

# SNMP Manager

---

## Description

The SNMP Manager feature allows a router to serve as an SNMP manager. As an SNMP manager, the router can send SNMP requests to agents and receive SNMP responses and notifications from agents. When the SNMP manager process is enabled, the router can query other SNMP agents and process incoming SNMP traps.

## Security Considerations

Most network security policies assume that routers will be accepting SNMP requests, sending SNMP responses, and sending SNMP notifications.

With the SNMP manager functionality enabled, the router may also be sending SNMP requests, receiving SNMP responses, and receiving SNMP notifications. Your security policy implementation may need to be updated prior to enabling this feature.

SNMP requests are typically sent to UDP port 161. SNMP responses are typically sent from UDP port 161. SNMP notifications are typically sent to UDP port 162.

## SNMP Sessions

Sessions are created when the SNMP manager in the router sends SNMP requests, such as inform requests, to a host or receives SNMP notifications from a host. One session is created for each destination host. If there is no further communication between the router and host within the session timeout period, the session will be deleted.

The router tracks statistics, such as the average round-trip time required to reach the host, for each session. Using the statistics for a session, the SNMP manager in the router can set reasonable timeout periods for future requests, such as informs, for that host. If the session is deleted, all statistics are lost. If another session with the same host is later created, the request timeout value for replies will return to the default value.

Sessions consume memory. A reasonable session timeout value should be large enough that regularly used sessions are not prematurely deleted, yet small enough such that irregularly used, or one-shot sessions, are purged expeditiously.

## Configuration Tasks

To configure the router to act as an SNMP manager, perform the tasks in the following sections:

- Enable the SNMP Manager
- Monitor the SNMP Manager

### Enable the SNMP Manager

To enable the SNMP manager process and optionally set the session timeout value, perform the following tasks in global configuration mode:

Task	Command
Enable the SNMP Manager.	<b>snmp-server manager</b>
(Optional) Change the session timeout value.	<b>snmp-server manager session-timeout</b> <i>seconds</i>

### Monitor the SNMP Manager

To monitor the SNMP manager process, perform the following tasks in EXEC mode:

Task	Command
Display global SNMP information.	<b>show snmp</b>
Display information about current sessions.	<b>show snmp sessions [brief]</b>
Display information about current pending requests.	<b>show snmp pending</b>

## Configuration Examples

The following example enables the SNMP manager and sets the session timeout to a larger value than the default:

```
snmp-server manager
snmp-server manager session-timeout 1000
```

## Command Reference

This section documents new or modified commands. All other commands used with this feature are documented in the Cisco IOS Release 11.3 command references.

## show snmp

To check the status of SNMP communications, use the **show snmp** EXEC command.

**show snmp**

### Syntax Description

This command has no arguments or keywords.

### Command Mode

EXEC

### Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

This command provides counter information for SNMP operations. It also displays the chassis ID string defined with the **snmp-server chassis-id** command.

### Sample Display

The following is sample output from the **show snmp** command:

```
Router# show snmp

Chassis: 01506199
37 SNMP packets input
  0 Bad SNMP version errors
  4 Unknown community name
  0 Illegal operation for community name supplied
  0 Encoding errors
  24 Number of requested variables
  0 Number of altered variables
  0 Get-request PDUs
  28 Get-next PDUs
  0 Set-request PDUs
78 SNMP packets output
  0 Too big errors (Maximum packet size 1500)
  0 No such name errors
  0 Bad values errors
  0 General errors
  24 Response PDUs
  13 Trap PDUs

SNMP logging: enabled
  Logging to 171.69.58.33.162, 0/10, 13 sent, 0 dropped.

SNMP Manager-role output packets
  4 Get-request PDUs
  4 Get-next PDUs
  6 Get-bulk PDUs
  4 Set-request PDUs
  23 Inform-request PDUs
  30 Timeouts
  0 Drops
SNMP Manager-role input packets
  0 Inform response PDUs
  2 Trap PDUs
  7 Response PDUs
```

1 Responses with errors

```
SNMP informs: enabled
Informs in flight 0/25 (current/max)
Logging to 171.69.217.141.162
    4 sent, 0 in-flight, 1 retries, 0 failed, 0 dropped
Logging to 171.69.58.33.162
    0 sent, 0 in-flight, 0 retries, 0 failed, 0 dropped
```

Table 1 describes the fields shown in the display.

**Table 1 Show SNMP Field Descriptions**

Field	Description
Chassis	Chassis ID string.
SNMP packets input	Total number of SNMP packets input.
Bad SNMP version errors	Number of packets with an invalid SNMP version.
Unknown community name	Number of SNMP packets with an unknown community name.
Illegal operation for community name supplied	Number of packets requesting an operation not allowed for that community.
Encoding errors	Number of SNMP packets that were improperly encoded.
Number of requested variables	Number of variables requested by SNMP managers.
Number of altered variables	Number of variables altered by SNMP managers.
Get-request PDUs	Number of get requests received.
Get-next PDUs	Number of get-next requests received.
Set-request PDUs	Number of set requests received.
SNMP packets output	Total number of SNMP packets sent by the router.
Too big errors	Number of SNMP packets that were larger than the maximum packet size.
Maximum packet size	Maximum size of SNMP packets.
No such name errors	Number of SNMP requests that specified a MIB object which does not exist.
Bad values errors	Number of SNMP set requests that specified an invalid value for a MIB object.
General errors	Number of SNMP set requests that failed due to some other error. (It was not a noSuchName error, badValue error, or any of the other specific errors.)
Response PDUs	Number of responses sent in reply to requests.
Trap PDUs	Number of SNMP traps sent.
SNMP logging	Indicates whether logging is enabled or disabled.
sent	Number of traps sent.
dropped	Number of traps dropped. Traps are dropped when the trap queue for a destination exceeds the maximum length of the queue, as set by the <b>snmp-server queue-length</b> command.
SNMP Manager-role output packets	Information related to packets sent by the router as an SNMP manager.
Get-request PDUs	Number of get requests sent.

**Table 1 Show SNMP Field Descriptions (Continued)**

<b>Field</b>	<b>Description</b>
Get-next PDUs	Number of get-next requests sent.
Get-bulk PDUs	Number of get-bulk requests sent.
Set-request PDUs	Number of set requests sent.
Inform-request PDUs	Number of inform requests sent.
Timeouts	Number of request timeouts.
Drops	Number of requests dropped. Reasons for drops include no memory, a bad destination address, or an unreasonable destination address.
SNMP Manager-role input packets	Information related to packets received by the router as an SNMP manager.
Inform response PDUs	Number of inform request responses received.
Trap PDUs	Number of SNMP traps received.
Response PDUs	Number of responses received.
Responses with errors	Number of responses containing errors.
SNMP informs	Indicates whether SNMP informs are enabled.
Informs in flight	Current and maximum possible number of informs waiting to be acknowledged.
Logging to	Destination of the following informs.
sent	Number of informs sent to this host.
in-flight	Number of informs currently waiting to be acknowledged.
retries	Number of inform retries sent.
failed	Number of informs that were never acknowledged.
dropped	Number of unacknowledged informs that were discarded to make room for new informs.

**Related Commands**

**show snmp pending**  
**show snmp sessions**  
**snmp-server chassis-id**  
**snmp-server manager**  
**snmp-server manager session-timeout**  
**snmp-server queue-length**

## show snmp pending

To display the current set of pending SNMP requests, use the **show snmp pending EXEC** command.

**show snmp pending**

### Syntax Description

This command has no arguments or keywords.

### Command Mode

EXEC

### Usage Guidelines

This command first appeared in Cisco IOS Release 11.3 T.

After the SNMP manager sends a request, the request is “pending” until the manager receives a response or the request timeout expires.

### Sample Display

The following is sample output from the **show snmp pending** command:

```
Router# show snmp pending

req id: 47, dest: 171.69.58.33.161, V2C community: public, Expires in 5 secs
req id: 49, dest: 171.69.58.33.161, V2C community: public, Expires in 6 secs
req id: 51, dest: 171.69.58.33.161, V2C community: public, Expires in 6 secs
req id: 53, dest: 171.69.58.33.161, V2C community: public, Expires in 8 secs
```

Table 2 describes the fields shown in the display.

**Table 2 Show SNMP Pending Field Descriptions**

Field	Description
req id	ID number of the pending request.
dest	IP address of the intended receiver of the request.
V2C Community	SNMP version 2C community string sent with the request.
Expires in	Remaining time before request timeout expires.

### Related Commands

**show snmp**  
**show snmp sessions**  
**snmp-server manager**  
**snmp-server manager session-timeout**

## show snmp sessions

To display the current SNMP sessions, use the **show snmp sessions EXEC** command.

```
show snmp sessions [brief]
```

### Syntax Description

*brief* (Optional) Display a list of sessions only. Do not display session statistics.

### Command Mode

EXEC

### Usage Guidelines

This command first appeared in Cisco IOS Release 11.3 T.

Sessions are created when the SNMP manager in the router sends SNMP requests, such as inform requests, to a host or receives SNMP notifications from a host. One session is created for each destination host. If there is no further communication between the router and host within the session timeout period, the corresponding session will be deleted.

### Sample Display

The following is sample output from the **show snmp sessions** command:

```
Router# show snmp sessions

Destination: 171.69.58.33.162, V2C community: public
Round-trip-times: 0/0/0 (min/max/last)
packets output
  0 Gets, 0 GetNexts, 0 GetBulks, 0 Sets, 4 Informs
  0 Timeouts, 0 Drops
packets input
  0 Traps, 0 Informs, 0 Responses (0 errors)
Destination: 171.69.217.141.162, V2C community: public, Expires in 575 secs
Round-trip-times: 1/1/1 (min/max/last)
packets output
  0 Gets, 0 GetNexts, 0 GetBulks, 0 Sets, 4 Informs
  0 Timeouts, 0 Drops
packets input
  0 Traps, 0 Informs, 4 Responses (0 errors)
```

The following is sample output from the **show snmp sessions brief** command:

```
Router# show snmp sessions brief

Destination: 171.69.58.33.161, V2C community: public, Expires in 55 secs
```

Table 3 describes the fields shown in these displays.

**Table 3 Show SNMP Sessions Field Descriptions**

<b>Field</b>	<b>Description</b>
Destination	IP address of the remote agent.
V2C community	SNMP version 2C community string used to communicate with the remote agent.
Expires in	Remaining time before the session timeout expires.
Round-trip-times	Minimum, maximum, and the last round trip time to the agent.
packets output	Packets sent by the router.
Gets	Number of get requests sent.
GetNexts	Number of get-next requests sent.
GetBulks	Number of get-bulk requests sent.
Sets	Number of set requests sent.
Informs	Number of inform requests sent.
Timeouts	Number of request timeouts.
Drops	Number of packets that could not be sent.
packets input	Packets received by the router.
Traps	Number of traps received.
Informs	Number of inform responses received.
Responses	Number of request responses received.
errors	Number of responses that contained an SNMP error code.

**Related Commands**

- show snmp**
- show snmp pending**
- snmp-server manager**
- snmp-server manager session-timeout**

## snmp-server manager

To start the SNMP manager process, use the **snmp-server manager** global configuration command. The **no** form of this command stops the SNMP manager process.

```
snmp-server manager  
no snmp-server manager
```

### Syntax Description

This command has no arguments or keywords.

### Default

Disabled

### Command Mode

Global configuration

### Usage Guidelines

This command first appeared in Cisco IOS Release 11.3 T.

The SNMP manager process sends SNMP requests to agents and receives SNMP responses and notifications from agents. When the SNMP manager process is enabled, the router can query other SNMP agents and process incoming SNMP traps.

Most network security policies assume that routers will be accepting SNMP requests, sending SNMP responses, and sending SNMP notifications. With the SNMP manager functionality enabled, the router may also be sending SNMP requests, receiving SNMP responses, and receiving SNMP notifications. The security policy implementation may need to be updated prior to enabling this functionality.

SNMP requests are typically sent to UDP port 161. SNMP responses are typically sent from UDP port 161. SNMP notifications are typically sent to UDP port 162.

### Example

The following example enables the SNMP manager process:

```
snmp-server manager
```

### Related Commands

```
show snmp  
show snmp pending  
show snmp sessions  
snmp-server manager session-timeout
```



# Debug Commands

This section documents new or modified **debug** commands. All other **debug** commands used with this feature are documented in the Cisco IOS Release 11.3 *Debug Command Reference*.

## debug snmp requests

To display information about every SNMP request made by the SNMP manager, use the **debug snmp requests EXEC** command. The **no** form of this command disables debugging output.

**[no] debug snmp requests**

### Sample Display

Figure 1 shows sample output from the **debug snmp requests** command.

**Figure 1 Sample Debug SNMP Requests Output**

```
Router# debug snmp requests

SNMP Manager API: request
  dest: 171.69.58.33.161, community: public
  retries: 3, timeout: 30, mult: 2, use session rtt
  userdata: 0x0
```

Table 4 describes the fields shown in the display.

**Table 4 Debug SNMP Requests Field Descriptions**

Field	Description
SNMP Manager API	Indicates that the router sent an SNMP request.
dest	Destination of the request.
community	Community string sent with the request.
retries	Number of times the request has been resent.
timeout	Request timeout, or how long the router will wait before resending the request.
mult	Timeout multiplier. The timeout for a resent request will be equal to the previous timeout multiplied by the timeout multiplier.
use session rtt	Indicates that the session's average round-trip time should be used in calculating the timeout value.
userdata	Internal IOS data.

### Related Command

**debug snmp sessions**

## debug snmp sessions

To display information when an SNMP session is created or destroyed, use the **debug snmp sessions** EXEC command. The **no** form of this command disables debugging output.

**[no] debug snmp sessions**

### Sample Display

Figure 2 shows sample output from the **debug snmp sessions** command. The first line of output indicates that a session was created with the host at 171.69.58.33.161 using the community string *public*; the second line indicates that the session was destroyed.

**Figure 2 Sample Debug SNMP Sessions Output**

```
Router# debug snmp sessions  
  
creating proxy session: dest=171.69.58.33.161, community=public  
destroying proxy session: dest=171.69.58.33.161, community=public
```

### Related Command

**debug snmp requests**