

# show snmp

To check the status of Simple Network Management Protocol (SNMP) communications, use the **show snmp** command in user EXEC or privileged EXEC mode.

**show snmp**

**Syntax Description** This command has no arguments or keywords.

**Command Modes** User EXEC (>  
Privileged EXEC (#)

| Command History | Release                  | Modification                                                                                                                                                                      |
|-----------------|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                 | 10.0                     | This command was introduced.                                                                                                                                                      |
|                 | 12.2(33)SRA              | This command was integrated into Cisco IOS Release 12.2(33)SRA.                                                                                                                   |
|                 | 12.2SX                   | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
|                 | Cisco IOS XE Release 2.1 | This command was integrated into Cisco IOS Release XE 2.1.                                                                                                                        |

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

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

```
Router# show snmp

Chassis: 12161083
0 SNMP packets input
  0 Bad SNMP version errors
  0 Unknown community name
  0 Illegal operation for community name supplied
  0 Encoding errors
  0 Number of requested variables
  0 Number of altered variables
  0 Get-request PDUs
  0 Get-next PDUs
  0 Set-request PDUs
  0 Input queue packet drops (Maximum queue size 1000)
0 SNMP packets output
  0 Too big errors (Maximum packet size 1500)
  0 No such name errors
  0 Bad values errors
  0 General errors
  0 Response PDUs
  0 Trap PDUs
```

```

SNMP logging: enabled
  SNMP Trap Queue: 0 dropped due to resource failure.
  Logging to 202.153.144.25.162, 0/10, 0 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 102 describes the significant fields shown in the display.

**Table 102** *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 which 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 that does not exist.      |
| Bad values errors                             | Number of SNMP set requests that specified an invalid value for a MIB object. |

**Table 102**      **show snmp Field Descriptions (continued)**

| Field                            | Description                                                                                                                                                                                           |
|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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> global configuration command. |
| SNMP Trap Queue                  | Number of traps that are getting dropped due to memory resource failure.                                                                                                                              |
| 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.                                                                                                                                                                          |
| 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**

| <b>Command</b>                             | <b>Description</b>                                                 |
|--------------------------------------------|--------------------------------------------------------------------|
| <b>show snmp pending</b>                   | Displays the current set of pending SNMP requests.                 |
| <b>show snmp sessions</b>                  | Displays the current SNMP sessions.                                |
| <b>snmp-server chassis-id</b>              | Provides a message line identifying the SNMP server serial number. |
| <b>snmp-server manager</b>                 | Starts the SNMP manager process.                                   |
| <b>snmp-server manager session-timeout</b> | Sets the amount of time before a nonactive session is destroyed.   |
| <b>snmp-server queue-length</b>            | Establishes the message queue length for each trap host.           |

# show snmp chassis

To display the Simple Network Management Protocol (SNMP) server serial number, use the **show snmp chassis** command in privileged EXEC mode.

**show snmp chassis**

**Syntax Description** This command has no arguments or keywords.

**Command Default** The system serial number will be displayed.

**Command Modes** Privileged EXEC (#)

| Command History | Release    | Modification                                                    |
|-----------------|------------|-----------------------------------------------------------------|
|                 | 12.4(12)T  | This command was introduced.                                    |
|                 | 12.2(31)SB | This command was integrated into Cisco IOS Release 12.2(31)SB2. |
|                 | 12.2SX     | This command was integrated into Cisco IOS Release 12.2SX.      |

**Usage Guidelines** To configure a message line identifying the SNMP server chassis ID, use the **snmp-server chassis-id** command.

**Examples** The following is sample output from the **show snmp chassis** command. The output is self-explanatory.

```
Router# show snmp chassis
01506199
```

| Related Commands | Command                       | Description                                                          |
|------------------|-------------------------------|----------------------------------------------------------------------|
|                  | <b>show snmp</b>              | Displays SNMP communication details.                                 |
|                  | <b>snmp-server chassis-id</b> | Configures a message line identifying the SNMP server serial number. |

# show snmp community

To display Simple Network Management Protocol (SNMP) community access strings, use the **show snmp community** command in privileged EXEC mode.

**show snmp community**

**Syntax Description** This command has no arguments or keywords.

**Command Default** All community access strings configured to enable access to SNMP entities are displayed.

**Command Modes** Privileged EXEC (#)

| Command History | Release    | Modification                                                    |
|-----------------|------------|-----------------------------------------------------------------|
|                 | 12.4(12)T  | This command was introduced.                                    |
|                 | 12.2(31)SB | This command was integrated into Cisco IOS Release 12.2(31)SB2. |
|                 | 12.2SX     | This command was integrated into Cisco IOS Release 12.2SX.      |

**Usage Guidelines** Community string consists of 1 to 32 alphanumeric characters and functions like a password enabling access to the SNMP entities.

To set up the community access string to permit access to the SNMP, use the **snmp-server community** command.

**Examples** The following is sample output from the **show snmp community** command. The output displays the community access strings configured for enabling access to an SNMP entity.

```
Router# show snmp community

Community name: ILMI
Community Index: ILMI
Community SecurityName: ILMI
storage-type: read-only active

Community name: private
Community Index: private
Community SecurityName: private
storage-type: nonvolatile active

Community name: private@1
Community Index: private@1
Community SecurityName: private
storage-type: read-only active

Community name: public
Community Index: public
```

```
Community SecurityName: public
storage-type: nonvolatile      active
```

[Table 103](#) describes the significant fields shown in the display.

**Table 103** *show snmp community Field Descriptions*

| Field                  | Description                                               |
|------------------------|-----------------------------------------------------------|
| Community name         | Displays the community name.                              |
| Community Index        | Displays the community index.                             |
| Community SecurityName | Displays the security name of the community string.       |
| storage-type           | Displays the access type stored for the community string. |

#### Related Commands

| Command                          | Description                                                     |
|----------------------------------|-----------------------------------------------------------------|
| <b>snmp-server<br/>community</b> | Sets up the community string to permit access to SNMP entities. |

# show snmp contact

To display Simple Network Management Protocol (SNMP) system contact information, use the **show snmp contact** command in privileged EXEC mode.

**show snmp contact**

---

**Syntax Description** This command has no arguments or keywords.

---

**Command Default** The SNMP system contact information is displayed.

---

**Command Modes** Privileged EXEC (#)

---

| Command History | Release    | Modification                                                    |
|-----------------|------------|-----------------------------------------------------------------|
|                 | 12.4(12)T  | This command was introduced.                                    |
|                 | 12.2(31)SB | This command was integrated into Cisco IOS Release 12.2(31)SB2. |
|                 | 12.2SX     | This command was integrated into Cisco IOS Release 12.2SX.      |

---

---

**Usage Guidelines** To set the system contact information, use the **snmp-server contact** command.

---

**Examples** The following is sample output from the **show snmp contact** command. The output is self-explanatory.

```
Router# show snmp contact  
  
Dial System Operator at beeper # 27345
```

---

| Related Commands | Command                    | Description                          |
|------------------|----------------------------|--------------------------------------|
|                  | <b>snmp-server contact</b> | Sets the system contact information. |

---

# show snmp engineID

To display the identification of the local Simple Network Management Protocol (SNMP) engine and all remote engines that have been configured on the router, use the **show snmp engineID** command in EXEC mode.

## show snmp engineID

**Syntax Description** This command has no arguments or keywords.

**Command Modes** EXEC

| Command History | Release     | Modification                                                                                                                                                                      |
|-----------------|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                 | 12.0(3)T    | This command was introduced.                                                                                                                                                      |
|                 | 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA.                                                                                                                   |
|                 | 12.2SX      | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

**Usage Guidelines** An SNMP engine is a copy of SNMP that can reside on a local or remote device.

**Examples** The following example specifies 00000009020000000C025808 as the local engineID and 123456789ABCDEF000000000 as the remote engine ID, 172.16.37.61 as the IP address of the remote engine (copy of SNMP) and 162 as the port from which the remote device is connected to the local device:

```
Router# show snmp engineID
```

```
Local SNMP engineID: 00000009020000000C025808
Remote Engine ID      IP-addr      Port
123456789ABCDEF000000000  172.16.37.61    162
```

Table 104 describes the fields shown in the display.

**Table 104** show snmp engineID Field Descriptions

| Field                | Definition                                                                   |
|----------------------|------------------------------------------------------------------------------|
| Local SNMP engine ID | A string that identifies the copy of SNMP on the local device.               |
| Remote Engine ID     | A string that identifies the copy of SNMP on the remote device.              |
| IP-addr              | The IP address of the remote device.                                         |
| Port                 | The port number on the local device to which the remote device is connected. |

| Related Commands | Command                           | Description                                                                 |
|------------------|-----------------------------------|-----------------------------------------------------------------------------|
|                  | <b>snmp-server engineID local</b> | Configures a name for either the local or remote SNMP engine on the router. |

# show snmp group

To display the names of configured SNMP groups, the security model being used, the status of the different views, and the storage type of each group, use the **show snmp group** command in privileged EXEC mode.

## show snmp group

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC

| Command History | Release     | Modification                                                                                                                                                                      |
|-----------------|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                 | 12.0(3)T    | This command was introduced.                                                                                                                                                      |
|                 | 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA.                                                                                                                   |
|                 | 12.2SX      | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

**Usage Guidelines** SNMP groups are configured using the `snmp-server group` command.

SNMP groups and users are used in the context of the View-based Access Control Model (VACM) for SNMP (for further information, see the “VACM for SNMP” IETF internet draft document).

**Examples** The following example specifies the group name as `public`, the security model as `v1`, the read view name as `vldefault`, the notify view name as `*tv.FFFFFFFFFF`, and the storage type as `volatile`:

Router# **show snmp group**

```

groupname: V1                                security model:v1
readview : vldefault                         writeview: <no writeview specified>
notifyview: <no notifyview specified>
row status: active

groupname: ILMI                              security model:v1
readview : *ilmi                             writeview: *ilmi
notifyview: <no notifyview specified>
row status: active

groupname: ILMI                              security model:v2c
readview : *ilmi                             writeview: *ilmi
notifyview: <no notifyview specified>
row status: active

groupname: group1                            security model:v1
readview : vldefault                         writeview: <no writeview specified>
notifyview: <no notifyview specified>
row status: active

```

Table 105 describes the fields shown in the example.

**Table 105** *show snmp group Field Descriptions*

| Field          | Definition                                                                                                                                                                                                                          |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| groupname      | The name of the SNMP group, or collection of users that have a common access policy.                                                                                                                                                |
| security model | The security model used by the group, either v1, v2c, or v3.                                                                                                                                                                        |
| readview       | A string identifying the read view of the group. <ul style="list-style-type: none"> <li>For further information on the SNMP views, use the <b>show snmp view</b> command.</li> </ul>                                                |
| writeview      | A string identifying the write view of the group.                                                                                                                                                                                   |
| notifyview     | A string identifying the notify view of the group.<br><br>The notify view indicates the group for SNMP notifications, and corresponds to the setting of the <b>snmp-server group group-name version notify notify-view</b> command. |

#### Related Commands

| Command                  | Description                                                                |
|--------------------------|----------------------------------------------------------------------------|
| <b>snmp-server group</b> | Configures a new SNMP group or a table that maps SNMP users to SNMP views. |
| <b>show snmp user</b>    | Displays the configured characteristics for SNMP users.                    |
| <b>show snmp view</b>    | Displays a list of configured SNMP views.                                  |

# show snmp host

To display the recipient details for Simple Network Management Protocol (SNMP) notification operations, use the **show snmp host** command in privileged EXEC mode.

## show snmp host

### Syntax Description

This command has no arguments or keywords.

### Command Default

The information configured for SNMP notification operation is displayed.

### Command Modes

Privileged EXEC (#)

### Command History

| Release    | Modification                                                    |
|------------|-----------------------------------------------------------------|
| 12.4(12)T  | This command was introduced.                                    |
| 12.2(31)SB | This command was integrated into Cisco IOS Release 12.2(31)SB2. |
| 12.2SX     | This command was integrated into Cisco IOS Release 12.2SX.      |

### Usage Guidelines

The **show snmp host** command displays details such as IP address of the Network Management System (NMS), notification type, SNMP version, and the port number of the NMS.

To configure these details, use the **snmp-server host** command.

### Examples

The following is sample output from the **show snmp host** command.

```
Router# show snmp host
```

```
Notification host: 10.2.28.6 udp-port: 162   type: inform
user: public      security model: v2c
traps: 00001000.00000000.00000000
```

[Table 106](#) describes the significant fields shown in the display.

**Table 106** *show snmp host Field Descriptions*

| Field             | Description                                                                   |
|-------------------|-------------------------------------------------------------------------------|
| Notification host | Displays the IP address of the host for which the notification is generated.  |
| udp-port          | Displays the port number.                                                     |
| type              | Displays the type of notification.                                            |
| user              | Displays the access type of the user for which the notification is generated. |

**Table 106**      *show snmp host Field Descriptions (continued)*

| Field          | Description                                           |
|----------------|-------------------------------------------------------|
| security model | Displays the SNMP version used to send notifications. |
| traps          | Displays details of the notification generated.       |

**Related Commands**

| Command                 | Description                                                        |
|-------------------------|--------------------------------------------------------------------|
| <b>snmp-server host</b> | Configures the recipient details for SNMP notification operations. |

# show snmp location

To display the Simple Network Management Protocol (SNMP) system location string, use the **show snmp location** command in privileged EXEC mode.

**show snmp location**

**Syntax Description** This command has no arguments or keywords.

**Command Default** The SNMP system location information is displayed.

**Command Modes** Privileged EXEC (#)

| Command History | Release    | Modification                                                    |
|-----------------|------------|-----------------------------------------------------------------|
|                 | 12.4(12)T  | This command was introduced.                                    |
|                 | 12.2(31)SB | This command was integrated into Cisco IOS Release 12.2(31)SB2. |
|                 | 12.2SX     | This command was integrated into Cisco IOS Release 12.2SX.      |

**Usage Guidelines** To configure system location details, use the **snmp-server location** command.

**Examples** The following is sample output from the **show snmp location** command. The output is self-explanatory.

```
Router# show snmp location
building 3/Room 214
```

| Related Commands | Command                     | Description                              |
|------------------|-----------------------------|------------------------------------------|
|                  | <b>snmp-server location</b> | Configures SNMP system location details. |

# show snmp mib

To display a list of the MIB module instance identifiers (OIDs) registered on your system, use the **show snmp mib** command in EXEC mode.

**show snmp mib**

**Syntax Description** This command has no arguments or keywords.

**Command Modes** EXEC

| Command History | Release     | Modification                                                                                                                                                                      |
|-----------------|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                 | 12.2(2)T    | This command was introduced.                                                                                                                                                      |
|                 | 12.2(28)SB  | This command was integrated into Cisco IOS Release 12.2(28)SB.                                                                                                                    |
|                 | 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA.                                                                                                                   |
|                 | 12.2SX      | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

**Usage Guidelines** SNMP management information is viewed as a collection of managed objects, residing in a virtual information store, termed the Management Information Base (MIB). Collections of related objects are defined in MIB modules. These modules are written using a subset of OSI's Abstract Syntax Notation One (ASN.1), termed the Structure of Management Information (SMI).

This command is intended for network administrators who are familiar with the SMI and ASN.1 syntax.

While this command can be used to display a list of MIB object identifiers (OIDs) registered on the system, the use of a network management system (NMS) application is the recommended alternative for gathering this information.

The **show snmp mib** command will display the instance identifiers for all the MIB objects on the system. The instance identifier is the final part of the OID. An object can have one or more instance identifiers. Before displaying the instance identifier, the system attempts to find the best match with the list of table names. The MIB module table names are registered when the system initializes.

The definitions for the OIDs displayed by this command can be found in the relevant RFCs and MIB modules. For example, RFC 1907 defines the system.x, sysOREntry.x, snmp.x, and snmpTrap.x OIDs, and this information is supplemented by the extensions defined in the CISCO-SYSTEM-MIB.



**Tip**

This command produces a high volume of output if SNMP is enabled on your system. To exit from a --More-- prompt, press Ctrl-Z.

## Examples

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

```
Router# show snmp mib
```

```
system.1
system.2
sysUpTime
system.4
system.5
system.6
system.7
system.8
sysOREntry.2
sysOREntry.3
sysOREntry.4
interfaces.1
ifEntry.1
ifEntry.2
ifEntry.3
ifEntry.4
ifEntry.5
ifEntry.6
ifEntry.7
ifEntry.8
ifEntry.9
ifEntry.10
ifEntry.11
--More--
.
.
.
captureBufferEntry.2
captureBufferEntry.3
captureBufferEntry.4
captureBufferEntry.5
captureBufferEntry.6
captureBufferEntry.7
capture.3.1.1
eventEntry.1
eventEntry.2
eventEntry.3
eventEntry.4
eventEntry.5
eventEntry.6
eventEntry.7
logEntry.1
logEntry.2
logEntry.3
logEntry.4
rmon.10.1.1.2
rmon.10.1.1.3
rmon.10.1.1.4
rmon.10.1.1.5
rmon.10.1.1.6
rmon.10.1.1.7
rmon.10.2.1.2
rmon.10.2.1.3
rmon.10.3.1.2
--More--
.
.
.
rmon.192.168.1.1
rmon.192.168.1.2
```

```

rmon.192.168.1.3
rmon.192.168.1.2
rmon.192.168.1.3
rmon.192.168.1.4
rmon.192.168.1.5
rmon.192.168.1.6
rmon.192.168.1.2
rmon.192.168.1.3
rmon.192.168.1.4
rmon.192.168.1.5
rmon.192.168.1.6
rmon.192.168.1.7
rmon.192.168.1.8
rmon.192.168.1.9
dot1dBase.1
dot1dBase.2
dot1dBase.3
dot1dBasePortEntry.1
dot1dBasePortEntry.2
dot1dBasePortEntry.3
dot1dBasePortEntry.4
--More--
.
.
.
ifXEntry.1
ifXEntry.2
ifXEntry.3
ifXEntry.4
ifXEntry.5
ifXEntry.6
ifXEntry.7
ifXEntry.8
ifXEntry.9
ifXEntry.10
ifXEntry.11
ifXEntry.12
ifXEntry.13
ifXEntry.14
ifXEntry.15
ifXEntry.16
ifXEntry.17
ifXEntry.18
ifXEntry.19
ifStackEntry.3
ifTestEntry.1
ifTestEntry.2
--More--
.
.
.

```

## Related Commands

| Command                            | Description                                                                                                                           |
|------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| <b>show snmp mib ifmib ifindex</b> | Displays SNMP Interface Index identification numbers (ifIndex values) for all the system interfaces or the specified system interface |

# show snmp mib bulkstat transfer

To display the transfer status of files generated by the Periodic MIB Data Collection and Transfer Mechanism (Bulk Statistics feature), use the **show snmp mib bulkstat transfer** command in privileged EXEC mode.

**show snmp mib bulkstat transfer** [*transfer-id*]

|                           |                    |                                                                                                                                                                                          |
|---------------------------|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <i>transfer-id</i> | (Optional) Name of a specific bulk statistics transfer configuration.<br>Use the <i>transfer-id</i> argument to display the status of a specific bulk statistics transfer configuration. |
|---------------------------|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                        |                                                                                                                               |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| <b>Command Default</b> | If the optional <i>transfer-id</i> argument is not used, the status of all configured bulk statistics transfers is displayed. |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------|

|                      |                     |
|----------------------|---------------------|
| <b>Command Modes</b> | Privileged EXEC (#) |
|----------------------|---------------------|

| Command History | Release                  | Modification                                                    |
|-----------------|--------------------------|-----------------------------------------------------------------|
|                 | 12.0(24)S                | This command was introduced.                                    |
|                 | 12.3(2)T                 | This command was integrated into Cisco IOS Release 12.3(2)T.    |
|                 | 12.2(25)S                | This command was integrated into Cisco IOS Release 12.2(25)S.   |
|                 | 12.2(33)SRA              | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
|                 | 12.2(33)SXH              | This command was integrated into Cisco IOS Release 12.2(33)SXH. |
|                 | 12.2(33)SB               | This command was integrated into Cisco IOS Release 12.2(33)SB.  |
|                 | Cisco IOS XE Release 2.1 | This command was integrated into Cisco IOS Release XE 2.1.      |

**Examples**

In the following example, the initial transfer attempt and the first retry for the file IfMIB\_objects\_Router\_030307\_102519739 to the primary and secondary URL have failed, and four additional retry attempts will be made. The time stamp for this file indicates the file was created on March 7, 2003, at 10:25:19 a.m.

```
Router# show snmp mib bulkstat transfer
```

```
Transfer Name : IfMIB_objects
```

```
Primary URL ftp://user:XXXXXXXX@192.168.1.229/
```

```
Secondary URL ftp://user:XXXXXXXX@192.168.1.230/
```

```
Retained files
```

```
File Name                               :Time Left (in seconds)      : STATE
-----
IfMIB_objects_Router_030307_102519739 : 1196      :Retry(5 Retry attempt(s) Left)
IfMIB_objects_Router_030307_102219739 : 1016      :Retained
```

```

IfMIB_objects_Router_030307_101919739 : 836 :Retained
IfMIB_objects_Router_030307_101619739 : 656 :Retained
IfMIB_objects_Router_030307_101319739 : 475 :Retained
IfMIB_objects_Router_030307_101119739 : 295 :Retained

```

Table 107 describes the significant fields shown in the output.

**Table 107** *show snmp mib bulkstat transfer Field Descriptions*

| Field                  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Transfer Name          | The name of the transfer configuration, specified in the <b>snmp mib bulkstat transfer</b> global configuration command.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Retained files         | Indicates that the following output shows the status of files that are in system memory (retained), as opposed to files that have already been set.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| File Name              | <p>The name of the bulk statistics file as it will appear after transfer. The filename of the file is generated using the following components:</p> <p><i>transfer-name_device-name_date_time-stamp</i></p> <p>The <i>transfer-name</i> is the name specified by the corresponding <b>snmp mib bulkstat transfer</b> command. The <i>device-name</i> is the name used in the command-line interface (CLI) router prompt. The format of the <i>date</i> and <i>time-stamp</i> depends on your system configuration, but is typically YYMMDD and HHMMSSmmm, where HH is hour, MM is minutes, SS is seconds and mmm is milliseconds.</p>                                                   |
| Time Left (in seconds) | <p>Indicates how much time is left before the specified file will be deleted (retention period), as specified with the <b>retain</b> Bulk Statistics Transfer configuration command.</p> <p><b>Note</b> Regardless of the configured retention period, all retry attempts will be made before the file is deleted.</p>                                                                                                                                                                                                                                                                                                                                                                  |
| STATE                  | <p>The state of the local bulk statistics file will be one of the following:</p> <ul style="list-style-type: none"> <li>Queued—Collection time for this file is completed and the file is waiting for transfer to configured primary and secondary URL.</li> <li>Retained—The file has been either successfully transferred to its destination or, if all transfer attempts have failed, all retry attempts have been completed.</li> <li>Retry—The local bulk statistics file will be in this state if an attempt to transfer it to its configured destination fails and one or more retries are pending. The number of retries left will also be displayed in parenthesis.</li> </ul> |

#### Related Commands

| Command                           | Description                                                                                            |
|-----------------------------------|--------------------------------------------------------------------------------------------------------|
| <b>snmp mib bulkstat transfer</b> | Names a bulk statistics transfer configuration and enters Bulk Statistics Transfer configuration mode. |

# show snmp mib context

To display Virtual Private Network (VPN)-aware MIBs, use the **show snmp mib context** command in privileged EXEC mode.

## show snmp mib context

**Syntax Description** This command has no arguments or keywords.

**Command Default** The list of VPN-aware MIBs is displayed.

**Command Modes** Privileged EXEC (#)

| Command History | Release     | Modification                                                    |
|-----------------|-------------|-----------------------------------------------------------------|
|                 | 12.4(15)T   | This command was introduced.                                    |
|                 | 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |
|                 |             |                                                                 |

**Usage Guidelines** Simple Network Management Protocol (SNMP) contexts provide VPN users with a secure way of accessing MIB data. When a VPN is mapped to a context, the data specific to that VPN exists in that context. Associating a VPN with a context enables service providers to manage networks with multiple VPNs. Creating and associating a context with a VPN enables a provider to prevent the users of one VPN from accessing information about users of other VPNs on the same networking device.

To configure SNMP contexts, use the **snmp-server context** command.

**Examples** The following is sample output from the **show snmp mib context** command. The example lists the MIBs that are VPN-aware. The output is self-explanatory.

```
Router# show snmp mib context
```

```
dot1dBridge
ciscoPingMIB
ciscoStpExtensionsMIB
ciscoIpSecFlowMonitorMIB
ciscoCat6kCrossbarMIB
ciscoIPsecMIB
mplsLdpMIB
```

| Related Commands | Command                    | Description                                       |
|------------------|----------------------------|---------------------------------------------------|
|                  | <b>context</b>             | Associates an SNMP context with a particular VRF. |
|                  | <b>snmp-server context</b> | Configures SNMP context.                          |

# show snmp mib ifmib traps

To display Simple Network Management Protocol (SNMP) linkUp and linkDown trap status for all system interfaces or a specified system interface, use the **show snmp mib ifmib traps** command in privileged EXEC mode.

## show snmp mib ifmib traps

**Syntax Description** This command has no arguments or keywords.

**Command Default** By default, trap status for all interfaces is displayed.

**Command Modes** Privileged EXEC (#)

### Command History

| Release                     | Modification                                                    |
|-----------------------------|-----------------------------------------------------------------|
| 12.2(33)SXI                 | This command was introduced.                                    |
| 12.2(33)SRE                 | This command was integrated into Cisco IOS Release 12.2(33)SRE. |
| Cisco IOS XE Release 3.1.0S | This command was integrated into Cisco IOS XE Release 3.1.0S.   |

### Usage Guidelines

The **show snmp mib ifmib traps** command allows you to use the command-line interface (CLI) to display information about the status of linkUp and linkDown traps for a particular interface.

### Examples

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

```
Router# show snmp mib ifmib traps
```

```
ifDescr              ifindex  TrapStatus
-----
FastEthernet3/6      14       enabled
FastEthernet3/19     27       enabled
GigabitEthernet5/1   57       enabled
unrouted VLAN 1005   73       disabled
FastEthernet3/4      12       enabled
FastEthernet3/39     47       enabled
FastEthernet3/28     36       enabled
FastEthernet3/48     56       enabled
unrouted VLAN 1003   74       disabled
FastEthernet3/2      10       enabled
Tunnel0              66       enabled
SPAN RP Interface    64       disabled
Tunnel10             67       enabled
FastEthernet3/44     52       enabled
GigabitEthernet1/3   3        enabled
FastEthernet3/11     19       enabled
FastEthernet3/46     54       enabled
```

```
GigabitEthernet1/1      1      enabled
FastEthernet3/13       21     enabled
```

Table 108 describes the fields shown in the display.

**Table 108** *show snmp mib ifmib traps Field Descriptions*

| Field      | Description                                                                                    |
|------------|------------------------------------------------------------------------------------------------|
| ifDescr    | Displays system interfaces configured for the device.                                          |
| ifindex    | Displays the interface index (ifIndex) identification numbers.                                 |
| TrapStatus | Displays the status of linkUp and linkDown traps for all interfaces configured for the device. |

#### Related Commands

| Command                            | Description                                                                                             |
|------------------------------------|---------------------------------------------------------------------------------------------------------|
| <b>show snmp mib</b>               | Displays a list of the MIB OIDs registered on the system.                                               |
| <b>show snmp mib ifmib ifindex</b> | Displays SNMP ifIndex identification numbers for all system interfaces or a specified system interface. |
| <b>snmp-server enable traps</b>    | Enables all SNMP notification types available on your system.                                           |

# show snmp mib ifmib ifindex

To display Simple Network Management Protocol (SNMP) Interface Index (ifIndex) identification numbers for all system interfaces or a specified system interface, use the **show snmp mib ifmib ifindex** command in privileged EXEC mode.

**show snmp mib ifmib ifindex** [*type number*] [**detail**] [**free-list**]

|                           |                    |                                                                                                                       |
|---------------------------|--------------------|-----------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <i>type number</i> | (Optional) Interface type and number. <a href="#">Table 109</a> lists the valid values for interface type and number. |
|                           | <b>detail</b>      | (Optional) Displays the trap status for all SNMP ifIndex identification numbers for the specified system interfaces.  |
|                           | <b>free-list</b>   | (Optional) Displays information about the ifIndex values that are not yet assigned.                                   |

**Command Default** The ifIndex values for all interfaces are displayed.

**Command Modes** Privileged EXEC (#)

| <b>Command History</b> | <b>Release</b> | <b>Modification</b>                                                   |
|------------------------|----------------|-----------------------------------------------------------------------|
|                        | 12.2(2)T       | This command was introduced.                                          |
|                        | 12.2(18)SXD    | Support for this command was introduced on the Supervisor Engine 720. |
|                        | 12.2(28)SB     | This command was integrated into Cisco IOS Release 12.2(28)SB.        |
|                        | 12.2(33)SXH    | The <b>detail</b> and <b>free-list</b> keywords were added.           |

**Usage Guidelines** The **show snmp mib ifmib ifindex** command allows you to use the command-line interface (CLI) to display SNMP ifIndex values assigned to interfaces and subinterfaces. By using the CLI, a network management station is not needed.

If an interface is not specified using the optional *type* and *number* arguments, the interface description (ifDescr) and ifIndex pairs of all interfaces and subinterfaces present on the system are shown.

[Table 109](#) shows the valid values for the *type* and *number* arguments.

**Table 109** *show snmp mib ifmib ifindex type and number*

| ifIndex Type         | Description                                                    |
|----------------------|----------------------------------------------------------------|
| <b>atm</b>           | Asynchronous transfer mode interface; <i>number</i> is 0 to 7. |
| <b>async</b>         | Asynchronous interface; <i>number</i> will vary by platform.   |
| <b>auto-template</b> | Auto-Template interface; <i>number</i> is 1 to 999.            |
| <b>ctunnel</b>       | CTunnel interface; <i>number</i> is 0 to 2147483647.           |
| <b>dialer</b>        | Dialer interface; <i>number</i> is 0 to 255.                   |
| <b>esconphy</b>      | Escon interface; <i>number</i> is 1 to 6.                      |

**Table 109**      *show snmp mib ifmib ifindex type and number*

| <b>ifIndex Type</b>      | <b>Description</b>                                                         |
|--------------------------|----------------------------------------------------------------------------|
| <b>ethernet</b>          | Ethernet interface; <i>number</i> is 0 to 15.                              |
| <b>fastethernet</b>      | Fast Ethernet interface; <i>number</i> is 1 to 6.                          |
| <b>fcpa</b>              | Fibre Channel Port Adapter interface; <i>number</i> is 1 to 6.             |
| <b>filter</b>            | Filter interface; <i>number</i> is 1 to 6.                                 |
| <b>filtergroup</b>       | Filter Group interface; <i>number</i> is 1 to 6.                           |
| <b>gigabitethernet</b>   | Gigabit Ethernet interface; <i>number</i> is 1 to 6.                       |
| <b>group-async</b>       | Asynchronous Group interface; <i>number</i> is 0 to 64.                    |
| <b>lex</b>               | Lex interface; <i>number</i> is 0 to 2147483647.                           |
| <b>longreachethernet</b> | Long-Reach Ethernet interface; <i>number</i> is 1 to 6.                    |
| <b>loopback</b>          | Loopback interface; <i>number</i> is 0 to 2147483647.                      |
| <b>mfr</b>               | Multilink Frame Relay bundle interface; <i>number</i> is 0 to 2147483647.  |
| <b>multilink</b>         | Multilink-group interface; <i>number</i> is 1 to 2147483647.               |
| <b>null</b>              | Null interface; <i>number</i> is 0 to 0.                                   |
| <b>port-channel</b>      | Port-Channel interface; <i>number</i> is 1 to 496.                         |
| <b>portgroup</b>         | Portgroup interface; <i>number</i> is 1 to 6.                              |
| <b>pos-channel</b>       | POS Channel interface; <i>number</i> is 1 to 4094.                         |
| <b>serial</b>            | Serial interface; <i>number</i> is 0 to 15.                                |
| <b>sysclock</b>          | SYSCLOCK interface; <i>number</i> is 1 to 6.                               |
| <b>tunnel</b>            | Tunnel interface; <i>number</i> is 0 to 2147483647.                        |
| <b>vif</b>               | Pragmatic General Multicast (PGM) Host interface; <i>number</i> is 0 to 1. |
| <b>virtual-ppp</b>       | Virtual Point-to-Point interface; <i>number</i> is 1 to 2147483647.        |
| <b>virtual-template</b>  | Virtual Template interface; <i>number</i> is 1 to 200.                     |
| <b>virtual-tokenring</b> | Virtual Token Ring interface; <i>number</i> is 0 to 2147483647.            |
| <b>vlan</b>              | VLAN interface; <i>number</i> is 1 to 4094.                                |
| <b>voabypassin</b>       | VOA-Bypass-In interface; <i>number</i> is 1 to 6.                          |
| <b>voabypassout</b>      | VOA-Bypass-Out interface; <i>number</i> is 1 to 6.                         |
| <b>voafilterin</b>       | VOA-Filter-In interface; <i>number</i> is 1 to 6.                          |
| <b>voafilterout</b>      | VOA-Filter-Out interface; <i>number</i> is 1 to 6.                         |
| <b>voain</b>             | VOA-In interface; <i>number</i> is 1 to 6.                                 |
| <b>voaout</b>            | VOA-Out interface; <i>number</i> is 1 to 6.                                |

The **show snmp mib ifmib ifindex** command when used with the **detail** keyword displays the details of trap status for all ifIndex values. It displays the list of unassigned ifIndexes when used with the **free-list** keyword.

## Examples

The following example shows sample output for Ethernet interface 2/0:

```
Router# show snmp mib ifmib ifindex Ethernet2/0
```

```
Ethernet2/0: Ifindex = 2
```

The following example shows sample output for all interfaces (no optional arguments are specified):

```
Router# show snmp mib ifmib ifindex
```

```
ATM1/0: Ifindex = 1
ATM1/0-aal5 layer: Ifindex = 12
ATM1/0-atm layer: Ifindex = 10
ATM1/0.0-aal5 layer: Ifindex = 13
ATM1/0.0-atm subif: Ifindex = 11
ATM1/0.9-aal5 layer: Ifindex = 32
ATM1/0.9-atm subif: Ifindex = 31
ATM1/0.99-aal5 layer: Ifindex = 36
ATM1/0.99-atm subif: Ifindex = 35
Ethernet2/0: Ifindex = 2
Ethernet2/1: Ifindex = 3
Ethernet2/2: Ifindex = 4
Ethernet2/3: Ifindex = 5
Null0: Ifindex = 14
Serial3/0: Ifindex = 6
Serial3/1: Ifindex = 7
Serial3/2: Ifindex = 8
Serial3/3: Ifindex = 9
```

Each line of output indicates the system interface followed by the ifIndex identification number.

The following example shows sample output for the ifIndex trap status details:

```
Router# show snmp mib ifmib ifindex detail
```

| Description        | ifIndex | Active | Persistent | Saved | TrapStatus |
|--------------------|---------|--------|------------|-------|------------|
| FastEthernet3/6    | 14      | yes    | disabled   | no    | enabled    |
| FastEthernet3/19   | 27      | yes    | disabled   | no    | enabled    |
| GigabitEthernet5/1 | 57      | yes    | disabled   | no    | enabled    |
| unrouted VLAN 1005 | 73      | yes    | disabled   | no    | disabled   |
| FastEthernet3/4    | 12      | yes    | disabled   | no    | enabled    |
| FastEthernet3/39   | 47      | yes    | disabled   | no    | enabled    |
| FastEthernet3/28   | 36      | yes    | disabled   | no    | enabled    |
| FastEthernet3/48   | 56      | yes    | disabled   | no    | enabled    |
| unrouted VLAN 1003 | 74      | yes    | disabled   | no    | disabled   |
| FastEthernet3/2    | 10      | yes    | disabled   | no    | enabled    |
| Tunnel0            | 66      | yes    | disabled   | no    | enabled    |
| SPAN RP Interface  | 64      | yes    | disabled   | no    | disabled   |
| Tunnel10           | 67      | yes    | disabled   | no    | enabled    |

Table 110 describes the fields shown in the display.

**Table 110** *show snmp mib ifmib ifindex Field Descriptions*

| Field       | Description                                                                                                                               |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| Description | Displays system interfaces configured for the device.                                                                                     |
| ifIndex     | Displays the ifIndex identification numbers.                                                                                              |
| Active      | Indicates if an interface is active.                                                                                                      |
| Persistent  | Indicates if the interface is persistent across reloads, that is, if it retains the same index values each time a network device reboots. |
| Saved       | Indicates if the ifIndex value for an interface is saved.                                                                                 |
| TrapStatus  | Displays the trap status for all ifIndex values.                                                                                          |

The following example shows sample output for unassigned ifIndexes:

```
Router# show snmp mib ifmib ifindex free-list
```

```
ifIndex range
-----
 75 - 2147483647
-----
Total free ifIndex : 2147483573
```

The output indicates the range and total number of unassigned ifIndexes.

#### Related Commands

| Command                            | Description                                                                                     |
|------------------------------------|-------------------------------------------------------------------------------------------------|
| <b>show snmp mib</b>               | Displays a list of the MIB OIDs registered on the system.                                       |
| <b>snmp ifindex persist</b>        | Enables ifIndex values in the IF-MIB that persist across reboots only on a specific interface.  |
| <b>snmp ifmib ifalias long</b>     | Configures the system to handle IfAlias descriptions of up to 256 characters in length.         |
| <b>snmp-server ifindex persist</b> | Enables ifIndex values in the IF-MIB that persist across reboots for all interfaces (globally). |

# show snmp mib notification-log

To display information about the state of local SNMP notification logging, use the **show snmp mib notification-log** command in EXEC mode.

**show snmp mib notification-log** [**all** | **default**]

| Syntax Description | <b>all</b>     | (Optional) Displays all notification log entries stored in the local Notification Log MIB database. |
|--------------------|----------------|-----------------------------------------------------------------------------------------------------|
|                    | <b>default</b> | (Optional) Displays summary information for the default (unnamed) SNMP Notification Log.            |

| Command Modes | EXEC |
|---------------|------|
|---------------|------|

| Command History | Release   | Modification                                        |
|-----------------|-----------|-----------------------------------------------------|
|                 | 12.0(22)S | This command was introduced.                        |
|                 | 12.2(13)T | This command was integrated into Release 12.2(13)T. |

**Usage Guidelines**

The SNMP Notification Log works in conjunction with the NOTIFICATION-LOG-MIB.my MIB module (available at <ftp://ftp.cisco.com/pub/mibs/v2/>). This MIB module is based on RFC 3014. The local logs can be polled by external network management applications to verify that they have not missed important SNMP notifications (traps and informs).

The **show snmp mib notification-log all** command displays all logged notification entries currently in the local MIB database. Entries are displayed from the oldest to the newest. The time of entry creation is determined using the system-up-time (sysUpTime) value; this means that the age of the entry is set using the amount of time that has passed since the router was last restarted. Other information for the entries includes the notificationID, and the filters (varbinds) associated with the log, if any.

**Examples**

The following is sample output from the **show snmp mib notification-log** command:

```
Router# show snmp mib notification-log

GlobalAgeout 15, GlobalEntryLimit 500
Total Notifications logged in all logs 0
Log Name "", Log entry Limit 500, Notifications logged 0
Logging status enabled
Created by cli
```

Note that in this example, the Log Name of "" indicates the default "null-named" Notification Log.

| Related Commands | Command                                  | Description                                     |
|------------------|------------------------------------------|-------------------------------------------------|
|                  | <b>snmp mib notification-log default</b> | Creates and activates an SNMP Notification Log. |

| Command                                       | Description                                                   |
|-----------------------------------------------|---------------------------------------------------------------|
| <b>snmp mib notification-log globalageout</b> | Sets the maximum age for a notification.                      |
| <b>snmp mib notification-log globalsize</b>   | Sets the maximum number of notifications allowed in all logs. |

# show snmp pending

To display the current set of pending Simple Network Management Protocol (SNMP) requests, use the **show snmp pending** command in user EXEC or privileged EXEC mode.

**show snmp pending**

---

**Syntax Description** This command has no arguments or keywords.

---

**Command Modes** User EXEC (>)  
Privileged EXEC (#)

---

| Command History | Release                  | Modification                                                                                                                                                                      |
|-----------------|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                 | 11.3T                    | This command was introduced.                                                                                                                                                      |
|                 | 12.2(33)SRA              | This command was integrated into Cisco IOS Release 12.2(33)SRA.                                                                                                                   |
|                 | 12.2SX                   | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
|                 | Cisco IOS XE Release 2.1 | This command was integrated into Cisco IOS Release XE 2.1.                                                                                                                        |

---

---

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

---

**Examples** 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 111](#) describes the significant fields shown in the display.

**Table 111** *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**

| Command                                    | Description                                                      |
|--------------------------------------------|------------------------------------------------------------------|
| <b>show snmp</b>                           | Checks the status of SNMP communications.                        |
| <b>show snmp sessions</b>                  | Displays the current SNMP sessions.                              |
| <b>snmp-server manager</b>                 | Starts the SNMP manager process.                                 |
| <b>snmp-server manager session-timeout</b> | Sets the amount of time before a nonactive session is destroyed. |

# show snmp sessions

To display the current Simple Network Management Protocol (SNMP) sessions, use the **show snmp sessions** command in user EXEC or privileged EXEC mode.

**show snmp sessions [brief]**

## Syntax Description

**brief** (Optional) Displays a list of sessions only. Does not display session statistics.

## Command Modes

User EXEC (>)  
Privileged EXEC (#)

## Command History

| Release                  | Modification                                                                                                                                                                      |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 11.3T                    | This command was introduced.                                                                                                                                                      |
| 12.2(33)SRA              | This command was integrated into Cisco IOS Release 12.2(33)SRA.                                                                                                                   |
| 12.2SX                   | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| Cisco IOS XE Release 2.1 | This command was integrated into Cisco IOS Release XE 2.1.                                                                                                                        |

## Usage Guidelines

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.

## Examples

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)
```

[Table 112](#) describes the significant fields shown in the output.

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 112** *show snmp sessions Field Descriptions*

| Field            | Description                                                                 |
|------------------|-----------------------------------------------------------------------------|
| 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

| Command                                    | Description                                                      |
|--------------------------------------------|------------------------------------------------------------------|
| <b>show snmp</b>                           | Checks the status of SNMP communications.                        |
| <b>show snmp pending</b>                   | Displays the current set of pending SNMP requests.               |
| <b>snmp-server manager</b>                 | Starts the SNMP manager process.                                 |
| <b>snmp-server manager session-timeout</b> | Sets the amount of time before a nonactive session is destroyed. |

# show snmp stats oid

To display all object identifiers (OIDs) recently requested by a network management system (NMS), their time stamps, and the number of times they were requested, use the **show snmp stats oid** command in privileged EXEC mode.

**show snmp stats oid**

**Syntax Description** This command has no arguments or keywords.

**Command Default** Simple Network Management Protocol (SNMP) statistics for all OIDs are shown.

**Command Modes** Privileged EXEC (#)

| Command History | Release                   | Modification                                                    |
|-----------------|---------------------------|-----------------------------------------------------------------|
|                 | 12.0(22)S                 | This command was introduced.                                    |
|                 | 12.4(20)T                 | This command was integrated into Cisco IOS Release 12.4(20)T.   |
|                 | 12.2(33)SRE               | This command was integrated into Cisco IOS Release 12.2(33)SRE. |
|                 | Cisco IOS XE Release 3.1S | This command was integrated into Cisco IOS XE Release 3.1S.     |

**Usage Guidelines** Before running the **show snmp stats oid** command, connect the device to the NMS. The command output displays the list of object identifiers (OIDs) recently requested by the NMS. It also displays the number of times an object identifier is requested by the NMS.

This information is useful for troubleshooting memory leaks and network failures when little information is available about MIBs that the NMS is querying. You can use this command at any time to view OIDs recently requested by the NMS.

**Examples** The following is sample output from a **show snmp stats oid** command:

Router# **show snmp stats oid**

| time-stamp              | #of times requested | OID                    |
|-------------------------|---------------------|------------------------|
| 02:58:00 UTC Jul 7 2008 | 159                 | cpmProcessExtTable.1.3 |
| 02:58:00 UTC Jul 7 2008 | 207                 | cpmProcessExtTable.1.1 |
| 02:57:59 UTC Jul 7 2008 | 207                 | cpmProcessExtTable.1.1 |
| 02:57:59 UTC Jul 7 2008 | 207                 | cpmProcessTable.1.6    |
| 02:57:59 UTC Jul 7 2008 | 207                 | cpmProcessTable.1.5    |
| 02:57:59 UTC Jul 7 2008 | 207                 | cpmProcessTable.1.4    |
| 02:57:57 UTC Jul 7 2008 | 207                 | cpmProcessTable.1.2    |
| 02:57:57 UTC Jul 7 2008 | 207                 | cpmProcessTable.1.1    |
| 02:57:57 UTC Jul 7 2008 | 1                   | cpmCPUTotalTable.1.11  |
| 02:57:57 UTC Jul 7 2008 | 1                   | cpmCPUTotalTable.1.10  |
| 02:57:57 UTC Jul 7 2008 | 1                   | cpmCPUTotalTable.1.9   |
| 02:57:57 UTC Jul 7 2008 | 1                   | cpmCPUTotalTable.1.8   |

Table 113 describes the significant fields shown in the display.

**Table 113** *show snmp stats oid Field Descriptions*

| Field               | Description                                                                      |
|---------------------|----------------------------------------------------------------------------------|
| time-stamp          | Displays the time and date when the object identifiers are requested by the NMS. |
| #of times requested | Displays the number of times an object identifier is requested.                  |
| OID                 | Displays the object identifiers recently requested by the NMS.                   |

# show snmp sysobjectid

To identify a Simple Network Management Protocol (SNMP) device, use the **show snmp sysobjectid** command in privileged EXEC mode.

**show snmp sysobjectid**

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC

| Command History | Release  | Modification                 |
|-----------------|----------|------------------------------|
|                 | 12.4(10) | This command was introduced. |

**Usage Guidelines** Using the **show snmp sysobjectid** command is a quick way to identify a device. The same information can be obtained by issuing an SNMP query on the MIB object sysObjectID. Output from the command shows the system object ID in dotted decimal format. The system object ID is the identifier of the network management subsystem, which is SNMP, and is typically the starting point at which network management applications try to discover a device.

**Examples** The following example shows the **show snmp sysobjectid** command and sample output. In this example, the object ID translates to iso.org.dod.internet.private.enterprises.cisco.ciscoProducts.ciscoGatewayServer.

```
Router# show snmp sysobjectid
1.3.6.1.4.1.9.1.1
```

| Related Commands | Command                   | Description                                                                                                                                         |
|------------------|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
|                  | <b>show snmp</b>          | Displays the status of SNMP communications.                                                                                                         |
|                  | <b>show snmp engineID</b> | Displays the identification of the local SNMP engine and all remote engines that have been configured on the router.                                |
|                  | <b>show snmp group</b>    | Displays the names of configured SNMP groups, the security model being used, the status of the different views, and the storage type of each group. |
|                  | <b>show snmp mib</b>      | Displays a list of the MIB module instance identifiers (OIDs) registered on your system.                                                            |
|                  | <b>show snmp pending</b>  | Displays the current set of pending SNMP requests.                                                                                                  |

| Command                   | Description                                                                                    |
|---------------------------|------------------------------------------------------------------------------------------------|
| <b>show snmp sessions</b> | Displays the current SNMP sessions.                                                            |
| <b>show snmp user</b>     | Displays information about the configured characteristics of SNMP users.                       |
| <b>show snmp view</b>     | Displays the family name, storage type, and status of a SNMP configuration and associated MIB. |

# show snmp user

To display information about the configured characteristics of Simple Network Management Protocol (SNMP) users, use the **show snmp user** command in privileged EXEC mode.

**show snmp user** [*username*]

## Syntax Description

|                 |                                                                                      |
|-----------------|--------------------------------------------------------------------------------------|
| <i>username</i> | (Optional) Name of a specific user or users about which to display SNMP information. |
|-----------------|--------------------------------------------------------------------------------------|

## Command Modes

Privileged EXEC (#)

## Command History

| Release     | Modification                                                                                                                                                                      |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 12.0(3)T    | This command was introduced.                                                                                                                                                      |
| 12.3(2)T    | The <i>username</i> argument was added. The output for this command was enhanced to show the authentication protocol (MD5 or SHA) and group name.                                 |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA.                                                                                                                   |
| 12.2(33)SRB | This command was integrated into Cisco IOS Release 12.2(33)SRB.                                                                                                                   |
| 12.2SX      | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 12.2(33)SB  | This command was integrated into Cisco IOS Release 12.2(33)SB.                                                                                                                    |

## Usage Guidelines

An SNMP user must be part of an SNMP group, as configured using the **snmp-server user** *username group-name* command.

When the *username* argument is not entered, the **show snmp user** command displays information about all configured users. If you specify the *username* argument, if one or more users of that name exists, the information pertaining to those users is displayed. Because this command displays users configured with the SNMP engine ID of the local agent and other engine IDs, there can be multiple users with the same username.

When configuring SNMP, you may see the logging message “Configuring snmpv3 USM user.” USM stands for the User-based Security Model for version 3 of the Simple Network Management Protocol (SNMPv3). For further information on the USM, see RFC 2574.

## Examples

The following is sample output from the **show snmp user** command. The output indicates the username as authuser, the engine ID string as 00000009020000000C025808, and the storage type as nonvolatile:

```
Router# show snmp user authuser
```

```
User name: authuser
Engine ID: 00000009020000000C025808
storage-type: nonvolatile      active access-list: 10
Rowstatus: active
```

Authentication Protocol: MD5  
 Privacy protocol: DES  
 Group name: VacmGroupName

Table 114 describes the significant fields shown in the display.

**Table 114** *show snmp user Field Descriptions*

| Field                   | Description                                                                                                                                                                                                                                                                                                |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| User name               | A string identifying the name of the SNMP user.                                                                                                                                                                                                                                                            |
| Engine ID               | A string identifying the name of the copy of SNMP on the device.                                                                                                                                                                                                                                           |
| storage-type            | Indicates whether the settings have been set in volatile or temporary memory on the device, or in nonvolatile or persistent memory where settings will remain after the device has been turned off and on again.                                                                                           |
| active access-list      | Standard IP access list associated with the SNMP user.                                                                                                                                                                                                                                                     |
| Rowstatus               | Indicates whether Rowstatus is active or inactive.                                                                                                                                                                                                                                                         |
| Authentication Protocol | Identifies which authentication protocol is used. Options are message digest algorithm 5 (MD5), Secure Hash Algorithm (SHA) packet authentication, or None. <ul style="list-style-type: none"> <li>If authentication is not supported in your software image, this field will not be displayed.</li> </ul> |
| Privacy protocol        | Indicates whether Data Encryption Standard (DES) packet encryption is enabled. <ul style="list-style-type: none"> <li>If DES is not supported in your software image, this field will not be displayed.</li> </ul>                                                                                         |
| Group name              | Indicates the SNMP group the user is a part of. <ul style="list-style-type: none"> <li>SNMP groups are defined in the context of a View-based Access Control Model (VACM).</li> </ul>                                                                                                                      |

# show snmp view

To display the family name, storage type, and status of a Simple Network Management Protocol (SNMP) configuration and associated MIB, use the **show snmp view** command in privileged EXEC mode.

## show snmp view

### Syntax Description

This command has no arguments or keywords.

### Command Modes

Privileged EXEC

### Command History

| Release   | Modification                                                  |
|-----------|---------------------------------------------------------------|
| 12.4(2)T  | This command was introduced.                                  |
| 12.0(31)S | This command was integrated into Cisco IOS Release 12.0(31)S. |

### Usage Guidelines

Use this command to display the SNMP view configuration.

### Examples

The following is sample output from the **show snmp view** command.

```
Router# show snmp view
```

```
View Family Name/View Family Subtree/View Family Mask/View Family Type/storage/status
```

```
myview          mib-2          -          included      nonvolatile active
myview          cisco          -          included      nonvolatile active
myview          atEntry        -          excluded      nonvolatile active
vldefault       iso            -          included      permanent active
vldefault       internet       -          included      volatile active
vldefault       internet.6.3.15 -          excluded      volatile active
vldefault       internet.6.3.16 -          excluded      volatile active
vldefault       internet.6.3.18 -          excluded      volatile active
```

[Table 115](#) describes the significant fields shown in the display.

**Table 115** *show snmp view* Field Descriptions

| Field               | Description                                                                  |
|---------------------|------------------------------------------------------------------------------|
| View Family Name    | Family name.                                                                 |
| View Family Subtree | MIB name.                                                                    |
| View Family Mask    | Family mask. A hyphen (-) appears in this column when no mask is associated. |
| View Family Type    | Type of family, either included or excluded.                                 |
| storage             | Type of memory storage, for example, volatile.                               |
| status              | Status of the configuration, either active or nonactive.                     |

# show sntp

To show information about the Simple Network Time Protocol (SNTP), use the **show sntp** command in EXEC mode on a Cisco 1003, Cisco 1004, Cisco 1005, Cisco 1600, Cisco 1720, or Cisco 1750 router.

## show sntp

**Syntax Description** This command has no arguments or keywords.

**Command Modes** EXEC

| Command History | Release     | Modification                                                                                                                                                                      |
|-----------------|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                 | 11.2        | This command was introduced.                                                                                                                                                      |
|                 | 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA.                                                                                                                   |
|                 | 12.2SX      | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

**Examples** The following is sample output from the **show sntp** command:

```
Router> show sntp
```

```
SNTP server      Stratum   Version   Last Receive
171.69.118.9     5         3         00:01:02
172.21.28.34     4         3         00:00:36   Synced   Bcast
```

```
Broadcast client mode is enabled.
```

[Table 116](#) describes the significant fields shown in the display.

**Table 116** *show sntp Field Descriptions*

| Field        | Description                                                                                                    |
|--------------|----------------------------------------------------------------------------------------------------------------|
| SNTP server  | Address of the configured or broadcast NTP server.                                                             |
| Stratum      | NTP stratum of the server. The stratum indicates how far away from an authoritative time source the server is. |
| Version      | NTP version of the server.                                                                                     |
| Last Receive | Time since the last NTP packet was received from the server.                                                   |
| Synced       | Indicates the server chosen for synchronization.                                                               |
| Bcast        | Indicates a broadcast server.                                                                                  |

| Related Commands | Command                      | Description                                                                                                                                                     |
|------------------|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                  | <b>sntp broadcast client</b> | Configures a Cisco 1003, Cisco 1004, Cisco 1005, Cisco 1600, Cisco 1720, or Cisco 1750 router to use SNTP to accept NTP traffic from any broadcast server.      |
|                  | <b>sntp server</b>           | Configures a Cisco 1003, Cisco 1004, Cisco 1005, Cisco 1600, Cisco 1720, or Cisco 1750 router to use SNTP to request and accept NTP traffic from a time server. |

# show time-range

To display information about configured time ranges, use the **show time-range** command in user EXEC or privileged EXEC mode.

## show time-range

**Syntax Description** This command has no arguments or keywords.

**Command Default** This command has no default behavior.

**Command Modes** User EXEC and Privileged EXEC

| Command History | Release     | Modification                                                                                                                                                                      |
|-----------------|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                 | 12.2        | This command was introduced.                                                                                                                                                      |
|                 | 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.33(SRA).                                                                                                                    |
|                 | 12.2SX      | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

**Usage Guidelines** Use this command to display configured time ranges.

**Examples** The following is sample output for the **show time-range** command. The word (active) indicates that the time range is in effect at that moment; otherwise, the output will indicate (inactive).

```
Router# show time-range
time-range entry: test (active)
  absolute start 00:00 01 January 2006 end 23:59 31 December 2006
  periodic weekdays 8:00 to 20:00
```

| Related Commands | Command    | Description                                                                                                          |
|------------------|------------|----------------------------------------------------------------------------------------------------------------------|
|                  | time-range | Specifies a time range by name and allows you configure a range during which an access list, for example, is active. |

# show track

To display information about objects that are tracked by the tracking process, use the **show track** command in privileged EXEC mode.

**show track** [*object-number* [**brief**] | **interface** [**brief**] | **ip route** [**brief**] | **resolution** | **timers**]

| Syntax Description   |                                                                                                 |
|----------------------|-------------------------------------------------------------------------------------------------|
| <i>object-number</i> | (Optional) Object number that represents the object to be tracked. The range is from 1 to 1000. |
| <b>brief</b>         | (Optional) Displays a single line of information related to the preceding argument or keyword.  |
| <b>interface</b>     | (Optional) Displays tracked interface objects.                                                  |
| <b>ip route</b>      | (Optional) Displays tracked IP-route objects.                                                   |
| <b>resolution</b>    | (Optional) Displays resolution of tracked parameters.                                           |
| <b>timers</b>        | (Optional) Displays polling interval timers.                                                    |

| Command Modes | Privileged EXEC (#) |
|---------------|---------------------|
|---------------|---------------------|

| Command History | Release                  | Modification                                                                                                                     |
|-----------------|--------------------------|----------------------------------------------------------------------------------------------------------------------------------|
|                 | 12.2(15)T                | This command was introduced.                                                                                                     |
|                 | 12.3(8)T                 | The output was enhanced to include the track-list objects.                                                                       |
|                 | 12.2(25)S                | This command was integrated into Cisco IOS Release 12.2(25)S.                                                                    |
|                 | 12.4(2)T                 | The output was enhanced to display stub objects.                                                                                 |
|                 | 12.2(28)SB               | This command was integrated into Cisco IOS Release 12.2(28)SB.                                                                   |
|                 | 12.2(33)SRA              | This command was integrated into Cisco IOS Release 12.2(33)SRA.                                                                  |
|                 | 12.4(9)T                 | This command was enhanced to display information about the status of an interface when carrier-delay detection has been enabled. |
|                 | 12.2(33)SXH              | This command was integrated into Cisco IOS Release 12.2(33)SXH.                                                                  |
|                 | Cisco IOS XE Release 2.1 | This command was integrated into Cisco IOS XE Release 2.1.                                                                       |
|                 | 12.4(20)T                | The output was enhanced to display IP SLAs information.                                                                          |
|                 | 15.1(3)T                 | This command was modified. The valid range of the <i>object-number</i> argument increased to 1000.                               |
|                 | 15.1(1)S                 | This command was modified. The valid range for the <i>object-number</i> argument increased to 1000.                              |

| Usage Guidelines | Use this command to display information about objects that are tracked by the tracking process. When no arguments or keywords are specified, information for all objects is displayed. |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

As of Cisco IOS Release 15.1(3)T, a maximum of 1000 objects can be tracked. Although 1000 tracked objects can be configured, each tracked object uses CPU resources. The amount of available CPU resources on a router is dependent upon variables such as traffic load and how other protocols are configured and run. The ability to use 1000 tracked objects is dependent upon the available CPU. Testing should be conducted on site to ensure that the service works under the specific site traffic conditions.

## Examples

The following example shows information about the state of IP routing on the interface that is being tracked:

```
Router# show track 1

Track 1
  Interface Ethernet0/2 ip routing
  IP routing is Down (no IP addr)
  1 change, last change 00:01:08
  Tracked by:
    HSRP Ethernet0/3 1
```

The following example shows information about the line-protocol state on the interface that is being tracked:

```
Router# show track 1

Track 1
  Interface Ethernet0/1 line-protocol
  Line protocol is Up
  1 change, last change 00:00:05
  Tracked by:
    HSRP Ethernet0/3 1
```

The following example shows information about the reachability of a route that is being tracked:

```
Router# show track 1

Track 1
  IP route 10.16.0.0 255.255.0.0 reachability
  Reachability is Up (RIP)
  1 change, last change 00:02:04
  First-hop interface is Ethernet0/1
  Tracked by:
    HSRP Ethernet0/3 1
```

The following example shows information about the threshold metric of a route that is being tracked:

```
Router# show track 1

Track 1
  IP route 10.16.0.0 255.255.0.0 metric threshold
  Metric threshold is Up (RIP/6/102)
  1 change, last change 00:00:08
  Metric threshold down 255 up 254
  First-hop interface is Ethernet0/1
  Tracked by:
    HSRP Ethernet0/3 1
```

The following example shows the object type, the interval in which it is polled, and the time until the next poll:

```
Router# show track timers

Object type   Poll Interval   Time to next poll
interface     1               expired
```

```
ip route      30      29.364
```

The following example shows the state of the IP SLAs tracking:

```
Router# show track 50
```

```
Track 50
  IP SLA 400 state
  State is Up
    1 change, last change 00:00:23
  Delay up 60 secs, down 30 secs
  Latest operation return code: Unknown
```

The following example shows whether a route is reachable:

```
Router# show track 3
```

```
Track 3
  IP SLA 1 reachability
  Reachability is Up
    1 change, last change 00:00:47
  Latest operation return code: over threshold
  Latest RTT (milliseconds) 4
  Tracked by:
    HSRP Ethernet0/1 3
```

[Table 117](#) describes the significant fields shown in the displays.

**Table 117** *show track Field Descriptions*

| Field                            | Description                                                                                                              |
|----------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| Track                            | Object number that is being tracked.                                                                                     |
| Interface Ethernet0/2 ip routing | Interface type, interface number, and object that is being tracked.                                                      |
| IP routing is                    | State value of the object, displayed as Up or Down. If the object is down, the reason is displayed.                      |
| 1 change, last change            | Number of times that the state of a tracked object has changed and the time (in <i>hh:mm:ss</i> ) since the last change. |
| Tracked by                       | Client process that is tracking the object.                                                                              |
| First-hop interface is           | Displays the first-hop interface.                                                                                        |
| Object type                      | Object type that is being tracked.                                                                                       |
| Poll Interval                    | Interval (in seconds) in which the tracking process polls the object.                                                    |
| Time to next poll                | Period of time, in seconds, until the next polling of the object.                                                        |

The following output shows that there are two objects. Object 1 has been configured with a weight of 10 “down,” and object 2 has been configured with a weight of 20 “up.” Object 1 is down (expressed as 0/10) and object 2 is up. The total weight of the tracked list is 20 with a maximum of 30 (expressed as 20/30). The “up” threshold is 20, so the list is “up.”

```
Router# show track
```

```
Track 6
List threshold weight
Threshold weight is Up (20/30)
  1 change, last change 00:00:08
```

```

object 1 Down (0/10)
object 2 weight 20 Up (20/30)
Threshold weight down 10 up 20
Tracked by:
  HSRP Ethernet0/3 1

```

The following example shows information about the Boolean configuration:

```
Router# show track
```

```

Track 3
List boolean and
Boolean AND is Down
  1 change, last change 00:00:08
    object 1 not Up
    object 2 Down
Tracked by:
  HSRP Ethernet0/3 1

```

Table 118 describes the significant fields shown in the displays.

**Table 118** *show track Field Descriptions*

| Field                 | Description                                                                                                              |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------|
| Track                 | Object number that is being tracked.                                                                                     |
| Boolean AND is Down   | Each object defined in the list must be in a down state.                                                                 |
| 1 change, last change | Number of times that the state of a tracked object has changed and the time (in <i>hh:mm:ss</i> ) since the last change. |
| Tracked by            | Client process that is tracking the object; in this case, HSRP.                                                          |

The following example shows information about a stub object that has been created to be tracked using Embedded Event Manager (EEM):

```
Router# show track
```

```

Track 1
  Stub-object
  State is Up
    1 change, last change 00:00:04, by Undefined

```

The following example shows information about a stub object when the **brief** keyword is used:

```
Router# show track brief
```

```

Track   Object                               Parameter      Value Last Change
1       Stub-object Undefined                Up           00:00:12

```

The following example shows information about the line-protocol state on an interface that is being tracked and which has carrier-delay detection enabled:

```
Router# show track
```

```

Track 101
Interface Ethernet1/0 line-protocol
Line protocol is Down (carrier-delay)
1 change, last change 00:00:03

```

Table 119 describes the significant fields shown in the displays.

**Table 119**      *show track brief Field Descriptions*

| Field                                    | Description                                                                       |
|------------------------------------------|-----------------------------------------------------------------------------------|
| Track                                    | Object number that is being tracked.                                              |
| Interface Ethernet1/0<br>line-protocol   | Interface type, interface number, and object that is being tracked.               |
| Line protocol is Down<br>(carrier-delay) | State of the interface with the carrier-delay parameter taken into consideration. |
| last change                              | Time (in <i>hh:mm:ss</i> ) since the state of a tracked object last changed.      |

Table 120 describes the significant fields shown in the displays.

**Table 120**      *show track brief Field Descriptions*

| Field       | Description                                                                  |
|-------------|------------------------------------------------------------------------------|
| Track       | Object number that is being tracked.                                         |
| Object      | Definition of stub object.                                                   |
| Parameter   | Tracking parameters.                                                         |
| Value       | State value of the object, displayed as Up or Down.                          |
| last change | Time (in <i>hh:mm:ss</i> ) since the state of a tracked object last changed. |

**Related Commands**

| Command                | Description                                                                   |
|------------------------|-------------------------------------------------------------------------------|
| <b>track interface</b> | Configures an interface to be tracked and enters tracking configuration mode. |
| <b>track ip route</b>  | Tracks the state of an IP route and enters tracking configuration mode.       |

# show wsma agent

To display the Web Services Management Agent (WSMAs) configured, use the **show wsma agent** command in user EXEC mode.

**show wsma agent** { **counters** | **schema** } [**config** | **exec** | **filesys** | **notify**]

| Syntax Description |            |                                        |
|--------------------|------------|----------------------------------------|
| <b>counters</b>    |            | Displays the WSMA counters.            |
| <b>schema</b>      |            | Displays the WSMA schema.              |
| <b>config</b>      | (Optional) | Displays the WSMA configuration agent. |
| <b>exec</b>        | (Optional) | Displays the WSMA executive agent.     |
| <b>filesys</b>     | (Optional) | Displays the WSMA file system agent.   |
| <b>notify</b>      | (Optional) | Displays the WSMA notify agent.        |

**Command Modes** User EXEC (>)

| Command History | Release   | Modification                                                                        |
|-----------------|-----------|-------------------------------------------------------------------------------------|
|                 | 12.4(24)T | This command was introduced.                                                        |
|                 | 15.1(1)T  | This command was modified. Additional information was added to the counters output. |

**Usage Guidelines** You can use the **show wsma agent** command to display the WSMAs.

[Table 121](#) describes the significant fields shown in the display when the keyword **counters** is used.

**Table 121** *show wsma agent Field Descriptions*

| Field             | Description                                                                                                                                                                                                                                                             |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| messages received | Total number of messages that were passed from the profile into the WSMA.<br><br>The number of messages sent and the number of fault messages together form the total number of messages received.                                                                      |
| replies sent      | Total number of reply messages sent to the profile.                                                                                                                                                                                                                     |
| faults            | Total number of faults that prevented a message from producing a reply. Faults are not a count of bad requests sent to the WSMA. It is meant to count the cases where the WSMA agent could not send a response for reasons out of its control (For example, no memory.) |

**Examples** The following example shows how to display the WSMA configuration agent counters:

```
Router# show wsma agent config counters
```

```
messages received 53, replies sent 53, faults 0
```

The following example shows how to display all WSMA counters information:

```
Router# show wsma agent counters
```

```
WSMA Exec Agent Statistics:
  messages received 0, replies sent 0, faults 0
WSMA Config Agent Statistics:
  messages received 4, replies sent 4, faults 0
WSMA Filesys Agent Statistics:
  messages received 1, replies sent 1, faults 0
WSMA Notification Agent Statistics:
  config silent
  messages received 0, replies sent 0, notifications sent 0, faults 0
```

#### Related Commands

| Command                  | Description                                                      |
|--------------------------|------------------------------------------------------------------|
| <b>show wsma id</b>      | Displays the WSMA ID configured on Cisco IOS networking devices. |
| <b>show wsma profile</b> | Displays information on the required WSMA profiles.              |

# show wsma id

To display the Web Services Management Agent (WSMA) ID configured on Cisco IOS networking devices, use the **show wsma id** command in user EXEC mode.

**show wsma id**

|                           |                                            |
|---------------------------|--------------------------------------------|
| <b>Syntax Description</b> | This command has no arguments or keywords. |
|---------------------------|--------------------------------------------|

|                      |               |
|----------------------|---------------|
| <b>Command Modes</b> | User EXEC (>) |
|----------------------|---------------|

| <b>Command History</b> | Release   | Modification                 |
|------------------------|-----------|------------------------------|
|                        | 12.4(24)T | This command was introduced. |

|                 |                                                         |
|-----------------|---------------------------------------------------------|
| <b>Examples</b> | The following example shows how to display the WSMA ID: |
|-----------------|---------------------------------------------------------|

```
Router# show wsma id
```

```
Router
```

```
Router#
```

| <b>Related Commands</b> | Command                  | Description                                         |
|-------------------------|--------------------------|-----------------------------------------------------|
|                         | <b>show wsma agent</b>   | Displays all WSMAAs configured.                     |
|                         | <b>show wsma profile</b> | Displays information on the required WSMA profiles. |

# show wsma profile

To display information on the required Web Services Management Agent (WSMA) profiles, use the **show wsma profile** command in user EXEC mode.

**show wsma profile** [*name profile-name*] { **connections** | **counters** | **schema** }

## Syntax Description

|                                 |                                                                                                |
|---------------------------------|------------------------------------------------------------------------------------------------|
| <b>name</b> <i>profile-name</i> | (Optional) Displays profile information of the profile name specified.                         |
| <b>connections</b>              | Displays information about the connections for all listener and initiator profiles configured. |
| <b>counters</b>                 | Displays various statistics about the listener and initiator profiles.                         |
| <b>schema</b>                   | Displays information about the WSMA profile schema configured.                                 |

## Command Modes

User EXEC (>)

## Command History

| Release   | Modification                                                                                                                                             |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| 12.4(24)T | This command was introduced.                                                                                                                             |
| 15.1(1)T  | This command was modified. Additional information was added to the output for counter statistics. The output for connection information was reformatted. |

## Usage Guidelines

If you do not specify a profile name, information for all profiles is displayed.

Specifying the **connection** keyword provides details about the connections to all the listener and initiator profiles.

[Table 122](#) describes the significant fields shown in the display.

**Table 122** *show wsma profile connection Field Descriptions*

| Field               | Description                                                                                                                                                                                                           |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| open connections    | The number of connections into the profile.                                                                                                                                                                           |
| closing connections | The number of connections that have initiated a close but the close is not complete yet.                                                                                                                              |
| sessions accepted   | The total number of sessions accepted (including closed ones) since the profile was configured or the counters were last cleared.                                                                                     |
| sessions rejected   | The total number of sessions rejected since the profile was configured or the counters were last cleared. Rejections may be due to the Access Control Lists (ACLs) or internal errors (For example, malloc failures). |

Specifying the **counters** keyword provides various statistics about the listeners and initiators.

Table 123 describes the significant fields shown in the display.

**Table 123** *show wsma profile counters Field Descriptions*

| Field                   | Description                                                                                                                                                                      |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| incoming total          | Total number of messages received.                                                                                                                                               |
| bad XML                 | Total number of incoming messages that could not be parsed by the XML parser.                                                                                                    |
| oversized               | Total number of messages exceeding the maximum message size configured.                                                                                                          |
| outgoing total          | Total number of messages sent.                                                                                                                                                   |
| absorbed                | Total number of messages that were absorbed by specifying the stealth command.                                                                                                   |
| message internal errors | Total number of internal errors that prevented the message from getting processed completely.                                                                                    |
| authentication errors   | Total number of messages with Simple Object Access Protocol (SOAP) Web Services Security (WSSE) headers that contained incorrect credentials resulting in authentication errors. |
| Connection Accepts      | Total number of connections that have been accepted.                                                                                                                             |
| local hangup            | Total number of connections that have had the hangup initiated from the IOS device.                                                                                              |
| remote hangup           | Total number of connections that have had the hangup initiated from the remote end.                                                                                              |
| keepalive hangup        | Total number of connections that have had the hangup initiated after reaching the configured number of keepalive retries.                                                        |
| session internal errors | Total number of internal errors preventing a connection from continuing.                                                                                                         |

## Examples

The following example shows how to display information about WSMA profile connections:

```
Router# show wsma profile connections
```

```
Listener Profile http: 0 open connections: 0 closing connections
  Encap: soap11
  WSSE header is required
  Max message (RX) is 50 Kbytes
  SOAP Faults are sent
  Idle timeout infinite
  Keepalive not configured
  Listening via http
Listening to path /wsma. Max Idle 0 ms. Accepting post on plain text connections.
Established at 01:11:04.207 UTC Tue Jan 12 2010
  Tx 493475 bytes (90 msg), Tx 0 errors,
  Last message sent at 05:18:08.539 UTC Sat Feb 20 2010
  Rx 59457 bytes (90 msg), 0 empty msg
  Last message received at 05:18:08.295 UTC Sat Feb 20 2010
Listener Profile ssh: 2 open connections: 0 closing connections
  Encap: soap11
  WSSE header is required
  Max message (RX) is 50 Kbytes
```

```

    SOAP Faults are sent
    Idle timeout infinite
    Keepalive not configured
    Listening via ssh
SSH listener, 10 sessions accepted, 0 sessions rejected
Connected sessions...

Remote connection via SSH by user(cisco) from 172.16.29.134:44457, state connect
Established at 01:14:03.184 UTC Thu Mar 11 2010
    Tx 1183 bytes (2 msg), Tx 0 errors,
    Last message sent at 01:14:48.565 UTC Thu Mar 11 2010
    Rx 10 bytes (1 msg), 0 empty msg
    Last message received at 01:14:48.565 UTC Thu Mar 11 2010

Remote connection via SSH by user(cisco) from 172.16.154.90:45404, state connect
Established at 01:14:28.041 UTC Thu Mar 11 2010
    Tx 1183 bytes (2 msg), Tx 0 errors,
    Last message sent at 01:14:54.437 UTC Thu Mar 11 2010
    Rx 7 bytes (1 msg), 1 empty msg
    Last message received at 01:14:54.437 UTC Thu Mar 11 2010

Initiator Profile ssh-init: 0 open connections: 0 closing connections
    Encap: soap11
    WSSE header is required
    Max message (RX) is 50 Kbytes
    SOAP Faults are sent
    Idle timeout infinite
    Keepalive not configured
    Reconnect time 60 seconds
No transport configured

```

The following example shows how to display information about WSMA profile counters:

```
Router# show wsma profile counters
```

```

Statistics for profile http
    incoming total 90, bad XML 0, authentication errors 0, oversized 0
    outgoing total 90, absorbed 0
    message internal errors 0
Connection Accepts 90, local hangup 0, remote hangup 90, keepalive hangup 0
    session internal errors 0
Statistics for profile ssh
    incoming total 9, bad XML 2, authentication errors 0, oversized 0
    outgoing total 20, absorbed 0
    message internal errors 0
Connection Accepts 8, local hangup 0, remote hangup 8, keepalive hangup 0
    session internal errors 0

```

The following example shows how to display information about WSMA profile schema:

```
Router# show wsma profile schema
```

```

Schema dog
New Name Space ''
<VirtualRootTag> [0, 1] required
    New Name Space 'http://schemas.xmlsoap.org/soap/envelope/'
    <Envelope> 1+ required
        <Header> any subtree is allowed
        <Body> 1 required
            <Fault> [0, 1] required
                <faultcode> 1 required
                <faultstring> 1 required
                <faultactor> [0, 1] required

```

```

    <detail> any subtree is allowed
  New Name Space 'urn:cisco:exec'
    <request> [0, 1] required
      <execCLI> 1+ required
        <cmd> 1 required
        <dialogue> 0+ required
        <expect> 1 required
        <reply> 1 required
  New Name Space 'urn:cisco:wsma-config'
    <request> [0, 1] required
  <config-data> 1 required
    <cli-config-data> [0, 1] required
      <cmd> 1+ required
      <cli-config-data-block> [0, 1] required
      <xml-config-data> [0, 1] required
      <Device-Configuration> [0, 1] required
      <> any subtree is allowed
  New Name Space 'urn:cisco:wsma-filesystem'
    <request> [0, 1] required
      <fileList> [0, 1] required
      <fileDelete> [0, 1] required
        <deleteFileList> 1 required
          <filename> 1+ required
      <fileCopy> [0, 1] required
        <srcURL> 1 required
        <dstURL> 1 required
        <validationInfo> [0, 1] required
          <md5Checksum> 1 required
        <deleteFileList> [0, 1] required
          <filename> 1+ required
  New Name Space 'urn:cisco:wsma-notify'
    <request> [0, 1] required
  Schema dog1
  New Name Space ''
  <VirtualRootTag> [0, 1] required
  New Name Space 'http://schemas.xmlsoap.org/soap/envelope/'
    <Envelope> 1+ required
      <Header> any subtree is allowed
      <Body> 1 required
        <Fault> [0, 1] required
          <faultcode> 1 required
          <faultstring> 1 required
          <faultactor> [0, 1] required
        <detail> any subtree is allowed

```

**Related Commands**

| Command                | Description                                                      |
|------------------------|------------------------------------------------------------------|
| <b>show wsma agent</b> | Displays all the WSMA's configured.                              |
| <b>show wsma id</b>    | Displays the WSMA ID configured on Cisco IOS networking devices. |

# show xsd-format

To generate XML Schema Definition (XSD) output for a command, use the **show xsd-format** command in privileged EXEC mode.

```
show xsd-format [location:local-filename] cli command
```

Syntax Description

|                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>location:local-filename</i> | (Optional) Command Operational Data Model (ODM) file location and filename. Valid locations are <b>bootflash:</b> , <b>flash:</b> , <b>nvr</b> am:, and any valid disk or slot number (such as <b>disk0:</b> or <b>slot1:</b> ).<br><br>ODM spec files have a .odm suffix. The pipe ( ) output modifier can be used in the command.<br><br><b>Note</b> These arguments are not required if you want to use a default ODM file defined with the <b>format global</b> command. |
| <i>cli command</i>             | Displays the XSD output for the specific command. Enter a fully expanded command name.                                                                                                                                                                                                                                                                                                                                                                                       |

Command Modes

Privileged EXEC (#)

Command History

| Release     | Modification                                                                     |
|-------------|----------------------------------------------------------------------------------|
| 12.4(20)T   | This command was introduced.                                                     |
| 12.2(33)SRE | This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE. |
| 12.2(54)SG  | This command was integrated into Cisco IOS Release 12.2(54)SG.                   |

Usage Guidelines

The **show xsd-format** command searches through the ODM spec file to find a match for the specified command name and generates XSD format. The spec file must exist on the local filesystem. If no spec entry is found, an error is returned.



Note

The **show running-config** command output is generated natively in Extensible Markup Language (XML), so the spec filename could be an empty file or, if a default spec file has been defined with the **format global** command, no filename is required.

## Examples

The following example displays the XSD generated for the **show arp** command:

Router# **show xsd-format disk2:spec3.3.odm cli show arp**

```
<?xml version="1.0"?>
  <xsd:schema elementFormDefault="qualified" attributeFormDefault="unqualified"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
    <xsd:complexType name="ShowArp_def">
      <xsd:sequence>
        <xsd:choice minOccurs="0" maxOccurs="unbounded">
          <xsd:element ref="Info"/>
          <xsd:element name="ARPTable" minOccurs="0">
            <xsd:complexType>
              <xsd:sequence>
                <xsd:element name="entry" minOccurs="0" maxOccurs="unbounded">
                  <xsd:complexType>
                    <xsd:sequence>
                      <xsd:element name="Protocol" minOccurs="0" type="string" />
                      <xsd:element name="Address" minOccurs="0" type="string" />
                      <xsd:element name="Age" minOccurs="0" type="integer" />
                      <xsd:element name="MAC" minOccurs="0" type="string" />
                      <xsd:element name="Type" minOccurs="0" type="string" />
                      <xsd:element name="Interface" minOccurs="0" type="string" />
                    </xsd:sequence>
                  </xsd:complexType>
                </xsd:element>
              </xsd:sequence>
            </xsd:complexType>
          </xsd:element>
        </xsd:choice>
      </xsd:sequence>
    </xsd:complexType>
    <xsd:element name="Info" type="xsd:string"/>
    <xsd:element name="ShowArp" type="ShowArp_def"/>
  </xsd:schema>
```

The display from the **show xsd-format** command is self-explanatory; see the "Usage Guidelines" section for more information.

## Related Commands

| Command                | Description                                                                                                                    |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| <b>format global</b>   | Specifies a default ODM spec file other than the built-in spec file for XML-formatted requests coming from NETCONF operations. |
| <b>show odm-format</b> | Displays the schema of the spec file.                                                                                          |

# show xsm status

To display information and subscription status of the XML Subscription Manager (XSM) server and clients (such as VPN Device Manager [VDM]), and to display a list of XML data from the XSM server, use the **show xsm status** command in privileged EXEC mode.

## show xsm status

### Syntax Description

This command has no arguments or keywords.

### Command Modes

Privileged EXEC

### Command History

| Release     | Modification                                                                                                                                                                      |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 12.1(6)E    | This command was introduced.                                                                                                                                                      |
| 12.2(9)YE   | This command was integrated into Cisco IOS Release 12.2(9)YE.                                                                                                                     |
| 12.2(9)YO1  | This command was integrated into Cisco IOS Release 12.2(9)YO1.                                                                                                                    |
| 12.2(13)T   | This command was integrated into Cisco IOS Release 12.2(13)T.                                                                                                                     |
| 12.2(14)S   | This command was integrated into Cisco IOS Release 12.2(14)S.                                                                                                                     |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA.                                                                                                                   |
| 12.2SX      | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

### Usage Guidelines

Use this command to display the following information: which subsystems and histories are enabled or disabled (XSM, Embedded Device Manager [EDM], VDM), XSM client version, number of XSM sessions, duration of XSM session, session IDs, client version and IP address, configuration and monitor privilege levels, and list of subscribed XML Request Descriptors (XRDs).

### Examples

The following example shows one XSM session (Session ID = 2) active on the Cisco device for the XSM client at IP address 172.17.129.134, and how long this session has been connected to the XSM server (Session 2: Connected since 22:47:07 UTC Mon Jan 8 2001). The output shows that the XSM, VDM, and EDM subsystems, and EDM and VDM history collecting are enabled. XSM configuration privilege level is set at 15, with XSM monitor privilege level set at 1.

This output also shows the active XRDs (and their version) for Session 2:

```
Router# show xsm status
```

```
XSM subsystem is Enabled.
VDM subsystem is Enabled.
EDM subsystem is Enabled.
EDM History is Enabled.
VDM History is Enabled.
XSM privilege configuration level 15.
XSM privilege monitor level 1.
```

Number of XSM Sessions : 1.

Session ID = 2.

XSM Client v0.0(0.0)- @ 172.17.129.134

Connected since 22:47:07 UTC Mon Jan 8 2001

List of subscribed xrd:

|                                    |      |
|------------------------------------|------|
| 0 ) device-about                   | v1.0 |
| 1 ) ios-image                      | v1.0 |
| 2 ) if-list                        | v1.0 |
| 3 ) device-health                  | v1.0 |
| 4 ) ike-stats                      | v1.0 |
| 5 ) ike                            | v1.0 |
| 6 ) ipsec-topn-tunnels-by-traffic  | v1.0 |
| 7 ) ipsec-topn-tunnels-by-duration | v1.0 |
| 8 ) ipsec-stats                    | v1.0 |
| 9 ) crypto-maps                    | v1.0 |
| 10) ipsec                          | v1.0 |

Table 124 describes the significant fields shown in the display. (See documentation of the **show xsm xrd-list** command for a full description of subscribed XRDs).

**Table 124** *show xsm status Field Descriptions*

| Field                             | Description                                                                                                  |
|-----------------------------------|--------------------------------------------------------------------------------------------------------------|
| XSM privilege configuration level | XSM configuration privilege level.                                                                           |
| XSM privilege monitor level       | XSM monitor privilege level.                                                                                 |
| Number of XSM Sessions            | Total number of concurrent XSM sessions.                                                                     |
| Session ID                        | Specific XSM session number.                                                                                 |
| XSM Client                        | Version and IP address of the XSM client.                                                                    |
| Connected since                   | Start time for each session connection to the XSM server.                                                    |
| List of subscribed xrd            | Details XRDs available from the XSM server (see <b>show xsm xrd-list</b> command for complete list of XRDs). |

#### Related Commands

| Command                                  | Description                                                 |
|------------------------------------------|-------------------------------------------------------------|
| <b>clear xsm</b>                         | Clears XSM client sessions.                                 |
| <b>show xsm xrd-list</b>                 | Displays all XRDs for clients subscribed to the XSM server. |
| <b>xsm</b>                               | Enables XSM client access to the router.                    |
| <b>xsm privilege configuration level</b> | Enables configuration privilege level to subscribe to XRDs. |
| <b>xsm privilege monitor level</b>       | Enables monitor privilege level to subscribe to XRDs.       |

# show xsm xrd-list

To display all XML Request Descriptors (XRDs) for XML Subscription Manager (XSM) clients (such as the VPN Device Manager [VDM]) made available by subscription to the XSM server and to identify the required privilege levels, use the **show xsm xrd-list** command in privileged EXEC mode.

**show xsm xrd-list**

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC

| Command History | Release     | Modification                                                                                                                                                                      |
|-----------------|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                 | 12.1(6)E    | This command was introduced.                                                                                                                                                      |
|                 | 12.2(9)YE   | This command was integrated into Cisco IOS Release 12.2(9)YE.                                                                                                                     |
|                 | 12.2(9)YO1  | This command was integrated into Cisco IOS Release 12.2(9)YO1.                                                                                                                    |
|                 | 12.2(13)T   | This command was integrated into Cisco IOS Release 12.2(13)T.                                                                                                                     |
|                 | 12.2(14)S   | This command was integrated into Cisco IOS Release 12.2(14)S.                                                                                                                     |
|                 | 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA.                                                                                                                   |
|                 | 12.2SX      | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

**Usage Guidelines** Use this command to display the XRD version and minimum privilege level and type (configuration or monitor) required to view each XRD.

**Examples** The following example shows some active XRDs on the XSM server. The end of each line displays the following:

- XRD version number.
- XRD privilege type (configuration or monitor), indicating the privilege level required.

This example displays all available XRDs because both relevant commands (**xsm edm** and **xsm vdm**) have been configured. However, if one command is not configured, only an abbreviated XRD list will appear.

```
Router# show xsm xrd-list
List of all available xrds:
0 ) vlan-db                v1.0  privilege=configuration
1 ) entity                 v1.0  privilege=configuration
2 ) ip                     v1.0  privilege=configuration
3 ) ios-users              v1.0  privilege=configuration
4 ) device-about           v1.0  privilege=monitor
5 ) ios-image              v1.0  privilege=configuration
6 ) if-stats               v1.0  privilege=monitor
7 ) if-list                v1.0  privilege=configuration
```

```

8 ) device-health          v1.0  privilege=monitor
9 ) time                   v1.0  privilege=monitor
10) access-lists           v1.0  privilege=configuration
11) ike-topn-tunnels-by-traffic v1.0  privilege=monitor
12) ike-topn-tunnels-by-errors v1.0  privilege=monitor
13) ike-topn-tunnels-by-duration v1.0  privilege=monitor
14) ike-stats              v1.0  privilege=monitor
15) ike                    v1.0  privilege=configuration
16) certificate-authorities v1.0  privilege=configuration
17) ipsec-topn-tunnels-by-traffic v1.0  privilege=monitor
18) ipsec-topn-tunnels-by-errors v1.0  privilege=monitor
19) ipsec-topn-tunnels-by-duration v1.0  privilege=monitor
20) ipsec-stats            v1.0  privilege=monitor
21) crypto-maps            v1.0  privilege=configuration
22) ipsec                  v1.0  privilege=configuration
23) vdm-history            v1.0  privilege=configuration
24) gre-tunnels            v1.0  privilege=monitor
end list.

```

Table 125 describes (in alphabetical order) typical XRDs shown in the display.

**Table 125** *show xsm xrd-list Field Descriptions*

| Field                          | Descriptions                                                                                                                   |
|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| access-lists                   | IOS access control list (ACL) configuration.                                                                                   |
| certificate-authorities        | IOS certificate authority (CA) configuration.                                                                                  |
| crypto-maps                    | IOS Crypto Map configuration.                                                                                                  |
| device-about                   | General network device information.                                                                                            |
| device-health                  | General network device health statistics.                                                                                      |
| edm-history                    | Selected, historical statistics related to general embedded device management. (This field is not shown in the example above.) |
| entity                         | Summary of all physical and logical entities within a device.                                                                  |
| gre-tunnels                    | All current GRE tunnels and respective statistics.                                                                             |
| if-list                        | List of all interfaces and their respective IOS configurations.                                                                |
| if-stats                       | Statistics for all interfaces and their respective IOS configurations.                                                         |
| ike                            | IOS Internet Key Exchange (IKE) configuration.                                                                                 |
| ike-stats                      | Statistics related to IKE.                                                                                                     |
| ike-topn-tunnels-by-duration   | Top 10 IKE tunnels by duration (time).                                                                                         |
| ike-topn-tunnels-by-errors     | Top 10 IKE tunnels by errors.                                                                                                  |
| ike-topn-tunnels-by-traffic    | Top 10 IKE tunnels by traffic volume.                                                                                          |
| ios-image                      | Information about the current running IOS image.                                                                               |
| ios-users                      | Local IOS user configuration.                                                                                                  |
| ip                             | IOS IP configuration statistics.                                                                                               |
| ipsec                          | IOS IPSec configuration.                                                                                                       |
| ipsec-stats                    | Interface name and IPSec input and output statistics including: number of packets, dropped packets, octets and errors.         |
| ipsec-topn-tunnels-by-duration | Top 10 IPSec tunnels by duration.                                                                                              |
| ipsec-topn-tunnels-by-errors   | Top 10 IPSec tunnels by errors.                                                                                                |

**Table 125**      *show xsm xrd-list Field Descriptions (continued)*

| Field                         | Descriptions                                                                                                    |
|-------------------------------|-----------------------------------------------------------------------------------------------------------------|
| ipsec-topn-tunnels-by-traffic | Top 10 IPSec tunnels by traffic.                                                                                |
| time                          | Device's clock reading in UTC.                                                                                  |
| vdm-history                   | Selected, historical VPN-related statistics.                                                                    |
| vlan-db                       | VLAN database configuration (switches only).                                                                    |
| xsm-session                   | Status of the current XSM session and related subscriptions.<br>(This field is not shown in the example above.) |

**Related Commands**

| Command                                  | Description                                                                 |
|------------------------------------------|-----------------------------------------------------------------------------|
| <b>clear xsm</b>                         | Clears XSM client sessions.                                                 |
| <b>show xsm status</b>                   | Displays information and status about clients subscribed to the XSM server. |
| <b>xsm</b>                               | Enables XSM client access to the router.                                    |
| <b>xsm privilege configuration level</b> | Enables configuration privilege level to subscribe to XRDs.                 |
| <b>xsm privilege monitor level</b>       | Enables monitor privilege level to subscribe to XRDs.                       |

## slot (ERM policy)

To configure line cards, use the **slot** command in ERM policy configuration mode.

**slot** *slot-number*

|                           |                    |                                                                         |
|---------------------------|--------------------|-------------------------------------------------------------------------|
| <b>Syntax Description</b> | <i>slot-number</i> | Integer that identifies a slot number or the start of a range of slots. |
|---------------------------|--------------------|-------------------------------------------------------------------------|

|                        |           |
|------------------------|-----------|
| <b>Command Default</b> | Disabled. |
|------------------------|-----------|

|                      |                          |
|----------------------|--------------------------|
| <b>Command Modes</b> | ERM policy configuration |
|----------------------|--------------------------|

| Command History | Release     | Modification                                                    |
|-----------------|-------------|-----------------------------------------------------------------|
|                 | 12.3(14)T   | This command was introduced.                                    |
|                 | 12.2(33)SRB | This command was integrated into Cisco IOS Release 12.2(33)SRB. |

|                         |                                                                                                                                                                                                                                                                                                 |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Usage Guidelines</b> | You can configure line cards using the <b>slot</b> <i>slot-number</i> command in ERM policy configuration mode. This command is available only in distributed platforms such as the Route Switch Processor (RSP). You must use a Cisco 7500 router with a line card for executing this command. |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                 |                                                               |
|-----------------|---------------------------------------------------------------|
| <b>Examples</b> | The following example shows how to configure the line card 0: |
|-----------------|---------------------------------------------------------------|

```
Router(config-erm-policy)# slot 0
```

| Related Commands | Command                 | Description                                                                                      |
|------------------|-------------------------|--------------------------------------------------------------------------------------------------|
|                  | <b>buffer public</b>    | Enters the buffer owner configuration mode and sets thresholds for buffer usage.                 |
|                  | <b>cpu interrupt</b>    | Enters the CPU owner configuration mode and sets thresholds for interrupt level CPU utilization. |
|                  | <b>cpu process</b>      | Enters the CPU owner configuration mode and sets thresholds for processor level CPU utilization. |
|                  | <b>cpu total</b>        | Enters the CPU owner configuration mode and sets thresholds for total CPU utilization.           |
|                  | <b>critical rising</b>  | Sets the critical level threshold values for the buffer, CPU, and memory ROs.                    |
|                  | <b>major rising</b>     | Sets the major level threshold values for the buffer, CPU, and memory ROs.                       |
|                  | <b>memory io</b>        | Enters the memory owner configuration mode and sets threshold values for I/O memory.             |
|                  | <b>memory processor</b> | Enters the memory owner configuration mode and sets threshold values for processor memory.       |

| Command                  | Description                                                                |
|--------------------------|----------------------------------------------------------------------------|
| <b>minor rising</b>      | Sets the minor level threshold values for the buffer, CPU, and memory ROs. |
| <b>policy (ERM)</b>      | Configures an ERM resource policy.                                         |
| <b>resource policy</b>   | Enters ERM configuration mode.                                             |
| <b>show resource all</b> | Displays all the resource details.                                         |

## snmp context (VRF)

To associate a Simple Network Management Protocol (SNMP) context with a particular VPN routing and forwarding (VRF) instance, use the **snmp context** command in VRF configuration mode. To disassociate an SNMP context from a VPN, use the **no** form of this command.

**snmp context** *context-name*

**no snmp context**

| Syntax Description | <i>context-name</i> | Name of the SNMP VPN context. The name can be up to 32 alphanumeric characters. |
|--------------------|---------------------|---------------------------------------------------------------------------------|
|--------------------|---------------------|---------------------------------------------------------------------------------|

| Command Default | No SNMP contexts are associated with VPNs. |
|-----------------|--------------------------------------------|
|-----------------|--------------------------------------------|

| Command Modes | VRF configuration (config-vrf) |
|---------------|--------------------------------|
|---------------|--------------------------------|

| Command History | Release  | Modification                                                                   |
|-----------------|----------|--------------------------------------------------------------------------------|
|                 | 15.0(1)M | This command was introduced. This command replaces the <b>context</b> command. |

| Usage Guidelines | Before you use the <b>snmp context</b> command to associate an SNMP context with a VPN, you must do the following: |
|------------------|--------------------------------------------------------------------------------------------------------------------|
|------------------|--------------------------------------------------------------------------------------------------------------------|

- Issue the **snmp-server context** command to create an SNMP context.
- Associate a VPN with a context so that the specific MIB data for that VPN exists in the context.
- Associate a VPN group with the context of the VPN using the **context** *context-name* keyword argument pair of the **snmp-server group** command.

SNMP contexts provide VPN users with a secure way of accessing MIB data. When a VPN is associated with a context, MIB data for that VPN exists in that context. Associating a VPN with a context helps service providers to manage networks with multiple VPNs. Creating and associating a context with a VPN enables a provider to prevent the users of one VPN from accessing information about other VPN users on the same networking device.

A route distinguisher (RD) is required to configure an SNMP context. An RD creates routing and forwarding tables and specifies the default route distinguisher for a VPN. The RD is added to the beginning of an IPv4 prefix to make it globally unique. An RD is either an autonomous system number (ASN) relative, which means that it is composed of an autonomous system number and an arbitrary number, or an IP address relative and is composed of an IP address and an arbitrary number.

## Examples

The following example shows how to create an SNMP context named context1 and associate the context with the VRF named vrf1:

```
Router(config)# snmp-server context context1
Router(config)# ip vrf vrf1
Router(config-vrf)# rd 100:120
Router(config-vrf)# snmp context context1
```

## Related Commands

| Command                                    | Description                                                                            |
|--------------------------------------------|----------------------------------------------------------------------------------------|
| <b>ip vrf</b>                              | Enters VRF configuration mode for the configuration of a VRF.                          |
| <b>snmp mib community-map</b>              | Associates an SNMP community with an SNMP context, engine ID, or security name.        |
| <b>snmp mib target list</b>                | Creates a list of target VRFs and hosts to associate with an SNMP v1 or v2c community. |
| <b>snmp-server context</b>                 | Creates an SNMP context.                                                               |
| <b>snmp-server group</b>                   | Configures a new SNMP group or a table that maps SNMP users to SNMP views.             |
| <b>snmp-server trap authentication vrf</b> | Controls VRF-specific SNMP authentication failure notifications.                       |
| <b>snmp-server user</b>                    | Configures a new user to an SNMP group.                                                |

# snmp get

To retrieve Simple Network Management Protocol (SNMP) object variables, use the **snmp get** command in privileged EXEC mode.

```
snmp get { v1 | v2c | v3 } ip-address [vrf vrf-name] community-string [retry number] [timeout seconds] oid oid-value
```

| Syntax Description            |                                                                                                                                                           |
|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>v1</b>                     | Specifies the use of the SNMPv1 security model for a get operation.                                                                                       |
| <b>v2c</b>                    | Specifies the use of the SNMPv2c security model for a get operation.                                                                                      |
| <b>v3</b>                     | Specifies the use of the SNMPv3 security model for a get operation.                                                                                       |
| <i>ip-address</i>             | IPv4 or IPv6 address of the SNMP host.                                                                                                                    |
| <b>vrf</b>                    | (Optional) Specifies the use of a Virtual Private Network (VPN) routing and forwarding (VRF) instance to send SNMP notifications.                         |
| <i>vrf-name</i>               | (Optional) Name or instance of a VPN VRF.                                                                                                                 |
| <i>community-string</i>       | SNMP community string. A community string functions like a password to access the SNMP entity. The string can consist of 1 to 32 alphanumeric characters. |
| <b>retry</b> <i>number</i>    | (Optional) Specifies the number of retries to consider during a get operation. The valid range is from 1 to 10.                                           |
| <b>timeout</b> <i>seconds</i> | (Optional) Specifies the interval of time between each attempt at a get operation, in seconds. The valid range is from 1 to 1000.                         |
| <b>oid</b>                    | Specifies the object identifier value of the variable to retrieve.                                                                                        |
| <i>oid-value</i>              | The object identifier value. For example, sysName.0 or 1.3.6.1.4.1.9.9.10.1.3.0.5.                                                                        |

**Command Default** No variables are retrieved by default.

**Command Modes** Privileged EXEC (#)

| Command History | Release     | Modification                                                    |
|-----------------|-------------|-----------------------------------------------------------------|
|                 | 12.2(33)SRC | This command was introduced.                                    |
|                 | 12.2(33)SXI | This command was integrated into Cisco IOS Release 12.2(33)SXI. |

**Usage Guidelines** The get requests are sent by the SNMP manager or the Network Management System (NMS) to retrieve SNMP object variables. The **snmp get** command is used to retrieve the exact object variable.

The community string for a get operation can be set to either of the following types:

- ro—Sets the read-only access to the SNMP entity. The default value for this community string is public.

- **rw**—Sets read-write access to the SNMP entity. The default value for this community string is **private**.

---

**Examples**

The following example shows how to send a get operation request for retrieving the sysName.0 variable by using SNMPv1:

```
Router# snmp get v1 10.16.2.8 public retry 2 timeout 60 oid sysName.0
```

```
SNMP Response: reqid 3, errstat 0, erridx 0  
system.1.0
```

---

**Related Commands**

| Command              | Description                                                                   |
|----------------------|-------------------------------------------------------------------------------|
| <b>snmp get-bulk</b> | Retrieves variables in bulk.                                                  |
| <b>snmp get-next</b> | Retrieves data about the lexicographical successor to the specified variable. |

# snmp get-bulk

To retrieve Simple Network Management Protocol (SNMP) MIB object variables in bulk, use the **snmp get-bulk** command in privileged EXEC mode.

**snmp get-bulk** { **v1** | **v2c** | **v3** } *ip-address* [**vrf** *vrf-name*] *community-string* [**retry** *number*] [**timeout** *seconds*] **non-repeaters** *number* **max-repetitions** *number* **oid** *oid-value* [*oid-1* *oid-n*]

| Syntax Description                   |  |                                                                                                                                                           |
|--------------------------------------|--|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>v1</b>                            |  | Specifies the use of the SNMPv1 security model for a getBulk operation.                                                                                   |
| <b>v2c</b>                           |  | Specifies the use of the SNMPv2c security model for a getBulk operation.                                                                                  |
| <b>v3</b>                            |  | Specifies the use of the SNMPv3 security model for a getBulk operation.                                                                                   |
| <i>ip-address</i>                    |  | IP address or IPv6 address of the SNMP host.                                                                                                              |
| <b>vrf</b>                           |  | (Optional) Specifies the use of a Virtual Private Network (VPN) routing and forwarding (VRF) instance to send SNMP notifications.                         |
| <i>vrf-name</i>                      |  | (Optional) Name or instance of a VPN VRF.                                                                                                                 |
| <i>community-string</i>              |  | SNMP community string. A community string functions like a password to access the SNMP entity. The string can consist of 1 to 32 alphanumeric characters. |
| <b>retry</b> <i>number</i>           |  | (Optional) Specifies the number of retries to consider during a getBulk operation. The valid range is from 1 to 10.                                       |
| <b>timeout</b> <i>seconds</i>        |  | (Optional) Specifies the interval of time between each attempt at a getBulk operation, in seconds. The valid range is from 1 to 1000.                     |
| <b>non-repeaters</b> <i>number</i>   |  | Specifies the number of objects that can be retrieved with a getNext operation.                                                                           |
| <b>max-repetitions</b> <i>number</i> |  | Specifies the maximum number of getNext attempts to make while the rest of the objects are retrieved.                                                     |
| <b>oid</b>                           |  | Specifies the object identifier value of the variable to retrieve.                                                                                        |
| <i>oid-value</i>                     |  | The object identifier value. For example, sysName.0 or 1.3.6.1.4.1.9.9.10.1.3.0.5.                                                                        |
| <i>oid-1</i> <i>oid-n</i>            |  | (Optional) The object identifier values for which the getNext attempts can be repeated.                                                                   |

**Command Default** Variables are not retrieved in bulk by default.

**Command Modes** Privileged EXEC (#)

| Command History | Release     | Modification                                                    |
|-----------------|-------------|-----------------------------------------------------------------|
|                 | 12.2(33)SRC | This command was introduced.                                    |
|                 | 12.2(33)SXI | This command was integrated into Cisco IOS Release 12.2(33)SXI. |

## Usage Guidelines

For getBulk operation, if you specify 1 as the value for the **non-repeaters** keyword, the first OID value specified in the command syntax is not repeated at the getNext operation. In other words, a simple getNext operation is performed to retrieve this variable. The **max-repetition** keyword specifies the number of getNext attempts to make while the remaining object variables are retrieved. If the **max-repetitions** keyword value is specified as 2, there will be two getNext attempts to retrieve the remaining variables.

For example, if the **non-repeaters** keyword is specified as 1 and variables to retrieve are specified as sysName.0, ifDescr, and ifName, a simple getNext operation is performed to retrieve the sysName.0 variable. The value specified for the **max-repetitions** keyword is used to determine the number of getNext attempts to make while the remaining object variables are retrieved.

The community string for a get-bulk operation can be set to either of the following types:

- ro—Sets the read-only access to the SNMP entity. The default value for this community string is public.
- rw—Sets read-write access to the SNMP entity. The default value for this community string is private.

## Examples

The following example shows how to send a getBulk operation request by using SNMPv2C:

```
Router# snmp get-bulk v2c 10.16.2.8 public retry 2 timeout 60 non-repeaters 1  
max-repetitions 2 oid sysName.0 ifDescr ifName
```

## Related Commands

| Command                      | Description                                                          |
|------------------------------|----------------------------------------------------------------------|
| <b>snmp get</b>              | Retrieves SNMP MIB object variables.                                 |
| <b>snmp-server community</b> | Sets the community access string to enable access to an SNMP entity. |

# snmp get-next

To retrieve data about the lexicographical successor to the specified Simple Network Management Protocol (SNMP) object variable, use the **snmp get-next** command in privileged EXEC mode.

**snmp get-next** { **v1** | **v2c** | **v3** } *ip-address* [**vrf** *vrf-name*] *community-string* [**retry** *number*] [**timeout** *seconds*] **oid** *oid-value*

| Syntax Description            |                                                                                                                                                           |
|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>v1</b>                     | Specifies the use of the SNMPv1 security model for a getNext operation.                                                                                   |
| <b>v2c</b>                    | Specifies the use of the SNMPv2c security model for a getNext operation.                                                                                  |
| <b>v3</b>                     | Specifies the use of the SNMPv3 security model for a getNext operation.                                                                                   |
| <i>ip-address</i>             | IPv4 or IPv6 address of the SNMP host.                                                                                                                    |
| <b>vrf</b>                    | (Optional) Specifies the use of a Virtual Private Network (VPN) routing and forwarding (VRF) instance to send SNMP notifications.                         |
| <i>vrf-name</i>               | (Optional) Name or instance of a VPN VRF.                                                                                                                 |
| <i>community-string</i>       | SNMP community string. A community string functions like a password to access the SNMP entity. The string can consist of 1 to 32 alphanumeric characters. |
| <b>retry</b> <i>number</i>    | (Optional) Specifies the number of retries to consider during a getNext operation. The valid range is from 1 to 10.                                       |
| <b>timeout</b> <i>seconds</i> | (Optional) Specifies the interval of time between each attempt at a getNext operation, in seconds. The valid range is from 1 to 1000.                     |
| <b>oid</b>                    | Specifies the object identifier value of the variable to retrieve.                                                                                        |
| <i>oid-value</i>              | The object identifier value. For example, sysName.0 or 1.3.6.1.4.1.9.9.10.1.3.0.5.                                                                        |

**Command Default** No variables are retrieved by default.

**Command Modes** Privileged EXEC (#)

| Command History | Release     | Modification                                                    |
|-----------------|-------------|-----------------------------------------------------------------|
|                 | 12.2(33)SRC | This command was introduced.                                    |
|                 | 12.2(33)SXI | This command was integrated into Cisco IOS Release 12.2(33)SXI. |

**Usage Guidelines** With the **snmp get-next** command, the Network Management System (NMS) can request data about the variable, which is a lexicographical successor to the specified variable.

The community string for the get-next operation can be set to either of the following types:

- ro—Sets the read-only access to the SNMP entity. The default value for this community string is public.

- **rw**—Sets read-write access to the SNMP entity. The default value for this community string is **private**.

## Examples

The following example shows how to send a get-next operation request for retrieving the variable, which is a lexicographical successor to the ifStackStatus.0 variable, by using SNMPv2c:

```
Router# snmp get-next v2c 10.16.2.8 public retry 2 timeout 60 oid ifStackStatus.0
```

```
SNMP Response: reqid 11, errstat 0, erridx 0
ifStackStatus.0.1 = 1
```

## Related Commands

| Command              | Description                              |
|----------------------|------------------------------------------|
| <b>snmp get</b>      | Retrieves SNMP object variables.         |
| <b>snmp get-bulk</b> | Retrieves SNMP object variables in bulk. |

# snmp ifindex clear

To clear previously configured Simple Network Management Protocol (SNMP) ifIndex commands issued for a specific interface or a specific service instance, use the **snmp ifindex clear** command in either interface configuration mode or service instance configuration mode. This command does not have a **no** form.

## snmp ifindex clear

### Syntax Description

This command has no arguments or keywords.

### Command Default

ifIndex values are not cleared.

### Command Modes

Interface configuration (config-if)  
Service instance configuration (config-if-srv)

### Command History

| Release      | Modification                                                                                                    |
|--------------|-----------------------------------------------------------------------------------------------------------------|
| 12.0(11)S    | This command was introduced.                                                                                    |
| 12.1(5)T     | This command was integrated into Cisco IOS Release 12.1(5)T.                                                    |
| 12.2(14)SX   | Support for this command was introduced on the Supervisor Engine 720.                                           |
| 12.2(17d)SXB | Support for this command was introduced on the Supervisor Engine 2.                                             |
| 12.2(33)SRA  | This command was integrated into Cisco IOS Release 12.2(33)SRA.                                                 |
| 12.2(33)SRD1 | Support for this command was extended to service instance configuration mode in Cisco IOS Release 12.2(33)SRD1. |

### Usage Guidelines

Interface Index Persistence means that ifIndex values in the IF-MIB persist across reboots, allowing for consistent identification of specific interfaces using SNMP.

Use the **snmp ifindex clear** command on a specific interface when you want that interface to use the global configuration setting for ifIndex persistence. This command clears all ifIndex configuration commands previously entered for that specific interface.

When you clear the ifIndex configuration, the ifIndex persistence is enabled for all interfaces as specified by the **snmp-server ifindex persist** command in global configuration mode.

### Examples

The following example shows how to enable ifIndex persistence for all interfaces:

```
Router(config)# snmp-server ifindex persist
```

The following example shows how to disable IfIndex persistence for Ethernet interface 0/1:

```
Router(config)# interface ethernet 0/1
Router(config-if)# no snmp ifindex persist
Router(config-if)# exit
```

The following example shows how to clear ifIndex persistence for service instance 100 on Ethernet interface 0/1:

```
Router(config)# interface ethernet 0/1
Router(config-if)# service instance 100 ethernet
Router(config-if-srv)# snmp ifindex clear
Router(config-if-srv)# exit
```

The following example shows how to clear the ifIndex configuration from Ethernet interface 0/1:

```
Router(config)# interface ethernet 0/1
Router(config-if)# snmp ifindex clear
Router(config-if)# exit
```

The ifIndex persistence configuration is now enabled for all interfaces, as specified by the **snmp-server ifindex persist** global configuration command.

#### Related Commands

| Command                            | Description                                                                                                                           |
|------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| <b>snmp ifindex persist</b>        | Enables ifIndex values in the Interfaces MIB (IF-MIB) that persist across reboots (ifIndex persistence) only on a specific interface. |
| <b>snmp-server ifindex persist</b> | Enables ifIndex values that will remain constant across reboots for use by SNMP.                                                      |

# snmp ifindex persist

To enable ifIndex values in the Interfaces MIB (IF-MIB) that persist across reboots (ifIndex persistence) on a specific interface or service instance, use the **snmp ifindex persist** command in either interface configuration mode or service instance configuration mode. To disable ifIndex persistence on a specific interface or service instance, use the **no** form of this command.

**snmp ifindex persist**

**no snmp ifindex persist**

**Syntax Description** This command has no arguments or keywords.

**Command Default** This command is disabled.

**Command Modes** Interface configuration (config-if)  
Service instance configuration (config-if-srv)

| Command History | Release      | Modification                                                                                                    |
|-----------------|--------------|-----------------------------------------------------------------------------------------------------------------|
|                 | 12.0(11)S    | This command was introduced.                                                                                    |
|                 | 12.1(5)T     | This command was integrated into Cisco IOS Release 12.1(5)T.                                                    |
|                 | 12.2(14)SX   | Support for this command was introduced on the Supervisor Engine 720.                                           |
|                 | 12.2(17d)SXB | Support for this command on the Supervisor Engine 2 was extended to 12.2(17d)SXB.                               |
|                 | 12.2(33)SRA  | This command was integrated into Cisco IOS Release 12.2(33)SRA.                                                 |
|                 | 12.2(33)SRD1 | Support for this command was extended to service instance configuration mode in Cisco IOS Release 12.2(33)SRD1. |

**Usage Guidelines** Interface Index Persistence means that ifIndex values in the IF-MIB persist across reboots, allowing for consistent identification of specific interfaces using Simple Network Management Protocol (SNMP).

The **snmp ifindex persist** command in interface configuration mode enables and disables ifIndex persistence for individual entries (corresponding to individual interfaces) in the ifIndex table of the IF-MIB.

The **snmp ifindex persist** command in service instance configuration mode enables and disables ifIndex persistence for individual service instances (Layer 2 VLAN interfaces) in the ifIndex table of the IF-MIB.

The **snmp-server ifindex persist** command in global configuration mode enables and disables ifIndex persistence for all interfaces on the routing device that have ifDescr and ifIndex entries in the ifIndex table of the IF-MIB.

IfIndex commands configured for an interface apply to all subinterfaces on that interface.

---

**Examples**

In the following example, ifIndex persistence is enabled for Ethernet interface 0/1 only:

```
Router(config)# interface ethernet 0/1
Router(config-if)# snmp ifindex persist
Router(config-if)# exit
```

In the following example, ifIndex persistence is enabled for all interfaces and then disabled for Ethernet interface 0/1 only:

```
Router(config)# snmp-server ifindex persist
Router(config)# interface ethernet 0/1
Router(config-if)# no snmp ifindex persist
Router(config-if)# exit
```

In the following example, ifIndex persistence is enabled for service instance 100 on Ethernet interface 0/1:

```
Router(config)# interface ethernet 0/1
Router(config-if)# service instance 100 ethernet
Router(config-if-srv)# snmp ifindex persist
Router(config-if-srv)# exit
```

---

**Related Commands**

| Command                            | Description                                                                                      |
|------------------------------------|--------------------------------------------------------------------------------------------------|
| <b>snmp ifindex clear</b>          | Clears previously configured SNMP ifIndex commands for a specific interface or service instance. |
| <b>snmp-server ifindex persist</b> | Enables ifIndex values that will remain constant across reboots for use by SNMP.                 |

# snmp ifmib ifalias long

To configure the system to handle IfAlias descriptions of up to 256 characters, use the **snmp ifmib ifalias long** command in global configuration mode. To limit the IfAlias description to 64 characters, use the **no** form of this command.

**snmp ifmib ifalias long**

**no snmp ifmib ifalias long**

**Syntax Description** This command has no arguments or keywords.

**Command Default** The ifAlias description is limited to 64 characters.

**Command Modes** Global configuration

| Command History | Release    | Modification                                                   |
|-----------------|------------|----------------------------------------------------------------|
|                 | 12.2(2)T   | This command was introduced.                                   |
|                 | 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |

**Usage Guidelines**

The ifAlias object (ifXEntry 18) of the Interfaces MIB (IF-MIB) is called the Interface Alias. The Interface Alias (ifAlias) is a user-specified description of an interface used for Simple Network Management Protocol (SNMP) network management. The ifAlias is an object in the Interfaces Group MIB (IF-MIB) which can be set by a network manager to “name” an interface.

The ifAlias value for an interface or subinterface can be set using the **description** command in interface configuration mode or subinterface configuration mode, or by using a Set operation from an NMS. Prior to the introduction of this command, ifAlias descriptions for subinterfaces were limited to 64 characters. (The OLD-CISCO-INTERFACES-MIB allows up to 255 characters for the locIfDescr MIB variable, but this MIB does not support subinterfaces.) IfAlias descriptions appear in the output of the **show interfaces** command in EXEC mode, and in the output of the **more system: running-config** or **show running-config** commands in EXEC mode.

**Examples**

In the following example, the system is configured to retain and return ifAlias values of up to 256 characters in length:

```
Router(config)# snmp ifmib ifalias long
```

| Related Commands | Command                            | Description                                                                                                                           |
|------------------|------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
|                  | <b>description</b>                 | Allows you to specify a description for the specified interface in human-readable form.                                               |
|                  | <b>show snmp mib</b>               | Displays a list of the MIB module instance identifiers (OIDs) registered on your system.                                              |
|                  | <b>show snmp mib ifmib ifindex</b> | Displays SNMP Interface Index identification numbers (ifIndex values) for all the system interfaces or the specified system interface |

# snmp inform

To send inform requests to the host address configured for Simple Network Management Protocol (SNMP) notifications, use the **snmp inform** command in privileged EXEC mode.

**snmp inform** {**v1** | **v2c** | **v3**} *ip-address* [**vrf** *vrf-name*] *community-string* [**retry** *number*] [**timeout** *seconds*] **trap-oid** *trap-oid* **oid** *oid-value* *oid-type* *oid-type-value*

| Syntax Description            |  |                                                                                                                                                           |
|-------------------------------|--|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>v1</b>                     |  | Specifies the use of the SNMPv1 security model to send inform requests.<br><b>Note</b> SNMPv1 does not support receiving or sending inform requests.      |
| <b>v2c</b>                    |  | Specifies the use of the SNMPv2c security model to send inform requests.                                                                                  |
| <b>v3</b>                     |  | Specifies the use of the SNMPv3 security model to send inform requests.                                                                                   |
| <i>ip-address</i>             |  | IPv4 or IPv6 address of the SNMP host.                                                                                                                    |
| <b>vrf</b>                    |  | (Optional) Specifies the use of a Virtual Private Network (VPN) routing and forwarding (VRF) instance to send SNMP notifications.                         |
| <i>vrf-name</i>               |  | (Optional) Name or instance of a VPN VRF.                                                                                                                 |
| <i>community-string</i>       |  | SNMP community string. A community string functions like a password to access the SNMP entity. The string can consist of 1 to 32 alphanumeric characters. |
| <b>retry</b> <i>number</i>    |  | (Optional) Specifies the number of retries to consider while an inform request is sent. The valid range is from 1 to 10.                                  |
| <b>timeout</b> <i>seconds</i> |  | (Optional) Specifies the interval of time between each attempt at sending an inform request, in seconds. The valid range is from 1 to 1000.               |
| <b>trap-oid</b>               |  | Specifies the object identifier value of the object generating the inform request.                                                                        |
| <i>trap-oid</i>               |  | The object identifier value of the object generating the inform request.                                                                                  |
| <b>oid</b>                    |  | Specifies the object identifier value of the object that generates the inform request.                                                                    |
| <i>oid-value</i>              |  | The object identifier value. For example, sysName.0 or 1.3.6.1.4.1.9.9.10.1.3.0.5.                                                                        |

|                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>oid-type</i>       | <p>The type of OID. The following values are valid:</p> <ul style="list-style-type: none"> <li>• <b>counter</b>—A 32-bit number with a minimum value of 0. When the maximum value is reached, the counter resets to 0.</li> <li>• <b>gauge</b>—A 32-bit number with a minimum value of 0. For example, the interface speed on a router is measured using a gauge object type.</li> <li>• <b>integer</b>—A 32-bit number used to specify a numbered type within the context of a managed object. For example, to set the operational status of a router interface, 1 represents up and 2 represents down.</li> <li>• <b>ip-address</b>—IP address.</li> <li>• <b>string</b>—An octet string in text notation used to represent text strings.</li> <li>• <b>timeticks</b>—Specifies a value based on time ticks. Time ticks represents an integer value that specifies the elapsed time between two events, in units of hundredth of a second.</li> </ul> |
| <i>oid-type-value</i> | <p>Integer or text string value of the OID type specified for the SNMP set operation. The following list describes the integer or text string values that are valid with each <i>oid-type</i> argument value:</p> <ul style="list-style-type: none"> <li>• <b>counter</b>—Integer value in the range from 0 to 4294967295.</li> <li>• <b>gauge</b>—Integer value in the range from 0 to 4294967295.</li> <li>• <b>integer</b>—Integer value in the range from 0 to 4294967295.</li> <li>• <b>ip-address</b>—IP address in dotted decimal notation.</li> <li>• <b>string</b>—Text string.</li> <li>• <b>timeticks</b>—Integer value in the range from 0 to 4294967295.</li> </ul>                                                                                                                                                                                                                                                                        |

**Command Default** No SNMP inform requests are sent by default.

**Command Modes** Privileged EXEC (#)

| Command History | Release     | Modification                                                    |
|-----------------|-------------|-----------------------------------------------------------------|
|                 | 12.2(33)SRC | This command was introduced.                                    |
|                 | 12.2(33)SXI | This command was integrated into Cisco IOS Release 12.2(33)SXI. |

**Usage Guidelines** SNMP inform requests are the SNMP notifications that alert the SNMP manager to a network condition and request confirmation of receipt from the SNMP manager.

The community string for sending inform requests can be set to either of the following types:

- **ro**—Sets the read-only access to the SNMP entity. The default value for this community string is public.
- **rw**—Sets read-write access to the SNMP entity. The default value for this community string is private.

## Examples

The following example shows how to send an inform request using SNMPv2c:

```
Router# snmp inform v2c 10.16.2.8 public retry 2 timeout 60 trap-oid system.2.0 oid  
sysUpTime.0 counter 20
```

```
SNMP: Inform request, reqid 24, errstat 0, erridx 0  
sysUpTime.0 = 10244391  
snmpTrapOID.0 = ciscoConfigManMIB.2.0.1  
ccmHistoryEventEntry.3.40 = 1
```

## Related Commands

| Command                         | Description                                                            |
|---------------------------------|------------------------------------------------------------------------|
| <b>snmp-server community</b>    | Sets the community access string to enable access to the SNMP entity.  |
| <b>snmp-server enable traps</b> | Enables all SNMP notification types that are available on your system. |
| <b>snmp-server host</b>         | Specifies the recipient of an SNMP notification operation.             |

# snmp mib bulkstat object-list

To configure a Simple Network Management Protocol (SNMP) bulk statistics object list, use the **snmp mib bulkstat object-list** command in global configuration mode. To remove an SNMP bulk statistics object list, use the **no** form of this command.

**snmp mib bulkstat object-list** *name*

**no snmp mib bulkstat object-list** *name*

## Syntax Description

|             |                                           |
|-------------|-------------------------------------------|
| <i>name</i> | Name of the object list to be configured. |
|-------------|-------------------------------------------|

## Command Default

No SNMP bulk statistics object list is configured.

## Command Modes

Global configuration (config)

## Command History

| Release                  | Modification                                                    |
|--------------------------|-----------------------------------------------------------------|
| 12.0(24)S                | This command was introduced.                                    |
| 12.3(2)T                 | This command was integrated into Cisco IOS Release 12.3(2)T.    |
| 12.2(25)S                | This command was integrated into Cisco IOS Release 12.2(25)S.   |
| 12.2(33)SRA              | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(33)SXH              | This command was integrated into Cisco IOS Release 12.2(33)SXH. |
| 12.2(33)SB               | This command was integrated into Cisco IOS Release 12.2(33)SB.  |
| Cisco IOS XE Release 2.1 | This command was integrated into Cisco IOS Release XE 2.1.      |

## Usage Guidelines

The **snmp mib bulkstat object-list** command allows you to name an object list. Bulk statistics object lists are used for the Periodic MIB Data Collection and Transfer Mechanism.

After you enter this command, the router enters Bulk Statistics Object List configuration mode, in which you can use the **add** command to add specific MIB objects to the list.

Bulk statistics object lists can be reused in multiple schemas.

## Examples

In the following example, a bulk statistics object list called ifMib is configured to include the ifInoctets, ifOutoctets, ifInUcastPkts, and ifInDiscards objects from the Interfaces Group MIB (IF-MIB):

```
Router(config)# snmp mib bulkstat object-list ifmib
Router(config-bulk-objects)# add ifInoctets
Router(config-bulk-objects)# add ifOutoctets
Router(config-bulk-objects)# add ifInUcastPkts
Router(config-bulk-objects)# add ifInDiscards
Router(config-bulk-objects)# end
```

**Related Commands**

| Command                         | Description                                                                                |
|---------------------------------|--------------------------------------------------------------------------------------------|
| <b>add</b>                      | Adds specific MIB objects to a defined SNMP bulk statistics object list.                   |
| <b>snmp mib bulkstat schema</b> | Names an SNMP bulk statistics schema and enters Bulk Statistics Schema configuration mode. |

# snmp mib bulkstat schema

To define a bulk statistics schema, use the **snmp mib bulkstat schema** command in global configuration mode. To delete a previously configured bulk statistics schema, use the **no** form of this command.

**snmp mib bulkstat schema** *schema-name*

**no snmp mib bulkstat schema** *schema-name*

|                           |                    |                                                      |
|---------------------------|--------------------|------------------------------------------------------|
| <b>Syntax Description</b> | <i>schema-name</i> | Name of the bulk statistics schema to be configured. |
|---------------------------|--------------------|------------------------------------------------------|

|                        |                         |
|------------------------|-------------------------|
| <b>Command Default</b> | No schemas are defined. |
|------------------------|-------------------------|

|                      |                               |
|----------------------|-------------------------------|
| <b>Command Modes</b> | Global configuration (config) |
|----------------------|-------------------------------|

| <b>Command History</b> | <b>Release</b>           | <b>Modification</b>                                             |
|------------------------|--------------------------|-----------------------------------------------------------------|
|                        | 12.0(24)S                | This command was introduced.                                    |
|                        | 12.3(2)T                 | This command was integrated into Cisco IOS Release 12.3(2)T.    |
|                        | 12.2(25)S                | This command was integrated into Cisco IOS Release 12.2(25)S.   |
|                        | 12.2(33)SRA              | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
|                        | 12.2(33)SXH              | This command was integrated into Cisco IOS Release 12.2(33)SXH. |
|                        | 12.2(33)SB               | This command was integrated into Cisco IOS Release 12.2(33)SB.  |
|                        | Cisco IOS XE Release 2.1 | This command was integrated into Cisco IOS Release XE 2.1.      |

|                         |                                                                                                                                                                                                                                                             |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Usage Guidelines</b> | The <b>snmp mib bulkstat schema</b> command names the schema and enters Bulk Statistics Schema configuration mode. Bulk Statistics Schema configuration mode is used to configure the object list, instance, and polling interval to be used in the schema. |
|                         | The specific instances of MIB objects for which data should be collected are determined by appending the value of the <b>instance</b> command to the objects specified in the object list.                                                                  |
|                         | Multiple schemas can be associated with a single bulk statistics file when configuring the bulk statistics transfer options.                                                                                                                                |

|                 |                                                                                                |
|-----------------|------------------------------------------------------------------------------------------------|
| <b>Examples</b> | The following example shows the configuration of a bulk statistics schema called ATM2/0-IFMIB: |
|-----------------|------------------------------------------------------------------------------------------------|

```
Router(config)# snmp mib bulkstat schema ATM2/0-IFMIB
Router(config-bulk-sc)# object-list ifmib
Router(config-bulk-sc)# poll-interval 5
Router(config-bulk-sc)# instance exact interface ATM2/0 subif
Router(config-bulk-sc)# exit
```

**Related Commands**

| <b>Command</b>                    | <b>Description</b>                                                                                                                               |
|-----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>instance</b>                   | Specifies the instance that, when appended to the object list, gives the OID of the object instance to be monitored in a bulk statistics schema. |
| <b>object-list</b>                | Adds specific MIB objects to a defined SNMP bulk statistics object list.                                                                         |
| <b>poll-interval</b>              | Configures the polling interval for a bulk statistics schema.                                                                                    |
| <b>snmp mib bulkstat transfer</b> | Names a bulk statistics transfer configuration and enters Bulk Statistics Transfer configuration mode.                                           |

# snmp mib bulkstat transfer

To identify the bulk statistics transfer configuration and enter Bulk Statistics Transfer configuration mode, use the **snmp mib bulkstat transfer** command in global configuration mode. To remove a previously configured transfer, use the **no** form of this command.

**snmp mib bulkstat transfer** *transfer-id*

**no snmp mib bulkstat transfer** *transfer-id*

## Syntax Description

|                    |                                     |
|--------------------|-------------------------------------|
| <i>transfer-id</i> | Name of the transfer configuration. |
|--------------------|-------------------------------------|

## Command Default

No bulk statistics transfer configuration exists.

## Command Modes

Global configuration (config)

## Command History

| Release                  | Modification                                                    |
|--------------------------|-----------------------------------------------------------------|
| 12.0(24)S                | This command was introduced.                                    |
| 12.3(2)T                 | This command was integrated into Cisco IOS Release 12.3(2)T.    |
| 12.2(25)S                | This command was integrated into Cisco IOS Release 12.2(25)S.   |
| 12.2(33)SRA              | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(33)SXH              | This command was integrated into Cisco IOS Release 12.2(33)SXH. |
| 12.2(33)SB               | This command was integrated into Cisco IOS Release 12.2(33)SB.  |
| Cisco IOS XE Release 2.1 | This command was integrated into Cisco IOS Release XE 2.1.      |

## Usage Guidelines

The name (*transfer-id*) you specify for the bulk statistics transfer configuration is used in the filename of the bulk statistics file when it is generated and is used to identify the transfer configuration in the output of the **show snmp mib bulkstat transfer** command.

This command enters Bulk Statistics Transfer configuration mode, as indicated by the prompt (config-bulk-tr).

## Examples

In the following example, the transfer configuration is given the name bulkstat1 and is configured to include the schemas ATM2/0-IFMIB and ATM2/0-CAR:

```
Router(config)# snmp mib bulkstat transfer bulkstat1
Router(config-bulk-tr)# schema ATM2/0-IFMIB
Router(config-bulk-tr)# schema ATM2/0-CAR
Router(config-bulk-tr)# url primary ftp://user1:pswrd@cbin2-host/users/user1/bulkstat1
Router(config-bulk-tr)# url secondary tftp://user1@10.1.0.1/tftpboot/user1/bulkstat1
Router(config-bulk-tr)# format schemaASCII
Router(config-bulk-tr)# transfer-interval 30
Router(config-bulk-tr)# retry 5
```

```
Router(config-bulk-tr)# buffer-size 1024  
Router(config-bulk-tr)# retain 30  
Router(config-bulk-tr)# end  
Router# copy running-config startup-config
```

**Related Commands**

| Command                                | Description                                                                                                 |
|----------------------------------------|-------------------------------------------------------------------------------------------------------------|
| <b>show snmp mib bulkstat transfer</b> | Displays the transfer status of files generated by the Periodic MIB Data Collection and Transfer Mechanism. |

## snmp mib community-map

To associate a Simple Network Management Protocol (SNMP) community with an SNMP context, engine ID, or security name, use the **snmp mib community-map** command in global configuration mode. To change an SNMP community mapping to its default mapping, use the **no** form of this command.

**snmp mib community-map** *community-name* [**context** *context-name*] [**engineid** *engine-id*] [**security-name** *security-name*] [**target-list** *vpn-list-name*]

**no snmp mib community-map** *community-name* [**context** *context-name*] [**engineid** *engine-id*] [**security-name** *security-name*] [**target-list** *vpn-list-name*]

| Syntax Description    |  |                                                                                                                  |
|-----------------------|--|------------------------------------------------------------------------------------------------------------------|
| <i>community-name</i> |  | String that identifies the SNMP community.                                                                       |
| <b>context</b>        |  | (Optional) Specifies that an SNMP context name is mapped to the SNMP community.                                  |
| <i>context-name</i>   |  | (Optional) String that identifies the name of the SNMP context.                                                  |
| <b>engineid</b>       |  | (Optional) Specifies that an SNMP engine ID is mapped to the SNMP community.                                     |
| <i>engine-id</i>      |  | (Optional) String that identifies the SNMP engine ID. Default is the local engine ID                             |
| <b>security-name</b>  |  | (Optional) Specifies that a security name is mapped to the SNMP community.                                       |
| <i>security-name</i>  |  | (Optional) String that identifies the SNMP security name. Default is the community name                          |
| <b>target-list</b>    |  | (Optional) Specifies that a VPN routing and forwarding (VRF) list is mapped to the SNMP community.               |
| <i>vpn-list-name</i>  |  | (Optional) String value that should correspond to the list name used in the <b>snmp mib target list</b> command. |

**Command Default** No SNMP communities and contexts are associated.

**Command Modes** Global configuration (config)

| Command History | Release     | Modification                                                    |
|-----------------|-------------|-----------------------------------------------------------------|
|                 | 12.0(23)S   | This command was introduced.                                    |
|                 | 12.3(2)T    | This command was integrated into Cisco IOS Release 12.3(2)T.    |
|                 | 12.2(25)S   | This command was integrated into Cisco IOS Release 12.2(25)S.   |
|                 | 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
|                 | 12.2(31)SB2 | This command was integrated into Cisco IOS Release 12.2(31)SB2. |
|                 | 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |

| Release    | Modification                                                                                                                                                                      |
|------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 12.2SX     | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 12.2(33)SB | This command was integrated into Cisco IOS Release 12.2(33)SB.                                                                                                                    |

### Usage Guidelines

Use this command to create a mapping between an SNMP community and an SNMP context, engine ID, or security name that is different from the default settings.

Use the **snmp-server community** command to configure an SNMP community. When an SNMP community is associated with an SNMP context and a request is made from this community, the request is applied to the context. You also can use the **snmp mib community-map** command to specify the source address validation for an SNMP community by associating a list of target VRFs. The target VRF list specifies the valid host or hosts for this SNMP community.

### Examples

The following example shows how to create an SNMP community named community1 and associate it with an SNMP context named context1:

```
Router(config)# snmp-server community community1
Router(config)# snmp mib community-map community1 context context1
```

The following example shows a mapping of community A (commA) to VPN list commAvpn and community B (commB) to VPN list commBvpn:

```
Router(config)# snmp mib community-map commA context A target-list commAvpn
Router(config)# snmp mib community-map commB context B target-list commBvpn
Router(config)# snmp mib target list commAvpn vrf CustomerA
Router(config)# snmp mib target list commBvpn vrf CustomerB
```

### Related Commands

| Command                      | Description                                                       |
|------------------------------|-------------------------------------------------------------------|
| <b>context</b>               | Associates an SNMP context with a particular VPN.                 |
| <b>snmp-server community</b> | Sets up the community access string to permit access to the SNMP. |

# snmp mib event object list

To configure a list of objects for an event, use the **snmp mib event object list** command in global configuration mode. To disable an object list, use the **no** form of this command.

**snmp mib event object list owner** *object-list-owner* **name** *object-list-name* *object-number*

**no snmp mib event object list owner** *object-list-owner* **name** *object-list-name* *object-number*

## Syntax Description

|                          |                                                                                                                    |
|--------------------------|--------------------------------------------------------------------------------------------------------------------|
| <b>owner</b>             | Specifies the object list owner.                                                                                   |
| <i>object-list-owner</i> | Name of the object list owner.                                                                                     |
| <b>name</b>              | Indicates the name of the object list.                                                                             |
| <i>object-list-name</i>  | Unique name that identifies the object list.                                                                       |
| <i>object-number</i>     | Number used to identify the object list. Two object lists can have the same name, but the object number is unique. |

## Command Default

No object list is configured for an event.

## Command Modes

Global configuration (config)

## Command History

| Release                   | Modification                                                    |
|---------------------------|-----------------------------------------------------------------|
| 12.4(20)T                 | This command was introduced.                                    |
| 12.2(33)SRE               | This command was integrated into Cisco IOS Release 12.2(33)SRE. |
| Cisco IOS XE Release 3.1S | This command was integrated into Cisco IOS XE Release 3.1S.     |

## Examples

The following example shows how to configure an object list:

```
Router(config-event)# snmp mib event object list owner owner1 name objectA 10
Router(config-event-objlist)#
```

## Related Commands

| Command                       | Description                                                      |
|-------------------------------|------------------------------------------------------------------|
| <b>snmp mib event trigger</b> | Specifies a trigger owner during an event trigger configuration. |
| <b>test</b>                   | Configures parameters for trigger test.                          |

# snmp mib event owner

To specify an owner for a management event, use the **snmp mib event owner** command in global configuration mode. To disable the configuration and set the default parameters, use the **no** form of this command.

**snmp mib event owner** *event-owner* **name** *event-name*

**no snmp mib event owner** *event-owner* **name** *event-name*

## Syntax Description

|                    |                                 |
|--------------------|---------------------------------|
| <i>event-owner</i> | Name of the event owner.        |
| <b>name</b>        | Indicates the name of an event. |
| <i>event-name</i>  | Name of an event.               |

## Command Default

By default, no event is configured.

## Command Modes

Global configuration (config)

## Command History

| Release                   | Modification                                                    |
|---------------------------|-----------------------------------------------------------------|
| 12.4(20)T                 | This command was introduced.                                    |
| 12.2(33)SRE               | This command was integrated into Cisco IOS Release 12.2(33)SRE. |
| Cisco IOS XE Release 3.1S | This command was integrated into Cisco IOS XE Release 3.1S.     |

## Usage Guidelines

The **snmp mib event owner** command configures management event information such as event owner and name. Events are identified by event owners and names. This command enables you to enter the event configuration mode and associate objects with events.

## Examples

The following example shows how to specify an event owner:

```
Router(config)# snmp mib event owner owner1 name eventA
Router(config-event)#
```

# snmp mib event sample

To set a value for scalar object sampling, use the **snmp mib event sample** command in global configuration mode. To reset the values, use the **no** form of this command.

**snmp mib event sample** {instance maximum | minimum} *value*

**no snmp mib event sample** {instance maximum | minimum}

## Syntax Description

|                 |                                                                                                                                                                                                                                          |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>instance</b> | Specifies the scalar object instance sampled for an event.                                                                                                                                                                               |
| <b>maximum</b>  | Specifies the maximum value to set for scalar object sampling.                                                                                                                                                                           |
| <b>minimum</b>  | Specifies the minimum value to set for scalar object sampling.                                                                                                                                                                           |
| <i>value</i>    | Minimum or maximum value for sampling scalar objects configured for an event. <ul style="list-style-type: none"> <li>The range for maximum value is 0 to 4294967295.</li> <li>The range for minimum value is 1 to 2147483647.</li> </ul> |

## Command Default

No value is set for scalar object sampling.

## Command Modes

Global configuration (config)

## Command History

| Release                   | Modification                                                    |
|---------------------------|-----------------------------------------------------------------|
| 12.4(20)T                 | This command was introduced.                                    |
| 12.2(33)SRE               | This command was integrated into Cisco IOS Release 12.2(33)SRE. |
| Cisco IOS XE Release 3.1S | This command was integrated into Cisco IOS XE Release 3.1S.     |

## Examples

The following example shows how to set a minimum value for scalar object sampling:

```
Router(config)# snmp mib event sample minimum 10
Router(config)#
```