sample (event trigger) through snmp mib event sample

sample (event trigger)

To specify the type of object sampling to use for an event, use the **sample**command in event trigger configuration mode. To disable teh configured settings, use the **no** form of this command.

sample {**absolute**| **delta**| **changed**}

no sample {**absolute**| **delta**| **changed**}

Syntax Description

absolute	Uses the present value of the MIB object while sampling.
delta	Uses the difference between the present value and the previous value sampled at the previous interval for sampling.
changed	Uses the Boolean condition to check if the present value is different from the previous value.

Command Default

The default sampling method is absolute.

Command Modes

Event trigger configuration (config-event-trigger)

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.

Usage Guidelines

The **sample** command enables the specified sampling method for the object. You can specify the following sampling methods.

- Absolute
- Delta
- Changed

Absolute sampling uses the value of the MIB object during sampling. The default sampling method is absolute.

Delta sampling uses the last sampling value maintained in the application. This method requires applications to do continuous sampling.

The changed sampling method uses the changed value of the object since the last sample.

Examples

The following example shows how to specify the sampling method as absolute:

```
Router(config)# snmp mib event trigger owner owner1 name triggerA
Router(config-event-trigger)# sample absolute
```

Related Commands

Command	Description
snmp mib event trigger owner	Specifies owner for an event trigger.

sample (expression)

To specify the method of sampling an object, use the **sample** command in expression object configuration mode. To disable the specified method of object sampling, use the **no** form of this command.

sample {**absolute**| **delta**| **changed**}

no sample

Syntax Description

absolute	Uses the present value of the MIB object while sampling.
delta	Uses the difference between the present value and the previous value sampled at the previous interval for sampling.
changed	Uses a Boolean condition to check if the present value is different from the previous value.

Command Default

The default sampling method is absolute.

Command Modes

Expression object configuration (config-expression-object)

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.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.

Usage Guidelines

The Expression MIB allows you to create expressions based on a combination of objects. The expressions are evaluated according to the sampling method. The Expression MIB supports the following types of object sampling:

- Absolute
- Delta
- Changed

The **sample** command enables the specified sampling method for the object. If there are no delta or changed values in an expression, the expression is evaluated when a requester attempts to read the value of the expression. In this case, all requesters get a newly calculated value.

For expressions with delta or change values, the evaluation is performed for every sampling. In this case, requesters get the value as the last sample period.

Examples

The following example shows how to specify the sampling method as absolute:

```
Router(config)# snmp mib expression owner owner1 name expressionA
Router(config-expression)# object 32
Router(config-expression-object)# sample absolute
Router(config-expression-object)# end
```

Related Commands

Command	Description
snmp mib expression owner	Specifies the owner for an expression.

schema

To specify the bulk statistics schema to be used in a specific bulk statistics transfer configuration, use the **schema** command in Bulk Statistics Transfer configuration mode. To remove a previously configured schema from a specific bulk statistics transfer configuration, use the **no** form of this command.

schema *schema-name*

no schema *schema-name*

Syntax Description

schema-name	Name of a previously configured bulk statistics schema.

Command Default

No bulk statistics schema is specified.

Command Modes

Bulk Statistics Transfer configuration (config-bulk-tr)

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

Repeat this command as desired for a specific bulk statistics transfer configuration. Multiple schemas can be associated with a single transfer configuration; all collected data will be in a single bulk statistics data file (VFile).

Examples

In the following example, the bulk statistics schemas ATM2/0-IFMIB and ATM2/0-CAR are associated with the bulk statistics transfer configuration called bulkstat1:

```
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://user:pswrd@host/folder/bulkstat1
Router(config-bulk-tr)# retry 2
Router(config-bulk-tr)# retain 10
Router(config-bulk-tr)# exit
```

Related Commands

Command	Description
snmp mib bulkstat transfer	Names a bulk statistics transfer configuration and enters Bulk Statistics Transfer configuration mode.

show management event

To display the Simple Network Management Protocol (SNMP) Event values that have been configured on your routing device through the use of the Event MIB, use the **show management event** command in privileged EXEC mode.

show management event

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.1(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.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

The Event MIB allows you to configure your own traps, informs, or set operations through the use of an external network management application. The **show management event** command is used to display the values for the Events configured on your system. For information on Event MIB functionality, see RFC 2981, available at http://www.ietf.org .

Examples

The following example is sample output from the **show management event** command:

```
Router# show management event
Mgmt Triggers:
 (1): Owner: joe_user
  (1): 01, Comment: TestEvent, Sample: Abs, Freq: 120
      Test: Existence Threshold Boolean
         ObjectOwner: aseem, Object: sethi
         OID: ifEntry.10.3, Enabled 1, Row Status 1
      Existence Entry: , Absent, Changed
      StartUp:  Present, Absent
         ObjOwn: , Obj: , EveOwn: aseem, Eve: 09
      Boolean Entry:
         Value: 10, Cmp: 1, Start: 1
         ObjOwn: , Obj: , EveOwn: aseem, Eve: 09
      Threshold Entry:
         Rising: 50000, Falling: 20000
         ObjOwn: ase, Obj: 01 RisEveOwn: ase, RisEve: 09 , FallEveOwn: ase, FallEve: 09
```

```
      Delta Value Table:
  (0): Thresh: Rising, Exis: 1, Read: 0, OID: ifEntry.10.3 , val: 69356097
Mgmt Events:
 (1): Owner: aseem
   (1)Name: 09 , Comment: , Action: Set, Notify, Enabled: 1 Status: 1
      Notification Entry:
         ObjOwn: , Obj: , OID: ifEntry.10.1
      Set:
         OID: ciscoSyslogMIB.1.2.1.0, SetValue: 199, Wildcard: 2 TAG: , ContextName:
 Object Table:
 (1): Owner: aseem
   (1)Name: sethi, Index: 1, OID: ifEntry.10.1, Wild: 1, Status: 1
```

Related Commands

Command	Description
debug management event	Allows real-time monitoring of Event MIB activities for the purposes of debugging.

show management expression

To display the Simple Network Management Protocol (SNMP) Expression values that have been configured on your routing device through the use of the Expression MIB, use the **show management expression** command in user EXEC or privileged EXEC mode.

show management expression

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC Privileged EXEC (#)

Command History

Release	Modification
12.2(1)	This command was introduced in a release earlier than Cisco IOS Release 12.2(1).
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.
12.2SR	This command is supported in the Cisco IOS Release 12.2SR train. Support in a specific 12.2SR release of this train depends on your feature set, platform, and platform hardware.
12.2SB	This command is supported in the Cisco IOS Release 12.2SB train. Support in a specific 12.2SB Release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show management expression** command:

```
Router# show management expression
Expression: 1 is active
  Expression Owner: me
  Expression Name: me
  Expression to be evaluated is $1 + 100 where:
  $1 = ifDescr
  Object Condition is not set
  Sample Type is absolute
  ObjectID is wildcarded
```

The output is self-explanatory.

Related Commands

Command	Description
debug management expression	Monitors the activities of the Expression MIB in real time on your routing device.

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
```

The table below describes the significant fields shown in the display.

Table 1: show snmp Field Descriptions

Field	Description
Chassis	Chassis ID string.
SNMP packets input	Total number of SNMP packets input.
Bad SNMP version errors	Number of packets with an invalid SNMP version.
Unknown community name	Number of SNMP packets with an unknown community name.
Illegal operation for community name supplied	Number of packets requesting an operation not allowed for that community.
Encoding errors	Number of SNMP packets that were improperly encoded.
Number of requested variables	Number of variables requested by SNMP managers.
Number of altered variables	Number of variables altered by SNMP managers.
Get-request PDUs	Number of get requests received.
Get-next PDUs	Number of get-next requests received.
Set-request PDUs	Number of set requests received.
SNMP packets output	Total number of SNMP packets sent by the router.
Too big errors	Number of SNMP packets which were larger than the maximum packet size.
Maximum packet size	Maximum size of SNMP packets.

Field	Description
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.
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 **snmp-server queue-length** 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.

Field	Description
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

Command	Description
show snmp pending	Displays the current set of pending SNMP requests.
show snmp sessions	Displays the current SNMP sessions.
snmp-server chassis-id	Provides a message line identifying the SNMP server serial number.
snmp-server manager	Starts the SNMP manager process.
snmp-server manager session-timeout	Sets the amount of time before a nonactive session is destroyed.
snmp-server queue-length	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
show snmp	Displays SNMP communication details.
snmp-server chassis-id	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
```

The table below describes the significant fields shown in the display.

Table 2: 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
snmp-server community	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
snmp-server contact	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 00000090200000000C025808 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: 00000090200000000C025808
Remote Engine ID           IP-addr          Port
123456789ABCDEF000000000   172.16.37.61     162
```

The table below describes the fields shown in the display.

Table 3: 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.

Field	Definition
Port	The port number on the local device to which the remote device is connected.

Related Commands

Command	Description
snmp-server engineID local	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 v1default, the notify view name as *tv.FFFFFFFF, and the storage type as volatile:

```
Router# show snmp group
groupname: V1                             security model:v1
readview : v1default                      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 : v1default                      writeview: <no writeview specified>
notifyview: <no notifyview specified>
row status: active
```

The table below describes the fields shown in the example.

Table 4: 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. • For further information on the SNMP views, use the **show snmp view** command.
writeview	A string identifying the write view of the group.
notifyview	A string identifying the notify view of the group. The notify view indicates the group for SNMP notifications, and corresponds to the setting of the **snmp-server group** *group-name version* **notify** *notify-view* command.

Related Commands

Command	Description
snmp-server group	Configures a new SNMP group or a table that maps SNMP users to SNMP views.
show snmp user	Displays the configured characteristics for SNMP users.
show snmp view	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
```

The table below describes the significant fields shown in the display.

Table 5: 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.

Field	Description
user	Displays the access type of the user for which the notification is generated.
security model	Displays the SNMP version used to send notifications.
traps	Displays details of the notification generated.

Related Commands

Command	Description
snmp-server host	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
snmp-server location	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 OSIs 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
show snmp mib ifmib ifindex	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*]

Syntax Description

transfer-id	(Optional) Name of a specific bulk statistics transfer configuration. Use the *transfer-id* argument to display the status of a specific bulk statistics transfer configuration.

Command Default

If the optional *transfer-id* argument is not used, the status of all configured bulk statistics transfers is displayed.

Command Modes

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 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
```

The table below describes the significant fields shown in the output.

Table 6: show snmp mib bulkstat transfer Field Descriptions

Field	Description
Transfer Name	The name of the transfer configuration, specified in the **snmp mib bulkstat transfer** 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	The name of the bulk statistics file as it will appear after transfer. The filename of the file is generated using the following components: *transfer-name _device-name _date _time-stamp* The *transfer-name* is the name *s* pecified by the corresponding **snmp mib bulkstat transfer** command. The *device-name* is the name used in the command-line interface (CLI) router prompt. The format of the *date* and *time-stamp* 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.
Time Left (in seconds)	Indicates how much time is left before the specified file will be deleted (retention period), as specified with the **retain** Bulk Statistics Transfer configuration command. **Note** Regardless of the configured retention period, all retry attempts will be made before the file is deleted.

Field	Description
STATE	The state of the local bulk statistics file will be one of the following: • Queued--Collection time for this file is completed and the file is waiting for transfer to configured primary and secondary URL. • Retained--The file has been either successfully transferred to its destination or, if all transfer attempts have failed, all retry attempts have been completed. • 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.

Related Commands

Command	Description
snmp mib bulkstat transfer	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
context	Associates an SNMP context with a particular VRF.
snmp-server context	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 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

The **show snmp mib ifmib traps**command displays 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
```

The table below describes the fields shown in the display.

Table 7: 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
show snmp mib	Displays a list of the MIB OIDs registered on the system.
show snmp mib ifmib ifindex	Displays SNMP ifIndex identification numbers for all system interfaces or a specified system interface.
snmp -server enable traps	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]**

Syntax Description

type number	(Optional) Interface type and number. The table below lists the valid values for interface type and number.
detail	(Optional) Displays the trap status for all SNMP ifIndex identification numbers for the specified system interfaces.
free-list	(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 (#)

Command History

Release	Modification
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 **detail**and **free-list**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.

The table below shows the valid values for the *type* and *number*arguments.

Table 8: show snmp mib ifmib ifindex type and number

ifIndex Type	Description
atm	Asynchronous transfer mode interface; *number* is 0 to 7.
async	Asynchronous interface; *number* will vary by platform.
auto-template	Auto-Template interface; *number* is 1 to 999.
ctunnel	CTunnel interface; *number* is 0 to 2147483647.
dialer	Dialer interface; *number* is 0 to 255.
esconphy	Escon interface; *number* is 1 to 6.
ethernet	Ethernet interface; *number* is 0 to 15.
fastethernet	Fast Ethernet interface; *number* is 1 to 6.
fcpa	Fibre Channel Port Adapter interface; *number* is 1 to 6.
filter	Filter interface; *number*is 1 to 6.
filtergroup	Filter Group interface; *number* is 1 to 6.
gigabitethernet	Gigabit Ethernet interface; *number* is 1 to 6.
group-async	Asynchronous Group interface; *number* is 0 to 64.
lex	Lex interface; *number* is 0 to 2147483647.
longreachethernet	Long-Reach Ethernet interface; *number* is 1 to 6.
loopback	Loopback interface; *number* is 0 to 2147483647.
mfr	Multilink Frame Relay bundle interface; *number* is 0 to 2147483647.
multilink	Multilink-group interface; *number* is 1 to 2147483647.
null	Null interface; *number* is 0 to 0.
port-channel	Port-Channel interface; *number* is 1 to 496.
portgroup	Portgroup interface; *number* is 1 to 6.

ifIndex Type	Description
pos-channel	POS Channel interface; *number* is 1 to 4094.
serial	Serial interface; *number* is 0 to 15.
sysclock	SYSCLOCK interface; *number* is 1 to 6.
tunnel	Tunnel interface; *number* is 0 to 2147483647.
vif	Pragmatic General Multicast (PGM) Host interface; *number* is 0 to 1.
virtual-ppp	Virtual Point-to-Point interface; *number* is 1 to 2147483647.
virtual-template	Virtual Template interface; *number* is 1 to 200.
virtual-tokenring	Virtual Token Ring interface; *number* is 0 to 2147483647.
vlan	VLAN interface; *number* is 1 to 4094.
voabypassin	VOA-Bypass-In interface; *number* is 1 to 6.
voabypassout	VOA-Bypass-Out interface; *number* is 1 to 6.
voafilterin	VOA-Filter-In interface; *number* is 1 to 6.
voafilterout	VOA-Filter-Out interface; *number* is 1 to 6.
voain	VOA-In interface; *number*is 1 to 6.
voaout	VOA-Out interface; *number* 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
```

The table below describes the fields shown in the display.

Table 9: 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
show snmp mib	Displays a list of the MIB OIDs registered on the system.
snmp ifindex persist	Enables ifIndex values in the IF-MIB that persist across reboots only on a specific interface.
snmp ifmib ifalias long	Configures the system to handle IfAlias descriptions of up to 256 characters in length.
snmp-server ifindex persist	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

all	(Optional) Displays all notification log entries stored in the local Notification Log MIB database.
default	(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
snmp mib notification-log default	Creates and activates an SNMP Notification Log.
snmp mib notification-log globalageout	Sets the maximum age for a notification.
snmp mib notification-log globalsize	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
```

The table below describes the significant fields shown in the display.

Table 10: 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.

Field	Description
Expires in	Remaining time before request timeout expires.

Related Commands

Command	Description
show snmp	Checks the status of SNMP communications.
show snmp sessions	Displays the current SNMP sessions.
snmp-server manager	Starts the SNMP manager process.
snmp-server manager session-timeout	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)
```

The table below 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 11: 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
show snmp	Checks the status of SNMP communications.
show snmp pending	Displays the current set of pending SNMP requests.
snmp-server manager	Starts the SNMP manager process.
snmp-server manager session-timeout	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), including their time stamps and the number of times OIDs 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.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.

Usage Guidelines

Before running the **show snmp stats oid** command, connect the device to the NMS. The command output displays the list of 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 the MIBs that the NMS is querying. You can use the **show snmp stats oid** command at any time to view OIDs recently requested by the NMS.

Examples

The following is sample output from the **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
```

The table below describes the significant fields shown in the display.

Table 12: show snmp stats oid Field Descriptions

Field	Description
time-stamp	Displays the time and date when the object identifiers were 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.

Cisco IOS Release 12.4(10) and Later Releases

show snmp sysobjectid

Cisco IOS Release 12.2(44)SE and Later Releases

show snmp sysobjectid type

Syntax Description

type	Displays the system object ID type.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(10)	This command was introduced.
12.2(44)SE	This command was integrated into Cisco IOS Release 12.2(44)SE and the **type** keyword was added.

Usage Guidelines

Use the **show snmp sysobjectid** command to quickly 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.

Use the **show snmp sysobjectid type** command to identify the system object ID type.

Examples

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

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

```
Router# show snmp sysobjectid type
Configured  value : use stack OID
Operational value : use stack OID
```

Related Commands

Command	Description
show snmp	Displays the status of SNMP communications.
show snmp engineID	Displays the identification of the local SNMP engine and all remote engines that have been configured on the router.
show snmp group	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.
show snmp mib	Displays a list of the MIB module OIDs registered on the system.
show snmp pending	Displays the current set of pending SNMP requests.
show snmp sessions	Displays the current SNMP sessions.
show snmp user	Displays information about the configured characteristics of SNMP users.
show snmp view	Displays the family name, storage type, and status of an 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

username	(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 *username* 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 00000090200000000C025808, and the storage type as nonvolatile:

```
Router# show snmp user
 authuser
User name: authuser
Engine ID: 00000090200000000C025808
storage-type: nonvolatile       active access-list: 10
Rowstatus: active
Authentication Protocol: MD5
Privacy protocol: DES
Group name: VacmGroupName
```

The table below describes the significant fields shown in the display.

Table 13: 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. • If authentication is not supported in your software image, this field will not be displayed.
Privacy protocol	Indicates whether Data Encryption Standard (DES) packet encryption is enabled. • If DES is not supported in your software image, this field will not be displayed.
Group name	Indicates the SNMP group the user is a part of. • SNMP groups are defined in the context of a View-based Access Control Model (VACM).

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
v1default            iso                  -          included         permanent   active
v1default            internet             -          included         volatile    active
v1default            internet.6.3.15      -          excluded         volatile    active
v1default            internet.6.3.16      -          excluded         volatile    active
v1default            internet.6.3.18      -          excluded         volatile    active
```

The table below describes the significant fields shown in the display.

Table 14: 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.

Field	Description
storage	Type of memory storage, for example, volatile.
status	Status of the configuration, either active or nonactive.

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

context-name	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 **context** command.

Usage Guidelines

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

v1	Specifies the use of the SNMPv1 security model for a get operation.
v2c	Specifies the use of the SNMPv2c security model for a get operation.
v3	Specifies the use of the SNMPv3 security model for a get operation.
ip-address	IPv4 or IPv6 address of the SNMP host.
vrf	(Optional) Specifies the use of a Virtual Private Network (VPN) routing and forwarding (VRF) instance to send SNMP notifications.
vrf-name	(Optional) Name or instance of a VPN VRF.
community-string	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.
retry *number*	(Optional) Specifies the number of retries to consider during a get operation. The valid range is from 1 to 10.
timeout *seconds*	(Optional) Specifies the interval of time between each attempt at a get operation, in seconds. The valid range is from 1 to 1000.
oid	Specifies the object identifier value of the variable to retrieve.
oid-value	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
snmp get-bulk	Retrieves variables in bulk.
snmp get-next	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

v1	Specifies the use of the SNMPv1 security model for a getBulk operation.
v2c	Specifies the use of the SNMPv2c security model for a getBulk operation.
v3	Specifies the use of the SNMPv3 security model for a getBulk operation.
ip-address	IP address or IPv6 address of the SNMP host.
vrf	(Optional) Specifies the use of a Virtual Private Network (VPN) routing and forwarding (VRF) instance to send SNMP notifications.
vrf-name	(Optional) Name or instance of a VPN VRF.
community-string	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.
retry *number*	(Optional) Specifies the number of retries to consider during a getBulk operation. The valid range is from 1 to 10.
timeout *seconds*	(Optional) Specifies the interval of time between each attempt at a getBulk operation, in seconds. The valid range is from 1 to 1000.
non-repeaters *number*	Specifies the number of objects that can be retrieved with a getNext operation.
max-repetitions *number*	Specifies the maximum number of getNext attempts to make while the rest of the objects are retrieved.
oid	Specifies the object identifier value of the variable to retrieve.

oid-value	The object identifier value. For example, sysName.0 or 1.3.6.1.4.1.9.9.10.1.3.0.5.
oid-1 oid-n	(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
snmp get	Retrieves SNMP MIB object variables.
snmp-server community	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

v1	Specifies the use of the SNMPv1 security model for a getNext operation.
v2c	Specifies the use of the SNMPv2c security model for a getNext operation.
v3	Specifies the use of the SNMPv3 security model for a getNext operation.
ip-address	IPv4 or IPv6 address of the SNMP host.
vrf	(Optional) Specifies the use of a Virtual Private Network (VPN) routing and forwarding (VRF) instance to send SNMP notifications.
vrf-name	(Optional) Name or instance of a VPN VRF.
community-string	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.
retry *number*	(Optional) Specifies the number of retries to consider during a getNext operation. The valid range is from 1 to 10.
timeout *seconds*	(Optional) Specifies the interval of time between each attempt at a getNext operation, in seconds. The valid range is from 1 to 1000.
oid	Specifies the object identifier value of the variable to retrieve.
oid-value	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
snmp get	Retrieves SNMP object variables.
snmp get-bulk	Retrieves SNMP object variables in bulk.

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
description	Allows you to specify a description for the specified interface in human-readable form.
show snmp mib	Displays a list of the MIB module instance identifiers (OIDs) registered on your system.
show snmp mib ifmib ifindex	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

v1	Specifies the use of the SNMPv1 security model to send inform requests. **Note** SNMPv1 does not support receiving or sending inform requests.
v2c	Specifies the use of the SNMPv2c security model to send inform requests.
v3	Specifies the use of the SNMPv3 security model to send inform requests.
ip-address	IPv4 or IPv6 address of the SNMP host.
vrf	(Optional) Specifies the use of a Virtual Private Network (VPN) routing and forwarding (VRF) instance to send SNMP notifications.
vrf-name	(Optional) Name or instance of a VPN VRF.
community-string	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.
retry *number*	(Optional) Specifies the number of retries to consider while an inform request is sent. The valid range is from 1 to 10.
timeout *seconds*	(Optional) Specifies the interval of time between each attempt at sending an inform request, in seconds. The valid range is from 1 to 1000.
trap-oid	Specifies the object identifier value of the object generating the inform request.
trap-oid	The object identifier value of the object generating the inform request.
oid	Specifies the object identifier value of the object that generates the inform request.

oid-value	The object identifier value. For example, sysName.0 or 1.3.6.1.4.1.9.9.10.1.3.0.5.
oid-type	The type of OID. The following values are valid: • **counter** --A 32-bit number with a minimum value of 0. When the maximum value is reached, the counter resets to 0. • **gauge** --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. • **integer** --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. • **ip-address** --IP address. • **string** --An octet string in text notation used to represent text strings. • **timeticks** --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.
oid-type-value	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 *oid-type* argument value: • **counter** --Integer value in the range from 0 to 4294967295. • **gauge** --Integer value in the range from 0 to 4294967295. • **integer** --Integer value in the range from 0 to 4294967295. • **ip-address** --IP address in dotted decimal notation. • **string** --Text string. • **timeticks** --Integer value in the range from 0 to 4294967295.

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
snmp-server community	Sets the community access string to enable access to the SNMP entity.
snmp-server enable traps	Enables all SNMP notification types that are available on your system.
snmp-server host	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

name	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
add	Adds specific MIB objects to a defined SNMP bulk statistics object list.
snmp mib bulkstat schema	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*

Syntax Description

schema-name	Name of the bulk statistics schema to be configured.

Command Default

No schemas are defined.

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 schema** 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 **instance** 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.

Examples

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

Command	Description
instance	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.
object-list	Adds specific MIB objects to a defined SNMP bulk statistics object list.
poll-interval	Configures the polling interval for a bulk statistics schema.
snmp mib bulkstat transfer	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

transfer-id	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
show snmp mib bulkstat transfer	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

community-name	String that identifies the SNMP community.
context	(Optional) Specifies that an SNMP context name is mapped to the SNMP community.
context-name	(Optional) String that identifies the name of the SNMP context.
engineid	(Optional) Specifies that an SNMP engine ID is mapped to the SNMP community.
engine-id	(Optional) String that identifies the SNMP engine ID. Default is the local engine ID
security-name	(Optional) Specifies that a security name is mapped to the SNMP community.
security-name	(Optional) String that identifies the SNMP security name. Default is the community name
target-list	(Optional) Specifies that a VPN routing and forwarding (VRF) list is mapped to the SNMP community.
vpn-list-name	(Optional) String value that should correspond to the list name used in the **snmp mib target list** 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.
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
context	Associates an SNMP context with a particular VPN.

Command	Description
snmp-server community	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

owner	Specifies the object list owner.
object-list-owner	Name of the object list owner.
name	Indicates the name of the object list.
object-list-name	Unique name that identifies the object list.
object-number	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.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.

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)# end
```

Related Commands

Command	Description
snmp mib event trigger	Specifies a trigger owner during an event trigger configuration.

Command	Description
test	Enables a 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 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

event-owner	Name of the event owner.
name	Indicates the name of an event.
event-name	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.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.

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)# end
```

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

instance	Specifies the scalar object instance sampled for an event.
maximum	Specifies the maximum value to set for scalar object sampling.
minimum	Specifies the minimum value to set for scalar object sampling.
value	Minimum or maximum value for sampling scalar objects configured for an event. • The range for maximum value is 0 to 4294967295. • The range for minimum value is 1 to 2147483647.

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.

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)#
```