

snmp-server host

Syntax To specify the SNMP version, community, UDP port, trap category and trap severity:

```
snmp-server host ipAddress [ version ver ] securityString [ udp-port port ]  
[ trapCategory ]* [ trapFilters trapFilter ]
```

```
no snmp-server host ipAddress
```

To specify the ping timeout and trap queue:

```
snmp-server host ipAddress pingTimeOut timeOutValue  
[ trapQueue { drainRate queueDrainRate | full queueFull |  
size queueSize }  
[ drainRate queueDrainRate | full queueFull | size queueSize ]*
```

```
snmp-server host ipAddress trapQueue  
{ drainRate queueDrainRate | full queueFull | size queueSize }  
[ drainRate queueDrainRate | full queueFull | size queueSize ]*  
[ pingTimeOut timeOutValue ]
```

```
no snmp-server host ipAddress { pingTimeOut | trapQueue { drainRate | full | size  
} }
```

Release Information Command introduced before JUNOS Release 7.1.0.
ip keyword added in JUNOS Release 7.1.0.
packetMirror keyword added in JUNOS Release 7.2.0.

Description Configures one or more hosts to receive an SNMP trap. The **no** version removes the specified host from the list of recipients.

- Options**
- *ipAddress*—IP address of the SNMP trap recipient
 - *ver*—SNMP protocol version for traps sent to host; one of the following values:
v1, v2c, or v3
 - *securityString*—SNMP community string
 - *port*—UDP port number of SNMP trap recipient
 - *trapCategory*—SNMP trap category
 - *addrPool*—Local address pool traps
 - *atmPing*—E-series router proprietary ATM ping traps
 - *bfdmib*—BFD MIB traps
 - *bgp*—BGP state change traps
 - *bulkstats*—Bulkstats file full and nearly full traps
 - *cliSecurityAlert*—Security alerts traps
 - *dosProtectionPlatform*—DoS protection platform traps

- dvmrp—DVMRP traps
- dvmrpUni—E-series router proprietary DVMRP traps
- environment—Power/temperature/fan traps
- fileXfer—File transfer status change traps
- inventory—Router inventory/status traps
- ip—Internet Protocol traps
- ldp—LDP traps
- link—SNMP linkUp/linkDown traps
- log—System log capacity traps
- mobileIpv4—Mobile IPv4 traps
- mplste—Mplste traps
- mrouter—Mrouter traps
- packetMirror—Secure packet mirroring traps; visible only if packet mirroring is enabled
- ospf—OSPF traps
- ping—Ping operation traps (in disman remops MIB)
- radius—RADIUS traps
- snmp—SNMP coldstart, warmstart, link, authenticationFailure traps
- traceroute—Traceroute operation traps (in disman remops MIB)
- *—Indicates that one or more parameters can be repeated multiple times in a list in the command line
- *trapFilter*—Minimum severity level for filtering traps sent to this host
 - alert—Severity level 1
 - critical—Severity level 2
 - debug—Severity level 7
 - emergency—Severity level 0
 - error—Severity level 3
 - informational—Severity level 6
 - notice—Severity level 5
 - warning—Severity level 4
- *timeOutValue*—Ping timeout in minutes, in the range 1–90; default value is 1
- *trapQueue*—Configures the SNMP trap queue for traps sent to this host

- *queueDrainRate*—Maximum number of traps per second to be sent to the host, in the range 0–2147483647; default value is 0
- *queueFull*—Method used to drop traps when the trap queue is full
 - *dropFirstIn*—Drops the oldest trap in the queue
 - *dropLastIn*—Drops the most recent trap added to the queue
- *queueSize*—Maximum number of traps to be kept in the trap queue, in the range 32–214748364; default value is 32

Mode Global Configuration

Related Topics ■ Monitoring SNMP Secure Packet Mirroring Traps

