]
user@host# set keepalive-time seconds
```
5. Configure the hold time from 5 through 250 seconds. Note that the hold time must be at least twice the keepalive time.


```
[edit protocols oam gre-tunnel interface interface-name]
user@host# set hold-time (OAM) seconds
```

Display GRE Keepalive Time Configuration

Purpose Display the configured keepalive time value as 10 and hold time value as 30 on a GRE tunnel interface (for example, gr-1/1/10.1):

Action To display the configured values on the GRE tunnel interface, run the **show oam gre-tunnel** command at the **[edit protocols]** hierarchy level:

```
[edit protocols]
user@host# show oam gre-tunnel
interface gr-1/1/10.1 {
  keepalive-time 10;
  hold-time 30;
}
```

Display Keepalive Time Information on a GRE Tunnel Interface

Purpose Display the current status information of a GRE tunnel interface when keepalive time and hold time parameters are configured on it and when the hold time expires.

Action To verify the current status information on a GRE tunnel interface (for example, gr-3/3/0.3), run the **show interfaces gr-3/3/0.3 terse** and **show interfaces gr-3/3/0.3 extensive** operational commands.

show interfaces gr-3/3/0.3 terse

```
user@host> show interfaces gr-3/3/0.3 terse
```

Interface	Admin	Link	Proto	Local	Remote
gr-3/3/0.3	up	up	inet mpls	200.1.3.1/24	

```
show interfaces gr-3/3/0.3 extensive
```

```

user@host> show interfaces gr-3/3/0.3 extensive
Logical interface gr-3/3/0.3 (Index 73) (SNMP ifIndex 594) (Generation 900)
  Flags: Point-To-Point SNMP-Traps 0x4000 IP-Header
10.1.19.11:10.1.19.12:47:df:64:0000000000000000 Encapsulation: GRE-NULL
  Gre keepalives configured: On, Gre keepalives adjacency state: down
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
  Traffic statistics:
    Input bytes : 15629992
    Output bytes : 15912273
    Input packets: 243813
    Output packets: 179476
  Local statistics:
    Input bytes : 15322586
    Output bytes : 15621359
    Input packets: 238890
    Output packets: 174767
  Transit statistics:
    Input bytes : 307406 0 bps
    Output bytes : 290914 0 bps
    Input packets: 4923 0 pps
    Output packets: 4709 0 pps
  Protocol inet, MTU: 1476, Generation: 1564, Route table: 0
    Flags: Sendbcast-pkt-to-re
    Addresses, Flags: Dest-route-down Is-Preferred Is-Primary
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
    Destination: 200.1.3/24, Local: 200.1.3.1, Broadcast: 200.1.3.255,
  Generation: 1366
  Protocol mpls, MTU: 1464, Maximum labels: 3, Generation: 1565, Route table:
0

```



NOTE:

When the hold time expires:

- The GRE tunnel will stay up even though the interface cannot send or receive traffic.
- The Link status will be Up and the Gre keepalives adjacency state will be Down.

Meaning	The current status information of a GRE tunnel interface with keepalive time and hold time parameters is displayed as expected when the hold time expires.
----------------	--

Related Documentation

- [GRE Keepalive Time Overview on page 6](#)
- [keepalive-time on page 40](#)
- [hold-time \(OAM\) on page 39](#)

Restricting Tunnels to Multicast Traffic

For interfaces that carry IPv4 or IP version 6 (IPv6) traffic, you can configure a tunnel interface to allow multicast traffic only. To configure a multicast-only tunnel, include the **multicast-only** statement:

```
multicast-only;
```

You can configure this statement at the following hierarchy levels:

- [edit interfaces *interface-name* unit *logical-unit-number* family *family*]
- [edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number* family *family*]

Multicast tunnels filter all unicast packets; if an incoming packet is not destined for a 224/8 or greater prefix, the packet is dropped and a counter is incremented.

You can configure this property on GRE, IP-IP, PIM, and multicast tunnel (**mt**) interfaces only.



NOTE: If your router has a Tunnel Services PIC, the Junos OS automatically configures one multicast tunnel interface (**mt**) for each virtual private network (VPN) you configure. You do not need to configure multicast tunnel interfaces.

Related Documentation

- [Tunnel Services Overview on page 3](#)
- [Configuring Unicast Tunnels on page 9](#)

Configuring Logical Tunnel Interfaces

Logical tunnel (**lt-**) interfaces provide quite different services depending on the host router:

- On M Series, MX Series, and T Series routers, logical tunnel interfaces allow you to connect logical systems, virtual routers, or VPN instances. M Series and T Series routers must be equipped with a Tunnel Services PIC or an Adaptive Services Module (only available on M7i routers). MX Series routers must be equipped with a Trio MPC/MIC module. For more information about connecting these applications, see the *Junos OS VPNs Library for Routing Devices*.
- On SRX Series Services Gateways, the logical tunnel interface is used to interconnect logical systems. See the *Junos OS Logical Systems Configuration Guide for Security Devices*.
- On J Series Services Routers, the logical tunnel interface is used to provide class-of-service (CoS) support for real-time performance monitoring (RPM) probe packets. Packets are routed to this internal interface for services. See the *Junos OS Class of Service Configuration Guide for Security Devices*.

For M Series, MX Series, and T Series routers, see the following section:

- [Connecting Logical Systems on page 18](#)

Connecting Logical Systems

To connect two logical systems, you configure a logical tunnel interface on both logical systems. Then you configure a peer relationship between the logical tunnel interfaces, thus creating a point-to-point connection.

To configure a point-to-point connection between two logical systems, configure the logical tunnel interface by including the **lt-fpc/pic/port** statement:

```
lt-fpc/pic/port {  
  unit logical-unit-number {  
    encapsulation encapsulation;  
    peer-unit unit-number; # peering logical system unit number  
    dlcil dlcil-number;  
    family (inet | inet6 | iso | mpls);  
  }  
}
```

You can include this statement at the following hierarchy levels:

- **[edit interfaces]**
- **[edit logical-systems *logical-system-name* interfaces]**

When configuring logical tunnel interfaces, note the following:

- You can configure each logical tunnel interface with one of the following encapsulation types: Ethernet, Ethernet circuit cross-connect (CCC), Ethernet VPLS, Frame Relay, Frame Relay CCC, VLAN, VLAN CCC, or VLAN VPLS.
- You can configure the IP, IPv6, International Organization for Standardization (ISO), or MPLS protocol family.
- The peering logical interfaces must belong to the same logical tunnel interface derived from the Tunnel Services PIC or Adaptive Services Module.
- You can configure only one peer unit for each logical interface. For example, unit 0 cannot peer with both unit 1 and unit 2.
- To enable the logical tunnel interface, you must configure at least one physical interface statement.
- Logical tunnels are not supported with Adaptive Services, Multiservices, or Link Services PICs (but they are supported on the Adaptive Services Module on M7i routers, as noted above).
- On M Series routers other than the M40e router, logical tunnel interfaces require an Enhanced Flexible PIC Concentrator (FPC).
- On MX Series routers, logical tunnel interfaces require Trio MPC/MIC modules. They do not require a Tunnel Services PIC in the same system.

For more information about configuring logical systems, see the *Junos OS Routing Protocols Library for Routing Devices*.

- Related Documentation**
- [Tunnel Services Overview on page 3](#)
 - [Example: Configuring Logical Tunnels on page 30](#)

Configuring Tunnel Interfaces for Routing Table Lookup

To configure tunnel interfaces to facilitate routing table lookups for VPNs, you specify a tunnel's endpoint IP addresses and associate them with a routing instance that belongs to a particular routing table. This enables the Junos OS to search in the appropriate routing table for the route prefix, because the same prefix can appear in multiple routing tables. To configure the destination VPN, include the **routing-instance** statement:

```
routing-instance {
  destination routing-instance-name;
}
```

You can include this statement at the following hierarchy levels:

- **[edit interfaces gr-fpc/pic/port unit logical-unit-number tunnel]**
- **[edit logical-systems logical-system-name interfaces gr-fpc/pic/port unit logical-unit-number tunnel]**

This configuration indicates that the tunnel's destination address is in routing instance **routing-instance-name**. By default, the tunnel route prefixes are assumed to be in the default Internet routing table **inet.0**.



NOTE: If you configure a virtual loopback tunnel interface and the **vrf-table-label** statement on the same routing instance, the **vrf-table-label** statement takes precedence over the virtual loopback tunnel interface. For more information, see [“Configuring Virtual Loopback Tunnels for VRF Table Lookup” on page 19](#).

For more information about VPNs, see the *Junos OS VPNs Library for Routing Devices*.

- Related Documentation**
- [Tunnel Services Overview on page 3](#)
 - [destination \(Routing Instance\) on page 35](#)

Configuring Virtual Loopback Tunnels for VRF Table Lookup

To enable egress filtering, you can either configure filtering based on the IP header, or you can configure a virtual loopback tunnel on routers equipped with a Tunnel PIC. [Table 4 on page 20](#) describes each method.

Table 4: Methods for Configuring Egress Filtering

Method	Interface Type	Configuration Guidelines	Comments
Filter traffic based on the IP header	Nonchannelized Point-to-Point Protocol / High Level Data Link Control (PPP/HDLC) core-facing SONET/SDH interfaces	Include the vrf-table-label statement at the [edit routing-instances instance-name] hierarchy level. For more information, see the <i>Junos OS VPNs Library for Routing Devices</i> .	There is no restriction on customer-edge (CE) router-to-provider edge (PE) router interfaces.
Configure a virtual loopback tunnel on routers equipped with a Tunnel PIC	All interfaces	See the guidelines in this section.	Router must be equipped with a Tunnel PIC. There is no restriction on the type of core-facing interface used or CE router-to-PE router interface used. You cannot configure a virtual loopback tunnel and the vrf-table-label statement at the same time.

You can configure a virtual loopback tunnel to facilitate VRF table lookup based on MPLS labels. You might want to enable this functionality so you can do either of the following:

- Forward traffic on a PE router to CE device interface, in a shared medium, where the CE device is a Layer 2 switch without IP capabilities (for example, a metro Ethernet switch).

The first lookup is done based on the VPN label to determine which VRF table to refer to, and the second lookup is done on the IP header to determine how to forward packets to the correct end hosts on the shared medium.

- Perform egress filtering at the egress PE router.

The first lookup on the VPN label is done to determine which VRF table to refer to, and the second lookup is done on the IP header to determine how to filter and forward packets. You can enable this functionality by configuring output filters on the VRF interfaces.

To configure a virtual loopback tunnel to facilitate VRF table lookup based on MPLS labels, you specify a virtual loopback tunnel interface name and associate it with a routing instance that belongs to a particular routing table. The packet loops back through the virtual loopback tunnel for route lookup. To specify a virtual loopback tunnel interface name, you configure the virtual loopback tunnel interface at the **[edit interfaces]** hierarchy level and include the **family inet** and **family mpls** statements:

```
vt-fpc/pic/port {
  unit 0 {
```



```

    family inet;
    family mpls;
  }
  unit 1 {
    family inet;
  }
}

```

To associate the virtual loopback tunnel with a routing instance, include the virtual loopback tunnel interface name at the **[edit routing-instances]** hierarchy level:

```
interface vt-fpc/pic/port;
```



NOTE: On virtual loopback tunnel interfaces, none of the logical interface statements except the family statement is supported. Note that you can configure only **inet** and **mpls** families, and you cannot configure IPv4 or IPv6 addresses on virtual loopback tunnel interfaces. Also, virtual loopback tunnel interfaces do not support class-of-service (CoS) configurations.

**Related
Documentation**

- [Tunnel Services Overview on page 3](#)
- [Example: Configuring a Virtual Loopback Tunnel for VRF Table Lookup on page 28](#)

Configuring PIM Tunnels

PIM tunnels are enabled automatically on routers that have a tunnel PIC and on which you enable PIM sparse mode. You do not need to configure the tunnel interface.

PIM tunnels are unidirectional.

In PIM sparse mode, the first-hop router encapsulates packets destined for the rendezvous point (RP) router. The packets are encapsulated with a unicast header and are forwarded through a unicast tunnel to the RP. The RP then de-encapsulates the packets and transmits them through its multicast tree. To perform the encapsulation and de-encapsulation, the first-hop and RP routers must be equipped with Tunnel PICs.

The Junos OS creates two interfaces to handle PIM tunnels:

- **pe**—Encapsulates packets destined for the RP. This interface is present on the first-hop router.
- **pd**—De-encapsulates packets at the RP. This interface is present on the RP.



NOTE: The **pe** and **pd** interfaces do not support class-of-service (CoS) configurations.

**Related
Documentation**

- [Tunnel Services Overview on page 3](#)

Configuring IPv6-over-IPv4 Tunnels

If you have a Tunnel PIC installed in your M Series or T Series router, you can configure IPv6-over-IPv4 tunnels. To define a tunnel, you configure a unicast tunnel across an existing IPv4 network infrastructure. IPv6/IPv4 packets are encapsulated in IPv4 headers and sent across the IPv4 infrastructure through the configured tunnel. You manually configure configured tunnels on each end point.

On SRX Series and J Series devices, Generic Routing Encapsulation (GRE) and IP-IP tunnels use internal interfaces, `gr-0/0/0` and `ip-0/0/0`, respectively. The Junos OS creates these interfaces at system bootup; they are not associated with a physical interface.

IPv6-over-IPv4 tunnels are defined in RFC 2893, *Transition Mechanisms for IPv6 Hosts and Routers*. For information about configuring a unicast tunnel, see [“Configuring Unicast Tunnels” on page 9](#). For an IPv6-over-IPv4 tunnel configuration example, see [“Example: Configuring an IPv6-over-IPv4 Tunnel” on page 29](#).

Related Documentation

- [Tunnel Services Overview on page 3](#)
- [Example: Configuring an IPv6-over-IPv4 Tunnel on page 29](#)

Configuring Dynamic Tunnels

A VPN that travels through a non-MPLS network requires a GRE tunnel. This tunnel can be either a static tunnel or a dynamic tunnel. A static tunnel is configured manually between two PE routers. A dynamic tunnel is configured using BGP route resolution.

When a router receives a VPN route that resolves over a BGP next hop that does not have an MPLS path, a GRE tunnel can be created dynamically, allowing the VPN traffic to be forwarded to that route. Only GRE IPv4 tunnels are supported.

To configure a dynamic tunnel between two PE routers, include the **dynamic-tunnels** statement:

```
dynamic-tunnels tunnel-name {  
    destination-networks prefix;  
    source-address address;  
}
```

You can configure this statement at the following hierarchy levels:

- **[edit routing-options]**
- **[edit routing-instances *routing-instance-name* routing-options]**
- **[edit logical-systems *logical-system-name* routing-options]**
- **[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* routing-options]**

For more information about configuring routing options or BGP, see the *Junos OS Routing Protocols Library for Routing Devices*. For more information about VPNs, see the *Junos OS VPNs Library for Routing Devices*.

- Related Documentation**
- [Tunnel Services Overview on page 3](#)
 - [dynamic-tunnels on page 38](#)

Configuring Tunnel Interfaces on MX Series Routers

Because the MX Series routers do not support Tunnel Services PICs, you create tunnel interfaces on MX Series routers by including the following statements at the **[edit chassis]** hierarchy level:

```
[edit chassis]
fpc slot-number {
  pic number {
    tunnel-services {
      bandwidth (1g | 10g | 20g | 40g);
    }
  }
}
```

fpc slot-number is the slot number of the DPC, MPC, or MIC. On the MX80 router, the range is 0 through 1. On other MX series routers, if two SCBs are installed, the range is 0 through 11. If three SCBs are installed, the range is 0 through 5 and 7 through 11.

The **pic number** On MX80 routers, if the FPC is 0, the PIC number can only be 0. If the FPC is 1, the PIC range is 0 through 3. For all other MX series routers, the range is 0 through 3.

bandwidth (1g | 10g | 20g | 40g) is the amount of bandwidth to reserve for tunnel traffic on each Packet Forwarding Engine.



NOTE: When you use MPCs and MICs, tunnel interfaces are soft interfaces and allow as much traffic as the forwarding-path allows, so it is advantageous to setup tunnel services without artificially limiting traffic by use of the **bandwidth** option. However, you *must* specify **bandwidth** when configuring tunnel services for MX Series routers with DPCs or FPCs. The GRE key option is not supported on the tunnel interfaces for DPCs on MX960 routers.

Bandwidth rates of 20 gigabits per second and 40 gigabits per second require use of an MX Series router with the 100-Gigabit Ethernet Modular Port Concentrator (MPC) and the 100-Gigabit CFP MIC.

1g indicates that 1 gigabit per second of bandwidth is reserved for tunnel traffic.

10g indicates that 10 gigabits per second of bandwidth is reserved for tunnel traffic.

20g indicates that 20 gigabits per second of bandwidth is reserved for tunnel traffic.

40g indicates that 40 gigabits per second of bandwidth is reserved for tunnel traffic.

If you specify a bandwidth that is not compatible, tunnel services are not activated. For example, you cannot specify a bandwidth of 1 Gbps for a Packet Forwarding Engine on a 10-Gigabit Ethernet 4-port DPC.

To verify that the tunnel interfaces have been created, issue the **show interfaces terse** operational mode command. For more information, see the *Junos Interfaces Command Reference*.

Related Documentation

- *Example: Configuring Tunnel Interfaces on a Gigabit Ethernet 40-Port DPC*
- *Example: Configuring Tunnel Interfaces on a 10-Gigabit Ethernet 4-Port DPC*
- *Example: Configuring Tunnel Interfaces on the MPC3E*
- *bandwidth (Tunnel Services)*
- *tunnel-services (Chassis)*
- *[edit chassis] Hierarchy Level*

Configuring Tunnel Interfaces on T4000 Routers

To create tunnel interfaces on a T4000 Core Router, include the following statements at the **[edit chassis]** hierarchy level:

```
[edit chassis]
fpc slot-number {
  pic number {
    tunnel-services {
      bandwidth bandwidth-value;
    }
  }
}
```

fpc slot-number denotes the slot number of the FPC. On the T4000 router, the range is 0 through 7.



NOTE:

- This applies only to the T4000 Type 5 FPC. If any other type of FPC is configured in this slot, this configuration is ignored and no tunnel physical interface is created.
- When you use Type 5 FPCs, the tunnel interfaces are soft interfaces and allow as much traffic as the forwarding-path allows. So, it is advantageous to setup tunnel services without artificially limiting traffic by setting the **bandwidth** statement.

pic number on the T4000 router is 0 or 1.

bandwidth bandwidth-value is the amount of bandwidth to reserve for the tunnel traffic on each Packet Forwarding Engine. The bandwidth value accepted includes every multiple of 10g up to 100g.

If you specify a bandwidth that is not compatible, tunnel services are not activated. For example, you cannot specify a bandwidth of 1 Gbps for a Packet Forwarding Engine on a 100-Gigabit Ethernet PIC with CFP.

To verify that the tunnel interfaces have been created, issue the **show interfaces terse** operational mode command. For more information, see the *Junos Interfaces Command Reference*.

- Related Documentation**
- *bandwidth (Tunnel Services)*
 - *tunnel-services (Chassis)*
 - *[edit chassis] Hierarchy Level*

CHAPTER 3

Examples

- [Examples: Configuring Unicast Tunnels on page 27](#)
- [Example: Configuring a Virtual Loopback Tunnel for VRF Table Lookup on page 28](#)
- [Example: Configuring an IPv6-over-IPv4 Tunnel on page 29](#)
- [Example: Configuring Logical Tunnels on page 30](#)

Examples: Configuring Unicast Tunnels

Configure two unnumbered IP-IP tunnels:

```
[edit interfaces]
ip-0/3/0 {
  unit 0 {
    tunnel {
      source 192.168.4.18;
      destination 192.168.4.253;
    }
    family inet;
  }
  unit 1 {
    tunnel {
      source 192.168.4.18;
      destination 192.168.4.254;
    }
    family inet;
  }
}
```

Configure numbered tunnel interfaces by including an address at the **[edit interfaces ip-0/3/0 unit (0 | 1) family inet]** hierarchy level:

```
[edit interfaces]
ip-0/3/0 {
  unit 0 {
    tunnel {
      source 192.168.4.18;
      destination 192.168.4.253;
    }
    family inet {
      address 10.5.5.1/30;
    }
  }
}
```

```
unit 1 {
  tunnel {
    source 192.168.4.18;
    destination 192.168.4.254;
  }
  family inet {
    address 10.6.6.100/30;
  }
}
```

Configure an MPLS over GRE tunnel by including the **family mpls** statement at the **[edit interfaces gr-1/2/0 unit 0]** hierarchy level:

```
[edit interfaces]
gr-1/2/0 {
  unit 0 {
    tunnel {
      source 192.168.1.1;
      destination 192.168.1.2;
    }
    family inet {
      address 10.1.1.1/30;
    }
    family mpls;
  }
}
```

- Related Documentation**
- [Tunnel Services Overview on page 3](#)
 - [Configuring Unicast Tunnels on page 9](#)

Example: Configuring a Virtual Loopback Tunnel for VRF Table Lookup

Configure a virtual loopback tunnel for VRF table lookup:

```
[edit routing-instances]
routing-instance-1 {
  instance-type vrf;
  interface vt-1/0/0.0;
  interface so-0/2/2.0;
  route-distinguisher 2:3;
  vrf-import VPN-A-import;
  vrf-export VPN-A-export;
  routing-options {
    static {
      route 10.0.0.0/8 next-hop so-0/2/2.0;
    }
  }
}
routing-instance-2 {
  instance-type vrf;
  interface vt-1/0/0.1;
  interface so-0/3/2.0;
  route-distinguisher 4:5;
```



```

vrf-import VPN-B-import;
vrf-export VPN-B-export;
routing-options {
  static {
    route 10.0.0.0/8 next-hop so-0/3/2.0;
  }
}
[edit interfaces]
vt-1/0/0 {
  unit 0 {
    family inet;
    family mpls;
  }
  unit 1 {
    family inet;
  }
}

```

- Related Documentation**
- [Tunnel Services Overview on page 3](#)
 - [Configuring Virtual Loopback Tunnels for VRF Table Lookup on page 19](#)

Example: Configuring an IPv6-over-IPv4 Tunnel

Configure a tunnel on both sides of the connection.

Configuration on Router 1

```

[edit]
interfaces {
  gr-1/0/0 {
    unit 0 {
      tunnel {
        source 10.19.2.1;
        destination 10.19.3.1;
      }
      family inet6 {
        address 2001:DB8:1:1/126;
      }
    }
  }
}

```

Configuration on Router 2

```

[edit]
interfaces {
  gr-1/0/0 {
    unit 0 {
      tunnel {
        source 10.19.3.1;
        destination 10.19.2.1;
      }
      family inet6 {
        address 2001:DB8:2:1/126;
      }
    }
  }
}

```

```
}
```

- Related Documentation**
- [Tunnel Services Overview on page 3](#)
 - [Configuring IPv6-over-IPv4 Tunnels on page 22](#)

Example: Configuring Logical Tunnels

Configure three logical tunnels:

```
[edit interfaces]
lt-4/2/0 {
  description "Logical tunnel interface connects three logical systems";
}
[edit logical-systems]
lr1 {
  interfaces lt-4/2/0 {
    unit 12 {
      peer-unit 21; #Peering with lr2
      encapsulation frame-relay;
      dlci 612;
      family inet;
    }
    unit 13 {
      peer-unit 31; #Peering with lr3
      encapsulation frame-relay-ccc;
      dlci 613;
    }
  }
}
lr2 {
  interfaces lt-4/2/0 {
    unit 21 {
      peer-unit 12; #Peering with lr1
      encapsulation frame-relay-ccc;
      dlci 612;
    }
    unit 23 {
      peer-unit 32; #Peering with lr3
      encapsulation frame-relay;
      dlci 623;
    }
  }
}
lr3 {
  interfaces lt-4/2/0 {
    unit 31 {
      peer-unit 13; #Peering with lr1
      encapsulation frame-relay;
      dlci 613;
      family inet;
    }
    unit 32 {
      peer-unit 23; #Peering with lr2
    }
  }
}
```

```
        encapsulation frame-relay-ccc;  
        dlci 623;  
    }  
}  
}
```

- Related Documentation**
- [Tunnel Services Overview on page 3](#)
 - [Configuring Logical Tunnel Interfaces on page 17](#)

CHAPTER 4

Configuration Statements

allow-fragmentation

Syntax	allow-fragmentation;
Hierarchy Level	[edit interfaces <i>gr-fpc/pic/port</i> unit <i>logical-unit-number</i> tunnel], [edit logical-systems <i>logical-system-name</i> interfaces <i>gr-fpc/pic/port</i> unit <i>logical-unit-number</i> tunnel]
Release Information	Statement introduced in Junos OS Release 9.2.
Description	Enable fragmentation of generic routing encapsulation (GRE) encapsulated packets regardless of maximum transmission unit (MTU) value.
Default	By default, the GRE-encapsulated packets are dropped if the packet size exceeds the MTU setting of the egress interface.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• reassemble-packets on page 42• Configuring Packet Reassembly on page 13

backup-destination

Syntax	<code>backup-destination destination-address;</code>
Hierarchy Level	<code>[edit interfaces interface-name unit logical-unit-number tunnel],[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number tunnel]</code>
Release Information	Statement introduced before Junos OS Release 7.4.
Description	For tunnel interfaces, specify the remote address of the backup tunnel.
Options	destination-address —Address of the remote side of the connection.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>destination (Interfaces)</i>• destination (Tunnel Remote End) on page 35• <i>Configuring IPsec Tunnel Redundancy</i>

copy-tos-to-outer-ip-header

Syntax	<code>copy-tos-to-outer-ip-header;</code>
Hierarchy Level	<code>[edit interfaces interface-name unit logical-unit-number],</code> <code>[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number]</code>
Release Information	Statement introduced in Junos OS Release 8.2.
Description	For GRE tunnel interfaces only, enable the inner IP header's ToS bits to be copied to the outer IP packet header.
Default	If you omit this statement, the ToS bits in the outer IP header are set to 0.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring a GRE Tunnel to Copy ToS Bits to the Outer IP Header on page 13

destination (Tunnel Remote End)

Syntax	<code>destination address;</code>
Hierarchy Level	[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> tunnel], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> tunnel]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 12.1 for EX Series switches.
Description	For tunnel interfaces, specify the remote address of the tunnel.
Options	<i>destination-address</i> —Address of the remote side of the connection.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring Unicast Tunnels on page 9 • Configuring Traffic Sampling • Configuring Flow Monitoring

destination (Routing Instance)

Syntax	<code>destination routing-instance-name;</code>
Hierarchy Level	[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> tunnel routing-instance]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Specify the destination routing instance that points to the routing table containing the tunnel destination address.
Default	The default Internet routing table inet.0 .
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring Tunnel Interfaces for Routing Table Lookup on page 19

destination-networks

Syntax	<code>destination-networks <i>prefix</i>;</code>
Hierarchy Level	<code>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> routing-options dynamic-tunnels <i>tunnel-name</i>],</code> <code>[edit logical-systems <i>logical-system-name</i> routing-options dynamic-tunnels <i>tunnel-name</i> rsvp-te <i>entry</i>],</code> <code>[edit logical-systems <i>logical-system-name</i> routing-options dynamic-tunnels <i>tunnel-name</i>],</code> <code>[edit routing-instances <i>routing-instance-name</i> routing-options dynamic-tunnels <i>tunnel-name</i>],</code> <code>[edit routing-instances <i>routing-instance-name</i> routing-options dynamic-tunnels <i>tunnel-name</i> rsvp-te <i>entry</i>],</code> <code>[edit routing-options dynamic-tunnels <i>tunnel-name</i>],</code> <code>[edit routing-options dynamic-tunnels <i>tunnel-name</i> rsvp-te <i>entry</i>]</code>
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 12.3 for ACX Series routers.
Description	Specify the IPv4 prefix range for the destination network. Only tunnels within the specified IPv4 prefix range can be created.
Options	<i>prefix</i> —Destination prefix of the network.
Required Privilege Level	<code>routing</code> —To view this statement in the configuration. <code>routing-control</code> —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring GRE Tunnels for Layer 3 VPNs• Configuring Dynamic Tunnels on page 22• Configuring RSVP Automatic Mesh

do-not-fragment

Syntax	do-not-fragment;
Hierarchy Level	[edit interfaces <i>gr-fpc/pic/port</i> unit <i>logical-unit-number</i> tunnel], [edit logical-systems <i>logical-system-name</i> interfaces <i>gr-fpc/pic/port</i> unit <i>logical-unit-number</i> tunnel]
Release Information	Statement introduced in Junos OS Release 9.2.
Description	Set the do-not-fragment (DF) bit on the packets entering the GRE tunnel so that they do not get fragmented anywhere in the path.
Default	By default, fragmentation is disabled.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• reassemble-packets on page 42• Configuring Packet Reassembly on page 13

dynamic-tunnels

Syntax	<pre>dynamic-tunnels <i>tunnel-name</i> { <i>destination-networks</i> <i>prefix</i>; gre; rsvp-te <i>entry-name</i> { <i>destination-networks</i> <i>network-prefix</i>; label-switched-path-template { default-template; <i>template-name</i>; } } source-address <i>address</i>; }</pre>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> routing-options], [edit logical-systems <i>logical-system-name</i> routing-options], [edit routing-instances <i>routing-instance-name</i> routing-options], [edit routing-options]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 12.3 for ACX Series routers.
Description	Configure a dynamic tunnel between two PE routers.
Options	<i>tunnel-name</i> —Name of the dynamic tunnel. The remaining statements are explained separately.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Example: Configuring a Two-Tiered Virtualized Data Center for Large Enterprise Networks</i>• <i>Configuring GRE Tunnels for Layer 3 VPNs</i>• Configuring Dynamic Tunnels on page 22


hold-time (OAM)

Syntax	<code>hold-time <i>seconds</i>;</code>
Hierarchy Level	<code>[edit protocols oam],</code> <code>[edit protocols oam gre-tunnel interface <i>interface-name</i>]</code>
Release Information	Statement introduced in Junos OS Release 10.2.
Description	Length of time the originating end of a GRE tunnel waits for keepalive packets from the other end of the tunnel before marking the tunnel as operationally down.
Options	<i>seconds</i> —Hold-time value. Default: 5 seconds Range: 5 through 250 seconds
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • GRE Keepalive Time Overview on page 6 • Configuring GRE Keepalive Time on page 14 • keepalive-time on page 40

interfaces

Syntax	<code>interfaces { ... }</code>
Hierarchy Level	<code>[edit]</code>
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Configure interfaces on the router.
Default	The management and internal Ethernet interfaces are automatically configured. You must configure all other interfaces.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Junos OS Network Interfaces Library for Routing Devices

keepalive-time

Syntax	keepalive-time <i>seconds</i> ;
Hierarchy Level	[edit protocols oam], [edit protocols oam gre-tunnel interface <i>interface-name</i>], [edit protocols oam gre-tunnel interface <i>interface-name.unit-number</i>]
Release Information	Statement introduced in Junos OS Release 10.2.
Description	Time difference between consecutive keepalive packets in a GRE tunnel.
	<div> NOTE: Support for GRE keepalive packets on MPC line cards became available as of Junos OS Release 11.4.</div>
Options	<i>seconds</i> —Keepalive time value. Default: 1 second Range: 1 through 50 seconds
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• GRE Keepalive Time Overview on page 6• Configuring GRE Keepalive Time on page 14• hold-time (OAM) on page 39

key

Syntax	<code>key number;</code>
Hierarchy Level	[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> tunnel], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> tunnel]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Identify an individual traffic flow within a tunnel, as defined in RFC 2890, <i>Key and Sequence Number Extensions to GRE</i> . On M Series and T Series routers, you can configure the GRE interface on an Adaptive Services, Multiservices, or Tunnel PIC. On MX Series routers, configure the interface on a Multiservices DPC.
Options	number —Value of the key. Range: 0 through 4,294,967,295
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring a Key Number on GRE Tunnels on page 11

multicast-only

Syntax	<code>multicast-only;</code>
Hierarchy Level	[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>inet</i>], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>inet</i>]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Configure the unit and family so that the interface can transmit and receive multicast traffic only. You can configure this property on the IP family only.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Restricting Tunnels to Multicast Traffic on page 17 • tunnel on page 46

peer-unit

Syntax	<code>peer-unit <i>unit-number</i>;</code>
Hierarchy Level	[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i>], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i>]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Configure a peer relationship between two logical systems.
Options	<i>unit-number</i> —Peering logical system unit number.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Logical Tunnel Interfaces on page 17

reassemble-packets

Syntax	<code>reassemble-packets;</code>
Hierarchy Level	[edit interfaces <i>gr-fpc/pic/port</i> unit <i>logical-unit-number</i>], [edit logical-systems <i>logical-system-name</i> interfaces <i>gr-fpc/pic/port</i> unit <i>logical-unit-number</i>]
Release Information	Statement introduced in Junos OS Release 9.2.
Description	Enable reassembly of fragmented tunnel packets on generic routing encapsulation (GRE) tunnel interfaces.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Packet Reassembly on page 13

routing-instance

Syntax	routing-instance { destination <i>routing-instance-name</i> ; }
Hierarchy Level	[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> tunnel], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> tunnel]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Specify the destination routing instance that points to the routing table containing the tunnel destination address.
Default	The default Internet routing table inet.0 .
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring Tunnel Interfaces for Routing Table Lookup on page 19

routing-instances

Syntax	routing-instances <i>routing-instance-name</i> { ... }
Hierarchy Level	[edit], [edit logical-systems <i>logical-system-name</i>]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Configure an additional routing entity for a router. You can create multiple instances of BGP, IS-IS, OSPF, OSPF version 3 (OSPFv3), and RIP for a router.
Default	Routing instances are disabled for the router.
Options	<i>routing-instance-name</i> —Name of the routing instance, a maximum of 31 characters. The remaining statements are explained separately.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring EVPN Routing Instances • Configuring Routing Instances on PE Routers in VPNs

routing-options

Syntax	routing-options { ... }
Hierarchy Level	[edit], [edit logical-systems <i>logical-system-name</i>], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i>], [edit routing-instances <i>routing-instance-name</i>]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Configure protocol-independent routing properties.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Protocol-Independent Routing Properties Feature Guide for Routing Devices</i>

source

Syntax	source <i>source-address</i> ;
Hierarchy Level	[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> tunnel]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 12.1 for EX Series switches.
Description	Specify the source address of the tunnel.
Default	If you do not specify a source address, the tunnel uses the unit's primary address as the source address of the tunnel.
Options	<i>source-address</i> —Address of the local side of the tunnel. This is the address that is placed in the outer IP header's source field.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Configuring Generic Routing Encapsulation Tunneling (CLI Procedure)</i>

source-address

Syntax	<code>source-address <i>address</i>;</code>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> routing-options dynamic-tunnels <i>tunnel-name</i>], [edit logical-systems <i>logical-system-name</i> routing-options dynamic-tunnels <i>tunnel-name</i>], [edit routing-instances <i>routing-instance-name</i> routing-options dynamic-tunnels <i>tunnel-name</i>], [edit routing-options dynamic-tunnels <i>tunnel-name</i>]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 12.3 for ACX Series routers.
Description	Configure the tunnel source address.
Options	address —Name of the source address.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring Dynamic Tunnels on page 22

ttl

Syntax	<code>ttl <i>value</i>;</code>
Hierarchy Level	[edit interfaces <i>interface-name</i> unit number tunnel]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 12.1 for EX Series switches.
Description	Set the time-to-live value bit in the header of the outer IP packet.
Options	value —Time-to-live value. Range: 0 through 255 Default: 64
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • <i>Tunnel Properties</i> • <i>Configuring Generic Routing Encapsulation Tunneling (CLI Procedure)</i>

tunnel

Syntax	<pre>tunnel { allow-fragmentation; backup-destination address; destination destination-address; do-not-fragment; key number; routing-instance { destination routing-instance-name; } source source-address; ttl number; }</pre>
Hierarchy Level	[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i>], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i>]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 12.1 for EX Series switches.
Description	<p>Configure a tunnel. You can use the tunnel for unicast and multicast traffic or just for multicast traffic. You can also use tunnels for encrypted traffic or virtual private networks (VPNs).</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Configuring Encryption Interfaces</i>• <i>Junos OS VPNs Library for Routing Devices</i>

unit (Interfaces)

Syntax	<pre> unit logical-unit-number { peer-unit unit-number; reassemble-packets; tunnel { allow-fragmentation; backup-destination address; destination destination-address; do-not-fragment; key number; routing-instance { destination routing-instance-name; } source source-address; ttl number; } } </pre>
Hierarchy Level	[edit interfaces interface-name], [edit logical-systems logical-system-name interfaces interface-name]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Configure a logical interface on the physical device. You must configure a logical interface to be able to use the physical device.
Options	<p>logical-unit-number—Number of the logical unit.</p> <p>Range: 0 through 16,384</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • <i>Junos OS Network Interfaces Library for Routing Devices</i> for other statements that do not affect services interfaces.

PART 3

Administration

- [Tunnel Services Interface Operational Mode Commands on page 51](#)

CHAPTER 5

Tunnel Services Interface Operational Mode Commands

show interfaces (GRE)


Syntax	<pre>show interfaces <i>interface-type</i> <brief detail extensive terse> <descriptions> <media> <snmp-index <i>snmp-index</i>> <statistics></pre>
Release Information	<p>Command introduced before Junos OS Release 7.4.</p> <p>Command introduced in Junos OS Release 12.1 for EX Series switches.</p>
Description	Display status information about the specified generic routing encapsulation (GRE) interface.
Options	<p><i>interface-type</i>—On M Series and T Series routers and EX Series switches, the interface type is <i>gr-fpc/pic/port</i>. On J Series routers, the interface type is <i>gr-pim/0/port</i>.</p> <p><i>brief detail extensive terse</i>—(Optional) Display the specified output level of interface information.</p> <p><i>descriptions</i>—(Optional) Display interface description strings.</p> <p><i>media</i>—(Optional) Display media-specific information about network interfaces.</p> <p><i>snmp-index snmp-index</i>—(Optional) Display information for the specified SNMP index of the interface.</p> <p><i>statistics</i>—(Optional) Display static interface statistics.</p>
	<div>  <p>NOTE: You can configure generic routing encapsulation (GRE) interfaces (<i>gre-x/y/z</i>) only for GMPLS control channels. GRE interfaces are not supported or configurable for other applications. For more information about GMPLS, see the <i>Junos OS MPLS Applications Library for Routing Devices</i> and the <i>Junos OS Feature Guides</i>.</p> </div>
Required Privilege Level	view
List of Sample Output	<p>show interfaces (GRE) on page 56</p> <p>show interfaces brief (GRE) on page 56</p> <p>show interfaces detail (GRE) on page 56</p> <p>show interfaces detail (GRE) on an EX4200 Virtual Chassis Member Switch on page 57</p> <p>show interfaces extensive (GRE) on page 58</p>
Output Fields	Table 5 on page 53 lists the output fields for the show interfaces (GRE) command. Output fields are listed in the approximate order in which they appear.

Table 5: GRE show interfaces Output Fields

Field Name	Field Description	Level of Output
Physical Interface		
Physical interface	Name of the physical interface.	All levels
Enabled	State of the interface. Possible values are described in the “Enabled Field” section under <i>Common Output Fields Description</i> .	All levels
Interface index	Physical interface's index number, which reflects its initialization sequence.	detail extensive none
SNMP ifIndex	SNMP index number for the physical interface.	detail extensive none
Generation	Unique number for use by Juniper Networks technical support only.	detail extensive
Type	Type of interface.	All levels
Link-level type	Encapsulation used on the physical interface.	All levels
MTU	MTU size on the physical interface.	All levels
Speed	Speed at which the interface is running.	All levels
Hold-times	Current interface hold-time up and hold-time down, in milliseconds.	detail extensive
Device Flags	Information about the physical device. Possible values are described in the “Device Flags” section under <i>Common Output Fields Description</i> .	All levels
Interface Flags	Information about the interface. Possible values are described in the “Interface Flags” section under <i>Common Output Fields Description</i> .	All levels
Input rate	Input rate in bits per second (bps) and packets per second (pps).	None specified
Output rate	Output rate in bps and pps.	None specified
Statistics last cleared	Time when the statistics for the interface were last set to zero.	detail extensive
Traffic statistics	<p>The number of and the rate at which input and output bytes and packets are received and transmitted on the physical interface.</p> <ul style="list-style-type: none"> • Input bytes—Number of bytes received on the interface. • Output bytes—Number of bytes transmitted on the interface. • Input packets—Number of packets received on the interface. • Output packets—Number of packets transmitted on the interface. 	detail extensive
Logical Interface		
Logical interface	Name of the logical interface.	All levels
Index	Logical interface index number, which reflects its initialization sequence.	detail extensive none

Table 5: GRE show interfaces Output Fields (*continued*)

Field Name	Field Description	Level of Output
SNMP ifIndex	Logical interface SNMP interface index number.	detail extensive none
Generation	Unique number for use by Juniper Networks technical support.	detail extensive
Flags	<p>Information about the logical interface. Possible values listed in the “Logical Interface Flags” section under <i>Common Output Fields Description</i>. describe general information about the logical interface.</p> <p>GRE-specific information about the logical interface is indicated by the presence or absence of the following value in this field:</p> <ul style="list-style-type: none"> • Reassemble-Pkts—If the Flags field includes this string, the GRE tunnel is configured to reassemble tunnel packets that were fragmented after tunnel encapsulation. 	All levels
IP-Header	<p>IP header of the logical interface. If the tunnel key statement is configured, this information is included in the IP Header entry.</p> <p>GRE-specific information about the logical interface is indicated by the presence or absence of the following value in this field:</p> <ul style="list-style-type: none"> • df—If the IP-Header field includes this string immediately following the 16 bits of identification information (that is, if :df: displays after the twelfth byte), the GRE tunnel is configured to allow fragmentation of GRE packets after encapsulation. 	All levels
Encapsulation	Encapsulation on the logical interface.	All levels
Copy-tos-to-outer-ip-header	<p>Status of type of service (ToS) bits in the GRE packet header:</p> <ul style="list-style-type: none"> • On—ToS bits were copied from the payload packet header into the header of the IP packet sent through the GRE tunnel. • Off—ToS bits were not copied from the payload packet header and are set to 0 in the GRE packet header. <p>NOTE: EX Series switches do not support copying ToS bits to the encapsulated packet, so the value of this field is always Off in switch output.</p>	detail extensive
Gre keepalives configured	<p>Indicates whether a GRE keepalive time and hold time are configured for the GRE tunnel.</p> <p>NOTE: EX Series switches do not support configuration of GRE tunnel keepalive times and hold times, so the value of this field is always Off in switch output.</p>	detail extensive
Gre keepalives adjacency state	Status of the other end of the GRE tunnel: Up or Down . If keepalive messages are not received by either end of the GRE tunnel within the hold-time period, the GRE keepalive adjacency state is down even when the GRE tunnel is up.	detail extensive
Input packets	Number of packets received on the logical interface.	None specified
Output packets	Number of packets transmitted on the logical interface.	None specified

Table 5: GRE show interfaces Output Fields (*continued*)

Field Name	Field Description	Level of Output
Traffic statistics	<p>Rate of bytes and packets received and transmitted on the logical interface. These statistics are the sum of the local and transit statistics. When a burst of traffic is received, the value in the output packet rate field might briefly exceed the peak cell rate. It takes awhile (generally, less than 1 second) for this counter to stabilize.</p> <ul style="list-style-type: none"> • Input rate—Rate of bits and packets received on the interface. • Output rate—Rate of bits and packets transmitted on the interface. 	detail extensive
Local statistics	Statistics for traffic received from and transmitted to the Routing Engine. When a burst of traffic is received, the value in the output packet rate field might briefly exceed the peak cell rate. It takes awhile (generally, less than 1 second) for this counter to stabilize.	detail extensive
Transit statistics	Statistics for traffic transiting the router. When a burst of traffic is received, the value in the output packet rate field might briefly exceed the peak cell rate. It takes awhile (generally, less than 1 second) for this counter to stabilize.	detail extensive none
Protocol	Protocol family configured on the logical interface, such as iso , inet6 , or mpls .	detail extensive none
<i>protocol-family</i>	Protocol family configured on the logical interface. If the protocol is inet , the IP address of the interface is also displayed.	brief
MTU	MTU size on the logical interface.	detail extensive none
Generation	Unique number for use by Juniper Networks technical support only.	detail extensive
Route table	Routing table in which the logical interface address is located. For example, 0 refers to the routing table inet.0 .	detail extensive
Flags	Information about the protocol family flags. Possible values are described in the “Family Flags” section under <i>Common Output Fields Description</i> .	detail extensive none
Addresses, Flags	Information about the address flags. Possible values are described in the “Addresses Flags” section under <i>Common Output Fields Description</i> .	detail extensive none
Destination	IP address of the remote side of the connection.	detail extensive none
Local	IP address of the logical interface.	detail extensive none
Broadcast	Broadcast address of the logical interface.	detail extensive none
Generation	Unique number for use by Juniper Networks technical support only.	detail extensive

Sample Output

show interfaces (GRE)

```
user@host> show interfaces gr-1/2/0
Physical interface: gr-0/0/0, Enabled, Physical link is Up
  Interface index: 132, SNMP ifIndex: 26
  Type: GRE, Link-level type: GRE, MTU: Unlimited, Speed: 800mbps
  Device flags   : Present Running
  Interface flags: Point-To-Point SNMP-Traps
  Input rate     : 0 bps (0 pps)
  Output rate    : 0 bps (0 pps)

Logical interface gr-0/0/0.0 (Index 68) (SNMP ifIndex 47)
  Flags: Point-To-Point SNMP-Traps 16384
  IP-Header 1.1.1.2:1.1.1.1:47:df:64:0000000000000000 Encapsulation: GRE-NULL
  Input packets : 0
  Output packets: 0
  Protocol inet, MTU: 1476
  Flags: None
  Addresses, Flags: Is-Primary
    Local: 1.10.1.1
```

show interfaces brief (GRE)

```
user@host> show interfaces gr-1/2/0 brief
Physical interface: gr-1/2/0, Enabled, Physical link is Up
  Type: GRE, Link-level type: GRE, MTU: Unlimited, Speed: 800mbps
  Device flags   : Present Running
  Interface flags: Point-To-Point SNMP-Traps

Logical interface gr-1/2/0.0
  Flags: Hardware-Down Point-To-Point SNMP-Traps 0x4000
  IP-Header 10.10.0.2:10.10.0.1:47:df:64:0000000000000000
  Encapsulation: GRE-NULL
  inet 10.100.0.1/30
  mpls
```

show interfaces detail (GRE)

```
user@host> show interfaces gr-1/2/0 detail
Physical interface: gr-0/0/0, Enabled, Physical link is Up
  Interface index: 132, SNMP ifIndex: 26, Generation: 13
  Type: GRE, Link-level type: GRE, MTU: Unlimited, Speed: 800mbps
  Hold-times      : Up 0 ms, Down 0 ms
  Device flags    : Present Running
  Interface flags: Point-To-Point SNMP-Traps
  Statistics last cleared: Never
  Traffic statistics:
    Input bytes : 0 0 bps
    Output bytes : 0 0 bps
    Input packets: 0 0 pps
    Output packets: 0 0 pps

Logical interface gr-0/0/0.0 (Index 68) (SNMP ifIndex 47) (Generation 8)
  Flags: Point-To-Point SNMP-Traps 16384
  IP-Header 1.1.1.2:1.1.1.1:47:df:64:0000000000000000 Encapsulation: GRE-NULL
  Traffic statistics:
    Input bytes : 0
    Output bytes : 0
    Input packets: 0
```

```

Output packets:                0
Local statistics:
Input bytes :                  0
Output bytes :                  0
Input packets:                 0
Output packets:                0
Transit statistics:
Input bytes :                  0          0 bps
Output bytes :                  0          0 bps
Input packets:                 0          0 pps
Output packets:                0          0 pps
Protocol inet, MTU: 1476, Generation: 12, Route table: 0
Flags: None
Addresses, Flags: Is-Primary
Destination: Unspecified, Local: 1.10.1.1, Broadcast: Unspecified,
Generation: 15

```

show interfaces detail (GRE) on an EX4200 Virtual Chassis Member Switch

```

user@switch> show interfaces gr-2/0/15 detail
Physical interface: gr-2/0/15, Enabled, Physical link is Up
Interface index: 195, SNMP ifIndex: 846, Generation: 198
Type: GRE, Link-level type: GRE, MTU: Unlimited, Speed: 1000mbps
Hold-times      : Up 0 ms, Down 0 ms
Current address: 00:1f:12:38:0f:d2, Hardware address: 00:1f:12:38:0f:d2
Device flags    : Present Running
Interface flags: Point-To-Point SNMP-Traps
Statistics last cleared: 2011-09-14 17:43:15 UTC (00:00:18 ago)
Traffic statistics:
Input bytes :                5600636          0 bps
Output bytes :                5600636          0 bps
Input packets:                20007          0 pps
Output packets:               20007          0 pps
IPv6 transit statistics:
Input bytes :                  0
Output bytes :                  0
Input packets:                 0
Output packets:                 0

Logical interface gr-2/0/15.0 (Index 75) (SNMP ifIndex 847) (HW Token 4093)
(Generation 140)
Flags: Point-To-Point SNMP-Traps 0x0
IP-Header 180.20.30.2:180.20.3:47:df:64:0000000000000000
Encapsulation: GRE-NULL
Copy-tos-to-outer-ip-header: Off
Gre keepalives configured: Off, Gre keepalives adjacency state: down
Traffic statistics:
Input bytes :                5600886
Output bytes :               2881784
Input packets:                20010
Output packets:               10018
Local statistics:
Input bytes :                  398
Output bytes :                  264
Input packets:                  5
Output packets:                  3
Transit statistics:
Input bytes :                5600488          0 bps
Output bytes :               2881520          0 bps
Input packets:                20005          0 pps
Output packets:               10015          0 pps

```

```
Protocol inet, Generation: 159, Route table: 0
Flags: None
Addresses, Flags: Is-Preferred Is-Primary
  Destination: 90.90.90/24, Local: 90.90.90.10, Broadcast: 90.90.90.255,
  Generation: 144
```

```
Logical interface gr-2/0/15.1 (Index 80) (SNMP ifIndex 848) (HW Token 4088)
(Generation 150)
```

```
Flags: Point-To-Point SNMP-Traps 0x0
IP-Header 160.20.40.2:160.20.30.1:47:df:64:0000000000000000
Encapsulation: GRE-NULL
Copy-tos-to-outer-ip-header: Off
Gre keepalives configured: Off, Gre keepalives adjacency state: down
```

```
Traffic statistics:
```

```
Input bytes :          260
Output bytes :        2880148
Input packets:           4
Output packets:       10002
```

```
Local statistics:
```

```
Input bytes :          112
Output bytes :           0
Input packets:           2
Output packets:           0
```

```
Transit statistics:
```

```
Input bytes :          148          0 bps
Output bytes :        2880148        0 bps
Input packets:           2          0 pps
Output packets:       10002        0 pps
```

```
Protocol inet, Generation: 171, Route table: 0
```

```
Flags: None
```

```
Addresses, Flags: Is-Preferred Is-Primary
```

```
  Destination: 70.70.70/24, Local: 70.70.70.10, Broadcast: 70.70.70.255,
  Generation: 160
```

[show interfaces extensive \(GRE\)](#)

The output for the **show interfaces extensive** command is identical to that for the **show interfaces detail** command. For sample output, see [show interfaces detail \(GRE\) on page 56](#) and [show interfaces detail \(GRE\) on an EX4200 Virtual Chassis Member Switch on page 57](#).

show interfaces (IP-over-IP)

Syntax	<pre>show interfaces <i>interface-type</i> <brief detail extensive terse> <descriptions> <media> <snmp-index <i>snmp-index</i>> <statistics></pre>
Release Information	Command introduced before Junos OS Release 7.4.
Description	Display status information about the specified IP-over-IP interface.
Options	<p><i>interface-type</i>—On M Series and T Series routers, the interface type is ip-fpc/pic/port. On J Series routers, the interface type is ip-pim/O/port.</p> <p>brief detail extensive terse—(Optional) Display the specified level of output.</p> <p>descriptions—(Optional) Display interface description strings.</p> <p>media—(Optional) Display media-specific information about network interfaces.</p> <p>snmp-index <i>snmp-index</i>—(Optional) Display information for the specified SNMP index of the interface.</p> <p>statistics—(Optional) Display static interface statistics.</p>
Required Privilege Level	view
List of Sample Output	<p>show interfaces (IP-over-IP) on page 61</p> <p>show interfaces brief (IP-over-IP) on page 62</p> <p>show interfaces detail (IP-over-IP) on page 62</p> <p>show interfaces extensive (IP-over-IP) on page 63</p>
Output Fields	<p>Table 6 on page 59 lists the output fields for the show interfaces (IP-over-IP) command. Output fields are listed in the approximate order in which they appear.</p>

Table 6: IP-over-IP show interfaces Output Fields

Field	Field Description	Level of Output
Physical Interface		
Physical interface	Name of the physical interface.	All levels
Enabled	State of the interface. Possible values are described in the “Enabled Field” section under <i>Common Output Fields Description</i> .	All levels
Interface index	Physical interface's index number, which reflects its initialization sequence.	detail extensive none
SNMP ifIndex	SNMP index number for the physical interface.	detail extensive none

Table 6: IP-over-IP show interfaces Output Fields (*continued*)

Field	Field Description	Level of Output
Generation	Unique number for use by Juniper Networks technical support only.	detail extensive
Type	Type of interface.	All levels
Link-level type	Encapsulation used on the physical interface.	All levels
MTU	MTU size on the physical interface.	All levels
Speed	Speed at which the interface is running.	All levels
Hold-times	Current interface hold-time up and hold-time down, in milliseconds.	detail extensive
Device flags	Information about the physical device. Possible values are described in the "Device Flags" section under <i>Common Output Fields Description</i> .	All levels
Interface flags	Information about the interface. Possible values are described in the "Interface Flags" section under <i>Common Output Fields Description</i> .	All levels
Input rate	Input rate in bits per second (bps) and packets per second (pps).	None specified
Output rate	Output rate in bps and pps.	None specified
Statistics last cleared	Time when the statistics for the interface were last set to zero.	detail extensive
Traffic statistics	Number and rate of bytes and packets received and transmitted on the physical interface. <ul style="list-style-type: none"> • Input bytes—Number of bytes received on the interface. • Output bytes—Number of bytes transmitted on the interface. • Input packets—Number of packets received on the interface. • Output packets—Number of packets transmitted on the interface. 	detail extensive
Logical Interface		
Logical interface	Name of the logical interface.	All levels
Index	Logical interface index number, which reflects its initialization sequence.	detail extensive none
SNMP ifIndex	Logical interface SNMP interface index number.	detail extensive none
Generation	Unique number for use by Juniper Networks technical support.	detail extensive
Flags	Information about the logical interface. Possible values are described in the "Logical Interface Flags" section under <i>Common Output Fields Description</i> .	All levels
IP Header	IP header of the logical interface.	All levels
Encapsulation	Encapsulation on the logical interface.	All levels

Table 6: IP-over-IP show interfaces Output Fields (*continued*)

Field	Field Description	Level of Output
Input packets	Number of packets received on the logical interface.	None specified
Output packets	Number of packets transmitted on the logical interface.	None specified
Traffic statistics	<p>Total number of bytes and packets received and transmitted on the logical interface. These statistics are the sum of the local and transit statistics. When a burst of traffic is received, the value in the output packet rate field might briefly exceed the peak cell rate. It takes awhile (generally, less than 1 second) for this counter to stabilize.</p> <ul style="list-style-type: none"> • Input rate—Rate of bits and packets received on the interface. • Output rate—Rate of bits and packets transmitted on the interface. 	detail extensive
Local statistics	Statistics for traffic received from and transmitted to the Routing Engine. When a burst of traffic is received, the value in the output packet rate field might briefly exceed the peak cell rate. It takes awhile (generally, less than 1 second) for this counter to stabilize.	detail extensive
Transit statistics	Statistics for traffic transiting the router. When a burst of traffic is received, the value in the output packet rate field might briefly exceed the peak cell rate. It takes awhile (generally, less than 1 second) for this counter to stabilize.	detail extensive
Protocol	Protocol family configured on the logical interface, such as iso , inet6 , or mpls .	detail extensive none
<i>protocol-family</i>	Protocol family configured on the logical interface. If the protocol is inet , the IP address of the interface is also displayed.	brief
MTU	MTU size on the logical interface.	detail extensive none
Generation	Unique number for use by Juniper Networks technical support only.	detail extensive
Route table	Routing table in which the logical interface address is located. For example, 0 refers to the routing table inet.0 .	detail extensive
Flags	Information about the protocol family flags. Possible values are described in the “Family Flags” section under <i>Common Output Fields Description</i> .	detail extensive none

Sample Output

show interfaces (IP-over-IP)

```

user@host> show interfaces ip-0/0/0
Physical interface: ip-0/0/0, Enabled, Physical link is Up
  Interface index: 133, SNMP ifIndex: 27
  Type: IPIP, Link-level type: IP-over-IP, MTU: Unlimited, Speed: 800mbps
  Device flags   : Present Running
  Interface flags: SNMP-Traps
  Input rate    : 0 bps (0 pps)
  Output rate   : 0 bps (0 pps)

  Logical interface ip-0/0/0.0 (Index 69) (SNMP ifIndex 49)

```

```
Flags: Point-To-Point SNMP-Traps 16384
IP-Header 2.2.2.1:2.2.2.2:4:df:64:00000000 Encapsulation: IPv4=NULL
Input packets : 0
Output packets: 0
Protocol inet, MTU: 1480
Flags: None
```

show interfaces brief (IP-over-IP)

```
user@host> show interfaces ip-0/0/0 brief
Physical interface: ip-0/0/0, Enabled, Physical link is Up
Type: IPIP, Link-level type: IP-over-IP, MTU: Unlimited, Speed: 800mbps
Device flags : Present Running
Interface flags: SNMP-Traps

Logical interface ip-0/0/0.0
Flags: Point-To-Point SNMP-Traps 16384
IP-Header 2.2.2.1:2.2.2.2:4:df:64:00000000 Encapsulation: IPv4=NULL
inet
```

show interfaces detail (IP-over-IP)

```
user@host> show interfaces ip-0/0/0 detail
Physical interface: ip-0/0/0, Enabled, Physical link is Up
Interface index: 133, SNMP ifIndex: 27, Generation: 14
Type: IPIP, Link-level type: IP-over-IP, MTU: Unlimited, Speed: 800mbps
Hold-times : Up 0 ms, Down 0 ms
Device flags : Present Running
Interface flags: SNMP-Traps
Statistics last cleared: Never
Traffic statistics:
Input bytes : 0 0 bps
Output bytes : 0 0 bps
Input packets: 0 0 pps
Output packets: 0 0 pps

Logical interface ip-0/0/0.0 (Index 69) (SNMP ifIndex 49) (Generation 9)
Flags: Point-To-Point SNMP-Traps 16384
IP-Header 2.2.2.1:2.2.2.2:4:df:64:00000000 Encapsulation: IPv4=NULL
Traffic statistics:
Input bytes : 0
Output bytes : 0
Input packets: 0
Output packets: 0
Local statistics:
Input bytes : 0
Output bytes : 0
Input packets: 0
Output packets: 0
Transit statistics:
Input bytes : 0 0 bps
Output bytes : 0 0 bps
Input packets: 0 0 pps
Output packets: 0 0 pps
Protocol inet, MTU: 1480, Generation: 13, Route table: 0
Flags: None
```

show interfaces extensive (IP-over-IP)

The output for the show interfaces extensive command is identical to that for the show interfaces detail command. For sample output, see [show interfaces detail \(IP-over-IP\) on page 62](#).

show interfaces (Logical Tunnel)

Syntax	<pre>show interfaces <i>interface-type</i> <brief detail extensive terse> <descriptions> <media> <snmp-index <i>snmp-index</i>> <statistics></pre>
Release Information	Command introduced before Junos OS Release 7.4.
Description	Display status information about the specified logical tunnel interface.
Options	<p><i>interface-type</i>—On M Series and T Series routers, the interface type is <i>lt-fpc/pic/port</i>. On J Series routers, the interface type is <i>lt-pim/O/port</i>.</p> <p>brief detail extensive terse—(Optional) Display the specified level of output.</p> <p>descriptions—(Optional) Display interface description strings.</p> <p>media—(Optional) Display media-specific information about network interfaces.</p> <p>snmp-index <i>snmp-index</i>—(Optional) Display information for the specified SNMP index of the interface.</p> <p>statistics—(Optional) Display static interface statistics.</p>
Required Privilege Level	view
List of Sample Output	show interfaces extensive (Logical Tunnel) on page 68
Output Fields	<p>Table 7 on page 64 lists the output fields for the show interfaces (logical tunnel) command. Output fields are listed in the approximate order in which they appear.</p>

Table 7: Logical Tunnel show interfaces Output Fields

Field Name	Field Description	Level of Output
Physical Interface		
Physical interface	Name of the physical interface.	All levels
Enabled	State of the interface. Possible values are described in the “Enabled Field” section under <i>Common Output Fields Description</i> .	All levels
Interface index	Physical interface index number, which reflects its initialization sequence.	detail extensive none
SNMP ifIndex	SNMP index number for the physical interface.	detail extensive none
Generation	Unique number for use by Juniper Networks technical support only.	detail extensive

Table 7: Logical Tunnel show interfaces Output Fields (*continued*)

Field Name	Field Description	Level of Output
Type	Type of interface. Software-Pseudo indicates a standard software interface with no associated hardware device.	All levels
Link-level type	Encapsulation used on the physical interface.	All levels
MTU	MTU size on the physical interface.	All levels
Clocking	Reference clock source: Internal or External when configured. Otherwise, Unspecified .	All levels
Speed	Speed at which the interface is running.	All levels
Device flags	Information about the physical device. Possible values are described in the "Device Flags" section under <i>Common Output Fields Description</i> .	All levels
Interface flags	Information about the interface. Possible values are described in the "Interface Flags" section under <i>Common Output Fields Description</i> .	All levels
Link type	Type of link.	All levels
Link flags	Information about the link. Possible values are described in the "Link Flags" section under <i>Common Output Fields Description</i> .	All levels
Physical info	Information about the physical interface.	All levels
Hold-times	Current interface hold-time up and hold-time down, in milliseconds.	detail extensive
Current address	Configured MAC address.	detail extensive none
Hardware address	Hardware MAC address.	detail extensive none
Alternate link address	Backup link address.	detail extensive none
Last flapped	Date, time, and how long ago the interface went from down to up. The format is Last flapped: year-month-day hour:minute:second timezone (hour:minute:second ago) . For example, Last flapped: 2002-04-26 10:52:40 PDT (04:33:20 ago) .	detail extensive none
Statistics last cleared	Time when the statistics for the interface were last set to zero.	detail extensive
Traffic statistics	Number and rate of bytes and packets received and transmitted on the physical interface. <ul style="list-style-type: none"> Input bytes, Output bytes—Number of bytes received and transmitted on the interface. Input packets, Output packets—Number of packets received and transmitted on the interface. 	detail extensive

Table 7: Logical Tunnel show interfaces Output Fields (*continued*)

Field Name	Field Description	Level of Output
Input errors	<p>Input errors on the interface. The following paragraphs explain the counters whose meaning might not be obvious:</p> <ul style="list-style-type: none"> • Errors—Sum of the incoming frame aborts and FCS errors. • Drops—Number of packets dropped by the input queue of the I/O Manager ASIC. If the interface is saturated, this number increments once for every packet that is dropped by the ASIC's RED mechanism. • Framing errors—Number of packets received with an invalid frame checksum (FCS). • Runts—Number of frames received that are smaller than the runt threshold. • Giants—Number of frames received that are larger than the giant threshold. • Policed discards—Number of frames that the incoming packet match code discarded because they were not recognized or not of interest. Usually, this field reports protocols that the Junos OS does not handle. • Resource errors—Sum of transmit drops. 	extensive
Output errors	<p>Output errors on the interface. The following paragraphs explain the counters whose meaning might not be obvious:</p> <ul style="list-style-type: none"> • Carrier transitions—Number of times the interface has gone from down to up. This number does not normally increment quickly, increasing only when the cable is unplugged, the far-end system is powered down and then up, or another problem occurs. If the number of carrier transitions increments quickly (perhaps once every 10 seconds), the cable, the far-end system, or the PIC is malfunctioning. • Errors—Sum of the outgoing frame aborts and FCS errors. • Drops—Number of packets dropped by the output queue of the I/O Manager ASIC. If the interface is saturated, this number increments once for every packet that is dropped by the ASIC's RED mechanism. • MTU errors—Number of packets larger than the MTU threshold. • Resource errors—Sum of transmit drops. 	extensive
Logical Interface		
Logical interface	Name of the logical interface.	All levels
Index	Logical interface index number, which reflects its initialization sequence.	detail extensive none
SNMP ifIndex	SNMP interface index number.	detail extensive none
Generation	Unique number for use by Juniper Networks technical support only.	detail extensive
Flags	Information about the logical interface. Possible values are described in the "Logical Interface Flags" section under <i>Common Output Fields Description</i> .	All levels
Encapsulation	Encapsulation on the logical interface.	All levels

Table 7: Logical Tunnel show interfaces Output Fields (*continued*)

Field Name	Field Description	Level of Output
Traffic statistics	<p>Total number of bytes and packets received and transmitted on the logical interface. These statistics are the sum of the local and transit statistics. When a burst of traffic is received, the value in the output packet rate field might briefly exceed the peak cell rate. It takes awhile (generally, less than 1 second) for this counter to stabilize.</p> <ul style="list-style-type: none"> • Input bytes—Rate of bytes received on the interface. • Output bytes—Rate of bytes transmitted on the interface. • Input packets—Rate of packets received on the interface. • Output packets—Rate of packets transmitted on the interface. 	detail extensive
Local statistics	Statistics for traffic received from and transmitted to the Routing Engine. When a burst of traffic is received, the value in the output packet rate field might briefly exceed the peak cell rate. It takes awhile (generally, less than 1 second) for this counter to stabilize.	detail extensive
Transit statistics	Statistics for traffic transiting the router. When a burst of traffic is received, the value in the output packet rate field might briefly exceed the peak cell rate. It takes awhile (generally, less than 1 second) for this counter to stabilize.	detail extensive
Protocol	Protocol family configured on the logical interface, such as iso , inet6 , mpls .	detail extensive none
MTU	MTU size on the logical interface.	detail extensive none
Generation	Unique number for use by Juniper Networks technical support only.	detail extensive
Route table	Route table in which this address exists. For example, Route table:0 refers to inet.0 .	detail extensive
Flags	Information about the protocol family flags. Possible values are described in the “Family Flags” section under <i>Common Output Fields Description</i> .	detail extensive none
Addresses, Flags	Information about the address flags. Possible values are described in the “Addresses Flags” section under <i>Common Output Fields Description</i> .	detail extensive none
Destination	IP address of the remote side of the connection.	detail extensive none
Local	IP address of the logical interface.	detail extensive none
Broadcast	Broadcast address of the logical interface.	detail extensive none
Generation	Unique number for use by Juniper Networks technical support only.	detail extensive

Sample Output

show interfaces extensive (Logical Tunnel)

```
user@host> show interfaces lt-1/0/0 extensive
Physical interface: lt-1/0/0, Enabled, Physical link is Up
  Interface index: 143, SNMP ifIndex: 70, Generation: 26
  Type: Logical-tunnel, Link-level type: Logical-tunnel, MTU: 0,
  Clocking: Unspecified, Speed: 800mbps
  Device flags   : Present Running
  Interface flags: Point-To-Point SNMP-Traps
  Link type      : Unspecified
  Link flags     : None
  Physical info  : 13
  Hold-times    : Up 0 ms, Down 0 ms
  Current address: 00:90:69:a6:48:7e, Hardware address: Unspecified
  Alternate link address: Unspecified
  Last flapped  : 2004-03-03 15:53:52 PST (22:08:46 ago)
  Statistics last cleared: Never
  Traffic statistics:
    Input bytes :                0                0 bps
    Output bytes :                0                0 bps
    Input packets:                0                0 pps
    Output packets:                0                0 pps
  Input errors:
    Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Giants: 0,
    Policed discards: 0
  Output errors:
    Carrier transitions: 1, Errors: 0, Drops: 0, MTU errors: 0

Logical interface lt-1/0/0.0 (Index 66) (SNMP ifIndex 467) (Generation 3024)
  Flags: Point-To-Point SNMP-Traps 16384 DLCI 100 Encapsulation: FR-NLPID
  Traffic statistics:
    Input bytes :                0
    Output bytes :                0
    Input packets:                0
    Output packets:                0
  Local statistics:
    Input bytes :                0
    Output bytes :                0
    Input packets:                0
    Output packets:                0
  Transit statistics:
    Input bytes :                0                0 bps
    Output bytes :                0                0 bps
    Input packets:                0                0 pps
    Output packets:                0                0 pps
  Protocol inet, MTU: 4470, Generation: 7034, Route table: 0
  Flags: None
  Addresses, Flags: Is-Preferred Is-Primary
    Destination: 10.1.1/24, Local: 10.1.1.1, Broadcast: Unspecified,
    Generation: 2054
```


show interfaces (Multicast Tunnel)

Syntax	<pre>show interfaces <i>interface-type</i> <brief detail extensive terse> <descriptions> <media> <snmp-index <i>snmp-index</i>> <statistics></pre>
Release Information	Command introduced before Junos OS Release 7.4.
Description	Display status information about the specified multicast tunnel interface and its logical encapsulation and de-encapsulation interfaces.
Options	<p><i>interface-type</i>—On M Series and T Series routers, the interface type is <i>mt-fpc/pic/port</i>. On J Series routers, the interface type is <i>mt-pim/0/port</i>.</p> <p><i>brief detail extensive terse</i>—(Optional) Display the specified level of output.</p> <p><i>descriptions</i>—(Optional) Display interface description strings.</p> <p><i>media</i>—(Optional) Display media-specific information about network interfaces.</p> <p><i>snmp-index snmp-index</i>—(Optional) Display information for the specified SNMP index of the interface.</p> <p><i>statistics</i>—(Optional) Display static interface statistics.</p>
Additional Information	The multicast tunnel interface has two logical interfaces: encapsulation and de-encapsulation. These interfaces are automatically created by the Junos OS for every multicast-enabled VPN routing and forwarding (VRF) instance. The encapsulation interface carries multicast traffic traveling from the edge interface to the core interface. The de-encapsulation interface carries traffic coming from the core interface to the edge interface.
Required Privilege Level	view

List of Sample Output [show interfaces \(Multicast Tunnel\) on page 71](#)
[show interfaces brief \(Multicast Tunnel\) on page 71](#)
[show interfaces detail \(Multicast Tunnel\) on page 71](#)
[show interfaces extensive \(Multicast Tunnel\) on page 71](#)
[show interfaces \(Multicast Tunnel Encapsulation\) on page 73](#)
[show interfaces \(Multicast Tunnel De-Encapsulation\) on page 73](#)

Output Fields [Table 8 on page 70](#) lists the output fields for the **show interfaces** (Multicast Tunnel) command. Output fields are listed in the approximate order in which they appear.

Table 8: Multicast Tunnel show interfaces Output Fields

Field Name	Field Description	Level of Output
Physical Interface		
Physical interface	Name of the physical interface.	All levels
Enabled	State of the interface. Possible values are described in the “Enabled Field” section under <i>Common Output Fields Description</i> .	All levels
Interface index	Physical interface's index number, which reflects its initialization sequence.	detail extensive none
SNMP ifIndex	SNMP index number for the physical interface.	detail extensive none
Generation	Unique number for use by Juniper Networks technical support only.	detail extensive
Type	Type of interface.	All levels
Link-level type	Encapsulation used on the physical interface.	All levels
MTU	MTU size on the physical interface.	All levels
Speed	Speed at which the interface is running.	All levels
Hold-times	Current interface hold-time up and hold-time down, in milliseconds.	detail extensive
Device flags	Information about the physical device. Possible values are described in the “Device Flags” section under <i>Common Output Fields Description</i> .	All levels
Interface flags	Information about the interface. Possible values are described in the “Interface Flags” section under <i>Common Output Fields Description</i> .	All levels
Input Rate	Input rate in bits per second (bps) and packets per second (pps).	None specified
Output Rate	Output rate in bps and pps.	None specified
Statistics last cleared	Time when the statistics for the interface were last set to zero.	detail extensive

Table 8: Multicast Tunnel show interfaces Output Fields (*continued*)

Field Name	Field Description	Level of Output
Traffic statistics	<p>Number and rate of bytes and packets received and transmitted on the physical interface.</p> <ul style="list-style-type: none"> • Input bytes—Number of bytes received on the interface. • Output bytes—Number of bytes transmitted on the interface. • Input packets—Number of packets received on the interface. • Output packets—Number of packets transmitted on the interface. 	All levels

Sample Output

show interfaces (Multicast Tunnel)

```
user@host> show interfaces mt-1/2/0
Physical interface: mt-1/2/0, Enabled, Physical link is Up
Interface index: 145, SNMP ifIndex: 41
Type: Multicast-GRE, Link-level type: GRE, MTU: Unlimited, Speed: 800mbps
Device flags   : Present Running
Interface flags: SNMP-Traps
Input rate     : 0 bps (0 pps)
Output rate    : 0 bps (0 pps)
```

show interfaces brief (Multicast Tunnel)

```
user@host> show interfaces mt-1/2/0 brief
Physical interface: mt-1/2/0, Enabled, Physical link is Up
Type: Multicast-GRE, Link-level type: GRE, MTU: Unlimited, Speed: 800mbps
Device flags   : Present Running
Interface flags: SNMP-Traps
```

show interfaces detail (Multicast Tunnel)

```
user@host> show interfaces mt-1/2/0 detail
Physical interface: mt-1/2/0, Enabled, Physical link is Up
Interface index: 145, SNMP ifIndex: 41, Generation: 28
Type: Multicast-GRE, Link-level type: GRE, MTU: Unlimited, Speed: 800mbps
Hold-times     : Up 0 ms, Down 0 ms
Device flags   : Present Running
Interface flags: SNMP-Traps
Statistics last cleared: Never
Traffic statistics:
  Input bytes   :          170664562          560000 bps
  Output bytes  :          112345376          368176 bps
  Input packets :           2439107           1000 pps
  Output packets:          2439120           1000 pps
```

show interfaces extensive (Multicast Tunnel)

```
user@host> show interfaces mt-1/2/0 extensive
Physical interface: mt-1/2/0, Enabled, Physical link is Up
Interface index: 141, SNMP ifIndex: 529, Generation: 144
Type: Multicast-GRE, Link-level type: GRE, MTU: Unlimited, Speed: 800mbps
Hold-times     : Up 0 ms, Down 0 ms
Device flags   : Present Running
Interface flags: SNMP-Traps
Statistics last cleared: Never
```

```
Traffic statistics:
Input bytes :          170664562          560000 bps
Output bytes :          112345376          368176 bps
Input packets:           2439107           1000 pps
Output packets:          2439120           1000 pps
IPv6 transit statistics:
Input bytes :              0
Output bytes :              0
Input packets:              0
Output packets:              0
```

Logical interface mt-1/2/0.32768 (Index 83) (SNMP ifIndex 556) (Generation 148)

Flags: Point-To-Point SNMP-Traps 0x4000 IP-Header
232.1.1.1:10.0.0.6:47:df:64:0000000800000000 Encapsulation: GRE=NULL

```
Traffic statistics:
Input bytes :          170418430
Output bytes :          112070294
Input packets:           2434549
Output packets:          2435593
IPv6 transit statistics:
Input bytes :              0
Output bytes :              0
Input packets:              0
Output packets:              0
Local statistics:
Input bytes :              0
Output bytes :             80442
Input packets:              0
Output packets:            1031
Transit statistics:
Input bytes :          170418430          560000 bps
Output bytes :          111989852          368176 bps
Input packets:           2434549           1000 pps
Output packets:          2434562           1000 pps
IPv6 transit statistics:
Input bytes :              0
Output bytes :              0
Input packets:              0
Output packets:              0
Protocol inet, MTU: 1572, Generation: 182, Route table: 4
Flags: None
Protocol inet6, MTU: 1572, Generation: 183, Route table: 4
Flags: None
```

Logical interface mt-1/2/0.1081344 (Index 84) (SNMP ifIndex 560) (Generation 149)

```
Flags: Point-To-Point SNMP-Traps 0x6000 Encapsulation: GRE=NULL
Traffic statistics:
Input bytes :          246132
Output bytes :          355524
Input packets:           4558
Output packets:          4558
IPv6 transit statistics:
Input bytes :              0
Output bytes :              0
Input packets:              0
Output packets:              0
Local statistics:
Input bytes :          246132
Output bytes :              0
```

```

Input packets:          4558
Output packets:         0
Transit statistics:
Input bytes :           0          0 bps
Output bytes :         355524      0 bps
Input packets:         0          0 pps
Output packets:        4558        0 pps
IPv6 transit statistics:
Input bytes :           0
Output bytes :           0
Input packets:         0
Output packets:        0
Protocol inet, MTU: Unlimited, Generation: 184, Route table: 4
Flags: None
Protocol inet6, MTU: Unlimited, Generation: 185, Route table: 4
Flags: None

```

show interfaces (Multicast Tunnel Encapsulation)

```

user@host> show interfaces mt-3/1/0.32768
Logical interface mt-3/1/0.32768 (Index 67) (SNMP ifIndex 0)
  Flags: Point-To-Point SNMP-Traps 0x4000
  IP-Header 239.1.1.1:10.255.70.15:47:df:64:0000000800000000
  Encapsulation: GRE-NULL
Input packets : 0
Output packets: 2
  Protocol inet, MTU: Unlimited
  Flags: None

```

show interfaces (Multicast Tunnel De-Encapsulation)

```

user@host> show interfaces mt-3/1/0.49152
Logical interface mt-3/1/0.49152 (Index 74) (SNMP ifIndex 0)
  Flags: Point-To-Point SNMP-Traps 0x6000 Encapsulation: GRE-NULL
Input packets : 0
Output packets: 2
  Protocol inet, MTU: Unlimited
  Flags: None

```

show interfaces (PIM)

Syntax	<pre>show interfaces <i>interface-type</i> <brief detail extensive terse> <descriptions> <media> <snmp-index <i>snmp-index</i>> <statistics></pre>
Release Information	Command introduced before Junos OS Release 7.4.
Description	Display status information about the specified Protocol Independent Multicast (PIM) de-encapsulation or PIM encapsulation interface, respectively.
Options	<p><i>interface-type</i>—On M Series and T Series routers, the PIM de-encapsulation interface type is pd-fpc/pic/port. On J Series routers, it is pd-pim/O/port. On M Series and T Series routers, the PIM encapsulation interface type is pe-fpc/pic/port. On J Series routers, it is pe-pim/O/port.</p> <p>brief detail extensive terse—(Optional) Display the specified level of output.</p> <p>descriptions—(Optional) Display interface description strings.</p> <p>media—(Optional) Display media-specific information about network interfaces.</p> <p>snmp-index <i>snmp-index</i>—(Optional) Display information for the specified SNMP index of the interface.</p> <p>statistics—(Optional) Display static interface statistics.</p>
Required Privilege Level	view
List of Sample Output	<p>show interfaces (PIM De-Encapsulation) on page 75</p> <p>show interfaces brief (PIM De-Encapsulation) on page 76</p> <p>show interfaces detail (PIM De-Encapsulation) on page 76</p> <p>show interfaces extensive (PIM Encapsulation) on page 76</p> <p>show interfaces (PIM Encapsulation) on page 76</p> <p>show interfaces brief (PIM Encapsulation) on page 76</p> <p>show interfaces detail (PIM Encapsulation) on page 77</p> <p>show interfaces extensive (PIM Encapsulation) on page 77</p>
Output Fields	Table 9 on page 74 lists the output fields for the show interfaces (PIM de-encapsulation or encapsulation) command. Output fields are listed in the approximate order in which they appear.

Table 9: PIM show interfaces Output Fields

Field Name	Field Description	Level of Output
Physical Interface		
Physical interface	Name of the physical interface.	All levels

Table 9: PIM show interfaces Output Fields (*continued*)

Field Name	Field Description	Level of Output
Enabled	State of the interface. Possible values are described in the “Enabled Field” section under <i>Common Output Fields Description</i> .	All levels
Interface index	Physical interface's index number, which reflects its initialization sequence.	detail extensive none
SNMP ifIndex	SNMP index number for the physical interface.	detail extensive none
Generation	Unique number for use by Juniper Networks technical support only.	detail extensive
Type	Type of interface.	All levels
Link-level type	Encapsulation used on the physical interface.	All levels
MTU	MTU size on the physical interface.	All levels
Speed	Speed at which the interface is running.	All levels
Hold-times	Current interface hold-time up and hold-time down, in milliseconds.	detail extensive
Device flags	Information about the physical device. Possible values are described in the “Device Flags” section under <i>Common Output Fields Description</i> .	All levels
Interface flags	Information about the interface. Possible values are described in the “Interface Flags” section under <i>Common Output Fields Description</i> .	All levels
Input Rate	Input rate in bits per second (bps) and packets per second (pps).	None specified
Output Rate	Output rate in bps and pps.	None specified
Statistics last cleared	Time when the statistics for the interface were last set to zero.	detail extensive
Traffic statistics	Number and rate of bytes and packets received and transmitted on the physical interface. <ul style="list-style-type: none"> • Input bytes—Number of bytes received on the interface. • Output bytes—Number of bytes transmitted on the interface. • Input packets—Number of packets received on the interface. • Output packets—Number of packets transmitted on the interface. 	detail extensive

Sample Output

show interfaces (PIM De-Encapsulation)

```

user@host> show interfaces pd-0/0/0
Physical interface: pd-0/0/0, Enabled, Physical link is Up
  Interface index: 130, SNMP ifIndex: 25
  Type: PIMD, Link-level type: PIM-Decapsulator, MTU: Unlimited, Speed: 800mbps
  Device flags   : Present Running

```

```
Interface flags: SNMP-Traps
Input rate      : 0 bps (0 pps)
Output rate     : 0 bps (0 pps)
```

show interfaces brief (PIM De-Encapsulation)

```
user@host> show interfaces pd-0/0/0 brief
Physical interface: pd-0/0/0, Enabled, Physical link is Up
Type: PIMD, Link-level type: PIM-Decapsulator, MTU: Unlimited, Speed: 800mbps
Device flags   : Present Running
Interface flags: SNMP-Traps
```

show interfaces detail (PIM De-Encapsulation)

```
user@host> show interfaces pd-0/0/0 detail
Physical interface: pd-0/0/0, Enabled, Physical link is Up
Interface index: 130, SNMP ifIndex: 25, Generation: 11
Type: PIMD, Link-level type: PIM-Decapsulator, MTU: Unlimited, Speed: 800mbps
Hold-times      : Up 0 ms, Down 0 ms
Device flags    : Present Running
Interface flags: SNMP-Traps
Statistics last cleared: Never
Traffic statistics:
Input bytes      : 0                      0 bps
Output bytes     : 0                      0 bps
Input packets    : 0                      0 pps
Output packets   : 0                      0 pps
```

show interfaces extensive (PIM Encapsulation)

```
user@host> show interfaces pd-0/0/0 extensive
Physical interface: pd-0/0/0, Enabled, Physical link is Up
Interface index: 130, SNMP ifIndex: 25, Generation: 11
Type: PIMD, Link-level type: PIM-Decapsulator, MTU: Unlimited, Speed: 800mbps
Hold-times      : Up 0 ms, Down 0 ms
Device flags    : Present Running
Interface flags: SNMP-Traps
Statistics last cleared: Never
Traffic statistics:
Input bytes      : 0                      0 bps
Output bytes     : 0                      0 bps
Input packets    : 0                      0 pps
Output packets   : 0                      0 pps
```

show interfaces (PIM Encapsulation)

```
user@host> show interfaces pe-0/0/0
Physical interface: pe-0/0/0, Enabled, Physical link is Up
Interface index: 131, SNMP ifIndex: 26
Type: PIME, Link-level type: PIM-Encapsulator, MTU: Unlimited, Speed: 800mbps
Device flags    : Present Running
Interface flags: SNMP-Traps
Input rate      : 0 bps (0 pps)
Output rate     : 0 bps (0 pps)
```

show interfaces brief (PIM Encapsulation)

```
user@host> show interfaces pe-0/0/0 brief
Physical interface: pe-0/0/0, Enabled, Physical link is Up
Type: PIME, Link-level type: PIM-Encapsulator, MTU: Unlimited, Speed: 800mbps
```



```
Device flags   : Present Running
Interface flags: SNMP-Traps
```

show interfaces detail (PIM Encapsulation)

```
user@host> show interfaces pe-0/0/0 detail
Physical interface: pe-0/0/0, Enabled, Physical link is Up
Interface index: 131, SNMP ifIndex: 26, Generation: 12
Type: PIME, Link-level type: PIM-Encapsulator, MTU: Unlimited, Speed: 800mbps
Hold-times     : Up 0 ms, Down 0 ms
Device flags   : Present Running
Interface flags: SNMP-Traps
Statistics last cleared: Never
Traffic statistics:
Input bytes   :                0                0 bps
Output bytes  :                0                0 bps
Input packets :                0                0 pps
Output packets:               0                0 pps
```

show interfaces extensive (PIM Encapsulation)

```
user@host> show interfaces pe-0/0/0 extensive
Physical interface: pe-0/0/0, Enabled, Physical link is Up
Interface index: 131, SNMP ifIndex: 26, Generation: 12
Type: PIME, Link-level type: PIM-Encapsulator, MTU: Unlimited, Speed: 800mbps
Hold-times     : Up 0 ms, Down 0 ms
Device flags   : Present Running
Interface flags: SNMP-Traps
Statistics last cleared: Never
Traffic statistics:
Input bytes   :                0                0 bps
Output bytes  :                0                0 bps
Input packets :                0                0 pps
Output packets:               0                0 pps
```

show interfaces (Virtual Loopback Tunnel)

Syntax	<pre>show interfaces vt-fpc/pic/port <brief detail extensive terse> <descriptions> <media> <snmp-index snmp-index> <statistics></pre>
Release Information	Command introduced before Junos OS Release 7.4.
Description	Display status information about the specified virtual loopback tunnel interface.
Options	<p>vt-fpc/pic/port—Display standard information about the specified virtual loopback tunnel interface.</p> <p>brief detail extensive terse—(Optional) Display the specified level of output.</p> <p>descriptions—(Optional) Display interface description strings.</p> <p>media—(Optional) Display media-specific information about network interfaces.</p> <p>snmp-index snmp-index—(Optional) Display information for the specified SNMP index of the interface.</p> <p>statistics—(Optional) Display static interface statistics.</p>
Required Privilege Level	view
List of Sample Output	show interfaces (Virtual Loopback Tunnel) on page 80 show interfaces brief (Virtual Loopback Tunnel) on page 81 show interfaces detail (Virtual Loopback Tunnel) on page 81 show interfaces extensive (Virtual Loopback Tunnel) on page 81
Output Fields	Table 10 on page 78 lists the output fields for the show interfaces (virtual loopback tunnel) command. Output fields are listed in the approximate order in which they appear.

Table 10: Virtual Loopback Tunnel show interfaces Output Fields

Field Name	Field Description	Level of Output
Physical Interface		
Physical interface	Name of the physical interface.	All levels
Enabled	State of the interface. Possible values are described in the "Enabled Field" section under <i>Common Output Fields Description</i> .	All levels
Interface index	Physical interface's index number, which reflects its initialization sequence.	detail extensive none
SNMP ifIndex	SNMP index number for the physical interface.	detail extensive none

Table 10: Virtual Loopback Tunnel show interfaces Output Fields (*continued*)

Field Name	Field Description	Level of Output
Generation	Unique number for use by Juniper Networks technical support only.	detail extensive
Type	Type of interface.	All levels
Link-level type	Encapsulation used on the physical interface.	All levels
MTU	MTU size on the physical interface.	All levels
Speed	Speed at which the interface is running.	All levels
Hold-times	Current interface hold-time up and hold-time down, in milliseconds.	detail extensive
Device flags	Information about the physical device. Possible values are described in the "Device Flags" section under <i>Common Output Fields Description</i> .	All levels
Input Rate	Input rate in bits per second (bps) and packets per second (pps).	None specified
Output Rate	Output rate in bps and pps.	None specified
Statistics last cleared	Time when the statistics for the interface were last set to zero.	detail extensive
Traffic statistics	Number and rate of bytes and packets received and transmitted on the physical interface. <ul style="list-style-type: none"> • Input bytes, Output bytes—Number of bytes received and transmitted on the interface. • Input packets, Output packets—Number of packets received and transmitted on the interface. 	detail extensive
Logical Interface		
Logical interface	Name of the logical interface.	All levels
Index	Logical interface index number, which reflects its initialization sequence.	detail extensive none
SNMP ifIndex	Logical interface SNMP interface index number.	detail extensive none
Generation	Unique number for use by Juniper Networks technical support only.	detail extensive
Flags	Information about the logical interface. Possible values are described in the "Interface Flags" section under <i>Common Output Fields Description</i> .	All levels
Encapsulation	Encapsulation on the logical interface.	All levels
Input packets	Number of packets received on the logical interface.	None specified
Output packets	Number of packets transmitted on the logical interface.	None specified

Table 10: Virtual Loopback Tunnel show interfaces Output Fields (*continued*)

Field Name	Field Description	Level of Output
Bandwidth	Bandwidth allotted to the logical interface, in kilobytes per second.	All levels
Traffic statistics	<p>Total number of bytes and packets received and transmitted on the logical interface. These statistics are the sum of the local and transit statistics. When a burst of traffic is received, the value in the output packet rate field might briefly exceed the peak cell rate. It takes awhile (generally, less than 1 second) for this counter to stabilize.</p> <ul style="list-style-type: none"> • Input bytes—Number of bytes received on the interface. • Output bytes—Number of bytes transmitted on the interface. • Input packets—Number of packets received on the interface. • Output packets—Number of packets transmitted on the interface. 	detail extensive
Transit statistics	Statistics for traffic transiting the router. When a burst of traffic is received, the value in the output packet rate field might briefly exceed the peak cell rate. It takes awhile (generally, less than 1 second) for this counter to stabilize.	detail extensive
<i>protocol-family</i>	Protocol family configured on the logical interface. Possible values are described in the “Family Flags” section under <i>Common Output Fields Description</i> .	brief
Protocol	Protocol family configured on the logical interface. Possible values are described in the “Family Flags” section under <i>Common Output Fields Description</i> .	detail extensive none
MTU	Maximum transmission unit size on the logical interface.	detail extensive none
Maximum labels	Maximum number of MPLS labels configured for the MPLS protocol family on the logical interface.	detail extensive none
Generation	Unique number for use by Juniper Networks technical support only.	detail extensive
Route Table	Routing table in which the logical interface address is located. For example, 0 refers to the routing table inet.0.	detail extensive
Flags	Information about protocol family flags. Possible values are described in the “Family Flags” section under <i>Common Output Fields Description</i> .	detail extensive none

Sample Output

show interfaces (Virtual Loopback Tunnel)

```

user@host> show interfaces vt-1/2/0
Physical interface: vt-1/2/0, Enabled, Physical link is Up
  Interface index: 144, SNMP ifIndex: 40
  Type: Loopback, Link-level type: Virtual-loopback-tunnel, MTU: Unlimited,
  Speed: 800mbps
  Device flags      : Present Running
  Input rate       : 0 bps (0 pps)
  Output rate      : 0 bps (0 pps)

Logical interface vt-1/2/0.0 (Index 76) (SNMP ifIndex 57)
  Flags: Point-To-Point 16384 Encapsulation: Virtual-loopback-tunnel

```

```

Input packets : 0
Output packets: 0
  Protocol inet, MTU: Unlimited
    Flags: None
  Protocol mpls, MTU: Unlimited, Maximum labels: 3
    Flags: None

```

show interfaces brief (Virtual Loopback Tunnel)

```

user@host> show interfaces vt-1/2/0 brief
Physical interface: vt-1/2/0, Enabled, Physical link is Up
  Type: Loopback, Link-level type: Virtual-loopback-tunnel, MTU: Unlimited,
  Speed: 800mbps
  Device flags   : Present Running

Logical interface vt-1/2/0.0
  Flags: Point-To-Point 16384 Encapsulation: Virtual-loopback-tunnel
  inet
  mpls

```

show interfaces detail (Virtual Loopback Tunnel)

```

user@host> show interfaces vt-1/2/0 detail
Physical interface: vt-1/2/0, Enabled, Physical link is Up
  Interface index: 144, SNMP ifIndex: 40, Generation: 27
  Type: Loopback, Link-level type: Virtual-loopback-tunnel, MTU: Unlimited,
  Speed: 800mbps
  Hold-times      : Up 0 ms, Down 0 ms
  Device flags    : Present Running
  Statistics last cleared: Never
  Traffic statistics:
    Input bytes   :                0                0 bps
    Output bytes  :                0                0 bps
    Input packets :                0                0 pps
    Output packets:                0                0 pps

Logical interface vt-1/2/0.0 (Index 76) (SNMP ifIndex 57) (Generation 17)
  Flags: Point-To-Point 16384 Encapsulation: Virtual-loopback-tunnel
  Traffic statistics:
    Input bytes   :                0
    Output bytes  :                0
    Input packets :                0
    Output packets:                0
  Transit statistics:
    Input bytes   :                0                0 bps
    Output bytes  :                0                0 bps
    Input packets :                0                0 pps
    Output packets:                0                0 pps
  Protocol inet, MTU: Unlimited, Generation: 33, Route table: 0
    Flags: None
  Protocol mpls, MTU: Unlimited, Maximum labels: 3, Generation: 34, Route table:
0
    Flags: None

```

show interfaces extensive (Virtual Loopback Tunnel)

```

user@host> show interfaces vt-1/2/0 extensive
Physical interface: vt-1/2/0, Enabled, Physical link is Up
  Interface index: 144, SNMP ifIndex: 40, Generation: 27
  Type: Loopback, Link-level type: Virtual-loopback-tunnel, MTU: Unlimited,
  Speed: 800mbps
  Hold-times      : Up 0 ms, Down 0 ms

```

Device flags : Present Running

Statistics last cleared: Never

Traffic statistics:

Input bytes :	0	0 bps
Output bytes :	0	0 bps
Input packets:	0	0 pps
Output packets:	0	0 pps

Logical interface vt-1/2/0.0 (Index 76) (SNMP ifIndex 57) (Generation 17)

Flags: Point-To-Point 16384 Encapsulation: Virtual-loopback-tunnel

Traffic statistics:

Input bytes :	0
Output bytes :	0
Input packets:	0
Output packets:	0

Transit statistics:

Input bytes :	0	0 bps
Output bytes :	0	0 bps
Input packets:	0	0 pps
Output packets:	0	0 pps

Protocol inet, MTU: Unlimited, Generation: 33, Route table: 0

Flags: None

Protocol mpls, MTU: Unlimited, Maximum labels: 3, Generation: 34, Route table:

0

Flags: None

PART 4

Index

- [Index on page 85](#)

Index

Symbols

#, comments in configuration statements.....	x
(), in syntax descriptions.....	x
< >, in syntax descriptions.....	x
[], in configuration statements.....	x
{ }, in configuration statements.....	x
(pipe), in syntax descriptions.....	x

A

allow-fragmentation statement.....	33
usage guidelines.....	13

B

backup-destination statement.....	34
braces, in configuration statements.....	x
brackets	
angle, in syntax descriptions.....	x
square, in configuration statements.....	x

C

clear-dont-fragment-bit statement	
usage guidelines.....	12
comments, in configuration statements.....	x
conventions	
text and syntax.....	ix
copy-tos-to-outer-ip-header statement.....	34
usage guidelines.....	13
CoS	
for tunnels	
GRE TOS bits.....	13
curly braces, in configuration statements.....	x
customer support.....	xi
contacting JTAC.....	xi

D

destination statement	
tunnel	
usage guidelines.....	9, 19
destination-networks statement	
tunnel.....	36
usage guidelines.....	22

do-not-fragment statement	
tunnel.....	37
usage guidelines.....	13
documentation	
comments on.....	xi
dynamic tunnels.....	38
destination.....	36
source.....	45
dynamic-tunnels statement.....	38
usage guidelines.....	22

F

font conventions.....	ix
fragmentation	
GRE tunnels.....	12

G

GRE interfaces	
status information, displaying.....	52
GRE tunnels	
fragmentation.....	12
key number.....	11

H

hold-time statement	
GRE tunnel interface.....	39

I

interfaces statement	
tunnel.....	39
usage guidelines.....	9
IP-over-IP interfaces	
status information, displaying.....	59
IPv6	
transition	
configured tunnel.....	22
IPv6-over-IPv4 tunnel	
example configuration.....	29
standards supported.....	22

K

keepalive-time statement	
GRE tunnel interface.....	40
key statement	
tunnel.....	41
usage guidelines.....	11

L

logical tunnel interfaces	
status information, displaying.....	64
logical tunnels.....	17
example configuration.....	30
loopback tunnels.....	19

M

manuals	
comments on.....	xi
multicast tunnel interfaces	
status information, displaying.....	69
multicast tunnels.....	17
multicast-only statement.....	41
usage guidelines.....	17

P

parentheses, in syntax descriptions.....	x
peer-unit statement	
tunnel.....	42
usage guidelines.....	17
PIM	
tunnels.....	21
PIM de-encapsulation interfaces	
status information, displaying.....	74
PIM encapsulation interfaces	
status information, displaying.....	74

R

reassemble-packets statement.....	42
usage guidelines.....	13
RFC 2890.....	11
routing-instance statement	
tunnel.....	43
usage guidelines.....	19
routing-instances statement.....	43
routing-options statement.....	44

S

show interfaces (GRE) command.....	52
show interfaces (IP-over-IP) command.....	59
show interfaces (Logical Tunnel) command.....	64
show interfaces (Multicast Tunnel) command.....	69
show interfaces (PIM) command.....	74
show interfaces (Virtual Loopback Tunnel)	
command.....	78
source statement	
tunnel.....	44

source-address statement	
tunnel.....	45
tunnel services	
usage guidelines.....	22
support, technical See technical support	
syntax conventions.....	ix

T

technical support	
contacting JTAC.....	xi
ttl statement	
tunnel.....	45
tunnel interfaces	
configuration statements.....	9, 17, 19
dynamic tunnels.....	22
example configuration.....	27
logical tunnels.....	17
loopback tunnels.....	19
multicast tunnels.....	17
PIM tunnels.....	21
unicast tunnels.....	9
tunnel services interfaces.....	82
tunnel statement.....	46
unicast	
usage guidelines.....	9
tunnels	
definition.....	3
GRE	
fragmentation of.....	12
key number.....	11
interface types.....	3
IPv6-over-IPv4.....	22, 29

U

unicast tunnels.....	9
unit statement	
tunnel.....	47
usage guidelines.....	9

V

virtual loopback tunnel	
configuration guidelines.....	19
VRF table lookup	
example configuration.....	28
virtual loopback tunnel interfaces	
status information, displaying.....	78