

# T-U-V-W-X-Y-Z Commands

## t1 bert

---

**Description** Enables bit error rate tests using the specified pattern on a T1 line on a CT3 module. The **no** version stops the test that is running.

**Syntax** `t1 channel bert pattern pattern interval time [ unframed ]`  
`no t1 channel bert`

- *channel*—One or more individual T1 channels, ranges of T1 channels, or combination of individual channels and ranges, in the range 1–28 (no spaces); for example, 3,7-15,19-13,27
- *pattern*—One of the following test patterns
  - 0s—Repetitive test pattern of all zeros, 00000...
  - 1s—Repetitive test pattern of all ones, 11111...
  - 2^11—Pseudorandom test pattern, 2047 bits in length
  - 2^15—Pseudorandom test pattern, 32767 bits in length
  - 2^20-O153—Pseudorandom test pattern, 1048575 bits in length
  - 2^20-QRSS—Pseudorandom QRSS test pattern, 1048575 bits in length
  - 2^23—Pseudorandom test pattern, 8388607 bits in length
  - alt-0-1—Repetitive alternating test pattern of zeros and ones, 01010101...
- *time*—Duration of the test in the range 1–1440 minutes
- *unframed*—Specifies that the test bit pattern occupies all bits on the link, overwriting the framing bits. If you do not specify the **unframed** keyword, then the test bit pattern occupies only T1 payload bits.

**Mode** Controller Configuration

**Release Information** Command introduced before JUNOS Release 7.1.0.

## t1 clock source

---

- Description** Determines which end of the T1 interface provides clocking. The **no** version uses the default value, **line**.
- Syntax** `t1 channel clock source { line | internal { module | chassis } }`  
`no t1 channel clock source`
- *channel*—One or more individual T1 channels, ranges of T1 channels, or combination of individual channels and ranges, in the range 1–28 (no spaces); for example, 3,7-15,19-13,27
  - *line*—Interface transmits data from a clock recovered from the line's receive data stream
  - *internal*—Interface transmits data using its internal clock. You must specify one of the following for internal clocking:
    - *module*—Internal clock is from the line module itself
    - *chassis*—Internal clock is from the configured system clock
- Mode** Controller Configuration
- Release Information** Command introduced before JUNOS Release 7.1.0.

## t1 description

---

- Description** Assigns a text description or an alias to a T1 or fractional T1 channel on a CT3 module. Use the **show controllers t1** command to display the text description. The **no** version removes the description or alias.
- Syntax** `t1 channel [ /subchannel ] description name`  
`no t1 channel [ /subchannel ] description`
- *channel*—One or more individual T1 channels, ranges of T1 channels, or combination of individual channels and ranges, in the range 1–28 (no spaces); for example, 3,7-15,19-13,27
  - *subchannel*—FT1 subchannel on a T1 interface in the range 1–24
  - *name*—Text string or alias of up to 80 characters for the T1 or fractional T1 channel on the CT3 module
- Mode** Controller Configuration
- Release Information** Command introduced before JUNOS Release 7.1.0.

**t1 fdl**


---

<b>Description</b>	Specifies the FDL standard used by a specific T1 channel on the CT3 interface. The <b>no</b> version restores the default, none.
<b>Syntax</b>	<p>t1 <i>channel</i> fdl { ansi   att   all   none }</p> <p>no t1 <i>channel</i> fdl [ ansi   att   all ]</p> <ul style="list-style-type: none"> <li>■ <i>channel</i>—One or more individual T1 channels, ranges of T1 channels, or combination of individual channels and ranges, in the range 1–28 (no spaces); for example, 3,7-15,19-13,27</li> <li>■ ansi—Specifies ANSI T1.403 Standard for extended superframe FDL exchange support</li> <li>■ att—Specifies AT&amp;T Technical Reference 54016 for extended superframe FDL exchange support</li> <li>■ all—Specifies both the AT&amp;T and ANSI mode for extended superframe FDL exchange support</li> <li>■ none—Removes the current FDL mode settings</li> </ul>
<b>Mode</b>	Controller Configuration
<b>Release Information</b>	Command introduced before JUNOS Release 7.1.0.

**t1 fdl carrier**


---

<b>Description</b>	Specifies that an interface is used in the carrier environment of a T1 channel on a CT3 interface. The <b>no</b> version restores the default situation, in which an interface does not operate in the carrier environment.
<b>Syntax</b>	<p>[ no ] t1 <i>channel</i> fdl carrier</p> <ul style="list-style-type: none"> <li>■ <i>channel</i>—One or more individual T1 channels, ranges of T1 channels, or combination of individual channels and ranges, in the range 1–28 (no spaces); for example, 3,7-15,19-13,27</li> </ul>
<b>Mode</b>	Controller Configuration
<b>Release Information</b>	Command introduced before JUNOS Release 7.1.0.

## t1 fdl string

---

**Description** Defines an FDL message on a T1 channel on a CT3 interface as defined in the ANSI T1.403 specification. Currently, FDL strings can be configured only locally. The **no** version restores the default value to the specified FDL message or to all FDL messages.

**Syntax** `t1 channel fdl string { eic eicValue | fic ficValue | lic licValue | unit unitValue | pfi pfiValue | port portValue | generator generatorValue }`  
`no t1 channel fdl string { eic | fic | lic | unit | pfi | port | generator }`

- *channel*—One or more individual T1 channels, ranges of T1 channels, or combination of individual channels and ranges, in the range 1–28 (no spaces); for example, 3,7-15,19-13,27
- *eicValue*—Equipment identification code; 1–10 characters; default value is the null value
- *ficValue*—Frame identification code; 1–10 characters; default value is the null value
- *licValue*—Line identification code; 1–10 characters; default value is the null value
- *unitValue*—Unit identification code; 1–6 characters; default value is the null value.
- *pfiValue*—Facility identification code to send in the FDL path message; 1–38 characters; default value is the null value.
- *portValue*—Equipment port number to send in the FDL idle signal message; 1–38 characters; default value is the null value.
- *generatorValue*—Generator number to send in the FDL test signal message; 1–38 characters; default value is the null value.

**Mode** Controller Configuration

**Release Information** Command introduced before JUNOS Release 7.1.0.

## t1 fdl transmit

---

**Description** Configures the router to send the specified FDL message on a T1 channel on a CT3 interface. The **no** version stops the router from sending the specified FDL message or all FDL messages.

**Syntax** `t1 channel fdl transmit { path-id | idle-signal | test-signal }`  
`no t1 channel fdl transmit [ path-id | idle-signal | test-signal ]`

- *channel*—One or more individual T1 channels, ranges of T1 channels, or combination of individual channels and ranges, in the range 1–28 (no spaces); for example, 3,7-15,19-13,27
- *path-id*—Transmits a path identification message every second; default value is disabled
- *idle-signal*—Transmits an idle signal message every second; default value is disabled
- *test-signal*—Transmits a test signal message every second; default value is disabled

**Mode** Controller Configuration

**Release Information** Command introduced before JUNOS Release 7.1.0.

## t1 framing

---

**Description** Specifies the type of framing used by a specific T1 channel on a CT3 interface. The **no** version restores the default value, *esf*.

**Syntax** `t1 channel framing { esf | sf }`  
`no t1 channel framing`

- *channel*—One or more individual T1 channels, ranges of T1 channels, or combination of individual channels and ranges, in the range 1–28 (no spaces); for example, 3,7-15,19-13,27
- *esf*—Specifies extended superframe
- *sf*—Specifies superframe

**Mode** Controller Configuration

**Release Information** Command introduced before JUNOS Release 7.1.0.

## t1 lineCoding

---

**Description** Specifies the type of line coding used by a specific T1 channel on a CT3 interface. The **no** version restores the default value, b8zs.

---



**NOTE:** This command is deprecated and may be removed completely in a future release. No alternate command exists, because line coding can be specified only on the bottom layer.

---

**Syntax** `t1 channel lineCoding { ami | b8zs }`  
`no t1 channel lineCoding`

- *channel*—One or more individual T1 channels, ranges of T1 channels, or combination of individual channels and ranges, in the range 1–28 (no spaces); for example, 3,7-15,19-13,27
- *ami*—Specifies alternate mark inversion
- *b8zs*—Specifies bipolar with eight-zero substitution

**Mode** Controller Configuration

**Release Information** Command introduced before JUNOS Release 7.1.0.

## t1 loopback

---

<b>Description</b>	Configures a loopback test for a T1 line on a CT3 module. The <b>no</b> version deactivates the loopback test; if you specify the <b>remote</b> keyword, the <b>no</b> version sends the 16-bit ESF data link code word or inband pattern to deactivate the loopback at the remote end based on the last activate request sent to the remote end. If you do not specify the <b>remote</b> keyword, the <b>no</b> version clears the local loopback configuration.
<b>Syntax</b>	<pre>t1 t1Channel loopback [ local   network { line   payload } ] no t1 t1Channel loopback  t1 t1Channel loopback remote { line { fdl { ansi   bellcore }   inband }   payload [ fdl ] [ ansi ] } no t1 t1Channel loopback remote</pre> <ul style="list-style-type: none"> <li>■ <i>t1Channel</i>—One or more individual T1 channels, ranges of T1 channels, or combination of individual channels and ranges, in the range 1–28 (no spaces); for example, 3,7-15,19-13,27</li> <li>■ <i>local</i>—Loops the router output data back toward the router at the T1 framer; on supported line modules also sends an alarm indication signal (AIS) out toward the network. This is the default setting if you specify no optional keywords.</li> <li>■ <i>network line</i>—Loops the data back toward the network before the T1 framer and automatically sets a local loopback at the HDLC controllers</li> <li>■ <i>network payload</i>—Loops the payload data back toward the network at the T1 framer and automatically sets a local loopback at the HDLC controllers</li> <li>■ <i>remote line fdl ansi</i>—Sends a repeating 16-bit ESF data link code word (00001110 11111111) to the remote end requesting that it enter into a network line loopback. The <b>ansi</b> keyword enables the remote line FDL ANSI bit loopback on the T1 channel, according to the ANSI T1.403 specification.</li> <li>■ <i>remote line fdl bellcore</i>—Sends a repeating 16-bit ESF data link code word (00010010 11111111) to the remote end, requesting that it enter into a network line loopback. The <b>bellcore</b> keyword enables the remote line FDL Bellcore bit loopback on the T1 channel, according to the Bellcore TR-TSY-000312 specification.</li> <li>■ <i>remote line inband</i>—Sends a repeating 5-bit inband pattern (00001) to the remote end, requesting that it enter into a network line loopback</li> <li>■ <i>remote payload [ fdl ] [ ansi ]</i>—Sends a repeating 16-bit ESF data link code word (00010100 11111111) to the remote end, requesting that it enter into a network payload loopback. Enables the remote payload FDL ANSI bit loopback on the T1 channel. You can optionally specify <i>fdl</i> and <i>ansi</i>, but it is not necessary.</li> </ul>
<b>Mode</b>	Controller Configuration
<b>Release Information</b>	Command introduced before JUNOS Release 7.1.0.

## t1 remote-loopback

---

**Description** Enables the acceptance of loopback commands issued from a remote router. The **no** version restores the default value, which is to reject loopback commands issued from a remote router.

**Syntax** [ no ] t1 *channel* remote-loopback

- *channel*—One or more individual T1 channels, ranges of T1 channels, or combination of individual channels and ranges, in the range 1–28 (no spaces); for example, 3,7-15,19-13,27

**Mode** Controller Configuration

**Release Information** Command introduced before JUNOS Release 7.1.0.

## t1 shutdown

---

**Description** Disables a T1 or fractional T1 channel on a CT3 interface. The **no** version restarts a disabled interface.

**Syntax** [ no ] t1 *channel* [ /*subchannel* ] shutdown

- *channel*—One or more individual T1 channels, ranges of T1 channels, or combination of individual channels and ranges, in the range 1–28 (no spaces); for example, 3,7-15,19-13,27
- *subchannel*—FT1 subchannel on a T1 interface, in the range 1–24

**Mode** Controller Configuration

**Release Information** Command introduced before JUNOS Release 7.1.0.

## t1 snmp trap link-status

---

**Description** Enables processing of SNMP link status information about a T1 or fractional T1 channel on a CT3 interface. The **no** version disables the processing of SNMP link status information.

**Syntax** [ no ] t1 *channel* [ /*subchannel* ] snmp trap link-status

- *channel*—One or more individual T1 channels, ranges of T1 channels, or combination of individual channels and ranges, in the range 1–28 (no spaces); for example, 3,7-15,19-13,27
- *subchannel*—Specifies the FT1 subchannel on a T1 interface, in the range 1–24

**Mode** Controller Configuration

**Release Information** Command introduced before JUNOS Release 7.1.0.



## t1 timeslots

---

<b>Description</b>	Configures the timeslots and data rate used on each T1 channel on the CT3 interface. The <b>no</b> version deletes the fractional T1 circuit.
<b>Syntax</b>	<pre>t1 <i>channel/subchannel</i> timeslots <i>range</i> [ <i>speed</i> { 56   64 } ]</pre> <pre>no t1 <i>subchannel</i></pre> <ul style="list-style-type: none"> <li>■ <i>channel</i>—T1 channel number in the range 1–28</li> <li>■ <i>subchannel</i>—Subchannel specifies the logical subchannel on a T1 in the range 1–24</li> <li>■ <i>range</i>—Specifies the timeslot assigned to the T1 channel, in the range 1–24. A dash represents a range of timeslots, and a comma separates timeslots. For example, 1-10, 15-18 assigns timeslots 1 through 10 and 15 through 18.</li> <li>■ <i>speed</i>—Specifies the data rate for the T1 channel, either 56 Kbps or 64 Kbps; default value is 64 Kbps</li> </ul>
<b>Mode</b>	Controller Configuration
<b>Release Information</b>	Command introduced before JUNOS Release 7.1.0.

## t1 yellow

---

<b>Description</b>	Generates or detects a yellow alarm for a T1 channel on a CT3 interface. The <b>no</b> version restores the default value, to not generate or to not detect a yellow alarm.
<b>Syntax</b>	<pre>[ no ] t1 <i>channel</i> yellow { generate   detect }</pre> <ul style="list-style-type: none"> <li>■ <i>channel</i>—One or more individual T1 channels, ranges of T1 channels, or combination of individual channels and ranges, in the range 1–28 (no spaces); for example, 3,7-15,19-13,27</li> </ul>
<b>Mode</b>	Controller Configuration
<b>Release Information</b>	Command introduced before JUNOS Release 7.1.0.

## table-map

---

- Description** Applies the specified route map to all BGP, IS-IS, OSPF, or RIP routes about to be added to the IP routing table. The **no** version halts application of the route map.
- Syntax** `table-map mapTag`  
For removing route maps for IS-IS IPv6 only:  
`no table-map`  
For removing route maps for all other cases:  
`no table-map [ mapTag ]`
- *mapTag*—A string of up to 32 alphanumeric characters that specifies the name of the route map; for each protocol, the route map can set only the following values:
    - BGP—Distance, IP next hop, level, metric, metric type, route type, and tag values
    - IS-IS—Distance, level, metric, metric type, origin, preference, route type, and tag values; IS-IS IPv6 supports only a single route map
    - OSPF—Distance, metric, metric type, route type, and tag values
    - RIP—Distance, metric, and tag values
- Mode** Address Family Configuration (BGP, IS-IS, RIP), Router Configuration (BGP, IS-IS, OSPF, RIP)
- Release Information** Command introduced before JUNOS Release 7.1.0.

## tacacs-server host

---

- Description** Adds or deletes a host to or from the list of TACACS+ servers. If the host is not assigned as the primary host, the router assigns an existing host as the primary. The **no** version deletes the host from the list of TACACS+ servers.
- Syntax** `tacacs-server host ipAddress [ port portNumber ] [ timeout timeoutValue ] [ key keyValueString ] [ primary ]`  
`no tacacs-server host ipAddress`
- *ipAddress*—IP address of the TACACS+ server
  - *portNumber*—TACACS+ server's TCP port number in the range 1–65535
  - *timeoutValue*—Response timeout interval for the TACACS+ client to server exchange; number in the range 1–255; default value is 5
  - *keyValueString*—Secret used in TACACS+ client to server exchange; string of up to 100 characters
  - *primary*—Assigns the host as the primary host
- Mode** Global Configuration
- Release Information** Command introduced before JUNOS Release 7.1.0.

## tacacs-server key

---

**Description** Sets or resets the authentication and encryption key value shared by all TACACS+ servers that do not have a server-specific key set up by the **tacacs-server host** command. The **no** version removes the key value shared by all TACACS+ servers.

**Syntax** `tacacs-server key keyValueString`  
`no tacacs-server key`

- *keyValueString*—String of up to 100 characters; must match key configured on the TACACS+ daemon

**Mode** Global Configuration

**Release Information** Command introduced before JUNOS Release 7.1.0.

## tacacs-server source-address

---

**Description** Sets or resets an alternative source address to be used for TACACS+ server communications. The **no** version removes the address.

**Syntax** `tacacs-server source-address ipAddress`  
`no tacacs-server source-address`

- *ipAddress*—IP address used as source by the TACACS+ server

**Mode** Global Configuration

**Release Information** Command introduced before JUNOS Release 7.1.0.

## tacacs-server timeout

---

**Description** Sets the interval in seconds that the server waits for the TACACS+ server host to reply. This value is shared by those TACACS+ servers that do not have a timeout interval set by the **tacacs-server host** command. The **no** version resets the timeout interval shared by all TACACS+ servers.

**Syntax** `tacacs-server timeout timeoutValue`  
`no tacacs-server timeout`

- *timeoutValue*—Response timeout interval for the TACACS+ client to server exchange; number in the range 1–255; default value is 5

**Mode** Global Configuration

**Release Information** Command introduced before JUNOS Release 7.1.0.

## tag

---

**Description** Specifies a user-defined tag. You can configure a tag for both echo and echoPath types. The **no** version removes the tag from the operation.

**Syntax** tag *tagValue*  
no tag

- *tagValue*—Name of a group to which the operation belongs; string of 0–255 ASCII characters; default value is to have no tag

**Mode** RTR Configuration

**Release Information** Command introduced before JUNOS Release 7.1.0.

## tag-group

---

**Description** Configures an interface tag group. The **no** version removes the tag group.

**Syntax** tag-group *tagGroup*  
no tag-group

- *tagGroup*—Name of the interface tag group

**Mode** Interface Configuration

**Release Information** Command introduced in JUNOS Release 8.1.0.

## tcp ack-rst-and-syn

---

**Description** Enables TCP ACK message validation along with TCP RST and SYN attack protection on the virtual router. The **no** version disables this protection.

**Syntax** [ no ] [ ip ] tcp ack-rst-and-syn [ vrf *vrfName* ]

- ip—Optional keyword for use with older scripts
- *vrfName*—Name of the VRF; string of 1–32 alphanumeric characters

**Mode** Global Configuration

**Release Information** Command introduced before JUNOS Release 7.1.0  
ip keyword made optional in JUNOS Release 7.2.0.

## tcp mss

---

**Description** Specifies the MSS value for TCP to use. The **no** version removes the MSS value, and the router uses the advertised MSS derived from the MTU of the output interface.



**NOTE:** The MSS value is equal to the MTU value minus the IP or IPv6 and TCP headers. This means that the MSS value is generally 40 bytes less than the MTU (for IPv4) and 60 bytes less than the MTU (for IPv6).

---

**Syntax** [ ip ] tcp mss [ vrf *vrfName* ] *mssValue*  
no [ ip ] tcp mss [ vrf *vrfName* ]

- *ip*—Optional keyword for use with older scripts
- *vrfName*—Name of the VRF; string of 1–32 alphanumeric characters
- *mssValue*—Value for MSS that you want TCP to use; in the range 536–65495 bytes for IPv4 and 1280–65495 bytes for IPv6

**Mode** Interface Configuration

**Release Information** Command introduced before JUNOS Release 7.1.0.  
**ip** keyword made optional in JUNOS Release 7.2.0.

## tcp path-mtu-discovery

---

**Description** Enables and configures path MTU discovery on the virtual router. Issuing the command without any keywords enables path MTU discovery. Using the keywords with the command configures specified values. The **no** version, when issued with a keyword, deletes the value. When issued without any keywords, the **no** version disables path MTU discovery on the virtual router.

**Syntax** [ ip ] tcp path-mtu-discovery [ vrf *vrfName* ] [ age-timer [ indefinite | *minutes* [ *minutes\_2* ] ] | max-mtu *maxMtu* | min-mtu *minMtu* | black-hole-detect-threshold *blackHoleThreshold* ]

no [ ip ] tcp path-mtu-discovery [ vrf *vrfName* ] [ age-timer | max-mtu | min-mtu | black-hole-detect-threshold ]

- *ip*—Optional keyword for use with older scripts
- *vrfName*—Name of the VRF; string of 1–32 alphanumeric characters
- *indefinite*—Disables aging functions. That is, TCP does not attempt to increase the path MTU; the path MTU decreases only in response to received ICMP Too Big messages.
- *minutes*—Time (in minutes) that TCP waits after receiving an ICMP Too Big message before attempting to increase the path MTU. The timer range is 1–30 minutes.
- *minutes\_2*—Time (in minutes) that TCP waits after a successful path MTU increase before attempting to increase it again. The timer range is 1–30 minutes.
- *maxMtu*—Maximum MTU size that the virtual router can accept; number, in the range 68–65535; default value is no limit
- *minMtu*—Minimum MTU value that the virtual router can accept; number, in the range 68–65535; default value is no limit
- *blackHoleThreshold*—Black hole threshold value that you want all connections on this virtual router to use. The range is 0–65535.

**Mode** Router Configuration

**Release Information** Command introduced before JUNOS Release 7.1.0.  
*ip* keyword made optional in JUNOS Release 7.2.0.

## tcp paws-disable

---

**Description** Disables the Protect Against Wrapped Sequence (PAWS) number option in TCP segments. The **no** version restores PAWS processing (the default mode).

**Syntax** [ no ] [ ip ] tcp paws-disable [ vrf *vrfName* ]

- *ip*—Optional keyword for use with older scripts
- *vrfName*—Name of the VRF; string of 1–32 alphanumeric characters

**Mode** Global Configuration

**Release Information** Command introduced in JUNOS Release 7.1.0.  
**ip** keyword made optional in JUNOS Release 7.2.0.

## tcp resequence-buffers connection-maximum

---

**Description** Defines the maximum number of buffers that connections on the current or specified virtual router can use. Specifying a value of zero (0) turns off the connection maximum. The **no** version reverts the connection maximum value to its default (10 buffers).

**Syntax** [ ip ] tcp resequence-buffers [ vrf *vrfName* ] connection-maximum *connMaxValue*  
 no [ ip ] tcp resequence-buffers [ vrf *vrfName* ] connection-maximum

- *ip*—Optional keyword for use with older scripts
- *vrfName*—Name of the VRF; string of 1–32 alphanumeric characters
- *connMaxValue*—Maximum number of buffers for each virtual router connection, in the range 1–65535

**Mode** Global Configuration

**Release Information** Command introduced before JUNOS Release 7.1.0.  
**ip** keyword made optional in JUNOS Release 7.2.0.

## tcp resequence-buffers default-connection-maximum

---

**Description** Specifies the default buffer limit assigned to all TCP connections on a virtual router unless a specific limit is set for the VR in which the connection is established. Specifying a value of zero (0) buffers turns off the default limit. The **no** version reverts the connection maximum value to its default (10 buffers).

**Syntax** [ ip ] tcp resequence-buffers default-connection-maximum *defaultConnMaxValue*  
no [ ip ] tcp resequence-buffers default-connection-maximum

- ip—Optional keyword for use with older scripts
- *defaultConnMaxValue*—Default number of maximum buffers for newly created connections on a virtual router, in the range 1–65535

**Mode** Global Configuration

**Release Information** Command introduced before JUNOS Release 7.1.0.  
**ip** keyword made optional in JUNOS Release 7.2.0.

## tcp resequence-buffers default-vr-maximum

---

**Description** Specifies the default buffer limit assigned to all virtual routers when the virtual router is established. Specifying a value of zero (0) turns off the limit assignment. The **no** version reverts the virtual router maximum value to its default (100 buffers).

**Syntax** [ ip ] tcp resequence-buffers default-vr-maximum *defaultVrMaxValue*  
no [ ip ] tcp resequence-buffers default-vr-maximum

- ip—Optional keyword for use with older scripts
- *defaultVrMaxValue*—Default number of maximum buffers for newly established virtual routers, in the range 1–65535

**Mode** Global Configuration

**Release Information** Command introduced before JUNOS Release 7.1.0.  
**ip** keyword made optional in JUNOS Release 7.2.0.



## tcp resequence-buffers global-maximum

---

**Description** Specifies a router-wide maximum number of buffers that resequencing queues can contain. Specifying a value of zero (0) turns off the limit. The **no** version reverts the global maximum buffer value to its default (1000 buffers).

**Syntax** ip tcp resequence-buffers global-maximum *globalMaxValue*  
 no [ ip ] tcp resequence-buffers global-maximum

- ip—Optional keyword for use with older scripts
- *globalMaxValue*—Maximum number of buffers in the range 1–65535

**Mode** Global Configuration

**Release Information** Command introduced before JUNOS Release 7.1.0.  
 ip keyword made optional in JUNOS Release 7.2.0.

## tcp resequence-buffers vr-maximum

---

**Description** Defines the maximum number of buffers that the current or specified virtual router can use. Specifying a value of zero (0) turns off the limit assignment. The **no** version reverts the virtual router maximum value to its default (100 buffers).

**Syntax** [ ip ] tcp resequence-buffers [ vrf *vrfName* ] vr-maximum *vrMaxValue*  
 no [ ip ] tcp resequence-buffers [ vrf *vrfName* ] vr-maximum

- ip—Optional keyword for use with older scripts
- *vrfName*—Name of the VRF; string of 1–32 alphanumeric characters
- *vrMaxValue*—Virtual router maximum in the range 1–65535

**Mode** Global Configuration

**Release Information** Command introduced before JUNOS Release 7.1.0.  
 ip keyword made optional in JUNOS Release 7.2.0.

## tech-support encoded-string

---

**Description** Executes the specified encoded command string to gather information to return to Juniper Networks customer support. Use this command only under the direction of Juniper Networks customer support. By default, this command requires level 15 access. There is no **no** version.

**Syntax** tech-support slot *slotNumber* [ connection { reliable | fast } ] encoded-string *string*

- *slotNumber*—Number of a selected slot in the router
- connection—Specifies the connection type:
  - reliable—Use a reliable connection with a slower response time, which is the default
  - fast—Use a less reliable connection with a faster response time, which could be unsuccessful for certain conditions
- *string*—Encoded string provided by Juniper Networks Customer Support

**Mode** Privileged Exec

**Release Information** Command introduced before JUNOS Release 7.1.0.  
**slot** and **connection** keywords added in JUNOS Release 9.1.0.

## telnet

---

**Description** Enables connections to remote routers via the embedded Telnet client. There is no **no** version.

**Syntax** `telnet ipAddress | hostname [ vrf vrfName ] [ ipPortNumber | ipPortType ]`  
`[ source-interface interfaceType interfaceSpecifier | noecho | line | debug | verbose ]*`

- *ipAddress*—IP address of the remote router
- *hostname*—Name of the remote router
- *vrfName*—Name of the VRF to which the command applies; string of 1–32 alphanumeric characters
- *ipPortNumber*—Number of the port for the connection to the remote router, in the range 0–65535; default value is port number 23, the Telnet port. For more information about port numbers and associated processes, see [www.iana.org](http://www.iana.org).
- *ipPortType*—Name of a well-known port, as follows:
  - *bgp*—Border Gateway Protocol (port 179)
  - *chargen*—Character generator (port 19)
  - *cmd*—Remote commands (port 514)
  - *daytime*—Daytime (port 13)
  - *discard*—Discard (port 9)
  - *domain*—Domain Name Service (port 53)
  - *echo*—Echo (port 7)
  - *exec* —Exec (port 512)
  - *finger*—Finger (port 79)
  - *ftp*—File Transfer Protocol (port 21)
  - *ftp-data*—FTP data connections (port 20)
  - *gopher*—Gopher (port 70)
  - *hostname*—NIC hostname server (port 101)
  - *ident*—Ident Protocol (port 113)
  - *irc*—Internet Relay Chat (port 194)
  - *klogin*—Kerberos login (port 543)

- kshell—Kerberos shell (port 544)
- login—Login (port 513)
- lpd—Printer service (port 515)
- nntp—Network News Transport Protocol (port 119)
- pim-auto-rp—Protocol Independent Multicast Auto RP (port 496)
- pop2—Post Office Protocol version 2 (port 109)
- pop3—Post Office Protocol version 2 (port 110)
- smtp—Simple Mail Transport Protocol (port 25)
- sunrpc—Sun Remote Procedure Call (port 111)
- syslog—Syslog (port 514)
- tacacs—Terminal Access Concentrator Access Control System (port 49)
- talk—Talk (port 517)
- telnet—Telnet (port 23)
- time—Time (port 37)
- uucp—Unix-to-Unix Copy Program (port 540)
- whois—Nickname (port 43)
- www —World Wide Web (port 80)
- source-interface—Forces Telnet to use the IP address of the specified interface as the source address for the Telnet connection
  - *interfaceType*—Type of interface to use to obtain the source address for the Telnet connection; see *Interface Types and Specifiers* in *About This Guide*
  - *interfaceSpecifier*—Number of interface to use to obtain the source address for the Telnet connection; format varies according to interface type; see *Interface Types and Specifiers* in *About This Guide*
- noecho—Disables local echo of user input
- line—Enables line mode
- debug—Enables debugging
- verbose—Enables verbose mode
- \*—Indicates that one or more parameters can be repeated multiple times in a list in the command line

**Mode** Privileged Exec

**Release Information** Command introduced before JUNOS Release 7.1.0.

## telnet listen

---

**Description** Sets the Telnet daemon to listen in a virtual router other than the default. The **no** version deletes the Telnet daemon.

**Syntax** telnet listen [ port *portValue* ]  
no telnet listen

- *portValue*—TCP port on which the Telnet daemon listens; if not specified, uses the default, port 23

**Mode** Global Configuration

**Release Information** Command introduced before JUNOS Release 7.1.0.

## terminal data-character-bits

---

**Description** Sets the number of data bits available for characters for the current session on the terminal screen. There is no **no** version.

**Syntax** terminal data-character-bits { 7 | 8 }

- 7—Seven data bits per character; this setting supports only characters in the standard ASCII set
- 8—Eight data bits per character; this is the default setting, which supports the full set of 8-bit international characters

**Mode** Privileged Exec, User Exec

**Release Information** Command introduced before JUNOS Release 7.1.0.

## terminal length

---

**Description** Sets the number of lines on the current terminal screen for the current session. There is no **no** version.

**Syntax** terminal length *value*

- *value*—Number for the screen length in the range 0–512. If 0, the router does not pause between screens of output. If not 0, the router pauses between screens.

**Mode** Privileged Exec, User Exec

**Release Information** Command introduced before JUNOS Release 7.1.0.

## terminal speed

---

**Description** Sets the speed for the current console session. There is no **no** version.

**Syntax** terminal speed *baudRate*

- *baudRate*—Terminal speed for the current console session; one of the following values: 2400, 4800, 9600, 14400, 19200, 28800, 38400, 57600, 115200

**Mode** Privileged Exec

**Release Information** Command introduced before JUNOS Release 7.1.0.

## terminal width

---

**Description** Sets the number of character columns on the current terminal screen for the current line for a session. There is no **no** version.

**Syntax** terminal width *value*

- *value*—Number of characters in the range 30–512

**Mode** Privileged Exec, User Exec

**Release Information** Command introduced before JUNOS Release 7.1.0.

## terminate-code

---

**Description** Configures custom mappings of application terminate reasons to RADIUS Acct-Terminate-Cause codes. The **no** version restores the default mappings.

**Syntax** terminate-code *application terminateReason translationApplication terminateCode*  
no terminate-code *application terminateReason translationApplication*

- *application*—Application; AAA, L2TP, PPP, or RADIUS client
- *terminateReason*—Reason that the subscriber's session was terminated
- *translationApplication*—Application whose terminate code is used for the mapping; for example, RADIUS
- *terminateCode*—Standards-based code used by the translation application to identify the terminate reason; for example, a RADIUS Acct-Terminate-Cause code

**Mode** Global Configuration

**Release Information** Command introduced in JUNOS Release 7.3.0.

## test aaa

---

**Description** Verifies RADIUS authentication and accounting and IP (or IPv6) address assignment setup. The test uses a username and password and attempts to authenticate a user, get an address assignment, and issue a start accounting request. The test immediately terminates the session by issuing a stop accounting request and an address release. Optionally, a virtual router context may be specified. There is no **no** version.

**Syntax** `test aaa { ppp | mlppp } userName [ password ] [ virtual-router vrContext ] [ aaa-profile profileName ] [ zero-stats ] [ filter ]`

- `ppp`—Indicates a PPP user
- `mlppp`—Simulates Multilink PPP
- *userName*—Username to test
- *password*—Password to associate with username; the password is optional—when omitted, the RADIUS access request has no User-Password attribute
- *vrContext*—Virtual router context in which to authenticate the user
- *profileName*—Name of AAA profile for the user
- `zero-stats`—Specifies that accounting statistics should be set to zero for this test
- *filter*—See *Filtering show Commands* in *About This Guide*

**Mode** Privileged Exec

**Release Information** Command introduced before JUNOS Release 7.1.0.

## test bgp ipv6 neighbor

---

**Description** Tests BGP policy for IPv6 BGP routes advertised to or received from peers without implementing the policy. There is no **no** version.

**Syntax** test bgp ipv6  
[ unicast | multicast | vpnv6 all | vpnv6 vrf *vrfName* | route-target signaling ]  
neighbor { *ipAddress* | *ipv6Address* | *peerGroupName* }  
{ advertised-routes | routes } [ *ipv6Prefix* ]  
[ distribute-list *accessListName* |  
filter-list *asPathAccessListName* [ weight *weightValue* ] |  
prefix-list *prefixListName* | prefix-tree *prefixTreeName* | route-map *mapTag* ]\*  
[ fields { *fieldOptions* } ] [ *filter* ]

- unicast—Specifies the IPv6 unicast address family and routing table; the default option
- multicast—Specifies the IPv6 multicast address family and routing table
- vpnv6 all—Specifies the VPN-IPv6 address family and all IPv6 VPN routing and forwarding instances
- vpnv6 vrf *vrfName*—Specifies the VPN-IPv6 address family and only the IPv6 VPN routing and forwarding instance with the name *vrfName*
- route-target signaling—Specifies the route-target address family
- *ipAddress*—IP address of BGP neighbor
- *ipv6Address*—IPv6 address of BGP neighbor
- *peerGroupName*—Name of a BGP peer group
- advertised-routes—Tests only the outgoing advertisements to the specified BGP neighbor or peer group
- routes—Tests only the incoming routes originating from the specified BGP neighbor or peer group
- *ipv6Prefix*—IPv6 prefix for which you want information displayed
- *accessListName*—Name of the access list to use as the distribute list to filter routes by prefix; string of up to 32 alphanumeric characters
- *asPathAccessListName*—Name of a single AS path access list used to filter routes by AS path; string of up to 32 characters
- *weightValue*—Weight assigned to incoming routes matched by the AS path access list; integer in the range 0–4294967295
- *prefixListName*—Name of a BGP prefix list used to filter routes by prefix
- *prefixTreeName*—Name of a BGP prefix tree used to filter routes by prefix
- *mapTag*—Name of a route map; string of up to 32 alphanumeric characters
- \*—Indicates that one or more parameters can be repeated multiple times in a list in the command line
- fields—Displays only the specified fields; the display order of the fields is hard-coded and not affected by the order in which you enter them



- *fieldOptions*—Fields to be displayed, in the format  
all | [ afi | aggregator | as-path | atomic-aggregate | best | clusters |  
communities | extended-communities | imported | intro | in-label | loc-pref |  
med | next-hop | next-hop-cost | origin | originator-id | out-label | peer |  
peer-type | rd | safi | stale | unknown-types | weight ]\*
- all—All available information; not recommended, because this information for each network does not fit on a single line and is difficult to read
- afi—Address family identifier
- aggregator—AS number and IP address of aggregator
- as-path—AS path through which this route has been advertised
- atomic-aggregate—Whether the atomic aggregate attribute is present
- best—Whether this is the best route for the prefix
- clusters—List of cluster IDs through which the route has been advertised
- communities—Community number associated with the route
- extended-communities—Extended community
- imported—Whether the route was imported
- intro—Introductory information about the state of various BGP attributes; this information is displayed only if you specify this keyword
- in-label—MPLS label for the route; the label received with incoming MPLS frames; typically, but not always, this is the label advertised to MP-BGP peers
- loc-pref—Local preference for the route
- med—Multiexit discriminator for the route
- next-hop—IP address of the next router that is used when forwarding a packet to the destination network
- next-hop-cost—Whether the indirect next hop of the route is unreachable, if not, displays IGP cost to the indirect next hop
- origin—Origin of the route
- originator-id—Router ID of the router in the local AS that originated the route
- out-label—MPLS label for the route; the label sent with outgoing MPLS frames; also the label received from MP-BGP peer; typically, but not always, this is the label received from MP-BGP peers

- peer—IP address of BGP peer from which route was learned
- peer-type—Type of BGP peer: internal, external, or confederation
- rd—Route distinguisher
- safi—Subsequent address family identifier
- stale—Route that has gone stale due to peer restart
- unknown-types—Attribute codes for unknown path attributes
- weight—Weight of the route
- \*—Indicates that one or more parameters can be repeated multiple times in a list in the command line
- *filter*—See *Filtering show Commands in About This Guide*

**Mode** Privileged Exec, User Exec

**Release Information** Command introduced before JUNOS Release 7.1.0.  
**route-target signaling** keywords added in JUNOS Release 8.2.0.

## test ip bgp neighbor

**Description** Tests BGP policy for routes advertised to or received from peers without implementing the policy. There is no **no** version.

**Syntax** test ip bgp  
 [ ipv4 unicast | ipv4 multicast | vpnv6 all | vpnv6 vrf *vrfName* | route-target signaling ]  
 neighbor { *ipAddress* | *ipv6Address* | *peerGroupName* } { advertised-routes | routes }  
 [ *routeAddr* [ *routeMask* [ *route-rd distinguisher* ] ] ]  
 [ distribute-list *accessListName* |  
 filter-list *asPathAccessListName* [ weight *weightValue* ] |  
 prefix-list *prefixListName* | prefix-tree *prefixTreeName* | route-map *mapTag* ]\*  
 [ fields { *fieldOptions* } ] [ *filter* ]

- *ipv4 unicast*—Specifies the IPv4 unicast address family and routing table; the default option
- *ipv4 multicast*—Specifies the IPv4 multicast address family and routing table
- *vpnv4 all*—Specifies the IPv4 VPN address family and all IPv4 VPN routing and forwarding instances
- *vpnv4 vrf vrfName*—Specifies the IPv4 VPN address family and only the IPv4 VPN routing and forwarding instance with the name *vrfName*
- *route-target signaling*—Specifies the route-target address family
- *ipAddress*—IP address of BGP neighbor
- *ipv6Address*—IPv6 address of BGP neighbor
- *peerGroupName*—Name of a BGP peer group. If you specify a BGP peer group by using the *peerGroupName* argument, all the members of the peer group inherit the characteristic configured with this command, unless it is overridden for a specific peer.
- *advertised-routes*—Tests only outgoing advertisements to the specified neighbor
- *routes*—Tests only the incoming advertisements from the specified neighbor
- *routeAddr*—Prefix advertised by BGP
- *routeMask*—Subnet mask associated with prefix; if not specified, a best match on *routeAddr* is performed
- *distinguisher*—Unique two-part identifier of the format *number1:number2* where:
  - *number1*—AS number or an IP address
  - *number2*—Unique integer; 32 bits if *number1* is an AS number; 16 bits if *number1* is an IP address

If not specified, considers all destinations with the same *routeAddress* and *routeMask*.

- *accessListName*—Name of an access list used as a distribute list to filter routes by prefix; string of up to 32 alphanumeric characters
- *asPathAccessListName*—Name of a single AS path access list used to filter routes by AS path; string of up to 32 characters
- *weightValue*—Weight assigned to incoming routes matched by the AS path access list; integer in the range 0–4294967295
- *prefixListName*—Name of a BGP prefix list used to filter routes by prefix
- *prefixTreeName*—Name of a BGP prefix tree used to filter routes by prefix
- *mapTag*—Name of a route map; a string of up to 32 alphanumeric characters
- \*—Indicates that one or more parameters can be repeated multiple times in a list in the command line
- *fields*—Displays only the specified fields; the display order of the fields is hard-coded and not affected by the order in which you enter them
- *fieldOptions*—Fields to be displayed, in the format  
all | [ afi | aggregator | as-path | atomic-aggregate | best | clusters | communities | extended-communities | imported | intro | in-label | loc-pref | med | next-hop | next-hop-cost | origin | originator-id | out-label | peer | peer-type | rd | safi | stale | unknown-types | weight ]\*
  - all—All available information; not recommended, because this information for each network does not fit on a single line and is difficult to read
  - afi—Address family identifier
  - aggregator—AS number and IP address of aggregator
  - as-path—AS path through which this route has been advertised
  - atomic-aggregate—Whether the atomic aggregate attribute is present
  - best—Whether this is the best route for the prefix
  - clusters—List of cluster IDs through which the route has been advertised
  - communities—Community number associated with the route
  - extended-communities—Extended community
  - imported—Whether the route was imported
  - intro—Introductory information about the state of various BGP attributes; this information is displayed only if you specify this keyword
  - in-label—MPLS label for the route; the label received with incoming MPLS frames; typically, but not always, this is the label advertised to MP-BGP peers

- loc-pref—Local preference for the route
- med—Multiexit discriminator for the route
- next-hop—IP address of the next router that is used when forwarding a packet to the destination network
- next-hop-cost—Whether the indirect next hop of the route is unreachable, if not, displays IGP cost to the indirect next hop
- origin—Origin of the route
- originator-id—Router ID of the router in the local AS that originated the route
- out-label—MPLS label for the route; the label sent with outgoing MPLS frames; also the label received from MP-BGP peer; typically, but not always, this is the label received from MP-BGP peers
- peer—IP address of BGP peer from which route was learned
- peer-type—Type of BGP peer: internal, external, or confederation
- rd—Route distinguisher
- safi—Subsequent address family identifier
- stale—Route that has gone stale due to peer restart
- unknown-types—Attribute codes for unknown path attributes
- weight—Weight of the route
- \*—Indicates that one or more parameters can be repeated multiple times in a list in the command line
- *filter*—See *Filtering show Commands* in *About This Guide*

**Mode** Privileged Exec, User Exec

**Release Information** Command introduced before JUNOS Release 7.1.0.  
**route-target signaling** keywords added in JUNOS Release 8.2.0.

## threshold

---

**Description** Sets the threshold values for bit error rates used in APS/MSP alarms. This command applies only to the protect interface, and not to the working interface. The **no** version restores the default value, 5 (for the sd-ber bit error rate) or 3 (for the sf-ber bit error rate), for the specified alarm.

**Syntax** threshold { sd-ber | sf-ber } rate  
no threshold { sd-ber | sf-ber }

- sd-ber—Bit error rate that specifies signal degradation
- sf-ber—Bit error rate that specifies signal failure
- *rate*—Integer *n* with available values depending on the bit error rate type you specify; a value of *n* corresponds to a rate of  $10^{-n}$  (10e-*n*) errors per second
  - For sd-ber, an integer in the range 5–9; default value is 5
  - For sf-ber, an integer in the range 3–5; default value is 3

**Mode** Controller Configuration

**Release Information** Command introduced before JUNOS Release 7.1.0.

## threshold-test

---

<b>Description</b>	Defines the values for an SNMP threshold-test trigger. The <b>no</b> version deletes the threshold-test values for this trigger or removes either the threshold startup condition or event binding.
<b>Syntax</b>	<pre>threshold-test startup { falling   rising   risingorfalling } threshold-test absolute-value rising <i>risingValue</i> falling <i>fallingValue</i> threshold-test event { rising <i>eventOwner eventName</i>   falling <i>eventOwner eventName</i>   delta-rising <i>eventOwner eventName</i>   delta-falling <i>eventOwner eventName</i> } threshold-test delta-value rising <i>risingValue</i> falling <i>fallingValue</i> no threshold-test [ startup   absolute-value   delta-value   event rising   event falling   event delta-rising   event delta-falling ]</pre> <ul style="list-style-type: none"> <li>■ <b>startup</b>—Startup threshold condition that you predict the sample to follow <ul style="list-style-type: none"> <li>■ <b>falling</b>—Specifies that the sample values are expected to be falling values</li> <li>■ <b>rising</b>—Specifies that the sample values are expected to be rising values</li> <li>■ <b>risingorfalling</b>—Specifies that the sample values might be either rising values or falling values</li> </ul> </li> <li>■ <b>absolute-value</b>—Specifies that the trigger is monitoring absolute threshold values</li> <li>■ <b><i>risingValue</i></b>—Rising threshold value for the trigger, in the range -2147483648–2147483648</li> <li>■ <b><i>fallingValue</i></b>—Falling threshold value for the trigger, in the range -2147483648–2147483648</li> <li>■ <b>event</b>—Binds an event owner and name to specific events on which the threshold-test might trigger: rising values within a sample, falling values within a sample, rising values between samples, or falling values between samples</li> <li>■ <b><i>eventOwner</i></b>—Event owner name; string of up to 32 alphanumeric characters</li> <li>■ <b><i>eventName</i></b>—Event name; string of up to 32 alphanumeric characters</li> <li>■ <b>delta-value</b>—Specifies that the trigger is monitoring the difference (delta) between sample values</li> </ul>
<b>Mode</b>	SNMP Trigger Configuration
<b>Release Information</b>	Command introduced before JUNOS Release 7.1.0.

## time

---

**Description** Configures the threshold for the amount of time that the service session can be active for a subscriber. The service is terminated when the time expires. The **no** version removes the time attribute from the service session profile.

**Syntax** time *seconds*  
no time

- *seconds*—Number of seconds in the range 0–16777251

**Mode** Service Session Profile Configuration

**Release Information** Command introduced in JUNOS Release 7.2.0.

## timeout

---

**Description** When used from RADIUS Configuration mode, specifies the interval, in seconds, before the router retransmits a RADIUS packet to an authentication or accounting server. The **no** version uses the default.

When used from RTR Configuration mode, specifies the timeout for a Response Time Reporter operation. The **no** version returns the operation to the default value. You can apply this parameter only to *echo* entries.

**Syntax** RADIUS:  
timeout *waitTime*  
no timeout

- *waitTime*—Specifies the number of seconds in the range 3–30; default value is 3

RTR:  
timeout *timeoutValue*  
no timeout

- *timeoutValue*—Number in milliseconds that the operation waits for a response; if the value is set to 0 or is larger than frequency, it will be ignored; default value is 5000

**Mode** RADIUS Configuration, RTR Configuration

**Release Information** Command introduced before JUNOS Release 7.1.0.



## timeout login response

---

**Description** Sets a time limit during which users must provide a password when they log into the console or a vty line. Specifying a value of 0 indicates that there is no time limit during which users must enter a password. The **no** version restores the default value, 30.

**Syntax** timeout login response *seconds*  
no timeout login response

- *seconds*—Length of the timeout in the range 0–300 seconds

**Mode** Line Configuration

**Release Information** Command introduced before JUNOS Release 7.1.0.

## timers

---

**Description** Configures RIP timers. The **no** version restores the default values.

**Syntax** timers *update invalid holddown flush*  
no timers

- *update*—Interval in seconds at which routing updates are sent; default value is 30
- *invalid*—Interval in seconds after which a route is declared invalid (null); default value is 180
- *holddown*—Interval in seconds during which routing information regarding better paths is disregarded by the router; default value is 120
- *flush*—Interval in seconds that must pass before a route is removed from the routing table; set this value greater than the invalid value; default value is 300

**Mode** Address Family Configuration, Router Configuration

**Release Information** Command introduced before JUNOS Release 7.1.0.

## timers bgp

---

<b>Description</b>	Sets keepalive and hold-time timers for all neighbors. The <b>no</b> version restores the default values.
<b>Syntax</b>	<pre>timers bgp <i>keepaliveTime</i> <i>holdTime</i> no timers bgp [ <i>keepaliveTime</i> [ <i>holdTime</i> ] ]</pre> <ul style="list-style-type: none"><li>■ <i>keepaliveTime</i>—Interval in seconds between keepalive messages, in the range 0–65535 seconds; default value is 30; a value of zero prevents BGP from sending keepalive messages</li><li>■ <i>holdTime</i>—Period in seconds that BGP waits for keepalive messages before declaring the neighbor to be unavailable, in the range 0–65535 seconds; default value is 90; a value of zero informs BGP not to expect any hold-time messages</li></ul>
<b>Mode</b>	Router Configuration
<b>Release Information</b>	Command introduced before JUNOS Release 7.1.0.

## timers spf

---

<b>Description</b>	Configures the delay time between when OSPF receives a topology change and when it starts an SPF calculation and the hold time between two consecutive SPF calculations. The <b>no</b> version restores the default value.
<b>Syntax</b>	<pre>[ no ] timers spf <i>holdTime</i></pre> <ul style="list-style-type: none"><li>■ <i>holdTime</i>—Number in the range 1–5 seconds; default value is 3; the hold time between consecutive SPF calculations</li></ul>
<b>Mode</b>	Router Configuration
<b>Release Information</b>	Command introduced before JUNOS Release 7.1.0.

## time-to-live

---

<b>Description</b>	Specifies a hop count by setting the value of the time-to-live field used by packets sent to a RIP remote neighbor. The <b>no</b> version restores the default value.
<b>Syntax</b>	<pre>time-to-live <i>ttlValue</i> no time-to-live</pre> <ul style="list-style-type: none"><li>■ <i>ttlValue</i>—Number in the range 1–16; default value is 16</li></ul>
<b>Mode</b>	Remote Neighbor Configuration
<b>Release Information</b>	Command introduced before JUNOS Release 7.1.0.

## timing disable-auto-upgrade

---

<b>Description</b>	Disables the autoupgrade feature of the router timing. The <b>no</b> version enables the autoupgrade feature.
<b>Syntax</b>	[ no ] timing disable-auto-upgrade
<b>Mode</b>	Global Configuration
<b>Release Information</b>	Command introduced before JUNOS Release 7.1.0.

## timing select

---

<b>Description</b>	Configures the preferred timing selector. There is no <b>no</b> version.
<b>Syntax</b>	timing select <i>selector</i> <ul style="list-style-type: none"><li>■ <i>selector</i>—Timing selector; one of the following:<ul style="list-style-type: none"><li>■ primary—Highest-priority preferred selection</li><li>■ secondary—Middle-priority preferred selection</li><li>■ tertiary—Lowest-priority preferred selection</li></ul></li></ul>
<b>Mode</b>	Global Configuration
<b>Release Information</b>	Command introduced before JUNOS Release 7.1.0.

## timing source

---

**Description** Configures the router's timing sources. Only one of these timing sources can be an external source received through an interface on an I/O module other than the SRP I/O module; the other two must be either internal sources or external sources received through the SRP I/O modules. There is no **no** version.

**Syntax** `timing source selector { internal | line lineType | uidType interfaceSpecifier }`

- *selector*—Priority of the timing source; in descending order: **primary**, **secondary**, or **tertiary**
- *internal*—Specifies the internal SC oscillator
- *line*—Specifies external timing input on the SRP module
- *lineType*—One of the following timing sources:
  - *e1:a*—E1 clock, port A on SRP module
  - *e1:b*—E1 clock, port B on SRP module
  - *t1:a*—T1 clock, port A on SRP module
  - *t1:b*—T1 clock, port B on SRP module
- *uidType*—One of the following interfaces:
  - *ds1*—Specifies a DS1 interface
  - *ds3*—Specifies a DS3 interface
  - *e1*—Specifies an E1 interface
  - *e3*—Specifies an E3 interface
  - *sonet*—Specifies a SONET interface
- *interfaceSpecifier*—Particular interface; in the form *slot/port[:subPort]*

**Mode** Global Configuration

**Release Information** Command introduced before JUNOS Release 7.1.0.

## tos

---

**Description** Defines a type of service byte in the RTR operation's IP header. The **no** version returns the operation to the default value.

**Syntax** `tos tosValue`  
`no tos`

- *tosValue*—ToS byte in the IP header; number in the range 0–255; default value is 0 for both RTR types

**Mode** RTR Configuration

**Release Information** Command introduced before JUNOS Release 7.1.0.

## trace mpls ip

---

**Description** Sends MPLS echo request packets with successively higher TTL values to the specified IP or IPv6 address. Discovers the path MPLS packets follow to the destination. There is no **no** version.

**Syntax** `trace mpls ip [ vrf vrfName ]  
 { targetIpAddress targetIpv4Mask | targetIpv6Prefix }  
 [ destination startIpAddress endIpAddress increment ]  
 [ source address sourceAddr ]  
 [ ttl ttlValue ] [ timeout timeOutVal ]  
 [ reply mode { ipv4-udp | ipv4-udp-with-router-alert } ]  
 [ reply pad-tlv ] [ reply dscp trafficClass ]  
 [ exp-bits bitValue ] [ detail ]`

- *vrfName*—Name of the VRF context
- *targetIpAddress*—IP address of the ping target
- *targetIpv4Mask*—Network mask for target IP address
- *targetIpv6Prefix*—IPv6 address of the ping target
- *startIpAddress*—First IP address within the 127.0.0.0/8 destination range
- *endIpAddress*—Last IP address within the 127.0.0.0/8 destination range
- *increment*—Number in the range 0–255 that specifies the increment between addresses in the destination address range
- *sourceAddr*—IP address used as the packet source address
- *ttlValue*—Hop count specified by setting the time-to-live field in the header, in the range 1–255; default value is 32
- *timeOutVal*—Number of seconds in the range 1–32 to wait for an MPLS echo reply packet before the connection attempt times out
- *reply mode*—Specifies the reply mode for the echo request packet
  - *ipv4-udp*—Specifies that the echo request packet is an IPv4 UDP packet
  - *ipv4-udp-with-router-alert*—Specifies that the echo request packet is an IPv4 UDP packet with the router alert bit set in the header so all routers examine this packet more closely to determine whether further processing is necessary
- *reply pad-tlv*—Requests sender of an echo reply to send a pad TLV
- *trafficClass*—Number in the range 0–255 that represents the value of the traffic class that the sender of an echo reply is requested to set
- *bitValue*—Value of the EXP bits in the range 0–7 included in the MPLS echo request packet
- *detail*—Displays detailed information about MPLS echo request sent and echo replies received

**Mode** Privileged Exec, User Exec

**Release Information** Command introduced in JUNOS Release 8.0.0.

## trace mpls l2transport

---

**Description** Sends MPLS echo request packets with successively higher TTL values to the specified layer 2 cross-connect virtual (Martini) circuit. Discovers the path MPLS packets follow to the destination. There is no **no** version.

**Syntax** `trace mpls l2transport [ vrf vrfName ]  
{ interfaceType interfaceSpecifier }  
[ destination startIpAddress endIpAddress increment ]  
[ source address sourceAddr ]  
[ ttl ttlValue ] [ timeout timeOutVal ]  
[ reply mode { ipv4-udp | ipv4-udp-with-router-alert } ]  
[ reply pad-tlv ] [ reply dscp trafficClass ]  
[ exp-bits bitValue ] [ bottom-label-ttl bottomLabelTtl ] [ detail ]`

- *vrfName*—Name of the VRF context
- *interfaceType*—Interface type; see *Interface Types and Specifiers* in *About This Guide*
- *interfaceSpecifier*—Particular interface; format varies according to interface type; see *Interface Types and Specifiers* in *About This Guide*
- *startIpAddress*—First IP address within the 127.0.0.0/8 destination range
- *endIpAddress*—Last IP address within the 127.0.0.0/8 destination range
- *increment*—Number in the range 0–255 that specifies the increment between addresses in the destination address range
- *sourceAddr*—IP address used as the packet source address
- *ttlValue*—Hop count specified by setting the time-to-live field in the header, in the range 1–255; default value is 32
- *timeOutVal*—Number of seconds in the range 1–32 to wait for an MPLS echo reply packet before the connection attempt times out
- *reply mode*—Specifies the reply mode for the echo request packet
  - *ipv4-udp*—Specifies that the echo request packet is an IPv4 UDP packet
  - *ipv4-udp-with-router-alert*—Specifies that the echo request packet is an IPv4 UDP packet with the router alert bit set in the header so all routers examine this packet more closely to determine whether further processing is necessary
- *reply pad-tlv*—Requests sender of an echo reply to send a pad TLV
- *trafficClass*—Number in the range 0–255 that represents the value of the traffic class that the sender of an echo reply is requested to set
- *bitValue*—Value of the EXP bits in the range 0–7 included in the MPLS echo request packet
- *bottomLabelTtl*—Time-to-live value of the bottom label in the stack
- *detail*—Displays detailed information about MPLS echo request sent and echo replies received

**Mode** Privileged Exec, User Exec

**Release Information** Command introduced in JUNOS Release 8.0.0.

## trace mpls l3vpn

---

<b>Description</b>	Sends MPLS echo request packets with successively higher TTL values to the specified L3VPN IP or IPv6 prefix. Discovers the path MPLS packets follow to the destination. There is no <b>no</b> version.
<b>Syntax</b>	<pre>trace mpls l3vpn [ vrf vrfName ] { targetAddress targetMask   targetIpv6Prefix } [ destination startIpAddress endIpAddress increment ] [ source address sourceAddr ] [ ttl ttlValue ] [ timeout timeOutVal ] [ reply mode { ipv4-udp   ipv4-udp-with-router-alert } ] [ reply pad-tlv ] [ reply dscp trafficClass ] [ exp-bits bitValue ] [ bottom-label-ttl bottomLabelTtl ] [ detail ]</pre> <ul style="list-style-type: none"> <li>■ <i>vrfName</i>—Name of the VRF context</li> <li>■ <i>targetAddress</i>—IP address of the target VPN network</li> <li>■ <i>targetMask</i>—Netmask for the target address</li> <li>■ <i>targetIpv6Prefix</i>—IPv6 prefix for the target VPN network</li> <li>■ <i>startIpAddress</i>—First IP address within the 127.0.0.0/8 destination range</li> <li>■ <i>endIpAddress</i>—Last IP address within the 127.0.0.0/8 destination range</li> <li>■ <i>increment</i>—Number in the range 0–255 that specifies the increment between addresses in the destination address range</li> <li>■ <i>sourceAddr</i>—IP address used as the packet source address</li> <li>■ <i>ttlValue</i>—Hop count specified by setting the time-to-live field in the header, in the range 1–255; default value is 32</li> <li>■ <i>timeOutVal</i>—Number of seconds in the range 1–32 to wait for an MPLS echo reply packet before the connection attempt times out</li> <li>■ <i>reply mode</i>—Specifies the reply mode for the echo request packet <ul style="list-style-type: none"> <li>■ <i>ipv4-udp</i>—Specifies that the echo request packet is an IPv4 UDP packet</li> <li>■ <i>ipv4-udp-with-router-alert</i>—Specifies that the echo request packet is an IPv4 UDP packet with the router alert bit set in the header so all routers examine this packet more closely to determine whether further processing is necessary</li> </ul> </li> <li>■ <i>reply pad-tlv</i>—Requests sender of an echo reply to send a pad TLV</li> <li>■ <i>trafficClass</i>—Number in the range 0–255 that represents the value of the traffic class that the sender of an echo reply is requested to set</li> <li>■ <i>bitValue</i>—Value of the EXP bits in the range 0–7 included in the MPLS echo request packet</li> <li>■ <i>bottomLabelTtl</i>—Time-to-live value of the bottom label in the stack</li> <li>■ <i>detail</i>—Displays detailed information about MPLS echo request sent and echo replies received</li> </ul>
<b>Mode</b>	Privileged Exec, User Exec
<b>Release Information</b>	Command introduced in JUNOS Release 8.0.0.

## trace mpls rsvp tunnel

---

**Description** Sends MPLS echo request packets with successively higher TTL values to the specified RSVP-TE tunnel. Discovers the path MPLS packets follow to the destination. There is no **no** version.

**Syntax** `trace mpls { traffic-eng | rsvp } [ vrf vrfName ] tunnel tunnelName  
[ destination startIpAddress endIpAddress increment ]  
[ source address sourceAddr ]  
[ ttl ttlValue ] [ timeout timeOutVal ]  
[ reply mode { ipv4-udp | ipv4-udp-with-router-alert } ]  
[ reply pad-tlv ] [ reply dscp trafficClass ]  
[ exp-bits bitValue ] [ detail ]`

- *traffic-eng*—Specifies optional keyword for compatibility with non-E-series implementations
- *vrfName*—Name of the VRF context
- *tunnelName*—Name of the RSVP-TE tunnel
- *startIpAddress*—First IP address within the 127.0.0.0/8 destination range
- *endIpAddress*—Last IP address within the 127.0.0.0/8 destination range
- *increment*—Number in the range 0–255 that specifies the increment between addresses in the destination address range
- *sourceAddr*—IP address used as the packet source address
- *ttlValue*—Hop count specified by setting the time-to-live field in the header, in the range 1–255; default value is 32
- *timeOutVal*—Number of seconds in the range 1–32 to wait for an MPLS echo reply packet before the connection attempt times out
- *reply mode*—Specifies the reply mode for the echo request packet
  - *ipv4-udp*—Specifies that the echo request packet is an IPv4 UDP packet
  - *ipv4-udp-with-router-alert*—Specifies that the echo request packet is an IPv4 UDP packet with the router alert bit set in the header so all routers examine this packet more closely to determine whether further processing is necessary
- *reply pad-tlv*—Requests sender of an echo reply to send a pad TLV
- *trafficClass*—Number in the range 0–255 that represents the value of the traffic class that the sender of an echo reply is requested to set
- *bitValue*—Value of the EXP bits in the range 0–7 included in the MPLS echo request packet
- *detail*—Displays detailed information about MPLS echo request sent and echo replies received

**Mode** Privileged Exec, User Exec

**Release Information** Command introduced in JUNOS Release 8.0.0.



## trace mpls vpls

---

**Description** Sends MPLS echo request packets with successively higher TTL values to the specified VPLS instance. Discovers the path MPLS packets follow to the destination. There is no **no** version.

**Syntax** `trace mpls vpls [ vrf vrfName ] vplsName`  
`[ sender-site-id senderSiteId ] remote-site-id remoteSiteId`  
`[ destination startIpAddress endIpAddress increment ]`  
`[ source address sourceAddr ]`  
`[ ttl ttlValue ] [ timeout timeOutVal ]`  
`[ reply mode { ipv4-udp | ipv4-udp-with-router-alert } ]`  
`[ reply pad-tlv ] [ reply dscp trafficClass ]`  
`[ exp-bits bitValue ] [ bottom-label-ttl bottomLabelTtl ] [ detail ]`

- *vrfName*—Name of the VRF context
- *vplsName*—Name of a VPLS instance created with the **bridge vpls transport-virtual-router** command
- *senderSiteId*—Numerical identifier for the site sending the MPLS echo request packet; must be an unsigned 16-bit integer greater than zero that is unique across the VPLS domain
- *remoteSiteId*—Numerical identifier for the site receiving the MPLS echo request packet; must be an unsigned 16-bit integer greater than zero that is unique across the VPLS domain
- *startIpAddress*—First IP address within the 127.0.0.0/8 destination range
- *endIpAddress*—Last IP address within the 127.0.0.0/8 destination range
- *increment*—Number in the range 0–255 that specifies the increment between addresses in the destination address range
- *sourceAddr*—IP address used as the packet source address
- *ttlValue*—Hop count specified by setting the time-to-live field in the header, in the range 1–255; default value is 32
- *timeOutVal*—Number of seconds in the range 1–32 to wait for an MPLS echo reply packet before the connection attempt times out
- *reply mode*—Specifies the reply mode for the echo request packet
  - *ipv4-udp*—Specifies that the echo request packet is an IPv4 UDP packet
  - *ipv4-udp-with-router-alert*—Specifies that the echo request packet is an IPv4 UDP packet with the router alert bit set in the header so all routers examine this packet more closely to determine whether further processing is necessary
- *reply pad-tlv*—Requests sender of an echo reply to send a pad TLV
- *trafficClass*—Number in the range 0–255 that represents the value of the traffic class that the sender of an echo reply is requested to set

- *bitValue*—Value of the EXP bits in the range 0–7 included in the MPLS echo request packet
- *bottomLabelTtl*—Time-to-live value of the bottom label in the stack
- *detail*—Displays detailed information about MPLS echo request sent and echo replies received

**Mode** Privileged Exec, User Exec

**Release Information** Command introduced in JUNOS Release 8.0.0.

## traceroute

---

**Description** Discovers the paths that router packets follow when traveling to their destinations. There is no **no** version.

**Syntax** `traceroute [ vrf vrfName ] destination [ ttl maxTTLCount ]  
[ timeout timeOutVal ] [ data-size sizeValue ]  
[ source { interface interfaceType interfaceSpecifier | address sourceAddress } ]  
[ extended [ tos tosVal ] [ set-dont-fragment-bit ] [ interface iType iNumber ]`

`traceroute ipv6 [ vrf vrfName ] destination [ hop-limit hopLimit ] [ timeout timeOutVal ]  
[ data-size sizeValue ] [ source { interface interfaceType interfaceSpecifier |  
address sourceAddress } ] [ extended [ dscp trafficClass ] [ flow-label flowLabel ] ]`

- *vrfName*—Name of the VRF context; string of 1–32 alphanumeric characters
- *ipv6*—Specifies the destination address as IPv6 format
- *destination*—IP address, IPv6 address, or domain name of the trace
- *hopLimit*—Maximum number of hops of the trace in the range 1–255; default value is 32
- *maxTTLCount*—Maximum number of hops of the trace in the range 1–255; default value is 32
- *timeOutVal*—Time in seconds to wait for trace responses in the range 1–20; default value is 2
- *sizeValue*—Number of bytes comprising the IP packet and reflected in the IP header in the range 0–64000
- source interface—Specifies an interface as the source for the transmitted packets
  - *interfaceType*—Interface type; see *Interface Types and Specifiers* in *About This Guide*
  - *interfaceSpecifier*—Particular interface; format varies according to interface type; see *Interface Types and Specifiers* in *About This Guide*
- source address—Specifies an IP address as source for the transmitted packets
  - *sourceAddress*—IP address or domain name used as the source address

- **extended**—Specifies extended IP header attributes
  - *tosVal*—Value of the ToS byte
  - **set-dont-fragment-bit**—Specifies the don't-fragment bit
  - *iType*—Interface type
  - *iNumber*—Interface location
  - *trafficClass*—Specifies the traffic class value to match in the Traffic Class field of each IPv6 packet header, in the range 1–255
  - *flowLabel*—Specifies the flow label value to match in the Flow Label field of each IPv6 packet header, in the range 1–1048576

**Mode** Privileged Exec, User Exec

**Release Information** Command introduced before JUNOS Release 7.1.0.  
**vrf** keyword and *vrfName* variable added to IPv6 version in JUNOS Release 7.2.0.

## track

---

**Description** Specifies the name of an object you want to track and tracks the reachability of that object by its IPv4 prefix. The **no** version deletes the object and stops tracking for that object.

**Syntax** `track objectName [ vrf vrfName ] ip-route ipPrefix reachability`  
`no track objectName`

- *objectName*—Name of the object you want to track; string of 1–32 alphanumeric characters
- *vrfName*—Name of the VRF on which the object resides; string of 1–32 alphanumeric characters
- *ipPrefix*—IP prefix (address and subnetwork mask) of the object you want to track

**Mode** Global Configuration

**Release Information** Command introduced in JUNOS Release 7.2.0.

## traffic-class

---

**Description** In Classifier Group Configuration mode, specifies a traffic class in a policy list for policy management. The **no** version removes a traffic class from a policy list; the **suspend** version temporarily suspends the policy rule; the **no suspend** version resumes application of a suspended rule.



**NOTE:** This command replaces the Policy List Configuration version of the **traffic-class** command, which may be removed completely in a future release.

---

In Global Configuration mode, configures a traffic class in the E-series router. In Traffic Class Group Configuration mode, specifies a traffic class that belongs to the traffic-class group. The **no** version deletes the traffic class.

**Syntax** In Policy List Configuration mode:  
[ no ] [ suspend ] traffic-class *trafficClassName*

- *trafficClassName*—Name of the traffic class; up to 40 characters

In Global Configuration and Traffic Class Group Configuration modes:  
[ no ] traffic-class *trafficClassName*

- *trafficClassName*—Name of the traffic class; up to 31 characters

**Mode** Classifier Group Configuration, Global Configuration, Traffic Class Group Configuration

**Release Information** Command introduced before JUNOS Release 7.1.0.

### Related Topics

- Configuring Traffic Classes That Define Service Levels
- Configuring Traffic-Class Groups That Define Service Levels
- Policy Rule Precedence

## traffic-class-group

---

**Description** Configures a traffic-class group. The **no** version deletes the selected traffic-class group. You must remove all local (slot-based) instances of a traffic-class group before you can remove the global group.

**Syntax** [ no ] traffic-class-group *trafficClassGroupName*  
 [ slot *slotNumber* | auto-strict-priority | extended ]

- *trafficClassGroupName*—Name of the traffic class group; up to 31 characters
- *slotNumber*—Number of the slot associated with the group, in the range 0—17
- auto-strict-priority—Specifies strict-priority scheduling for the group, regardless of whether the scheduler profile associated with the group node specifies strict-priority scheduling. Only one auto-strict-priority group can exist; this is the default behavior for a group.
- extended—Specifies that strict-priority scheduling for the group is determined by the scheduler profile associated with the group node; scheduling is either hierarchical round-robin or strict priority, but if a strict-priority traffic-class group already exists, this group must be scheduled via HRR

**Mode** Global Configuration

**Release Information** Command introduced before JUNOS Release 7.1.0.

### Related Topics

- Configuring Traffic Classes That Define Service Levels
- Configuring Traffic-Class Groups That Define Service Levels
- Configuring QoS for an L2TP Session

## transform

---

**Description** Specifies the eligible transforms for this profile for IPSec source address negotiations. You can specify up to six transform algorithms for this profile. The **no** version resets the transform to the default, esp-3des-sha1.

**Syntax** transform *transform0*  
 [ *transform1* [ *transform2* [ *transform3* [ *transform4* [ *transform5* ] ] ] ] ]  
 no transform

- *transform0* through *transform5*—AH or ESP transform

**Mode** IPSec Tunnel Profile Configuration

**Release Information** Command introduced in JUNOS Release 7.3.0.

## transform-set

---

**Description** Specifies the transform set(s) that an IPSec transport connection can use to negotiate a transform algorithm. You can specify up to six transform algorithms. The **no** version resets the transform to the default, esp-3des-hmac-sha.

**Syntax** transform-set *transform0*  
[ *transform1* [ *transform2* [ *transform3* [ *transform4* [ *transform5* ] ] ] ] ]  
no transform-set

- *transform0* through *transform5*—AH or ESP transform; use the online Help to view available transforms

**Mode** IPSec Transport Profile Configuration

**Release Information** Command introduced before JUNOS Release 7.1.0.

## translate

---

**Description** Maps the original domain name to the mapped domain name for domain map lookup. The **no** version negates the command.

**Syntax** translate *domainName mappedDomainName*  
no translate *domainName*

- *domainName*—Name of the domain; maximum of 64 characters
- *mappedDomainName*—Name of the mapped domain name; maximum of 64 characters

**Mode** AAA Profile Configuration

**Release Information** Command introduced before JUNOS Release 7.1.0.

## transmit-delay

---

**Description** Sets the estimated time it takes to transmit a link-state update packet on the OSPF remote-neighbor interface. The **no** version restores the default value.

**Syntax** transmit-delay *transmDelay*  
no transmit-delay

- *transmDelay*—Link-state transmit delay in seconds; a number in the range 0–3600; default value is 1

**Mode** Remote Neighbor Configuration

**Release Information** Command introduced before JUNOS Release 7.1.0.

## traps

---

**Description** Specifies OSPF trap settings. The **no** version removes all OSPF trap settings or any specified traps.

**Syntax** [ no ] traps { all | [ virtIfStateChange | nbrStateChange | virtNbrStateChange | ifConfigError | virtIfConfigError | ifAuthFailure | virtIfAuthFailure | ifRxBadPkt | virtIfRxBadPkt | txRetransmit | virtTxRetransmit | originateLsa | maxAgeLsa | ifStateChange ]\* }

- all—Enables all OSPF traps
- virtIfStateChange—Sets a trap to indicate a state change on an OSPF virtual interface
- nbrStateChange—Sets a trap to indicate a state change on a nonvirtual OSPF neighbor
- virtNbrStateChange—Sets a trap to indicate a state change on a virtual OSPF neighbor
- ifConfigError—Sets a trap to indicate a configuration mismatch with a nonvirtual neighbor
- virtIfConfigError—Sets a trap to indicate a configuration mismatch with a virtual neighbor
- ifAuthFailure—Sets a trap to indicate an authentication failure on a nonvirtual interface
- virtIfAuthFailure—Sets a trap to indicate an authentication failure on a virtual interface
- ifRxBadPkt—Sets a trap to indicate that a packet has been received that cannot be parsed
- virtIfRxBadPkt—Sets a trap to indicate that a packet has been received on a virtual interface that cannot be parsed
- txRetransmit—Sets a trap to indicate that a packet has been retransmitted on a nonvirtual interface
- virtTxRetransmit—Sets a trap to indicate that a packet has been retransmitted on a virtual interface
- originateLsa—Sets a trap to indicate that a new LSA has been originated by this router
- maxAgeLsa—Sets a trap to indicate that an LSA in this router LSDB has reached MaxAge
- ifStateChange—Sets a trap to indicate a state change on an OSPF interface
- \*—Indicates that one or more parameters can be repeated multiple times in a list in the command line

**Mode** Router Configuration

**Release Information** Command introduced before JUNOS Release 7.1.0.

## trigger

---

**Description** Creates an event and launches the event configuration mode in the SNMP server event manager. The **no** version removes the trigger.

**Syntax** `trigger triggerOwner triggerName`

- *triggerOwner*—Owner associated with this trigger; string of up to 32 alphanumeric characters
- *triggerName*—Name associated with this trigger; string of up to 32 alphanumeric characters

**Mode** SNMP Event Manager Configuration

**Release Information** Command introduced before JUNOS Release 7.1.0.

## trigger delay

---

**Description** Specifies the time duration used to determine when a SONET/SDH defect at the line or section layer becomes an alarm. The **no** version restores the default setting, 2500 milliseconds.

**Syntax** `trigger delay msec delayTime`  
`no trigger delay`

- *delayTime*—Time in the range 0–2500 milliseconds

**Mode** Controller Configuration

**Release Information** Command introduced before JUNOS Release 7.1.0.

## triggered-update-disable

---

**Description** Specifies that RIP does not send triggered routing updates. The **no** version restores the default condition, wherein RIP does send triggered updates.

**Syntax** `[ no ] triggered-update-disable`

**Mode** Address Family Configuration, Router Configuration

**Release Information** Command introduced before JUNOS Release 7.1.0.



**tth**

**Description** Specifies a hop count by setting the value of the time-to-live field used by packets sent to an OSPF remote neighbor. The **no** version restores the default value.

**Syntax** `tth tthValue`  
`no tth`

- *tthValue*—Number in the range 1–255; default value is 1

**Mode** Remote Neighbor Configuration

**Release Information** Command introduced before JUNOS Release 7.1.0.

**tunnel**

**Description** Specifies an L2TP tunnel and changes the mode to Domain Map Tunnel Configuration. In Domain Map Tunnel Configuration mode, you can set the attributes of the tunnel. The **no** version deletes the L2TP tunnel configuration from the router.

From Tunnel Group Configuration mode, adds up to 31 tunnel definitions to the L2TP tunnel group and changes the mode to Tunnel Group Tunnel Configuration mode. In Tunnel Group Tunnel Configuration mode, you can set tunnel attributes. The **no** version deletes the L2TP tunnel group configuration from the router.

**Syntax** `[ no ] tunnel tag`

- *tag*—Number in the range 1–31

**Mode** Domain Map Configuration, Tunnel Group Configuration

**Release Information** Command introduced before JUNOS Release 7.1.0.

**tunnel checksum**

**Description** In Interface Configuration mode, enables end-to-end checksum computation for static GRE tunnels.

In IP Tunnel Destination Profile Configuration mode, enables end-to-end checksum computation for dynamic GRE tunnels. The **no** version disables the checksum option.

**Syntax** `[ no ] tunnel checksum`

**Mode** Interface Configuration, IP Tunnel Destination Profile Configuration

**Release Information** Command introduced before JUNOS Release 7.1.0.  
 IP Tunnel Destination Profile Configuration mode added in JUNOS Release 8.2.0.

## tunnel destination

---

**Description** For DVMRP or GRE in Interface Configuration mode, configures the tunnel endpoint for static tunnels. The **no** version deletes the endpoint.

For DVMRP or GRE in IP Tunnel Destination Profile Configuration mode, configures the tunnel endpoint for dynamic tunnels. The **no** version deletes the endpoint.

For IPSec, configures the remote tunnel endpoint. You can identify the remote peer by either IP address or fully qualified domain name (FQDN). The **no** version deletes the endpoint.

For MPLS in Interface Configuration mode, configures the tunnel endpoint for static MPLS tunnels. The **no** version deletes the endpoint.

For MPLS in Tunnel Profile Configuration mode, configures the source of tunnel endpoints (destinations) within a tunnel profile. You can specify that the endpoints are to be learned from IS-IS or OSPF, or you can provide one or more IP addresses as the endpoint(s). If you specify the destination address, it must be the address of the MPLS interface or the router ID of the destination router. The **no** version deletes the endpoints.

**Syntax** For DVMRP and GRE in Interface Configuration mode:

tunnel destination { *ipAddress* | *hostname* }

no tunnel destination

- *ipAddress*—IP address of the interface on the remote router
- *hostname*—Name of the host to serve as the tunnel endpoint

For DVMRP and GRE in IP Tunnel Destination Profile Configuration mode:

tunnel destination { subnet *ipAddress mask* | range *ipAddressLow ipAddressHigh* }

- *ipAddress*—IP address of the tunnel destination address subnet
- *mask*—IP mask of the tunnel destination address subnet
- *ipAddressLow*—First IP address in a destination address range
- *ipAddressHigh*—Last IP address in a destination address range

For IPSec:

tunnel destination { *ipAddress* | identity *fqdn* }

no tunnel destination

- *ipAddress*—IP address of the interface on the remote router or the router ID of the destination router that serves as the tunnel endpoint
- *fqdn*—Fully qualified domain name of the interface on the remote router that serves as the tunnel endpoint; a maximum of 80 characters

For MPLS in Interface Configuration mode:

tunnel destination *ipAddress*

no tunnel destination

For MPLS in Tunnel Profile Configuration mode:

[ no ] tunnel destination

{ { isis-level-2 | ospf-bdr } [ { access-list | prefix-list } *listName* ] |

{ *ipAddress* [ *ipAddress* ]\* }

- *isis-level-2*—Specifies IS-IS level-2 routers as acceptable destinations
- *ospf-bdr*—Specifies OSPF border routers as acceptable destinations
- *listName*—Name of access list or prefix list that contains the IP addresses that are acceptable as tunnel endpoints
- *ipAddress*—IP address of the interface on the remote router or the router ID of the destination router that serves as the tunnel endpoint; for a tunnel profile, you can list multiple addresses
- *\**—Indicates that one or more parameters can be repeated multiple times in a list in the command line

**Mode** Interface Configuration, IP Tunnel Destination Profile Configuration, Tunnel Profile Configuration

**Release Information** Command introduced before JUNOS Release 7.1.0.  
IP Tunnel Destination Profile Configuration mode added in JUNOS Release 8.2.0.

## tunnel destination backup

---

**Description** Configures a backup tunnel destination for the remote IPsec tunnel endpoint. The backup tunnel is used when the IPsec tunnel destination is detected as unreachable by DPD. You can use either the IP address or fully qualified domain name (FQDN) to identify the backup tunnel; however, you must use the same type of identity that is used for the regular tunnel destination. The **no** version restores the default, in which the regular tunnel destination is also the backup tunnel destination.

**Syntax** tunnel destination backup [ *ipAddress* | identity *fqdn* ]  
no tunnel destination backup

- *ipAddress*—IP address of the interface on the destination router that serves as the backup IPsec tunnel endpoint
- *fqdn*—Fully qualified domain name of the interface on the destination router that serves as the backup IPsec tunnel endpoint; a maximum of 80 characters

**Mode** Interface Configuration

**Release Information** Command introduced before JUNOS Release 7.1.0.

## tunnel group

---

**Description** Assigns the specified tunnel group to the domain map. The **no** version deletes the tunnel group.



**NOTE:** By default, no tunnel group is assigned to the domain map. You can assign a tunnel group to the domain map only if tunnels are not currently defined for the domain map in Domain Map Tunnel mode.

**Syntax** tunnel group *tunnelGroupName*  
no tunnel group

- *tunnelGroupName*—String of up to 64 characters (no spaces)

**Mode** Domain Map Configuration

**Release Information** Command introduced before JUNOS Release 7.1.0.

## tunnel group-address-pool

---

**Description** Configures a group address pool for a data MDT tunnel. The **no** version deletes the group address pool.

**Syntax** tunnel group-address-pool [ *poolName* ]  
no tunnel group-address-pool

- *poolName*—Name of the group address pool

**Mode** IP PIM Data MDT Configuration

**Release Information** Command introduced in JUNOS Release 8.2.0.

## tunnel ip profile

---

**Description** Assigns an IP profile to the MPLS tunnel. The **no** version removes the IP profile from the tunnel. The **no mpls tunnels profile** command deletes the IP profile.

**Syntax** tunnel ip profile *ipProfileId*  
no tunnel ip profile

- *ipProfileId*—Name of an IP profile

**Mode** Tunnel Profile Configuration

**Release Information** Command introduced before JUNOS Release 7.1.0.

## tunnel lifetime

---

**Description** Sets the lifetime of IPSec SAs running on this tunnel. You can specify the lifetime in seconds and/or volume of traffic. Before either limit is reached, the SA is renegotiated, ensuring that the tunnel does not go down before the renegotiation is finished. The **no** version sets the lifetime to the default lifetime of 28800 seconds and an unlimited volume.

**Syntax** tunnel lifetime { kilobytes *kbytes* | seconds *secs* | seconds *secs* kilobytes *kbytes* }  
no tunnel lifetime { seconds | kilobytes }

- *secs*—Number of seconds security SAs on this tunnel live before expiring, in the range 1800–864000
- *kbytes*—Volume of traffic in kilobytes that can pass between the tunnel endpoints using a given SA before the SA expires, in the range 102400–4294967295

**Mode** Interface Configuration

**Release Information** Command introduced before JUNOS Release 7.1.0.

## tunnel local-identity

---

**Description** Specifies the local identity of the IPSec tunnel. The **no** version removes the local endpoint and sets the default identity, which is subnet 0.0.0.0 0.0.0.0.

**Syntax** tunnel local-identity { address *ipAddress* | subnet *ipAddress subnetMask* | range *ipAddressLow ipAddressHigh* }  
no tunnel local-identity

- *ipAddress*—IP address of the local identity
- *subnetMask*—Mask applied to the subnet IP address of the local identity
- *ipAddressLow*—Lower bound of the range of IP addresses of the local identity
- *ipAddressHigh*—Upper bound of the range of IP addresses of the local identity

**Mode** Interface Configuration

**Release Information** Command introduced before JUNOS Release 7.1.0.

## tunnel mdt

---

<b>Description</b>	Enables multicast distribution tree operation by allowing the IP tunnel component to create an MDT interface. This command functions for static GRE and DVMRP tunnel interfaces only. The <b>no</b> version disables MDT on the interface.
<b>Syntax</b>	[ no ] tunnel mdt
<b>Mode</b>	Interface Configuration
<b>Release Information</b>	Command introduced before JUNOS Release 7.1.0.

## tunnel mdt profile

---

<b>Description</b>	Enables multicast distribution tree operation by enabling the IP tunnel component to create an MDT interface. This command also defines an IP profile with parameters that are used to stack an upper IP interface over a dynamic GRE or DVMRP tunnel. This command functions for dynamic GRE and DVMRP tunnel interfaces only. The <b>no</b> version disables MDT on the interface.
<b>Syntax</b>	[ no ] tunnel mdt profile <i>profileName</i> <ul style="list-style-type: none"><li>■ <i>profileName</i>—Profile name of up to 80 characters</li></ul>
<b>Mode</b>	IP Tunnel Destination Profile Configuration
<b>Release Information</b>	Command introduced in JUNOS Release 8.2.0.

## tunnel mpls affinity

---

<b>Description</b>	Assigns an affinity to the tunnel. The <b>no</b> version removes the affinity from the tunnel.
<b>Syntax</b>	tunnel mpls [ traffic-eng ] affinity <i>affinity</i> [ mask <i>mask</i> ] no tunnel mpls [ traffic-eng ] affinity <ul style="list-style-type: none"><li>■ <i>traffic-eng</i>—Specifies optional keyword for compatibility with non-E-series implementations</li><li>■ <i>affinity</i>—Attributes that must be configured on the interface in order to be considered by the tunnel; in the range 0x0–0xFFFFFFFF; default value is 0x0</li><li>■ <i>mask</i>—Mask to identify attributes to be checked; a 1 signifies that the attribute value must match, a 0 signifies that the attribute value does not matter; in the range 0x0–0xFFFFFFFF; default value is 0x0000FFFF</li></ul>
<b>Mode</b>	Interface Configuration, Tunnel Profile Configuration
<b>Release Information</b>	Command introduced before JUNOS Release 7.1.0.

## tunnel mpls autoroute announce

---

**Description** Configures the LSP tunnel to register its endpoint (the egress router) with the configured routing protocol. If you do not specify a routing protocol, the default is IS-IS and OSPF. The **no** version disables endpoint announcements.

**Syntax** [ no ] tunnel mpls [ traffic-eng ] autoroute announce [ ospf | isis ]

- traffic-eng—Specifies optional keyword for compatibility with non-E-series implementations
- ospf—Endpoint is announced to OSPF
- isis—Endpoint is announced to IS-IS

**Mode** Interface Configuration, Tunnel Profile Configuration

**Release Information** Command introduced before JUNOS Release 7.1.0.

## tunnel mpls autoroute metric

---

**Description** Specifies the tunnel metric. The value determines tunnel preference when there is more than one tunnel or native IP path to a tunnel endpoint. A lower value is preferred to a higher value. When you set up multiple tunnels, if the primary tunnel goes down, the existing tunnel with the lowest metric is used immediately. If you specify an absolute value from 1–2147483647, this value overrides the metric for the path provided by the IGP. If you specify a relative value from –10 to +10, this value is subtracted from (–) or added to (+) the metric for the path provided by the IGP. The **no** version restores the default value, relative 0, meaning that the tunnel metric is the IGP value.

**Syntax** tunnel mpls [ traffic-eng ] autoroute metric { absolute | relative } *metricValue*  
no tunnel mpls [ traffic-eng ] autoroute metric

- traffic-eng—Specifies optional keyword for compatibility with non-E-series implementations
- absolute—Specifies that the metric is an absolute value
- relative—Specifies that the metric is a signed relative value
- *metricValue*—Preference value for a path; absolute values are in the range 1–2147483647; relative values are in the range –10– +10

**Mode** Interface Configuration, Tunnel Profile Configuration

**Release Information** Command introduced before JUNOS Release 7.1.0.

## tunnel mpls bandwidth

---

**Description** Specifies the bandwidth required for the tunnel. The **no** version removes the bandwidth constraint from the tunnel.

**Syntax** tunnel mpls [ traffic-eng ] bandwidth *bandwidth*  
no tunnel mpls [ traffic-eng ] bandwidth

- *traffic-eng*—Specifies optional keyword for compatibility with non-E-series implementations
- *bandwidth*—Amount of bandwidth required for the tunnel in kilobits per second, in the range 0–4294967295; default value is 0

**Mode** Interface Configuration, Tunnel Profile Configuration

**Release Information** Command introduced before JUNOS Release 7.1.0.

## tunnel mpls description

---

**Description** Associates a description with the MPLS tunnel. The **no** version deletes the description.

**Syntax** tunnel mpls description *textString*  
no tunnel mpls description

- *textString*—Description or name of the tunnel; string of up to 40 alphanumeric characters

**Mode** Interface Configuration, Tunnel Profile Configuration

**Release Information** Command introduced before JUNOS Release 7.1.0.



## tunnel mpls diff-serv phb-id

---

**Description** Specifies the PHB supported by a signaled tunnel.

For E-LSPs, this command also maps the PHB to the specified EXP bits *bitValue*. You can repeat the command for up to eight PHB mappings.

For L-LSPs, the exp-bits keyword is not used. If you repeat the command, the most recent command overwrites the previous command.

The **no** version removes the mapping association.

**Syntax** tunnel mpls diff-serv phb-id { private *privateId* | standard *standardId* } [ exp-bits *expBits* ]  
 no tunnel mpls diff-serv phb-id { private *privateId* | standard *standardId* }

- *privateId*—Number, in the range 0–4095, designating the private PHB identifier
- *standardId*—Number, in the range 0–63, designating the standard identifier using the DSCP bits
- *expBits*—Number, in the range 0–7, designating the EXP bits

**Mode** Interface Configuration, Tunnel Profile Configuration

**Release Information** Command introduced before JUNOS Release 7.1.0.

## tunnel mpls fast-reroute

---

**Description** Configures local protection for the ingress router of the primary LSP by causing RSVP-TE to signal at LSP setup that the primary LSP needs local protection. The **no** version removes the configuration.

**Syntax** [ no ] tunnel mpls [ traffic-eng ] fast-reroute

- *traffic-eng*—Specifies optional keyword for compatibility with non-E-series implementations

**Mode** Interface Configuration

**Release Information** Command introduced before JUNOS Release 7.1.0.

## tunnel mpls no-route retries

---

**Description** Specifies for a particular tunnel the number of attempts that will be made to set up an LSP for RSVP-TE after a failure due to no available route. The **no** version restores the default value, 0, which means the attempts will be made until successful.

**Syntax** tunnel mpls no-route retries *retryNum*  
no tunnel mpls no-route retries

- *retryNum*—Number of retry attempts in the range 0–65535

**Mode** Interface Configuration, Tunnel Profile Configuration

**Release Information** Command introduced before JUNOS Release 7.1.0.

## tunnel mpls no-route retry-time

---

**Description** Specifies for a particular tunnel the interval in seconds between attempts to set up an LSP for RSVP-TE after a failure due to no available route. The **no** version restores the default value, 5 seconds.

**Syntax** tunnel mpls no-route retry-time *retryTime*  
no tunnel mpls no-route retry-time

- *retryTime*—Number of seconds in the range 1–60

**Mode** Interface Configuration, Tunnel Profile Configuration

**Release Information** Command introduced before JUNOS Release 7.1.0.

## tunnel mpls path-option

---

**Description** Specifies the path options for a tunnel. You can configure one or more path options—each identified by a unique number—for a given tunnel. The path option number expresses the preference for that option; lower numbers have a higher preference, with 1 having the highest preference. The **no** version deletes the path options.

**Syntax** `tunnel mpls [ traffic-eng ] path-option number`  
`{ dynamic | explicit { name pathName | identifier idNumber } }`  
`[ hop-by-hop | ospf | isis ] [ lockdown ]`

`no tunnel mpls [ traffic-eng ] path-option number`

- *traffic-eng*—Specifies optional keyword for compatibility with non-E-series implementations
- *number*—Identifier for a set of path options
- *dynamic*—Specifies that the path is dynamically calculated
- *explicit*—Specifies that an explicit path is used
- *pathName*—Name of the explicit path; string of up to 20 characters
- *idNumber*—Number identifying the explicit path; in the range 1–65535
- *hop-by-hop*—Specifies that hop-by-hop routing is used for this path option
- *ospf*—Specifies that OSPF routing is used for this path option
- *isis*—Specifies that IS-IS routing is used for this path option
- *lockdown*—Specifies that optimization is not done for this path option

**Mode** Interface Configuration, Tunnel Profile Configuration

**Release Information** Command introduced before JUNOS Release 7.1.0.

## tunnel mpls priority

---

**Description** Assigns a setup priority and optionally a hold priority to the tunnel. The priority can range from 0 (the highest) to 7 (the lowest). The hold priority, if set, must be equal to or better (lower numerically) than the setup priority. In the event of insufficient resources when a tunnel is being established, its setup priority is evaluated against the hold priorities of existing tunnels. Tunnels with lower hold priorities (higher values) are preempted and torn down to free their resources for the new tunnel. The **no** version restores the default value.

**Syntax** tunnel mpls [ *traffic-eng* ] priority *setupPriority* [ *holdPriority* ]  
no tunnel mpls [ *traffic-eng* ] priority

- *traffic-eng*—Specifies optional keyword for compatibility with non-E-series implementations
- *setupPriority*—Priority for the tunnel as it is being established; default value is 4
- *holdPriority*—Priority for the tunnel after it has been established; default value is equal to the configured value of the setup priority

**Mode** Interface Configuration, Tunnel Profile Configuration

**Release Information** Command introduced before JUNOS Release 7.1.0.

## tunnel mpls retries

---

**Description** Specifies for a particular tunnel the number of attempts that will be made to set up an LSP for RSVP-TE after a failure other than one due to no available route. The **no** version restores the default value, 0, which means the attempts will be made until successful.

**Syntax** tunnel mpls retries *retryNum*  
no tunnel mpls retries

- *retryNum*—Number of retry attempts in the range 0–65535

**Mode** Interface Configuration, Tunnel Profile Configuration

**Release Information** Command introduced before JUNOS Release 7.1.0.

## tunnel mpls retry-time

---

<b>Description</b>	Specifies for a particular tunnel the interval in seconds between attempts to set up an LSP for RSVP-TE after a failure other than one due to no available route. The <b>no</b> version restores the default value, 5 seconds.
<b>Syntax</b>	tunnel mpls [ no-route ] retry-time <i>retryTime</i> no tunnel mpls retry-time <ul style="list-style-type: none"> <li>■ <i>retryTime</i>—Number of seconds in the range 1–60</li> </ul>
<b>Mode</b>	Interface Configuration, Tunnel Profile Configuration
<b>Release Information</b>	Command introduced before JUNOS Release 7.1.0.

## tunnel mtu

---

<b>Description</b>	Configures the maximum transmission unit size for the particular tunnel. The <b>no</b> version restores the default value, 1024 for static DVMRP and GRE tunnels, 10240 for dynamic DVMRP and GRE tunnels, 1440 for static IPsec tunnels, and 1400 for dynamic IPsec tunnels.
<b>Syntax</b>	tunnel mtu <i>mtuSize</i> no tunnel mtu <ul style="list-style-type: none"> <li>■ <i>mtuSize</i>—Packet size in bytes allowed for transmission through the tunnel in the range; in the range 1024–10240 for DVMRP and GRE tunnels, in the range 160–9000 for IPsec tunnels.</li> </ul>
<b>Mode</b>	Interface Configuration, IP Tunnel Destination Profile Configuration, IPsec Tunnel Profile Configuration
<b>Release Information</b>	Command introduced before JUNOS Release 7.1.0 IPsec Tunnel Profile Configuration mode added in JUNOS Release 7.3.0. IP Tunnel Destination Profile Configuration mode added in JUNOS Release 8.2.0.

## tunnel password

---

<b>Description</b>	Configures a password for the L2TP tunnel. The <b>no</b> version removes the password.
<b>Syntax</b>	tunnel password <i>tunnelPassword</i> no tunnel password <ul style="list-style-type: none"> <li>■ <i>tunnelPassword</i>—Password used for challenge response to the tunnel peer; in the domain map, it is used only by the LAC</li> </ul>
<b>Mode</b>	L2TP Destination Profile Host Configuration
<b>Release Information</b>	Command introduced before JUNOS Release 7.1.0.

## tunnel peer-identity

---

<b>Description</b>	Specifies the peer identity of the IPsec tunnel. The <b>no</b> version removes the peer endpoint.
<b>Syntax</b>	tunnel peer-identity { address <i>ipAddress</i>   subnet <i>ipAddress subnetMask</i>   range <i>ipAddressLow ipAddressHigh</i> } no tunnel peer-identity <ul style="list-style-type: none"><li>■ <i>ipAddress</i>—IP address of the peer identity</li><li>■ <i>subnetMask</i>—Mask applied to the subnet IP address of the peer identity</li><li>■ <i>ipAddressLow</i>—Lower bound of the range of IP addresses of the peer identity</li><li>■ <i>ipAddressHigh</i>—Upper bound of the range of IP addresses of the peer identity</li></ul>
<b>Mode</b>	Interface Configuration
<b>Release Information</b>	Command introduced before JUNOS Release 7.1.0.

## tunnel pfs group

---

<b>Description</b>	Configures perfect forward secrecy for the IPsec tunnel by assigning a Diffie-Hellman prime modulus group. The <b>no</b> version removes PFS from this tunnel.
<b>Syntax</b>	tunnel pfs group { 1   2   5 } no tunnel pfs group <ul style="list-style-type: none"><li>■ 1—Assigns a 768-bit Diffie-Hellman prime modulus group</li><li>■ 2—Assigns a 1024-bit Diffie-Hellman prime modulus group</li><li>■ 5—Assigns a 1536-bit Diffie-Hellman prime modulus group</li></ul>
<b>Mode</b>	Interface Configuration
<b>Release Information</b>	Command introduced before JUNOS Release 7.1.0.

## tunnel sequence-datagrams

---

<b>Description</b>	Enables the use of GRE sequence numbers. The <b>no</b> version disables the use of GRE sequence numbers.
<b>Syntax</b>	[ no ] tunnel sequence-datagrams
<b>Mode</b>	Global Configuration, IP Tunnel Destination Profile Configuration
<b>Release Information</b>	Command introduced before JUNOS Release 7.1.0. IP Tunnel Destination Profile Configuration mode added in JUNOS Release 8.2.0.

## tunnel-server

---

**Description** Specifies the location of a dedicated or shared tunnel-server port on a module and accesses Tunnel Server Configuration mode, which enables you to provision the maximum number of tunnel-service interfaces to be used on the tunnel-server port. The **default** version restores the default configuration. On dedicated tunnel-server ports, the default configuration is the maximum number of tunnel-service interfaces that the tunnel-service module supports. On shared tunnel-server ports, the default configuration is zero tunnel-service interfaces provisioned. The **no** version unprovisions the tunnel-server port by reducing the number of provisioned tunnel-service interfaces to zero.

**Syntax** [ no ] tunnel-server *interfaceSpecifier*

- *interfaceSpecifier*—Particular interface; format varies according to interface type; see *Interface Types and Specifiers* in *About This Guide*; port number specified must have the tunnel-server port assigned to it

**Mode** Global Configuration

**Release Information** Command introduced before JUNOS Release 7.1.0.

### Related Topics

- Configuring QoS for Tunnel-Server Ports for L2TP LNS Sessions

## tunnel session-key-inbound

---

**Description** Specifies the encryption and authentication algorithm set and session keys for manual inbound SAs. The **no** version removes the keys.

**Syntax** tunnel session-key-inbound *inSaAlgorithms* { *encryptKey* *authKey* | *authKey* }  
no tunnel session-key-inbound

- *inSaAlgorithms*—Algorithms to use for manual inbound SAs; use the online Help to see a list of available algorithms
- *encryptKey*—Encryption key; string of up to 48 characters
- *authKey*—Authentication key; string of up to 48 characters

**Mode** Interface Configuration

**Release Information** Command introduced before JUNOS Release 7.1.0.

## tunnel session-key-outbound

---

**Description** Specifies the encryption and authentication algorithm set, SPI, and session keys for manual outbound SAs. The **no** version removes the keys.

**Syntax** tunnel session-key-outbound *outSAalgorithms spi*  
{ *encryptKey authKey* | *encryptKey* | *authKey* }  
no tunnel session-key-outbound

- *outSAalgorithms*—Algorithms to use for manual outbound SAs; use the online Help to see a list of available algorithms
- *spi*—Number that uniquely identifies an SA, in the range 256–4294967295 (0xFFFFFFFF)
- *encryptKey*—Encryption key; string of up to 48 characters
- *authKey*—Authentication key; string of up to 48 characters

**Mode** Interface Configuration

**Release Information** Command introduced before JUNOS Release 7.1.0.

## tunnel signaling

---

**Description** Sets the signaling protocol used to negotiate security parameters and keys. The **no** version restores the default, isakmp.

**Syntax** tunnel signaling { *isakmp* | *manual* }  
no tunnel signaling

- *isakmp*—Uses ISAKMP/IKE to negotiate parameters
- *manual*—Specifies that security parameters are configured manually

**Mode** Interface Configuration

**Release Information** Command introduced before JUNOS Release 7.1.0.



## tunnel source

---

**Description** In Interface Configuration mode, configures the source for a DVMRP, GRE, or IPSec tunnel. The **no** version deletes the tunnel source.

In IP Tunnel Destination Profile Configuration mode, configures the source in the destination profile for dynamic IP tunnels. The **no** version deletes the tunnel source.

In IP PIM Data MDT Configuration mode, configures the source in the IP PIM Data MT profile for multicast VPNs. The **no** version deletes the tunnel source.

**Syntax** For DVMRP and GRE tunnels in Interface Configuration mode:

tunnel source { *ipAddress* | *interfaceType interfaceSpecifier* }

no tunnel source

For IPSec tunnels in Interface Configuration mode:

tunnel source { *ipAddress* | identity *fqdn* }

no tunnel source

For DVMRP and GRE tunnels in IP PIM Data MDT Configuration mode and in IP Tunnel Destination Profile Configuration mode:

[ no ] tunnel source *ipAddress*

- *ipAddress*—IP address of an existing interface that will serve as the tunnel's source
- *interfaceType*—Interface type; see *Interface Types and Specifiers* in *About This Guide*
- *interfaceSpecifier*—Particular interface; format varies according to interface type; see *Interface Types and Specifiers* in *About This Guide*
- *fqdn*—Fully qualified domain name of the interface to serve as the tunnel's source; a maximum of 80 characters

**Mode** Interface Configuration, IP PIM Data MDT Configuration, IP Tunnel Destination Profile Configuration

**Release Information** Command introduced before JUNOS Release 7.1.0.  
IP PIM Data MDT Profile Configuration mode, and IP Tunnel Destination Profile Configuration mode added in JUNOS Release 8.2.0.

## tunnel-subscriber authentication

---

**Description** Configures whether tunnel subscribers within the domain map are authenticated with the authentication server or are granted access without individual authentication. The **no** version restores the default condition, where users are not authenticated by an authentication server.

**Syntax** tunnel-subscriber authentication { enable | disable }  
no tunnel-subscriber authentication

- enable—Enables tunnel subscriber authentication by the authentication server
- disable—Disables tunnel subscriber authentication by the authentication server; all users in the domain are granted access without individual authentication; this is the default condition

**Mode** Domain Map Configuration

**Release Information** Command introduced in JUNOS Release 9.1.0.

### Related Topics

- [Configuring Tunnel Subscriber Authentication](#)

## tunnel transform-set

---

**Description** Specifies a transform set that ISAKMP uses during SA negotiations on this tunnel. Transform sets used for manually configured tunnels can have only one transform. The **no** version removes the transform set from a tunnel.

**Syntax** [ no ] tunnel transform-set *transformSetName*

- *transformSetName*—Name of the transform set

**Mode** Interface Configuration

**Release Information** Command introduced before JUNOS Release 7.1.0.

## tx-connect-speed-method

---

**Description** Configures for an AAA domain map (when used from Domain Map Tunnel Configuration mode) or for an AAA tunnel group (when used from Tunnel Group Tunnel Configuration mode) the method used to calculate the transmit connect speed of the subscriber's access interface for establishing a tunneled L2TP session. This speed is reported in L2TP Transmit (TX) Speed AVP 24. The **no** version removes configuration of the transmit connect speed calculation method from the AAA domain map or AAA tunnel group.

**Syntax** tx-connect-speed-method { static-layer2 | dynamic-layer2 | qos | actual }  
no tx-connect-speed-method

- static-layer2—Calculates the transmit connect speed of the subscriber's access interface based on statically configured settings for the underlying layer 2 interface
- dynamic-layer2—Calculates the transmit connect speed of the subscriber's access interface based on dynamically configured settings for the underlying layer 2 interface
- qos—Calculates the transmit connect speed of the subscriber's access interface based on settings determined by QoS
- actual—Calculates the transmit connect speed of the subscriber's access interface as the lesser of the **dynamic-layer2** value or the **qos** value

**Mode** Domain Map Tunnel Configuration, Tunnel Group Tunnel Configuration

**Release Information** Command introduced in JUNOS Release 8.0.0.

## type

---

**Description** From RTR Configuration mode, configures an RTR operation. The **no** version removes the configured type from the operation and resets all configuration for an RTR index.

---



**NOTE:** You must configure the operation's type before you can configure any other characteristics of the operation.

---

From Domain Map Configuration and Tunnel Group Tunnel Configuration modes, specifies the L2TP tunnel type (RADIUS attribute 64, Tunnel-Type).

**Syntax** To configure the RTR operation:

```
[ no ] type rtrType protocol iplcmpEcho destination  
[ source-ipaddr srcAddr | source interfaceType interfaceSpecifier ]
```

- *rtrType*—One of the following types of operation:
  - echo—Performs end-to-end operation only
  - pathEcho—Discovers a path to the destination and echoes each device on the path
- *destination*—IP address or an IP hostname or domain name
- *srcAddr*—Source IP address
- *interfaceType*—Interface type; see *Interface Types and Specifiers* in *About This Guide*
- *interfaceSpecifier*—Particular interface; format varies according to interface type; see *Interface Types and Specifiers* in *About This Guide*

To specify the L2TP tunnel type:

```
type tunnelType  
no type
```

- *tunnelType*—L2TP tunnel type

**Mode** Domain Map Configuration, RTR Configuration, Tunnel Group Tunnel Configuration

**Release Information** Command introduced before JUNOS Release 7.1.0.

## ubr

---

**Description** In ATM VC Configuration mode, configures the unspecified bit rate (UBR) service category on an ATM PVC. Optionally, you can specify a peak cell rate (PCR). The **ubr** command is valid only for data PVCs; you cannot use this command for control (ILMI or signaling) PVCs. The **no** version restores the default service category, UBR without a PCR.

In ATM VC Class Configuration mode, configures the UBR service category as part of a VC class definition that you assign to an ATM data PVC. The **no** version restores the default service category, UBR without a PCR, in the VC class.

**Syntax**    **ubr** [ *pcr* ]  
               **no** ubr

- *pcr*—Peak cell rate, in Kbps, in the range 0–149760 (for OC3 ATM modules) or 0–599040 (for OC12 ATM modules)

**Mode**      ATM VC Configuration, ATM VC Class Configuration

**Release Information** Command introduced in JUNOS Release 7.1.0.  
 ATM VC Class Configuration mode added in JUNOS Release 7.3.0.

## udp-port

---

**Description** From RADIUS Configuration mode, specifies the UDP port on the router where the RADIUS authentication, accounting, or dynamic-request servers reside. The router uses this port to communicate with the RADIUS servers. The **no** version restores the default value.

From RADIUS Relay Configuration mode, specifies the UDP port on the router where the RADIUS relay authentication or accounting server resides. The router uses this port to communicate with the RADIUS relay servers. The **no** version restores the default value.

**Syntax**    **udp-port** *port*  
               **no** udp-port

- *port*—Port number in the range 1–65535
  - 1812—Default for RADIUS and RADIUS relay authentication servers
  - 1813—Default for RADIUS and RADIUS relay accounting servers
  - 1700—Default for RADIUS dynamic-request servers

**Mode**      RADIUS Configuration, RADIUS Relay Configuration

**Release Information** Command introduced before JUNOS Release 7.1.0.

### Related Topics

- [Configuring RADIUS-Based Mirroring](#)

## undebg ip bgp

---

**Description** Turns off the display of information previously enabled with the **debug ip bgp** command. There is no **no** version.

**Syntax** undebg ip bgp [ in | out ] [ *peerAddress* [ *peerAddressMask* ] ]  
[ *bgpLog* ] [ router *routerName* ] [ filtering-router *filteringRouterName* ]  
[ *accessClassName* ] [ route-map *mapName* ]

- in—Displays information for inbound events
- out—Displays information for outbound events
- *peerAddress*—IP address of BGP peer for which information is displayed
- *peerAddressMask*—Network mask of BGP peer for which information is displayed
- *bgpLog*—BGP log of interest; one of the following options:
  - dampening—BGP dampening event; route is suppressed or no longer suppressed by route-flap dampening
  - events—BGP finite state machine events and transitions
  - keepalives—BGP keepalive message events
  - next-hops—BGP next hop events
  - updates—BGP routing table update events
- *routerName*—Name of the virtual router that owns the BGP router for which information is being displayed
- *filteringRouterName*—Name of the virtual router that owns the access class and route map parameters
- *accessClassName*—Name of an access list to filter output
- *mapName*—Name of a route map to filter output

**Mode** Privileged Exec

**Release Information** Command introduced before JUNOS Release 7.1.0.

## undebg ip mbgp

---

**Description** Turns off the display of information previously enabled with the **debug ip mbgp** command. There is no **no** version.

**Syntax** undebg ip mbgp [ in | out ] [ *peerAddress* [ *peerAddressMask* ] ]  
 [ *bgpLog* ] [ router *routerName* ] [ filtering-router *filteringRouterName* ]  
 [ *accessClassName* ] [ route-map *mapName* ]

- *in*—Displays information for inbound events
- *out*—Displays information for outbound events
- *peerAddress*—IP address of BGP peer for which information is displayed
- *peerAddressMask*—Network mask of BGP peer for which information is displayed
- *bgpLog*—BGP log of interest; one of the following options:
  - *dampening*—BGP dampening event; route is suppressed or no longer suppressed by route-flap dampening
  - *events*—BGP finite state machine events and transitions
  - *keepalives*—BGP keepalive message events
  - *next-hops*—BGP next hop events
  - *updates*—BGP routing table update events
- *routerName*—Name of the virtual router that owns the BGP router for which information is being displayed
- *filteringRouterName*—Name of the virtual router that owns the access class and route map parameters
- *accessClassName*—Name of an access list to filter output
- *mapName*—Name of a route map to filter output

**Mode** Privileged Exec

**Release Information** Command introduced before JUNOS Release 7.1.0.

## undebg ip ospf

---

**Description** Turns off the display of information for the selected variable. See **debug ip ospf** command for a complete list of the ospfLog variables. There is no **no** version.

**Syntax** undebg ip ospf *ospfLog*

- *ospfLog*—OSPF log of interest; one of the following options:
  - adj—OSPF adjacency events
  - elect-dr—OSPF designated router election
  - events—OSPF general events
  - lsa—OSPF link-state advertisements events
  - neighbor—OSPF neighbor state machine
  - packets-rcvd—OSPF packets received
  - packets-sent—OSPF packets sent
  - route—OSPF route events
  - spf—All OSPF shortest path first calculation events
  - spf-ext—OSPF shortest path first external route calculation events
  - spf-inter—OSPF shortest path first interarea route calculation events
  - spf-intra—OSPF shortest path first intra-area route calculation events

**Mode** Privileged Exec

**Release Information** Command introduced before JUNOS Release 7.1.0.

## undebg ip pim

---

**Description** Turns off the display of information previously enabled with the **debug ip pim** command. There is no **no** version.

**Syntax** undebg ip pim *pimLog*

- *pimLog*—PIM log of interest

**Mode** Privileged Exec

**Release Information** Command introduced before JUNOS Release 7.1.0.



## undebg ip rip

---

- Description** Turns off the display of information previously enabled with the **debug ip rip** command. There is no **no** version.
- Syntax** undebg ip rip *ripLog*
- *ripLog*—RIP log of interest; one of the following options:
    - events—General RIP events, such as removing RIP from an interface or creating the RIP process
    - route—Events associated with two RIP routers exchanging routes
- Mode** Privileged Exec
- Release Information** Command introduced before JUNOS Release 7.1.0.

## undebg ipv6 ospf

---

- Description** Turns off the display of information for the selected variable. See **debug ipv6 ospf** command for a complete list of the ospfLog variables. There is no **no** version.
- Syntax** undebg ipv6 ospf *ospfLog*
- *ospfLog*—OSPF log of interest; one of the following options:
    - adj—OSPF adjacency events
    - elect-dr—OSPF designated router election
    - events—OSPF general events
    - lsa—OSPF link-state advertisements events
    - neighbor—OSPF neighbor state machine
    - packets-rcvd—OSPF packets received
    - packets-sent—OSPF packets sent
    - route—OSPF route events
    - spf—All OSPF shortest path first calculation events
    - spf-ext—OSPF shortest path first external route calculation events
    - spf-inter—OSPF shortest path first interarea route calculation events
    - spf-intra—OSPF shortest path first intra-area route calculation events
- Mode** Privileged Exec
- Release Information** Command introduced before JUNOS Release 7.1.0.

## undebg ipv6 pim

---

**Description** Turns off the display of information previously enabled with the **debug ipv6 pim** command. There is no **no** version.

**Syntax** undebg ipv6 pim *pimLog*

- *pimLog*—PIM log of interest

**Mode** Privileged Exec

**Release Information** Command introduced before JUNOS Release 7.1.0.

## undebg isis

---

**Description** Turns off the display of information for the selected variable. See the **debug isis** command for a complete list of the IS-IS log variables. There is no **no** version.

**Syntax** undebg isis *isisLog*

- *isisLog*—IS-IS log of interest; one of the following options:
  - adj-packets—IS-IS adjacency-related packets, such as hello packets sent and IS-IS received adjacencies going up and down
  - mpls traffic-eng advertisements—MPLS traffic-engineering agent advertisements
  - mpls traffic-eng agents—MPLS traffic-engineering agents
  - snp-packets—IS-IS CSNPs/PSNPs
  - spf-events—Shortest path first events
  - spf-statistics—SPF timing and statistic data
  - spf-triggers—SPF triggering events
  - update-packets—Update-related packets

**Mode** Privileged Exec

**Release Information** Command introduced before JUNOS Release 7.1.0.

## unicast

---

**Description** Modifies the subscriber policy for the unicast (user-to-user) protocol to define whether the subscriber (client) interfaces that belong to a bridge group or to a VPLS instance forward (permit) or filter (deny) unicast packets. The **no** version restores the default value, permit unicast packets.

You cannot change the default subscriber policy values for trunk (server) interfaces that belong to a bridge group or to a VPLS instance. You also cannot change the default subscriber policy values for a VPLS virtual core interface, which acts as a trunk interface. The VPLS virtual core interface represents all the MPLS tunnels from the router to the remote VPLS edge (VE) devices.

**Syntax** unicast { permit | deny }

no unicast

- permit—Specifies that the subscriber interface associated with the bridge group or VPLS instance forwards unicast packets
- deny—Specifies that the subscriber interface associated with the bridge group or VPLS instance filters unicast packets

**Mode** Subscriber Policy Configuration

**Release Information** Command introduced before JUNOS Release 7.1.0.

## unknown-destination

---

**Description** Modifies the subscriber policy for packets with unknown unicast destination addresses (DAs) to define whether the subscriber (client) interfaces that belong to a bridge group or to a VPLS instance forward (permit) or filter (deny) packets with unknown unicast DAs. The **no** version restores the default value, deny packets with unknown unicast DAs.

You cannot change the default subscriber policy values for trunk (server) interfaces that belong to a bridge group or to a VPLS instance. You also cannot change the default subscriber policy values for a VPLS virtual core interface, which acts as a trunk interface. The VPLS virtual core interface represents all of the MPLS tunnels from the router to the remote VPLS edge (VE) devices.

**Syntax** unknown-destination { permit | deny }

no unknown-destination

- permit—Specifies that the subscriber interface associated with the bridge group or VPLS instance forwards packets with unknown unicast DAs
- deny—Specifies that the subscriber interface associated with the bridge group or VPLS instance filters packets with unknown unicast DAs

**Mode** Subscriber Policy Configuration

**Release Information** Command introduced before JUNOS Release 7.1.0.

## unknown-protocol

---

**Description** Modifies the subscriber policy for packets containing an unknown protocol to define whether the subscriber (client) interfaces that belong to a bridge group or to a VPLS instance forward (permit) or filter (deny) these packets. The **no** version restores the default value, permit unknown protocol packets.

You cannot change the default subscriber policy values for trunk (server) interfaces that belong to a bridge group or to a VPLS instance. You also cannot change the default subscriber policy values for a VPLS virtual core interface, which acts as a trunk interface. The VPLS virtual core interface represents all of the MPLS tunnels from the router to the remote VPLS edge (VE) devices.

**Syntax** unknown-protocol { permit | deny }  
no unknown-protocol

- permit—Specifies that the subscriber interface associated with the bridge group or VPLS instance forwards packets containing an unknown protocol
- deny—Specifies that the subscriber interface associated with the bridge group or VPLS instance filters packets containing an unknown protocol

**Mode** Subscriber Policy Configuration

**Release Information** Command introduced before JUNOS Release 7.1.0.

## update-source

---

**Description** Specifies the loopback interface whose local address is used as the source address for the OSPF, PIM, or RIP connection to a remote neighbor. The **no** version deletes the source address from the connection.



**NOTE:** For PIM, this command is typically used when you configure PIM remote neighbors to run multicast services over BGP/MPLS VPNs. That functionality is no longer supported.

**Syntax** For OSPF:  
`[ no ] update-source loopback interfaceSpecifier`

- *interfaceSpecifier*—Integer, in the range 1–4294967293, identifying the loopback interface

For PIM:  
`update-source interfaceType interfaceSpecifier`  
`no update-source [ interfaceType interfaceSpecifier ]`

For RIP:  
`[ no ] update-source interfaceType interfaceSpecifier`

- *interfaceType*—Interface type; see *Interface Types and Specifiers* in *About This Guide*
- *interfaceSpecifier*—Particular interface; format varies according to interface type; see *Interface Types and Specifiers* in *About This Guide*

**Mode** Remote Neighbor Configuration

**Release Information** Command introduced before JUNOS Release 7.1.0.

## use canned-group

---

**Description** Creates a DoS protection group that uses a preconfigured (canned) set of parameters. The **revert** keyword returns to the original values, which are the default for the group. The **no** version associates the group with the default preconfigured group settings.

**Syntax** `use canned-group groupName [ revert ]`  
`no use canned-group`

- *groupName*—Name of the DoS protection template

**Mode** DoS Protection Group Configuration

**Release Information** Command introduced in JUNOS Release 8.1.0.

## use-release-grace-period

---

**Description** Applies the grace period, which is specified by the **grace-period** command, to the DHCP local address pool addresses that are explicitly released by clients. When a client releases an address, the address enters the grace period and can be reassigned only to the original client. The **no** version restores the default, which disables the use of the grace period for explicitly released addresses.

**Syntax** [ no ] use-release-grace-period

**Mode** DHCP Local Pool Configuration

**Release Information** Command introduced in JUNOS Release 8.0.0.

## username

---

**Description** Configures a user entry and optional password or secret in the default local user database. This command creates the database if it does not already exist. The **no** version deletes the username entry from the default local user database. The **nopassword** keyword removes the password or secret.

**Syntax** username *userName* [ nopassword | password [ *encryptionType* ] *passwordValue* | secret [ *encryptionType* ] *secretValue* ]

no username *userName*

- *userName*—Name of user
- nopassword—Specifies that a password is not required for the specified username; deletes the password or secret from an existing username
- *encryptionType*—One of the following:
  - 0—Unencrypted password or secret (the default)
  - 5—MD5-encrypted secret
  - 8—Two-way encrypted password
- *passwordValue*—Character string that specifies the password. The string can contain any alphanumeric character, including spaces, up to 64 characters. Passwords are case sensitive.
- *secretValue*—Character string that specifies the secret. The string can contain any alphanumeric characters, including spaces, up to 64 characters. Secrets are case sensitive.

**Mode** Global Configuration

**Release Information** Command introduced before JUNOS Release 7.1.0.

## user-name

---

**Description** Specifies the username for an IP service profile. The **no** version removes the username.

**Syntax** `user-name serviceUsername`  
`no user-name`

- *serviceUsername*—Up to 32-character username

**Mode** IP Service Profile Configuration

**Release Information** Command introduced before JUNOS Release 7.1.0.

## user-packet-class

---

**Description** Adds a user packet class rule to a policy list that sets the user packet class attribute of packets that match the current classifier control list. The **no** version removes a user packet class from a policy list; the **suspend** version temporarily suspends the policy rule; the **no suspend** version resumes application of a suspended rule.



**NOTE:** This command replaces the Policy List Configuration version of the **user-packet-class** command, which may be removed completely in a future release.

**Syntax** `[ no ] [ suspend ] user-packet-class userPacketClassValue`

- *userPacketClassValue*—User packet class value assigned to packets, in the range 0–15

**Mode** Classifier Group Configuration

**Release Information** Command introduced before JUNOS Release 7.1.0.

### Related Topics

- Policy Rule Precedence

## user-prefix

---

**Description** Specifies the user prefix for an IP service profile. The **no** version removes the user prefix.

**Syntax** `user-prefix prefixString`  
`no user-prefix`

- *prefixString*—Appends the interface physical location to the username

**Mode** IP Service Profile Configuration

**Release Information** Command introduced before JUNOS Release 7.1.0.

## vbr-nrt

---

**Description** In ATM VC Configuration mode, configures the variable bit rate, nonreal time (VBR-NRT) service category on an ATM PVC. You must specify the peak cell rate (PCR), sustained cell rate (SCR), and maximum burst size (MBS). The **vbr-nrt** command is valid only for data PVCs; you cannot use this command for control (ILMI or signaling) PVCs. The **no** version restores the default service category, unspecified bit rate (UBR) without a PCR.

In ATM VC Class Configuration mode, configures the VBR-NRT service category as part of a VC class definition that you assign to an ATM PVC. The **no** version restores the default service category, UBR without a PCR, in the VC class.

**Syntax** `vbr-nrt pcr scr mbs`  
`no vbr-nrt`

- *pcr*—Peak cell rate, in Kbps, in the range 0–149760 (for OC3 ATM modules) or 0–599040 (for OC12 ATM modules)
- *scr*—Sustained cell rate, in Kbps, in the range 0–149760 (for OC3 ATM modules) or 0–599040 (for OC12 ATM modules)
- *mbs*—Maximum burst size, in cells, in the range 0–16777215

**Mode** ATM VC Configuration, ATM VC Class Configuration

**Release Information** Command introduced in JUNOS Release 7.1.0.  
ATM VC Class Configuration mode added in JUNOS Release 7.3.0.



**vbr-rt**

---

**Description** In ATM VC Configuration mode, configures the variable bit rate, real time (VBR-RT) service category on an ATM PVC. You must specify the peak cell rate (PCR), sustained cell rate (SCR), and maximum burst size (MBS). The **vbr-rt** command is valid only for data PVCs; you cannot use this command for control (ILMI or signaling) PVCs. The **no** version restores the default service category, unspecified bit rate (UBR) without a PCR.

In ATM VC Class Configuration mode, configures the VBR-RT service category as part of a VC class definition that you assign to an ATM PVC. The **no** version restores the default service category, UBR without a PCR, in the VC class.

**Syntax** `vbr-rt pcr scr mbs`  
`no vbr-rt`

- *pcr*—Peak cell rate, in Kbps, in the range 0–149760 (for OC3 ATM modules) or 0–599040 (for OC12 ATM modules)
- *scr*—Sustained cell rate, in Kbps, in the range 0–149760 (for OC3 ATM modules) or 0–599040 (for OC12 ATM modules)
- *mbs*—Maximum burst size, in cells, in the range 0–16777215

**Mode** ATM VC Configuration, ATM VC Class Configuration

**Release Information** Command introduced in JUNOS Release 7.1.0.  
 ATM VC Class Configuration mode added in JUNOS Release 7.3.0.

## vc-class atm

---

**Description** Creates and names a VC class for an ATM data PVC. This command accesses ATM VC Class Configuration mode, from which you can configure a set of attributes for an ATM data PVC. The VC class can include attributes for the service category, encapsulation method, F5 OAM options, and Inverse ARP. You then apply the attributes as a group by assigning the VC class to an individual PVC, to all PVCs created on a specified ATM major interface, to all PVCs created on a specified ATM 1483 subinterface, or to a base profile from which bulk-configured VC ranges are dynamically created. The **no** version removes the named VC class from the router.

You cannot remove a VC class that is currently assigned to at least one ATM PVC, ATM 1483 subinterface, or ATM major interface without first issuing the **no class-vc** command or the **no class-int** command to remove the VC class association with the PVC, interface, or subinterface.



**NOTE:** For information about the total number of ATM VC classes supported on the router, see *JUNOS Release Notes, Appendix A, System Maximums*.

---

**Syntax** [ no ] vc-class atm *vcClassName*

- *vcClassName*—Name of the VC class; a string of up to 32 alphanumeric characters

**Mode** Global Configuration

**Release Information** Command introduced in JUNOS Release 7.3.0.

## version

---

**Description** Specifies the global RIP version. The **no** version reverts to the default value, RIP version 1. Use the **ip rip receive** and **ip rip send version** commands to specify the RIP version for a specific interface.

**Syntax** version { 1 | 2 }

no version

- 1—RIP version 1
- 2—RIP version 2

**Mode** Address Family Configuration, Router Configuration

**Release Information** Command introduced before JUNOS Release 7.1.0.

## virtual-router

**Description** Creates a virtual router or accesses the context of a previously created virtual router or a VRF. The **no** version deletes the virtual router, and the router defaults to the default virtual router. Issuing a **no** version that specifies an existing VRF only displays the error message: “Cannot delete a VRF with this command.” You must use the **no ip vrf** command to remove a VRF.



**NOTE:** In Domain Map Configuration mode, the **virtual-router** command has been replaced by the **router-name** command and may be removed completely from Domain Map Configuration mode in a future release.

**Syntax** `virtual-router vrName | :vrfName | vrName:vrfName`  
`no virtual-router vrName [ wait-for-completion [ waitSeconds ] ]`

- *vrName*—Name of the virtual router; a string of 1–32 alphanumeric characters
- *:vrfName*—Name of a VRF in the current VR context; a string of 1–32 alphanumeric characters
- *vrName:vrfName*—Name of a VRF in the context of a VR other than the current VR
- *wait-for-completion*—Specifies (in the absence of *waitSeconds*) that the CLI waits for completion of the **no** version operation before it returns a prompt, regardless of how long that takes
- *waitSeconds*—Number of seconds, in the range 1–64000, that the CLI waits before it returns a prompt, regardless of whether the **no** version operation has been completed

**Mode** Global Configuration, Privileged Exec

**Release Information** Command introduced before JUNOS Release 7.1.0.

## vlan advisory-rx-speed

**Description** Sets an advisory receive (Rx) speed that the LAC sends to the LNS. The **no** version restores the default behavior, in which the Rx speed is not sent to the LNS.

**Syntax** `vlan advisory-rx-speed speed`  
`no vlan advisory-rx-speed`

- *speed*—Speed in the range 0–2147483647 kbps; 0 indicates no advisory speed setting

**Mode** Profile Configuration, Subinterface Configuration

**Release Information** Command introduced in JUNOS Release 7.2.0.

## vlan advisory-tx-speed

---

**Description** Sets an advisory connect (Tx) speed that the LAC sends in the Tx connect speed to the LNS. The **no** version restores the default behavior, in which the Tx speed is not sent to the LNS.

**Syntax** `vlan advisory-tx-speed speed`  
`no vlan advisory-rx-speed`

- *speed*—Speed in the range 0–2147483647 kbps; 0 indicates no advisory speed setting

**Mode** Profile Configuration, Subinterface Configuration

**Release Information** Command introduced in JUNOS Release 7.2.0.

## vlan auto-configure

---

**Description** Specifies the types of dynamic upper interface encapsulations that are accepted or detected by a dynamic VLAN subinterface. You can issue this command repeatedly in Profile Configuration mode to include autodetection of multiple upper interface encapsulation types within the base profile for a dynamic VLAN subinterface. The **no** version terminates detection of the specified encapsulation type.

**Syntax** `vlan auto-configure upperInterfaceType [ lockout-time { minTime maxTime | none } ]`  
`no vlan auto-configure upperInterfaceType [ lockout-time ]`

- *upperInterfaceType*—One of the following dynamic encapsulation types:
  - `ip`
  - `pppoe`
- *minTime*—Minimum lockout time in the range 1–86400 seconds (24 hours); default value is 1 second
- *maxTime*—Maximum lockout time in the range 1–86400 seconds (24 hours); default value is 1 second
- `none`—Disables lockout time for the specified dynamic encapsulation type

**Mode** Profile Configuration

**Release Information** Command introduced in JUNOS Release 7.1.0.  
**lockout-time** keyword added in JUNOS Release 7.3.0.

## vlan auto-configure agent-circuit-identifier

---

**Description** Configures the router to dynamically create VLAN subinterfaces based on the agent-circuit-id option (suboption 1) of the option 82 field in DHCP messages, or based on the DSL Forum VSA 26-1 (Agent-Circuit-Id) in PPPoE PADR and PADI packets. The **no** version disables the creation of VLAN subinterfaces based on agent-circuit-identifier information.

**Syntax** [ no ] vlan auto-configure agent-circuit-identifier

**Mode** Profile Configuration

**Release Information** Command introduced in JUNOS Release 7.3.0.

## vlan bulk-config

---

**Description** Configures a range of single-tagged VLAN IDs and double-tagged S-VLAN IDs for use by a dynamic VLAN subinterface, and assigns a name to the VLAN range. Each VLAN range consists of one or more nonoverlapping VLAN subranges. A VLAN subrange is a group of VLAN IDs that resides within the specified VLAN ID ranges. You can configure multiple VLAN ranges on a major VLAN interface. The **no** version removes the specified VLAN range (including all subranges in the range) from the VLAN major interface or the specified subrange from the VLAN range. The **no** version also removes any overriding profile assignments for VLAN IDs within the deleted VLAN range or VLAN subrange.

**Syntax** To configure or remove a bulk configuration or a specific VLAN range:  
 vlan bulk-config *bulkConfigName* [ vlan-range *vlanIdStart* *vlanIdEnd* ]\*  
 no vlan bulk-config *bulkConfigName* [ vlan-range *vlanIdStart* *vlanIdEnd* ]  
 To configure a VLAN range containing double-tagged S-VLAN IDs:  
 vlan bulk-config *bulkConfigName* [ svlan-range *s-vlanIdStart* *s-vlanIdEnd* *vlanIdStart* *vlanIdEnd* ]\*  
 To configure a VLAN range containing S-VLAN IDs with any VLAN ID:  
 vlan bulk-config *bulkConfigName* [ svlan-range *s-vlanIdStart* *s-vlanIdEnd* any ]\*  
 To configure a VLAN range that is based on agent-circuit-identifier information:  
 vlan bulk-config *bulkConfigName* [ svlan-range *s-vlanIdStart* *s-vlanIdEnd* agent-circuit-identifier ]\*

To remove a VLAN range containing S-VLAN IDs or agent-circuit-identifier information:

```
no vlan bulk-config bulkConfigName [ svlan-range s-vlanIdStart s-vlanIdEnd  
{ vlanIdStart vlanIdEnd | any | agent-circuit-identifier } ]
```

- *bulkConfigName*—Name of the VLAN range; string of up to 80 characters
- *vlanIdStart*—Starting VLAN ID of the VLAN subrange you are configuring
- *vlanIdEnd*—Ending VLAN ID of the VLAN subrange you are configuring
- *s-vlanIdStart*—Starting S-VLAN ID of the VLAN subrange you are configuring
- *s-vlanIdEnd*—Ending S-VLAN ID of the VLAN subrange you are configuring
- any—Specifies the VLAN ID as a wildcard
- agent-circuit-identifier—Specifies a VLAN range that is based on agent-circuit-identifier information
- \*—Indicates that one or more parameters can be repeated multiple times in a list in the command line

**Mode** Interface Configuration

**Release Information** Command introduced in JUNOS Release 7.3.0.

## vlan bulk-config modify

---

**Description** Modifies the VLAN subrange values for the specified bulk configuration VLAN range. If the new subrange encompasses previously configured subranges within that range, those subranges are merged into the new one, freeing subrange resources. There is no **no** version.

**Syntax** To modify VLAN ranges containing single-tagged VLAN IDs:  
`vlan bulk-config bulkConfigName modify vlan-range vlanIdStart vlanIdEnd`

To modify VLAN ranges containing double-tagged S-VLAN IDs or based on agent-circuit-identifier:  
`vlan bulk-config bulkConfigName modify svlan-range s-vlanIdStart s-vlanIdEnd  
{ vlanIdStart vlanIdEnd | any | agent-circuit-identifier }`

- *bulkConfigName*—Name of the VLAN range; string of up to 80 characters
- *vlanIdStart*—Starting VLAN ID of the VLAN subrange you are configuring
- *vlanIdEnd*—Ending VLAN ID of the VLAN subrange you are configuring
- *s-vlanIdStart*—Starting S-VLAN ID of the S-VLAN subrange you are configuring
- *s-vlanIdEnd*—Ending S-VLAN ID of the S-VLAN subrange you are configuring
- any—Specifies the VLAN ID as a wildcard
- agent-circuit-identifier—Specifies a VLAN range that is based on agent-circuit-identifier information

**Mode** Interface Configuration

**Release Information** Command introduced in JUNOS Release 7.3.0.

## vlan bulk-config shutdown

---

**Description** Administratively disables (shuts down) the specified bulk configuration, or a specified VLAN range or subrange. When you shut down a specified bulk configuration, all VLAN ranges, including those based on double-tagged S-VLAN IDs or agent-circuit-identifier information, are disabled. The **no** version reenables the specified bulk configuration, the specified VLAN range, or the specified subranges; this is the default condition.

**Syntax** To shut down or reenables the specified bulk configuration or a specific VLAN range:  
`[ no ] vlan bulk-config bulkConfigName shutdown`

`[ no ] vlan bulk-config bulkConfigName shutdown vlan-range vlanIdStart vlanIdEnd`

To shut down or reenables VLAN ranges containing double-tagged S-VLAN IDs or based on agent-circuit-identifier information:

`[ no ] vlan bulk-config bulkConfigName shutdown svlan-range s-vlanIdStart s-vlanIdEnd { vlanIdStart vlanIdEnd | any | agent-circuit-identifier }`

- *bulkConfigName*—Name of the VLAN range; string of up to 80 characters
- *vlanIdStart*—Starting VLAN ID of the VLAN subrange you are configuring
- *vlanIdEnd*—Ending VLAN ID of the VLAN subrange you are configuring
- *s-vlanIdStart*—Starting S-VLAN ID of the S-VLAN subrange you are configuring
- *s-vlanIdEnd*—Ending S-VLAN ID of the S-VLAN subrange you are configuring
- any—Specifies the VLAN ID as a wildcard
- agent-circuit-identifier—Specifies a VLAN range that is based on agent-circuit-identifier information

**Mode** Interface Configuration

**Release Information** Command introduced in JUNOS Release 7.3.0.

## vlan classifier-list

---

**Description** Creates or modifies a VLAN classifier control list. The **no** version deletes the classifier control list.

**Syntax** `vlan classifier-list classifierName`  
`[ traffic-class className ] [ color { green | yellow | red } ]`  
`[ user-packet-class userPacketClassValue ] [ user-priority userPriorityValue ]`  
`no vlan classifier-list classifierName [ classifierNumber ]`

- *classifierName*—Name of a classifier list entry
- *className*—Name of a traffic class; the router supports up to eight traffic classes
- *green*—Matches packet color to green, indicating a low drop preference
- *yellow*—Matches packet color to yellow, indicating a medium drop preference
- *red*—Matches packet color to red, indicating a high drop preference
- *userPacketClassValue*—Value of the user packet class in the range 0–15
- *userPriorityValue*—Value of the user priority bits in the range 0–7
- *classifierNumber*—Index of the classifier control list entry to be deleted; an integer in the range 1–10000

**Mode** Global Configuration

**Release Information** Command introduced before JUNOS Release 7.1.0.

**Related Topics**

- Creating or Modifying Classifier Control Lists for VLAN Policy Lists

## vlan description

---

**Description** Assigns an alias or a description to a VLAN subinterface. The **no** version removes the description.

**Syntax** `vlan description aliasName`  
`no vlan description`

- *aliasName*—Alias or description; string of up to 64 characters

**Mode** Interface Configuration, Profile Configuration

**Release Information** Command introduced before JUNOS Release 7.1.0.  
Profile Configuration mode added in JUNOS Release 7.2.0.



## vlan dos-protection-group

---

**Description** Attaches a VLAN denial of service (DoS) protection group to an interface. The **no** version removes the attachment of the DoS protection group from the interface.

**Syntax** `vlan dos-protection-group groupName`  
`no vlan dos-protection-group`

- *groupName*—Name of the DoS protection group

**Mode** Interface Configuration

**Release Information** Command introduced in JUNOS Release 8.1.0.

## vlan id

---

**Description** Specifies a VLAN ID. There is no **no** version.

**Syntax** `vlan id idValue [ untagged ] [ mac-address macAddress ]`

- *idValue*—Number unique within the Ethernet interface, in the range 0–4095
- *untagged*—Specifies that frames be sent untagged; valid only for VLAN ID 0
- *macAddress*—MAC address of the interface; when you do not specify a unique MAC address, the VLAN uses the MAC address of the Ethernet interface

**Mode** Interface Configuration

**Release Information** Command introduced before JUNOS Release 7.1.0.

### Related Topics

- Configuring Ethernet/VLAN Layer 2 Services
- Configuring Local ATM Cross-Connects with AAL5 Encapsulation
- Configuring Local Cross-Connects Between Ethernet/VLAN Interfaces

## vlan policy

---

**Description** Assigns a VLAN policy list to an interface. If you enter the **vlan policy** command and the policy list does not exist, the router creates a policy list with no rules, the default. When no rules are found in a policy list, the router performs a routing table lookup and forwards packets on the interface based on the routing table information. You must specify the **input** or **output** keyword to assign the policy list to the ingress or egress of the interface.

In Profile Configuration mode, assigns the policy list to a profile, which then assigns the policy to an interface.

In Interface Configuration mode, the **no** version removes the association between a policy list and an interface. In Profile Configuration mode, the **no** version removes the policy reference from the profile.

**Syntax** `vlan policy { input | output } policyName`  
`[ statistics { enabled [ baseline { enabled | disabled } ] [ preserve | merge ] | disabled [ merge ] } ] merge ]`  
`no vlan policy { input | output } [ policyName ]`

- **input**—Applies policy to data arriving at this interface
- **output**—Applies policy to data leaving this interface
- ***policyName***—Name of the policy; a maximum of 40 characters
- **statistics**—Enables or disables collection of policy routing statistics
  - **enabled**—Enables collection of policy routing statistics
  - **baseline enabled**—Enables baselining of policy routing statistics
  - **baseline disabled**—Disables baselining of policy routing statistics
  - **preserve**—Preserves existing statistics for any classifier list that is the same for both the new and old policy attachments when you attach a new policy to an interface
  - **disabled**—Disables collection of policy routing statistics
- **merge**—Enables merging of multiple policies to form a single policy

**Mode** Interface Configuration, Profile Configuration

**Release Information** Command introduced before JUNOS Release 7.1.0.  
**merge** keyword added in JUNOS Release 7.2.0.  
Profile Configuration mode added in JUNOS Release 7.2.0.

### Related Topics

- [Setting a Statistics Baseline for Policies](#)

## vlan policy-list

---

**Description** Creates the specified policy list and accesses Policy List Configuration mode. The **no** version deletes the policy list.

**Syntax** [ no ] vlan policy-list *policyName*

- *policyName*—Name of a policy list; string of up to 40 alphanumeric characters

**Mode** Global Configuration

**Release Information** Command introduced before JUNOS Release 7.1.0.

**Related Topics**

- Creating Policy Lists for VLANs

## vlan profile

---

**Description** Adds a nested profile assignment to a base profile for a dynamic VLAN subinterface. A nested profile assignment references another profile that dynamically configures upper interface encapsulation types over the VLAN subinterface. The **no** version removes the profile assignment for the upper interface type.

**Syntax** vlan profile *upperInterfaceType* *profileName*  
no vlan profile *upperInterfaceType* *profileName*

- *upperInterfaceType*—One of the following dynamic encapsulation types:
  - ip
  - pppoe
- *profileName*—Profile name of up to 80 characters

**Mode** Profile Configuration

**Release Information** Command introduced in JUNOS Release 7.1.0.

## vlan service-profile

---

**Description** Assigns an IP service profile to a VLAN subinterface. The service profile must be defined in the default virtual router. The **no** version removes the IP service profile from the VLAN subinterface.

**Syntax** [ no ] vlan service-profile *profileName*

- *profileName*—Name of the IP service profile

**Mode** Profile Configuration

**Release Information** Command introduced in JUNOS Release 7.1.0.

## volume

---

**Description** Configures the threshold for the volume of traffic allowed for the service session. The service is terminated when the threshold is exceeded. The **no** version removes the volume attribute from the service session profile.

**Syntax** volume *megabytes*  
no volume

- *megabytes*—Number of megabytes in the range 0–16777251

**Mode** Service Session Profile Configuration

**Release Information** Command introduced in JUNOS Release 7.2.0.

## warning

---

**Description** Sets the minimum and maximum threshold values for DHCP local address pool utilization. If you issue the **snmp-server view** command, SNMP traps are generated when utilization occurs above or below the specified threshold values. The **no** version restores the default threshold values for local address pool utilization.

**Syntax** warning *maximumUtilization minimumUtilization*  
no warning

- *maximumUtilization*—Maximum utilization value for the DHCP local address pool
- *minimumUtilization*—Minimum utilization value for the DHCP local address pool

**Mode** DHCP Local Pool Configuration

**Release Information** Command introduced before JUNOS Release 7.1.0.


## weight

---

- Description** Sets the weighted round-robin weight of the scheduler node or queue. A queue weight of 0 (zero) gives the queue infinite weight. The **no** version restores the default value, 8.
- Syntax** `weight weightValue [ operator operandValue ]*`  
`no weight`
- *weightValue*—Number in the range 0–4080; default value is 8
  - *operator*—Mathematical function
  - *operandValue*—Input for the operator; can be a QoS parameter definition name or an integer
  - \*—Indicates that one or more parameters can be repeated multiple times in a list in the command line
- Mode** Scheduler Profile Configuration
- Release Information** Command introduced before JUNOS Release 7.1.0.
- Related Topics**
- Configuring the HRR Weight for a Scheduler Node or Queue

## write core

---

- Description** Reboots the active SRP module, the standby SRP module, or the module in a specified slot, and writes the core dump to a file. There is no **no** version.
- Syntax** `write core [ standby-srp | slot slotNumber ] [ force ] [ reason reasonText ]`
- *standby-srp*—Specifies the standby SRP module
  - *slotNumber*—Number of a selected slot in the router; for ERX-7xx models, a number in the range 0–6; for ERX-14xx models, a number in the range 0–13; for the ERX-310 router, a number in the range 0–2; for the E120 router, a number in the range 0–5; for the E320 router, a number in the range 0–16
  - *force*—Prompts for confirmation to reboot when the router is in certain states, such as during the synchronization of SRP modules, that can lead to a loss of configuration data or an NVS corruption
- 
-  **NOTE:** The **force** keyword is available when you specify a slot only if that slot is an SRP module slot.
- 
- *reasonText*—Alphanumeric text string (1–255 characters long) that explains the request for a core dump and logs it in the reboot
- Mode** Privileged Exec
- Release Information** Command introduced in JUNOS Release 7.3.0.

## write memory

---

**Description** Saves all outstanding (unsaved) configuration changes to nonvolatile storage; an exact alias of the **copy running-configuration startup-configuration** command. Available if the router is in either Automatic Commit mode or Manual Commit mode. If issued while in Automatic Commit mode, the CLI notifies you that the command is not necessary, but allows you to proceed. There is no **no** version.

**Syntax** write memory

**Mode** Privileged Exec

**Release Information** Command introduced before JUNOS Release 7.1.0.

## yellow-mark

---

**Description** Applies ToS mark value to yellow packets, which can be from policy actions, earlier policies, or rate-limit hierarchies. The **no** version deletes the ToS mark value.

**Syntax** [ no ] yellow-mark *colorMarkValue*

- *colorMarkValue*—Value of the ToS mark to be applied, in the range 0–255

**Mode** Color Mark Profile Configuration

**Release Information** Command introduced in JUNOS Release 7.2.0.

### Related Topics

- Hierarchical Rate Limits Overview
- Policy Rule Precedence

