snmp mib event trigger owner through snmp-server enable informs

snmp mib event trigger owner

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

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

Syntax Description

trigger-owner	Name of the trigger owner.
name	Indicates the name of the trigger.
trigger-name	Unique name of the trigger that is within the scope of the trigger owner. The trigger names are assigned by the administrator.

Command Default

By default, the trigger name and trigger owner are not defined.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.

Usage Guidelines

The **snmp mib event trigger owner** command enables event trigger configuration mode to configure conditions to trigger events. While configuring a trigger, you can associate each trigger to an event and configure the objects to be monitored.

Examples

The following example shows how to specify a trigger owner:

```
Router(config)# snmp mib event trigger owner owner1 name trigger1
Router(config-event-trigger)# end
```

Related Commands

Command	Description
description	Provides a description of the function and use of a trigger.
enable	Enables an event.
frequency	Specifies an interval between trigger samples.
object id	Specifies the object identifier of an object.
object list owner	Specifies the list of objects that can be added to notifications according to trigger type.

snmp mib expression delta

To specify a delta interval for object sampling, use the **snmp mib expression delta** command in global configuration mode. To disable the specified interval, use the **no** form of this command.

snmp mib expression delta {**minimum** {*delta-valueseconds*} | **wildcard maximum** *wildcard-instance*}
no snmp mib expression delta {**minimum** | **wildcard maximum**}

Syntax Description

minimum	Specifies the minimum value for object sampling.
delta-value	The delta value to use during object sampling.
seconds	Minimum number of seconds between delta samples. The default is 1.
wildcard	Specifies the number of instances that can be wildcarded during object sampling.
maximum	Specifies the maximum value for object.
wildcard-instance	The maximum number of dynamic instance entries. The default is 0.

Command Default

The default value for minimum delta interval is 1 second.

The default wildcard maximum value is 0.

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

Applications may use larger values for minimum delta interval to lessen the impact of constantly computing delta. The **snmp mib expression delta minimum** command enforces a lower overhead for all expressions created after it is set.

For every instance of a delta object, one dynamic instance entry is required to restrict the instance value from the previous sample. The **snmp mib expression delta wildcard maximum** command limits the maximum number of dynamic instance entries that the system supports for wildcarded delta objects in expressions. For a given delta expression, the number of dynamic instances is the number of delta value (that meet all criteria) multiplied by the number of delta values in the expression.

A value of 0 indicates no preset limit. There is a dynamic limit based on system operation and resources. However, changing this value will not eliminate the existing delta wildcard instance objects, but will prevent the creation of more such objects.

Examples

The following example shows how to set the minimum delta interval to 60 seconds:

```
Router(config)# snmp mib expression delta minimum 60
Router(config-expression)# end
```

Related Commands

Command	Description
sample	Specifies the method of sampling an object.

snmp mib expression owner

To specify the owner of an expression, use the **snmp mib expression owner** command in global configuration mode. To disable the expression configuration, use the **no** form of this command.

snmp mib expression owner *expr-owner* **name** *expr-name*
no snmp mib expression owner *expr-owner* **name** *expr-name*

Syntax Description

expr-owner	Name of an expression owner.
name	Indicates the name of the expression.
expr-name	Name of the expression.

Command Default

By default, the expression owner and expression name are not defined.

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 expression owner** command enables expression configuration mode and configures expression information such as expression owner and name. You can configure expression properties by using commands such as **expression**, **delta interval**, and **expression**.

Examples

The following example shows how to specify an expression owner:

```
Router(config)# snmp mib expression owner owner1 name expression1
Router(config-expression)# end
```

Related Commands

Command	Description
delta interval	Specifies an interval for the delta sampling of objects used while evaluating an expression.
description (event)	Describes the function and use of an event.
enable (event)	Enables an event or event trigger.
expression	Specifies an expression for evaluation.
object	Specifies the objects to be used while evaluating an expression.
prefix object	Enables the application to determine the object based on the instance indexing.

Command	Description
value type	Specifies the type of expression value.

snmp mib flash cache

To enable the data collection process for Flash MIB, use the **snmp mib flash cache**command in global configuration mode. To set the command to its default interval, use the **no** form of this command.

snmp mib flash cache [**interval** *minutes*]
no snmp mib flash cache [**interval** *minutes*]

Syntax Description

interval	(Optional) Specifies the interval for Flash MIB data collection process.
minutes	(Optional) Data collection interval, in minutes. The values are 1 to 60. The default is 2.

Command Default

The Flash MIB data collection process is disabled.

Command Modes

Global configuration (config)

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.

Usage Guidelines

The data collection process collects the data required for sorting the ciscoFlashFileTable in the Flash MIB according to device, partition, file indexes, and file type.

Examples

The following example shows how to set the data collection interval to 10 minutes:

```
Router# configure terminal
Router(config)# snmp mib flash cache interval 10
Router(config)#
```

snmp mib flowmon alarmhistorysize

To set the maximum number of entries maintained by the flow monitor alarm history log, use the **snmp mib flowmon alarmhistorysize**command in global configuration mode. To remove the setting for the maximum number of alarm history log entries, use the **no** form of this command.

snmp mib flowmon alarmhistorysize *num*
no snmp mib flowmon alarmhistorysize *num*

Syntax Description

num	Specifies the maximum number of entries maintained by the flow monitor

Command Default

Flow monitor maintains a maximum number of 500 entries in the alarm history log.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)S	This command was introduced.

Examples

The following example shows how to set the maximum number of entries maintained by the flow monitor to 400:

```
Router(config)# snmp mib flowmon alarmhistorysize 400
```

Related Commands

Command	Description
snmp -server community	Enables SNMP and sets the community string and access privileges.
snmp -server host	Specifies the recipient of an SNMP notification operation.

snmp mib notification-log default

To create an unnamed Simple Network Management Protocol (SNMP) notification log, use the **snmp mib notification-log default** command in global configuration mode. To delete the log, use the **no** form of this command.

snmp mib notification-log default [**size** *number*]
no snmp mib notification-log default [**size** *number*]

Syntax Description

size	(Optional) Sets the maximum number of entries that the log can contain.
number	(Optional) Maximum number of entries. The default is 500.

Command Default

500 entries

Command Modes

Global configuration

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

This command creates an unnamed default SNMP notification log. The default log has a zero length string as its name (appears in the output of the **show snmp mib notification-log** command asLog Name"").

Creation and removal of the default log can be performed using only the command-line interface (CLI). Creation of named logs using the CLI or SNMP tools (SET operations) is not currently supported. No filters (varbinds) can be associated with the default log.

SNMP notification logging is enabled by default, but logging does not start until either a specific log is created and defined using thiscommand or a named log is created using a SNMP Set operation from a network management station (NMS).

The **no** form of this command deletes the default notification log and removes the notifications that were a part of this log from the Notification Log MIB database (recursively deletes the log and all its entries).

Examples

The following example shows how to create and activate a default SNMP notification log with a size of 600:

```
Router(config)# snmp mib notification-log default size 600
```

Related Commands

Command	Description
show snmp mib notification-log	Displays information about the state of local SNMP notification logging.
snmp mib notification-log globalageout	Sets the maximum age for a notification.

Command	Description
snmp mib notification-log globalsize	Sets the maximum number of notifications allowed in all logs.

snmp mib notification-log default disable

To disable Simple Network Management Protocol (SNMP) notification logging to the "default" log without deleting existing notification log entries, use the **snmp mib notification-log default disable** command in global configuration mode. To reenable logging, use the **no** form of this command.

snmp mib notification-log default disable
no snmp mib notification-log default disable

Syntax Description

This command has no arguments or keywords

Command Default

Logging is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

The "default" notification log is the null-named notification log.

This command disables SNMP notification logging. However, this command does not delete existing logs. To clear the existing "default" log, use the **no snmp mib notification-log default** command.

SNMP notification logging is enabled by default, but logging does not start until a specific log is created and defined using the **snmp mib notification-log default**command, or a named log is created using an SNMP Set operation from a network management station (NMS).

Examples

In the following example, SNMP notification logging is disabled, but existing logs are not deleted:

```
Router(config)# snmp mib notification-log default ?

  disable  disable logging
  size     size of the default log
  <cr>
Router(config)# snmp mib notification-log default disable

Router(config)#
```

Related Commands

Command	Description
show snmp mib notification-log	Displays information about the state of local SNMP notification logging.
snmp mib notification-log default	Creates an SNMP notification log.
snmp mib notification-log globalageout	Sets the maximum age for a notification.

Command	Description
snmp mib notification-log globalsize	Sets the maximum number of notifications allowed in all logs.

snmp mib notification-log globalageout

To set the maximum amount of time Simple Network Management Protocol (SNMP) notification log entries remain in the system memory, use the **snmp mib notification-log globalageout**command in global configuration mode. To restore the default value, use the **no** form of this command.

snmp mib notification-log globalageout minutes
no snmp mib notification-log globalageout minutes

Syntax Description

minutes	Maximum age (in minutes) that a notification entry is retained in the system memory. The default is 15.

Command Default

The default global ageout value is 15 minutes.

Command Modes

Global configuration

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

The ageout value specifies the maximum time a notification log can remain in the Notification Log MIB database. This value applies to all logs (default log and named logs) in the Notification Log MIB database.

The **no** form of the command restores the default value.

Examples

In the following example, the system is configured to delete entries in the SNMP Notification Log that were logged more than 20 minutes ago:

```
Router(config)# snmp mib notification-log globalageout 20
```

Related Commands

Command	Description
show snmp mib notification-log	Provides a summary of logs.
snmp mib notification-log default	Creates the default log in the MIB.
snmp mib notification-log globalsize	Sets the maximum number of notifications allowed in all logs.

snmp mib notification-log globalsize

To set the maximum number of entries that can be stored in all Simple Network Management Protocol (SNMP) notification Logs, use the **snmp mib notification-log globalsize**command in global configuration mode. To restore the default value, use the **no** form of this command.

snmp mib notification-log globalsize *number*
no snmp mib notification-log globalsize *number*

Syntax Description

number	Maximum number of log entries. The range is from 1 to 15000. This value cannot be set to 0 (limitless). The default is 500.

Command Default

The default global log size is 500 entries.

Command Modes

Global configuration

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

The size of the SNMP notification log database can be set globally (for all SNMP notification logs combined) or for each named log. The **snmp mib notification-log globalsize** command sets the maximum number of entries for all notification logs on the local system; in other words, this setting affects the whole Notification Log MIB database. This value is saved to the nlmConfigGlobalEntryLimit object in the SNMP Notification Log MIB.

The default global log size is 500 log entries. The default log size for each individual log (such as the “default log”) is 500 log entries. The maximum size for all logs combined is 15,000 log entries.

Examples

In the following example, the system is configured to delete older log entries when there are more than 600 log entries in all SNMP notification logs on the system:

```
Router(config)# snmp mib notification-log globalsize 600
```

Related Commands

Command	Description
show snmp mib notification-log	Provides a summary of logs.
snmp mib notification-log default	Creates the default log in the MIB.
snmp mib notification-log globalageout	Sets the maximum age for a notification.

snmp mib persist

To enable MIB persistence, use the **snmp mib persist**command in global configuration mode. To disable MIB persistence, use the **no** form of this command.

snmp mib persist [{**event** | **expression** | **circuit** | **cbqos** | **v3mibs**}]
no snmp mib persist [{**event** | **expression** | **circuit** | **cbqos** | **v3mibs**}]

Syntax Description

event	(Optional) Enables Event MIB persistence.
expression	(Optional) Enables Expression MIB persistence.
circuit	(Optional) Enables Circuit MIB persistence.
cbqos	(Optional) Enables class-based (CB) quality of service (QoS) MIB persistence.
v3mibs	(Optional) Enables persistence for Version 3 MIBs.

Command Default

MIB persistence is disabled.

Command Modes

Global configuration (config)

Command History

T Release	Modification
12.2(2)T	This command was introduced.
12.2(4)T3	The **event** and **expression** keywords were added.
12.4(4)T	The **cbqos** keyword was added.
12.4(20)T	The **event** and **expression** keywords were removed.
OS Release	Modification
12.0(32)S	This command was integrated into Cisco IOS Release 12.0(32)S. The **event**, **expression**, and **cbqos** keywords were added.
SB Release	Modification
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB. The **v3mibs** and **cbqos** keywords were added.
SX Release	Modification
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI. The **cbqos** keyword was added.
SR Release	Modification
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB. The **cbqos** keyword was added.

T Release	Modification
12.2(33)SRC	The **v3mibs** keyword was added.

Usage Guidelines

After entering the **snmp mib persist** command, you must enter the **write mib-data** command to save MIB persistence configuration data to NVRAM.

The Circuit Interface MIB provides a MIB object (cciDescr) that can be used to identify individual circuit-based interfaces for Simple Network Management Protocol (SNMP) monitoring. Circuit interface identification persistence maintains the user-defined name of the circuit across reboots by retaining the value of the cciDescr object in the Circuit Interface MIB (CISCO-CIRCUIT-INTERFACE-MIB). A consistent value for specific circuits is useful for network management applications that use SNMP. Circuit interface identification persistence is enabled using the **snmp mib persist circuit** global configuration command. This command is disabled by default because it uses NVRAM memory.

To enable MIB persistence for all available MIB types, use the **snmp mib persist**command without keywords.

Examples

The following example shows how to enable Event MIB persistence:

```
Router(config)# snmp mib persist cbqos
Router(config)# end

Router# write mib-data
```

Related Commands

Command	Description
snmp ifindex persist	Enables SNMP interface index values that remain constant across reboots only on a specific interface.
snmp-server ifindex persist	Globally enables SNMP interface index values that remain constant across reboots.
write mib-data	Saves MIB persistence configuration data to NVRAM.

snmp mib target list

To create a list of target virtual private network (VPN) routing and forwarding (VRF) instance and hosts to associate with a Simple Network Management Protocol (SNMP) community, use the **snmp mib target list** command in global configuration mode. To delete the list of VRF instances and hosts or to delete a particular VRF or host from the list, use the **no** form of this command.

snmp mib target list *vpn-list-name* {**vrf** *vrf-name* | **host** *ip-address*}
no snmp mib target list *vpn-list-name* {**vrf** *vrf-name* | **host** *ip-address*}

Syntax Description

vpn-list-name	Name of the target list.
vrf	Adds a specified VRF to the target list.
vrf-name	Name of a VRF to include in the list.
host	Adds a specified host to the target list.
ip-address	IP address of the host.

Command Default

No target list is created.

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 when using SNMPv1 or SNMPv2 in a VPN environment to configure a list of VRFs or hosts for source address validation. Configuring the target list ensures that the community is valid only if the incoming packet is received from a VRF or host on the target list.

- Only the following MIBs are context aware and all the tables in these MIBs can be polled:
  - CISCO-IPSEC-FLOW-MONITOR-MIB (Cisco IOS Release 12.4T and later)

- CISCO-IPSEC-MIB (Cisco IOS Release 12.4T and later)
- CISCO-PING-MIB
- IP-FORWARD-MIB
- MPLS-LDP-MIB

- Currently, two SNMP variables in the IP-FORWARD-MIB can be polled: 1.3.6.1.2.1.4.24.3 (ipCidrRouteNumber - Scalar) and 1.3.6.1.2.1.4.24.4.1 (ipCidrRouteEntry - Table).

Note It is recommended that you use SNMPv3 with the authNoPriv or higher level of security when using SNMP in a VPN environment.

Examples

The following example shows how to add a target list named target1 and add a VRF named vrf1 to the newly created target list:

```
Router(config)# snmp mib target list target1 vrf vrf1
```

Related Commands

Command	Description
snmp mib community-map	Associates an SNMP community with an SNMP context, engine ID, or security name.

snmp trap link-status

To enable Simple Network Management Protocol (SNMP) link trap generation, use the **snmp trap link-status** command in either interface configuration mode or service instance configuration mode. To disable SNMP link trap generation, use the **no** form of this command.

snmp trap link-status [**permit duplicates**]
no snmp trap link-status [**permit duplicates**]

Syntax Description

permit duplicates	(Optional) Permits duplicate SNMP linkup and linkdown traps.

Command Default

SNMP link traps are generated when an interface goes up or down.

Command Modes

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

Command History

Release	Modification
10.0	This command was introduced.
12.2(30)S	This command was modified. The **permit duplicates** keyword pair was added.
12.3(8)T	This command was integrated into Cisco IOS Release 12.3(8)T.
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.
12.2(33)SB	This command's behavior was modified on the Cisco 10000 series router for the PRE3 and PRE4 as described in the Usage Guidelines.
12.2(33)SRD1	Support for this command was extended to service instance configuration mode.
12.2(33)SRE6	This command was modified. This command must be enabled on each subinterface from this release onwards.
15.1(3)S3	This command was integrated into Cisco IOS Release 15.1(3)S3.

Usage Guidelines

By default, SNMP link traps are sent when an interface goes up or down. For interfaces such as ISDN interfaces, expected to go up and down during normal usage, the output generated by these traps may not be useful. The **no** form of this command disables these traps.

The **permit** and **duplicates** keywords are used together and cannot be used individually. Use the **permit duplicates** keyword pair when an interface is not generating SNMP linkup traps, linkdown traps, or both. When the **snmp trap link-status permit duplicates** command is configured, more than one trap may be sent for the same linkup or linkdown transition.

The **permit duplicates** keyword pair does not guarantee that SNMP link traps will be generated nor should configuring these keywords be required to receive traps.

By default, in service instance configuration mode, SNMP link traps are not sent. Also, the **permit duplicates** keyword pair is not available in service instance configuration mode.

The **snmp trap link-status** command must be used in conjunction with the **snmp-server enable traps atm subif** command in order to enable SNMP trap notifications on ATM subinterfaces. The **snmp-server enable traps atm subif** command must be configured in global configuration mode, and then the **snmp trap link-status** command must be configured on each ATM subinterface for which you want to enable SNMP trap notifications.

Cisco 10000 Series Router

In Cisco IOS Release 12.2(33)SB, the **virtual-template snmp** command has a new default configuration. Instead of being enabled by default, **no virtual-template snmp** is the default configuration. This setting enhances scaling and prevents large numbers of entries in the MIB ifTable, thereby avoiding CPU Hog messages as SNMP uses the interfaces MIB and other related MIBs.

If you configure the **no virtual-template snmp** command, the device no longer accepts the **snmp trap link-status** command under a virtual-template interface. Instead, the device displays a configuration error message such as the following:

```
Device(config)# interface virtual-template 1
Device(config-if)# snmp trap link-status
%Unable set link-status enable/disable for interface
```

If your configuration already has the **snmp trap link-status** command configured under a virtual-template interface and you upgrade to Cisco IOS Release 12.2(33)SB, the configuration error occurs when the device reloads even though the virtual template interface is already registered in the interfaces MIB.

Examples

The following example shows how to disable SNMP link traps related to the ISDN BRI interface 0:

```
Device(config)# interface bri 0
Device(config-if)# no snmp trap link-status
```

The following example shows how to enable SNMP link traps for service instance 50 on Ethernet interface 0/1:

```
Device(config)# interface ethernet 0/1
Device(config-if)# service instance 50 ethernet
Device(config-if-srv)# snmp trap link-status
Device(config-if-srv)# end
```

Related Commands

Command	Description
snmp-server enable traps atm subif	Enables the sending of ATM subinterface SNMP notifications.
virtual-template snmp	Allows virtual access interfaces to register with SNMP when they are created or reused.

snmp set

To set or modify the value of an object variable during the Simple Network Management Protocol (SNMP) set operation, use the **snmp set**command in privileged EXEC mode.

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

Syntax Description

v1	Specifies the use of the SNMPv1 security model for a set operation.
v2c	Specifies the use of the SNMPv2c security model for a set operation.
v3	Specifies the use of the SNMPv3 security model for a set 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 for a set operation. The valid range is from 1 to 10.
timeout *seconds*	(Optional) Specifies the interval of time between each attempt to set data, in seconds. The valid range is from 1 to 1000.
oid	Specifies the object identifier value of the variable to set.
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 variable is set 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 SNMP set operation modifies the individual variables in the SNMP entity.

The community string for a set 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 set the variable using SNMPv2c:

```
Router# snmp set v2c 10.16.2.8 public retry 2 timeout 60 oid 1.3.6.1.4.1.9.9.96.1.1.1.1.2.17
 integer 4
SNMP Response: reqid 10, errstat 0, erridx 0
 ccCopyTable.1.2.17 = 4
```

Related Commands

Command	Description
snmp-server community	Sets the community access string to enable access to an SNMP entity.

snmp-server cache

To enable the Simple Network Management Protocol (SNMP) cache and configure the SNMP cache expiry interval, use the **snmp-server cache** command in global configuration mode. To disable the cache for MIBs that are kept by the SNMP engine, use the **no** form of this command.

snmp-server cache [**interval** *seconds*]
no snmp-server cache

Syntax Description

interval	(Optional) Specifies the SNMP cache interval.
seconds	(Optional) SNMP cache interval, in seconds. Valid values are from 1 to 300. Default is 5.

Command Default

By default, the SNMP cache is enabled. The default expiry interval value is 5 seconds .

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.

Usage Guidelines

This command is used in distributed or modular environments. The SNMP engine cache maintains the cache for MIBs.

Examples

The following example shows how to set the SNMP cache interval to 60 seconds:

```
Router(config)# snmp-server cache interval 60
```

This example shows how to disable the SNMP cache:

```
Router(config)# no snmp-server cache
```

Related Commands

Command	Description
snmp-server community	Sets the community access string to enable access to the SNMP entity.
snmp-server manager	Starts the SNMP server manager configuration process.

snmp-server chassis-id

To provide a message line identifying the Simple Network Management Protocol (SNMP) server serial number, use the **snmp-server chassis-id** command in global configuration mode. To restore the default value, if any, use the **no** form of this command.

snmp-server chassis-id *text*
no snmp-server chassis-id

Syntax Description

text	Message that identifies the chassis serial number.

Command Default

On hardware platforms where the serial number can be machine read, the default is the serial number. For example, a Cisco 7000 router has a default chassis-id value of its serial number.

Command Modes

Global configuration

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 3.2SE	This command was implemented in Cisco IOS XE Release 3.2SE.
Cisco IOS XE Release 3.3SE	This command was implemented in Cisco IOS XE Release 3.3SE.

Usage Guidelines

The Cisco MIB provides a chassis MIB variable that enables the SNMP manager to gather data on system card descriptions, chassis type, chassis hardware version, chassis ID string, software version of ROM monitor, software version of system image in ROM, bytes of processor RAM installed, bytes of NVRAM installed, bytes of NVRAM in use, current configuration register setting, and the value of the configuration register at the next reload. The following installed card information is provided: type of card, serial number, hardware version, software version, and chassis slot number.

The chassis ID message can be seen with the **show snmp** command.

Examples

In the following example, the chassis serial number specified is 1234456:

```
Router(config)# snmp-server chassis-id 1234456
```

Related Commands

Command	Description
show snmp	Checks the status of SNMP communications.

Command	Description
show snmp chassis	Displays the SNMP server serial number.

snmp-server community

To set up the community access string to permit access to the Simple Network Management Protocol (SNMP), use the **snmp-server community** command in global configuration mode. To remove the specified community string, use the **no**form of this command.

snmp-server community *string* [**view** *view-name*] [{**ro** | **rw**}] [**ipv6** *nacl*] [{*access-list-numberextended-access-list-numberaccess-list-name*}]
no snmp-server community *string*

Syntax Description

string	Community string that consists of 1 to 32 alphanumeric characters and functions much like a password, permitting access to SNMP. Blank spaces are not permitted in the community string. **Note** The @ symbol is used for delimiting the context information. Avoid using the @ symbol as part of the SNMP community string when configuring this command.
view	(Optional) Specifies a previously defined view. The view defines the objects available to the SNMP community.
view-name	(Optional) Name of a previously defined view.
ro	(Optional) Specifies read-only access. Authorized management stations can retrieve only MIB objects.
rw	(Optional) Specifies read-write access. Authorized management stations can both retrieve and modify MIB objects.
ipv6	(Optional) Specifies an IPv6 named access list.
nacl	(Optional) IPv6 named access list.
access-list-number	(Optional) Integer from 1 to 99 that specifies a standard access list of IP addresses or a string (not to exceed 64 characters) that is the name of a standard access list of IP addresses allowed access to the SNMP agent. Alternatively, an integer from 1300 to 1999 that specifies a list of IP addresses in the expanded range of standard access list numbers that are allowed to use the community string to gain access to the SNMP agent.

Command Default

An SNMP community string permits read-only access to all objects.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.
12.0(14)ST	This command was integrated into Cisco IOS Release 12.0(14)ST.

Release	Modification
12.0(17)S	This command was integrated into Cisco IOS Release 12.0(17)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.3(2)T	The access list values were enhanced to support the expanded range of standard access list values and to support named standard access lists.
12.0(27)S	The **ipv6** *nacl* keyword and argument pair was added to support assignment of IPv6 named access lists. This keyword and argument pair is not supported in Cisco IOS 12.2S releases.
12.3(14)T	The **ipv6** *nacl* keyword and argument pair was integrated into Cisco IOS Release 12.3(14)T to support assignment of IPv6 named access lists. This keyword and argument pair is not supported in Cisco IOS 12.2S releases.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
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.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Aggregation Series Routers.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SRE	This command was modified. The automatic insertion of the **snmp-server community** command into the configuration, along with the community string specified in the **snmp-server host** command, is changed. The **snmp-server community** command has to be manually configured.
15.1(0)M	This command was modified. The automatic insertion of the **snmp-server community** command into the configuration, along with the community string specified in the **snmp-server host** command, is changed. The **snmp-server community** command has to be manually configured.
Cisco IOS XE Release 3.2SE	This command was implemented in Cisco IOS XE Release 3.2SE.
Cisco IOS XE Release 3.3SE	This command was implemented in Cisco IOS XE Release 3.3SE.

Usage Guidelines

The **no snmp-server** command disables all versions of SNMP (SNMPv1, SNMPv2C, SNMPv3).

The first **snmp-server** command that you enter enables all versions of SNMP.

To configure SNMP community strings for the MPLS LDP MIB, use the **snmp-server community** command on the host network management station (NMS).

Note In Cisco IOS Release 12.0(3) to 12.2(33)SRD, if a community string was not defined using the **snmp-server community** command prior to using the **snmp-server host** command, the default form of the **snmp-server community** command was automatically inserted into the configuration. The password (community string) used for this automatic configuration of the **snmp-server community** was same as specified in the **snmp-server host** command. However, in Cisco IOS Release 12.2(33)SRE and later releases, you have to manually configure the **snmp-server community** command.

The **snmp-server community** command can be used to specify only an IPv6 named access list, only an IPv4 access list, or both. For you to configure both IPv4 and IPv6 access lists, the IPv6 access list must appear first in the command statement.

Note The @ symbol is used as a delimiter between the community string and the context in which it is used. For example, specific VLAN information in BRIDGE-MIB may be polled using community@VLAN_ID (for example, public@100) where 100 is the VLAN number. Avoid using the @ symbol as part of the SNMP community string when configuring this command.

Examples

The following example shows how to set the read/write community string to newstring:

```
Router(config)# snmp-server community newstring rw
```

The following example shows how to allow read-only access for all objects to members of the standard named access list lmnop that specify the comaccess community string. No other SNMP managers have access to any objects.

```
Router(config)# snmp-server community comaccess ro lmnop
```

The following example shows how to assign the string comaccess to SNMP, allow read-only access, and specify that IP access list 4 can use the community string:

```
Router(config)# snmp-server community comaccess ro 4
```

The following example shows how to assign the string manager to SNMP and allow read-write access to the objects in the restricted view:

```
Router(config)# snmp-server community manager view restricted rw
```

The following example shows how to remove the community comaccess:

```
Router(config)# no snmp-server community comaccess
```

The following example shows how to disable all versions of SNMP:

```
Router(config)# no snmp-server
```

The following example shows how to configure an IPv6 access list named list1 and links an SNMP community string with this access list:

```
Router(config)# ipv6 access-list list1
```

```
Router(config-ipv6-acl)# permit ipv6 2001:DB8:0:12::/64 any
Router(config-ipv6-acl)# exit
Router(config)# snmp-server community comaccess rw ipv6 list1
```

Related Commands

Command	Description
access-list	Configures the access list mechanism for filtering frames by protocol type or vendor code.
show snmp community	Displays SNMP community access strings.
snmp-server enable traps	Enables the router to send SNMP notification messages to a designated network management workstation.
snmp-server host	Specifies the targeted recipient of an SNMP notification operation.
snmp-server view	Creates or updates a view entry.

snmp-server contact

To set the system contact (sysContact) string, use the **snmp-server contact** command in global configuration mode. To remove the system contact information, use the **no** form of this command.

snmp-server contact *text*
no snmp-server contact

Syntax Description

text	String that describes the system contact information.

Command Default

No system contact string is set.

Command Modes

Global configuration

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 3.2SE	This command was implemented in Cisco IOS XE Release 3.2SE.
Cisco IOS XE Release 3.3SE	This command was implemented in Cisco IOS XE Release 3.3SE.

Examples

The following is an example of a system contact string:

```
Router(config)#snmp-server contact '{"phone": "123-456-7899", "name": "Bob"}'
```

Related Commands

Command	Description
show snmp contact	Displays SNMP system contact information.
snmp-server location	Sets the system location string.

snmp-server context

To create a Simple Network Management Protocol (SNMP) context, use the **snmp-server context** command in global configuration mode. To delete an SNMP context, use the **no** form of this command.

snmp-server context *context-name*
no snmp-server context *context-name*

Syntax Description

context-name	Name of the SNMP context being created.

Command Default

No SNMP contexts are configured.

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.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

When you use the **no snmp-server context** command, all SNMP instances in that context are deleted.

A route distinguisher (RD) is required when you 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 a IPv4 prefix to make it globally unique. An RD is either ASN relative, which means it is composed of an autonomous system number and an arbitrary number, or it is IP address relative and composed of an IP address and an arbitrary number.

Examples

The following example shows how to create an SNMP context named contextA and associate it with a virtual private network (VPN) routing and forwarding (VRF) instance named CustomerA:

```
Router(config)#
snmp-server context contextA
Router(config)# ip vrf CustomerA
```

```
Router(config-vrf)# rd 100:120
Router(config-vrf)# context contextA
```

Related Commands

Command	Description
context	Associates an SNMP context with a particular VRF.

snmp-server drop report access

To apply a policy for restricting an SNMPv3 unknown user report to be sent out to NMS, use the **snmp-server drop report access** command in the configuration mode.

snmp-server drop report access *ipv4-access-list*

snmp-server drop report access ipv6 *ipv6-access-list*

Syntax Description

access	Specifies IP Access policy.

Command Default

Unknown user reports will be sent to all polling stations (even if other ACLs are configured).

Command Modes

Configuration mode

Usage Guidelines

To drop an unknown user report, you can either configure IPv4/IPv6 ACL name or both. When router is polled with wrong user or no user during a SNMPv3 packet exchange, the unknown user report will be sent based on the ACL policy that is configured.

Unknown user reports will be sent only to polling station addresses that are permitted by ACL.

Task ID

Task ID	Operation
snmp	read, write

Example

This example shows how to configure the SNMP server to drop the unknown user report:

```
(config) #  snmp-server drop report access ipv4-access-list
```

snmp-server drop unknown-user

To avoid error PDUs being sent out of router when polled with incorrect SNMPv3 user name, use the **snmp-server drop unknown-user** command in the appropriate mode. If the configuration is not set, by default it will respond with error PDUs.

snmp-server drop unknown-user

Syntax Description

drop unknown-user	Drop the error PDUs to be sent when router is polled with incorrect SNMPv3 user name.

Command Default

Unknown error PDUs will be sent when router is polled with incorrect SNMPv3 user name.

Task ID

Task ID	Operation
snmp	read, write

Example

This example shows how to configure the SNMP server to drop the error PDUs:

```
(config) #  snmp-server drop unknown-user
```

snmp-server drop vrf-traffic

To configure a router to drop Simple Network Management Protocol (SNMP) packets coming from virtual routing and forwarding (VRF) interfaces, use the **snmp-server drop vrf-traffic** command in global configuration mode. To disable the configuration, use the **no** form of this command.

snmp-server drop vrf-traffic
no snmp-server drop vrf-traffic

Syntax Description

This command has no arguments or keywords.

Command Default

SNMP packets are not dropped from VRF interfaces.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.

Examples

The following example shows how to configure a router to drop SNMP packets coming from VRF interfaces:

```
Router(config)# snmp-server drop vrf-traffic
```

Related Commands

Command	Description
snmp-server chassis-id	Provides a message line identifying the SNMP server serial number.

snmp-server enable informs

Note Effective with Cisco IOS Release 12.2(33)SXI, the **snmp-server enable informs** command is not available in Cisco IOS software.

This command has no functionality. To enable the sending of Simple Network Management Protocol (SNMP) inform notifications, use one of the **snmp-server enable traps***notification-type* commands in global configuration mode combined with the **snmp-server host***host-address* **informs** command in global configuration mode.

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SXI	This command was removed. Instead use one of the **snmp-server enable traps***notification-type* commands in global configuration mode combined with the **snmp-server host***host-address* **informs** command in global configuration mode.