

Simple Network Management Protocol (SNMP) Server Commands

This chapter describes the Cisco IOS XR software commands used to configure and monitor the Simple Network Management Protocol (SNMP) for network monitoring and management.

For detailed information about SNMP concepts, configuration tasks, and examples, see the *Implementing SNMP on Cisco IOS XR Software* configuration module in *System Management Configuration Guide for Cisco ASR 9000 Series Routers*.

Note The **snmp-server** commands enable SNMP on Management Ethernet interfaces by default. For information about how to enable SNMP server support on other inband interfaces, see the *Implementing Management Plane Protection on Cisco IOS XR Software* module in *System Security Configuration Guide for Cisco ASR 9000 Series Routers*.

- add (bulkstat object), on page 5
- buffer-size, on page 6
- clear snmp counters, on page 7
- enable (bulkstat), on page 8
- format (bulkstat), on page 10
- index persistence, on page 12
- instance (bulkstat schema), on page 13
- instance range, on page 15
- instance repetition, on page 16
- notification linkupdown, on page 18
- object-list, on page 20
- poll-interval, on page 21
- retain, on page 22
- retry, on page 24
- schema, on page 26
- show snmp, on page 27
- show snmp context, on page 30
- show snmp context-mapping, on page 31
- show snmp engineid, on page 33

- show snmp entity, on page 34
- show snmp group, on page 37
- show snmp host, on page 39
- show snmp interface, on page 41
- show snmp interface notification, on page 43
- show snmp interface regular-expression, on page 45
- show snmp mib, on page 46
- show snmp mib bulkstat transfer, on page 49
- show snmp request duplicates, on page 51
- show snmp request incoming-queue detail, on page 52
- show snmp request type summary, on page 54
- show snmp request type detail, on page 56
- show snmp request drop summary, on page 57
- show snmp request overload stats, on page 59
- show snmp statistics oid group, on page 60
- show snmp statistics pdu, on page 62
- show snmp statistics slow oid, on page 64
- show snmp statistics poll oid all, on page 66
- Show snmp statistics poll oid nms, on page 68
- show snmp statistics slow oid [after/before] hh:mm:ss day mday year, on page 69
- show snmp mib ifmib general, on page 71
- show snmp mib ifmib cache, on page 73
- show snmp mib ifmib statsd, on page 75
- show snmp traps details, on page 77
- show snmp informs details, on page 79
- show snmp users, on page 81
- show snmp view, on page 83
- snmp-server chassis-id, on page 84
- snmp-server community, on page 85
- snmp-server community-map, on page 87
- snmp-server contact, on page 89
- snmp-server context, on page 90
- snmp-server context mapping, on page 91
- snmp-server drop report acl, on page 93
- snmp-server drop unknown-user, on page 94
- snmp-server engineid local, on page 95
- snmp-server engineid remote, on page 96
- snmp-server entityindex persist, on page 97
- snmp-server group, on page 98
- snmp-server host, on page 101
- snmp-server ifindex persist, on page 105
- snmp-server ifmib ifalias long, on page 106
- snmp-server ifmib internal cache max-duration, on page 107
- snmp-server ifmib ipsubscriber, on page 108
- snmp-server ifmib stats cache, on page 109
- snmp-server inform, on page 110

- snmp-server interface, on page 111
- snmp-server interface subset, on page 113
- snmp-server ipv4 dscp, on page 115
- snmp-server ipv4 precedence , on page 116
- snmp-server location, on page 118
- snmp-server mib bulkstat max-procmem-size, on page 119
- snmp-server mib bulkstat object-list, on page 120
- snmp-server mib bulkstat schema, on page 121
- snmp-server mib bulkstat transfer-id, on page 123
- snmp-server mibs cbqosmib cache, on page 125
- snmp-server mibs cbqosmib persist, on page 127
- snmp-server mibs eventmib congestion-control, on page 128
- snmp-server mibs eventmib packet-loss, on page 130
- snmp-server mibs sensormib cache, on page 132
- snmp-server mibs subscriber threshold, on page 133
- snmp-server mibs subscriber threshold access-if, on page 135
- snmp-server notification-log-mib, on page 137
- snmp-server packetsize, on page 139
- snmp-server queue-length, on page 140
- snmp-server target list, on page 141
- snmp-server throttle-time, on page 142
- snmp-server timeouts subagent, on page 143
- snmp-server timeouts duplicate, on page 144
- snmp-server trap authentication vrf disable, on page 145
- snmp-server trap link ietf, on page 146
- snmp-server trap throttle-time, on page 147
- snmp-server traps, on page 148
- snmp-server traps bgp updown, on page 155
- snmp-server traps cbgp2 updown, on page 157
- snmp-server traps mpls l3vpn, on page 159
- snmp-server traps ospf errors, on page 161
- snmp-server traps ospf lsa, on page 163
- snmp-server traps ospf retransmit, on page 165
- snmp-server traps ospf state-change, on page 167
- snmp-server traps ospfv3 errors, on page 169
- snmp-server traps ospfv3 state-change, on page 171
- snmp-server traps pim interface-state-change, on page 173
- snmp-server traps pim invalid-message-received, on page 175
- snmp-server traps pim neighbor-change, on page 177
- snmp-server traps pim rp-mapping-change, on page 179
- snmp-server traps rsvp, on page 181
- snmp-server traps selective-vrf-download role-change, on page 182
- snmp-server traps snmp, on page 183
- snmp-server traps syslog, on page 185
- snmp-server trap-source, on page 186
- snmp-server traps subscriber session-aggregation, on page 188

- snmp-server traps updown, on page 189
- snmp-server trap-timeout, on page 191
- snmp-server user, on page 192
- snmp-server view, on page 195
- snmp-server vrf, on page 197
- snmp test trap all, on page 199
- snmp test trap entity, on page 201
- snmp test trap infra, on page 203
- snmp test trap interface, on page 205
- snmp test trap snmp, on page 206
- transfer-interval, on page 207
- url, on page 209

add (bulkstat object)

To add a MIB object to a Simple Network Management Protocol (SNMP) bulk statistics object list, use the **add** command in bulk statistics object list configuration mode. To remove a MIB object from an SNMP bulk statistics object list, use the **no** form of this command.

add {*object-nameOID*}
no add {*object-nameOID*}

Syntax Description

object-name	Name of the MIB object to add to the list. Object names are limited to those with mappings shown in the **show snmp mib object-name** command.
OID	Object identifier (OID) of the MIB object to add to the list.

Command Default

No MIB objects are configured for an object list.

Command Modes

Bulk statistics object list configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

All object names and OIDs in a single object list should belong to the same MIB index, but the objects need not belong to the same MIB table. For example, it is possible to group ifInoctets and a CISCO-IF-EXTENSION-MIB object in the same schema because the containing tables are indexed by the ifIndex (in the IF-MIB).

The **add** command should be repeated as necessary until all MIB objects have been added to the object list.

Task ID

Task ID	Operation
snmp	read, write

The following example shows how to add various MIB objects to an object list.

```
RP/0/RSP0/CPU0:router(config-bulk-objects)# add 1.3.6.1.2.1.2.2.1.11
RP/0/RSP0/CPU0:router(config-bulk-objects)# add ifAdminStatus
RP/0/RSP0/CPU0:router(config-bulk-objects)# add ifDescr
```

Related Topics

show snmp mib, on page 46

buffer-size

To configure a maximum buffer size for the transfer of bulk statistics files, use the **buffer-size** command in bulk statistics transfer configuration mode. To remove a previously configured buffer size from the configuration, use the **no** form of this command.

buffer-size *bytes*
no buffer-size [*bytes*]

Syntax Description

bytes	Size of the bulk statistics transfer buffer, in bytes. The valid range is from 1024 to 2147483647. The default is 2048.

Command Default

The default bulk statistics transfer buffer is 2048 bytes.

Command Modes

Bulk statistics transfer configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

A configured buffer size limit is available primarily as a safety feature. Normal bulk statistics files should not generally meet or exceed the default value while being transferred.

Task ID

Task ID	Operation
snmp	read, write

This example shows how to set the buffer size to 1024 bytes:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# snmp-server mib bulkstat transfer bulkstat1
RP/0/RSP0/CPU0:router(config-bulk-tr)# buffer-size 1024
```

clear snmp counters

To clear the Simple Network Management Protocol (SNMP) packet statistics shown by the **show snmp** command, use the **clear snmp counters** command in EXEC mode.

clear snmp counters

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The **clear snmp counters** command provides the ability to clear all SNMP counters used in the **show snmp** command without restarting any processes.

Task ID

Task ID	Operations
snmp	read, write

The following example shows how to clear the SNMP counters:

```
RP/0/RSP0/CPU0:router# clear snmp counters
```

Related Topics

show snmp, on page 27

enable (bulkstat)

To begin the bulk statistics data collection and transfer process for a specific bulk statistics configuration, use the **enable** command in bulk statistics transfer configuration mode. To disable the bulk statistics data collection and transfer process for a specific bulk statistics configuration, use the **no** form of this command.

enable
no enable

Syntax Description

This command has no keywords or arguments.

Command Default

Bulk statistics transfer is disabled.

Command Modes

Bulk statistics transfer configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Specific bulk statistics configurations are identified with a name, as specified in the **snmp-server mib bulkstat transfer-id** command. The **enable** command begins the periodic MIB data collection and transfer process.

Collection (and subsequent file transfer) starts only if this command is used. Conversely, the **no enable** command stops the collection process. Subsequently, issuing the **enable** command starts the operations again.

Each time the collection process is started using the **enable** command, data is collected into a new bulk statistics file. When the **no enable** command is used, the transfer process for any collected data immediately begins (in other words, the existing bulk statistics file are transferred to the specified management station).

To successfully enable a bulk statistics configuration, at least one schema with a non-zero number of objects must be configured.

Task ID

Task ID	Operation
snmp	read, write

The following example shows the bulk statistics transfer configuration named bulkstat1 as enabled:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# snmp-server mib bulkstat transfer bulkstat1
RP/0/RSP0/CPU0:router(config-bulk-tr)# schema ATM2/0-IFMIB
RP/0/RSP0/CPU0:router(config-bulk-tr)# url primary ftp://user:pswrd@host/folder/bulkstat1
RP/0/RSP0/CPU0:router(config-bulk-tr)# enable
RP/0/RSP0/CPU0:router(config-bulk-tr)# exit
```

Related Topics

show snmp mib bulkstat transfer, on page 49
snmp-server mib bulkstat transfer-id, on page 123

format (bulkstat)

To specify the format to be used for the bulk statistics data file, use the **format** command in bulk statistics transfer configuration mode. To disable a previously configured format specification and return to the default, use the **no** form of this command.

format {**bulkBinary** | **bulkASCII** | **schemaASCII**}
no format [**bulkBinary** | **bulkASCII** | **schemaASCII**]

Syntax Description

bulkBinary	Binary format.
bulkASCII	ASCII format.
schemaASCII	A human-readable ASCII format that contains additional bulk statistics schema tags. This is the default.

Command Default

The default bulk statistics transfer format is schemaASCII

Command Modes

Bulk statistics transfer configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The bulk statistics data file (VFile) contains two types of fields: tags and data. Tags are used to set off data to distinguish fields of the file. All other information is in data fields.

Transfers can only be performed using schemaASCII format.

For each transfer/schema pair there is a header with tags for each object collected, followed by the collected data. For example, if the transfer name is T1 and the schemas in it are S1 (which collects ifInOctets and ifOutOctets) and S2 (which collects ifInUcastPkts and ifInDiscards). Then the output file looks like this:

```
Schema-def cempt1.cempWild "%u, %s, %s, %d" Epochtime instanceoid
1.3.6.1.4.1.9.9.221.1.1.1.1.3 1.3.6.1.4.1.9.9.221.1.1.1.1.2
cempt1.cempWild: 1339491515, 8695772.1, processor, 2
cempt1.cempWild: 1339491515, 8695772.2, reserved, 11
cempt1.cempWild: 1339491515, 8695772.3, image, 12
cempt1.cempWild: 1339491575, 8695772.1, processor, 2
cempt1.cempWild: 1339491575, 8695772.2, reserved, 11
cempt1.cempWild: 1339491575, 8695772.3, image, 12
Schema-def cempt1.cempRepeat "%u, %s, %s, %d" Epochtime instanceoid
1.3.6.1.4.1.9.9.221.1.1.1.1.3 1.3.6.1.4.1.9.9.221.1.1.1.1.2
cempt1.cempRepeat: 1339491515, 8695772.1, processor, 2
cempt1.cempRepeat: 1339491515, 8695772.2, reserved, 11
cempt1.cempRepeat: 1339491515, 8695772.3, image, 12
cempt1.cempRepeat: 1339491515, 26932192.1, processor, 2
cempt1.cempRepeat: 1339491515, 26932192.2, reserved, 11
cempt1.cempRepeat: 1339491515, 26932192.3, image, 12
```

```
cempt1.cempRepeat: 1339491515, 35271015.1, processor, 2
cempt1.cempRepeat: 1339491515, 35271015.2, reserved, 11
cempt1.cempRepeat: 1339491515, 35271015.3, image, 12
cempt1.cempRepeat: 1339491515, 36631989.1, processor, 2
cempt1.cempRepeat: 1339491515, 36631989.2, reserved, 11
cempt1.cempRepeat: 1339491515, 36631989.3, image, 12
cempt1.cempRepeat: 1339491515, 52690955.1, processor, 2
cempt1.cempRepeat: 1339491515, 52690955.2, reserved, 11
cempt1.cempRepeat: 1339491515, 52690955.3, image, 12
```

Task ID

Task ID	Operation
snmp	read, write

This example shows how to specify the data format:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# snmp-server mib bulkstat transfer bulkstat1
RP/0/RSP0/CPU0:router(config-bulk-tr)# format schemaASCII
```

Related Topics

show snmp mib bulkstat transfer, on page 49
snmp-server mib bulkstat transfer-id, on page 123

index persistence

To enable index persistence on an Simple Network Management Protocol (SNMP) interface, use the **index persistence** command in SNMP interface configuration mode. To restore the default conditions with respect to this command, use the **no** form of this command.

index persistence
no index persistence

Syntax Description

This command has no keywords or arguments.

Command Default

Index persistence is disabled.

Command Modes

SNMP interface configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **index persistence** command to enable ifIndex persistence for individual entries (corresponding to individual interfaces) in the ifIndex table of the IF-MIB. IfIndex persistence retains the mapping between the ifName object values and the ifIndex object values (generated from the IF-MIB) across reboots, allowing for consistent identification of specific interfaces using SNMP.

Task ID

Task ID	Operations
snmp	read, write

The following example shows how to assign ifIndex persistence on interface 0/0/1/0:

```
RP/0/RSP0/CPU0:router(config)# snmp-server interface tengige 0/0/1/0
RP/0/RSP0/CPU0:router(config-snmp-if)# index persistence
```

Related Topics

show snmp interface, on page 41
snmp-server engineid local, on page 95
snmp-server ifindex persist, on page 105
snmp-server interface, on page 111

instance (bulkstat schema)

To configure the MIB object instances to be used in a Simple Network Management Protocol (SNMP) bulk statistics schema, use the **instance** command in bulk statistics configuration mode. To remove the instance definition, use the **no** form of this command.

instance {**exact** | **wild** } {**interface** *interface-id* [**sub-if**] | **oid** *oid*}
no instance

Syntax Description

exact	Specifies that the specified interface or object identifier (OID), when appended to the object list, is the complete OID to be used in this schema.
wild	Specifies that all instances that fall within the the specified OID or interface are included in this schema.
interface *interface-id*	Specifies an interface to be used to define the schema instance.
[**sub-if**]	(Optional) Specifies that the object instances are polled for all subinterfaces of the specified interface in addition to the object instances for the main interface.
oid *oid*	Specifies an OID to be used to define the schema instance.

Command Default

No instances are configured.

Command Modes

Bulk statistics schema configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The **instance** command specifies the instance information for objects in the schema being configured. The specific instances of MIB objects for which data is collected are determined by appending the value of the instance command to the objects specified in the associated object list. In other words, the schema object-list when combined with the schema instance specifies a complete MIB object identifier.

The **instance exact** command indicates that the specified instance, when appended to the object list, is the complete OID.

The **instance wild** command indicates that all subindices of the specified OID belong to this schema. For example, the command `instance wild oid 1` includes all subindices of the instance, such as 1.1, 1.2 and so on. It does not include other instances that start with the number 1, such as 10 and 11.

Instead of specifying an OID, you can specify a specific interface. The **interface** *interface-id* keyword and argument allow you to specify an interface name and number (for example, gigabitethernet 0/6/5/0) instead of specifying the ifIndex OID for the interface.

The optional **sub-if** keyword, when added after specifying an interface, includes the ifIndexes for all subinterfaces of the interface you specified.

Only one **instance** command can be configured per schema. If multiple **instance** commands are used, the later commands overwrite the earlier ones.

Task ID

Task ID	Operation
snmp	read, write

The following examples show two different ways to configure an instance.

```
RP/0/RSP0/CPU0:router(config-bulk-sc)# instance wild oid 1
```

```
RP/0/RSP0/CPU0:router(config-bulk-sc)# instance exact interface FastEthernet 0/1.25
```

Related Topics

instance range, on page 15
instance repetition, on page 16
snmp-server mib bulkstat schema, on page 121

instance range

To specify a range of instances for objects in a schema, use the **instance** command in bulk statistics schema configuration mode. To remove the configured instance information, use the **no** form of this command.

instance range start *start-oid* **end** *end-oid*
no instance

Syntax Description

start *start-oid*	Specifies the first OID value of a range of values.
end *end-oid*	Specifies the last OID value of a range of values.

Command Default

No instances are configured.

Command Modes

Bulk statistics schema configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Only one **instance** command can be configured per schema. If multiple **instance** commands are used, the later commands overwrite the earlier ones.

Task ID

Task ID	Operation
snmp	read, write

The following example shows how to configure a range of instances.

```
RP/0/RSP0/CPU0:router(config-bulk-sc)# instance range start 1 end 2
```

Related Topics

instance (bulkstat schema), on page 13
snmp-server mib bulkstat schema, on page 121

instance repetition

To configure bulk statistics data collection to begin at a particular instance of a MIB object and to repeat for a given number of instances , use the **instance repetition** command in bulk statistics schema configuration mode. To delete a previously configured repetition of instances, use the **no** form of this command.

instance repetition *oid-instance* **max** *repeat-number*
no instance

Syntax Description

oid-instance	Object ID of the instance to be monitored.
max *repeat-number*	Specifies the number of times the instance should repeat.

Command Default

No instance repetition is configured.

Command Modes

Bulk statistics schema configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The **instance repetition** command is used to configure data collection to repeat for a certain number of instances of a MIB object.

Only one **instance** command can be configured per schema. If multiple **instance** commands are used, the later commands overwrite the earlier ones.

Task ID

Task ID	Operation
snmp	read, write

The following example configures 4 repetitions of the OID of value 1.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# snmp-server mib bulkstat object-list ifmib
RP/0/RSP0/CPU0:router(config-bulk-objects)# add ifOutOctets
RP/0/RSP0/CPU0:router(config-bulk-objects)# add ifInOctets

RP/0/RSP0/CPU0:router(config-bulk-objects)# exit
RP/0/RSP0/CPU0:router(config)# snmp mib-server bulkstat schema IFMIB

RP/0/RSP0/CPU0:router(config-bulk-sc)# object-list ifmib
RP/0/RSP0/CPU0:router(config-bulk-sc)# poll-interval 1
```

```
RP/0/RSP0/CPU0:router(config-bulk-sc)# instance repetition 1 max 4
```

Related Topics

instance (bulkstat schema), on page 13
instance range, on page 15
snmp-server mib bulkstat schema, on page 121

notification linkupdown

To enable or disable linkUp and linkDown trap notifications on a Simple Network Management Protocol (SNMP) interface, use the **notification linkupdown** command in SNMP interface configuration mode. To revert to the default setting, use the **no** form of this command.

notification linkupdown disable
no notification linkupdown disable

Syntax Description

disable	Disables linkUp and linkDown trap notifications on an SNMP interface.

Syntax Description

This command has no keywords or arguments.

Command Default

By default, for all main interfaces the linkUp and linkDown trap notifications are enabled; for all subinterfaces they are disabled.

Command Modes

SNMP interface configuration

SNMP interface subset configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.
Release 3.9.0	This command was supported in the SNMP interface subset configuration mode.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Enabling of linkUp and linkDown notifications is performed globally using the **snmp-server traps snmp** command. Issue the **notification linkupdown** command to disable linkUp and linkDown notifications on an interface.

Use the **no** form of this command to enable linkUp and linkDown notifications on an interface, if linkUp and linkDown notifications have been disabled.

You can also use the **snmp-server interface subset** command to enable or disable groups of interfaces.

Task ID

Task ID	Operations
snmp	read, write

The following example shows how to disable linkUp and linkDown trap notifications on interface 0/0/1/0:

```
RP/0/RSP0/CPU0:router(config)# snmp-server interface tengige 0/0/1/0
RP/0/RSP0/CPU0:router(config-snmp-if)# notification linkupdown disable
```

Related Topics

show snmp interface, on page 41
snmp-server engineid local, on page 95
snmp-server ifindex persist, on page 105
snmp-server interface, on page 111
snmp-server interface subset, on page 113
snmp-server traps snmp, on page 183

object-list

To specify the bulk statistics object list to be used in the bulk statistics schema, use the **object-list** command in bulk statistics schema configuration mode. To remove an object list from the schema, use the **no** form of this command.

object-list *list-name*
no object-list [*list-name*]

Syntax Description

list-name	Name of a previously configured bulk statistics object list.

Command Default

No bulk statistics object list is specified.

Command Modes

Bulk statistics schema configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

This command associates a bulk statistics object list with the schema being configured. The object list should contain a list of MIB objects to be monitored. Only one object list can be specified for each schema. Use the **snmp-server mib bulkstat object-list** command to create an object list.

Task ID

Task ID	Operation
snmp	read, write

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# snmp-server mib bulkstat schema schema1
RP/0/RSP0/CPU0:router(config-bulk-sc)# object-list obj1
```

Related Topics

show snmp mib bulkstat transfer, on page 49
snmp-server mib bulkstat schema, on page 121
snmp-server mib bulkstat object-list, on page 120

poll-interval

To configure the polling interval for a bulk statistics schema, use the **poll-interval** command in bulk statistics schema configuration mode. To remove a previously configured polling interval, use the **no** form of this command.

poll-interval *minutes*
no poll-interval

Syntax Description

minutes	Integer in the range from 1 to 20000 that specifies, in minutes, the polling interval of data for this schema. The default is 5.

Command Default

Object instances are polled once every five minutes.

Command Modes

Bulk statistics schema configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The **poll-interval** command sets how often the MIB instances specified by the schema and associated object list are to be polled. Collected data is stored in the local bulk statistics file for later transfer.

Task ID

Task ID	Operation
snmp	read, write

In this example, the polling interval for bulk statistics collection is set to once every 3 minutes in the schema called GigE2/1-CAR:

```
RP/0/RSP0/CPU0:router# config
RP/0/RSP0/CPU0:router(config)# snmp-server mib bulk schema GigE2/1-CAR
RP/0/RSP0/CPU0:router(config-bulk-sc)# poll-interval 3
```

Related Topics

snmp-server mib bulkstat schema, on page 121

retain

To configure the retention interval for bulk statistics files, use the **retain** command in bulk statistics transfer configuration mode. To remove a previously configured retention interval from the configuration, use the **no** form of this command.

retain *minutes*
no retain [*minutes*]

Syntax Description

minutes	Length of time, in minutes, that the local bulk statistics file should be kept in system memory (the retention interval). The valid range is 0 to 20000. The default is 0.

Command Default

The bulk statistics file retention interval is 0 minutes.

Command Modes

Bulk statistics transfer configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The **retain** command specifies how long the bulk statistics file should be kept in system memory, in minutes, after the completion of the collection interval and a transmission attempt is made. The default value of zero (0) indicates that the file is deleted immediately from local memory after a successful transfer.

If the **retry** command is used, you should configure a retention interval greater than 0. The interval between retries is the retention interval divided by the retry number. For example, if **retain 10** and **retry 2** are configured, retries are attempted once every 5 minutes. Therefore, if the **retain** command is not configured (retain default is 0), no retries are attempted.



Note Once a successful transmission has occurred the bulk file is not retained regardless of the retain time.

Task ID

Task ID	Operation
snmp	read, write

In the following example, the bulk statistics transfer retention interval is set to 10 minutes:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# snmp-server mib bulkstat transfer bulkstat1
RP/0/RSP0/CPU0:router(config-bulk-tr)# schema ATM2/0-IFMIB
```

```
RP/0/RSP0/CPU0:router(config-bulk-tr)# url primary ftp://user:pswrd@host/folder/bulkstat1
RP/0/RSP0/CPU0:router(config-bulk-tr)# retry 2
RP/0/RSP0/CPU0:router(config-bulk-tr)# retain 10
RP/0/RSP0/CPU0:router(config-bulk-tr)# exit
```

Related Topics

retry, on page 24
show snmp mib bulkstat transfer, on page 49
snmp-server mib bulkstat transfer-id, on page 123

retry

To configure the number of retries that should be attempted for a bulk statistics file transfer, use the **retry** command in bulk statistics transfer configuration mode. To return the number of bulk statistics retries to the default, use the **no** form of this command.

retry *number*
no retry [*number*]

Syntax Description

number	Number of transmission retries. The valid range is from 0 to 100.

Command Default

No retry attempts are made.

Command Modes

Bulk statistics transfer configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

If an attempt to send the bulk statistics file fails, the system can be configured to attempt to send the file again using the **retry** command. One retry includes an attempt first to the primary destination and then, if the transmission fails, to the secondary location; for example, if the retry value is 1, an attempt will be made first to the primary URL, then to the secondary URL, then to the primary URL again, and then to the secondary URL again.

If the **retry** command is used, you should also use the **retain** command to configure a retention interval greater than 0. The interval between retries is the retention interval divided by the retry number. For example, if **retain 10** and **retry 2** are configured, retries are attempted once every 5 minutes. Therefore, if the **retain** command is not configured (or the **retain 0** command is used) no retries are attempted.

Task ID

Task ID	Operation
snmp	read, write

In the following example, the number of retries for the bulk statistics transfer is set to 2:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# snmp-server mib bulkstat transfer bulkstat1
RP/0/RSP0/CPU0:router(config-bulk-tr)# schema ATM2/0-IFMIB
RP/0/RSP0/CPU0:router(config-bulk-tr)# url primary ftp://user:pswrd@host/folder/bulkstat1
RP/0/RSP0/CPU0:router(config-bulk-tr)# retry 2
RP/0/RSP0/CPU0:router(config-bulk-tr)# retain 10
```

```
RP/0/RSP0/CPU0:router(config-bulk-tr)# exit
```

Related Topics

retain, on page 22
show snmp mib bulkstat transfer, on page 49
snmp-server mib bulkstat transfer-id, on page 123

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

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The schema must be previously defined using the **snmp-server mib bulkstat schema** command.

Repeat the **schema** 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).

Task ID

Task ID	Operation
snmp	read, write

This example adds three different schemas to a bulk statistics transfer configuration:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# snmp-server mib bulkstat transfer-id bulkstat1
RP/0/RSP0/CPU0:router(config-bulk-tr)# schema ATM2/0-IFMIB
RP/0/RSP0/CPU0:router(config-bulk-tr)# schema ATM2/0-CAR
RP/0/RSP0/CPU0:router(config-bulk-tr)# schema Ethernet2/1-IFMIB
```

Related Topics

show snmp mib bulkstat transfer, on page 49
snmp-server mib bulkstat schema, on page 121

show snmp

To display the status of Simple Network Management Protocol (SNMP) communications, use the **show snmp** command in

EXEC

mode.

show snmp

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the `show snmp` command to show counter information for SNMP operations. It also displays the chassis ID string defined with the **snmp-server chassis-id** command.

Task ID

Task ID	Operations
snmp	read

This example shows sample output from the `show snmp` command:

```
RP/0/RSP0/CPU0:router# show snmp

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

```
24 Response PDUs
13 Trap PDUs
SNMP logging: enabled
Logging to 172.25.58.33.162, 0/10, 13 sent, 0 dropped.
```

Table 1: show snmp Field Descriptions, on page 28 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 device.
Too big errors	Number of SNMP packets that were larger than the maximum packet size.
Maximum packet size	Maximum size of SNMP packets.
No such name errors	Number of SNMP requests that specified a MIB object 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 is 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.

Field	Description
SNMP logging	Enabled or disabled logging.
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** command.

Related Topics

show snmp mib, on page 46
snmp-server chassis-id, on page 84
snmp-server queue-length, on page 140

show snmp context

To display the enhanced SNMP context mappings, use the **show snmp context** command in EXEC mode.

show snmp context

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **show snmp context** command to display the protocol instance, topology and VRF mappings associated with an SNMP context.

Task ID

Task ID	Operation
snmp	read

This example illustrates sample output from the **show snmp context** command:

```
RP/0/RSP0/CPU0:router# show snmp context

Tue Dec 21 03:41:08.065 PST
Context-name       Vrf-name      Topology-Name   Instance-Name             Feature
con5                  vf5           tp5             in5                     OSPF
con6                  vf6           tp6             in6                     OSPF
con7                  vf7           tp7             in7                     OSPF
con8                  vf8           tp8             in8                     OSPF
```

Related Topics

snmp-server context mapping, on page 91

show snmp context-mapping

To display the SNMP context mapping table, use the **show snmp context-mapping** command in

EXEC

mode.

show snmp context-mapping

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.8.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The SNMP agent handles queries based on SNMP contexts created by client features. Use the **show snmp context-mapping** command to display the SNMP context mapping table. Each entry in the table includes the name of an SNMP context created by a client instance and the name of the client that created the context.

Task ID

Task ID	Operations
snmp	read

The following example shows sample output from the **show snmp context-mapping** command:

```
RP/0/RSP0/CPU0:router# show snmp context-mapping

Wed Aug 6 01:42:35.227 UTC
Context-name                  Feature-name                  Feature
ControlEthernet0_RP0_CPU0_S0  ControlEthernet0_RP0_CPU0_S0  BRIDGEINST
ControlEthernet0_RP1_CPU0_S0     ControlEthernet0_RP1_CPU0_S0     BRIDGEINST
```

Table 2: show snmp context-mapping Field Descriptions

Field	Definition
Context-name	Name of an SNMP context.
Feature-name	Name of the instance that created the context.

Field	Definition
Feature	Name of the client whose instance created the context.

show snmp engineid

To display the identification of the local Simple Network Management Protocol (SNMP) engine that has been configured on the router, use the **show snmp engineid** command in EXEC mode.

show snmp engineid

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

An *SNMP engine* is a copy of SNMP that can reside on a local device.

Task ID

Task ID	Operations
snmp	read

The following example shows sample output from the **show snmp engineid** command:

```
RP/0/RSP0/CPU0:router# show snmp engineid

  Local SNMP engineID: 0000000902000000C025808
```

Related Topics

snmp-server engineid local, on page 95

show snmp entity

To display the entPhysicalName and entPhysicalIndex mappings, use the **show snmp entity** command in

EXEC

mode.

show snmp entity

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.9.1	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **show snmp entity** command to view the entity index to use in the **snmp test trap entity** command. To use the **show snmp entity** command, SNMP must be configured on the router.

Task ID

Task ID	Operation
snmp	read

This example illustrates sample output from the **show snmp entity** command:

```
RP/0/RSP0/CPU0:router# show snmp entity

Thu Aug 13 02:10:06.741 UTC
entPhysicalIndex:      22001 entPhysicalName: portslot 0/0/CPU0/7
entPhysicalIndex:      23006 entPhysicalName: portslot 0/0/CPU0/129
entPhysicalIndex:      23557 entPhysicalName: portslot 0/0/CPU0/3
entPhysicalIndex:      47719 entPhysicalName: 0/0/* - ingresspse - 1.2V
entPhysicalIndex:     320862 entPhysicalName: 0/0/* - host - 5V_C
entPhysicalIndex:     322450 entPhysicalName: 0/0/* - host - 1.5V
entPhysicalIndex:     428209 entPhysicalName: 0/PL2/*
entPhysicalIndex:    1038801 entPhysicalName: 0/0/* - ingressq - 2.5V
entPhysicalIndex:    1040485 entPhysicalName: 0/0/* - ingressq - 1.25V_0123
entPhysicalIndex:    1152042 entPhysicalName: 0/2/CPU0/7
entPhysicalIndex:    2031334 entPhysicalName: 0/SM0/* - host - Inlet1
entPhysicalIndex:    2032954 entPhysicalName: 0/SM0/* - host - 1.8V_L
entPhysicalIndex:    2034510 entPhysicalName: 0/SM0/* - host - brd-ok-led
entPhysicalIndex:    2110001 entPhysicalName: 0/PL2/* - plimasic - Exhaust0
entPhysicalIndex:    2111557 entPhysicalName: 0/PL2/* - plimasic - 1.8V
entPhysicalIndex:    2358084 entPhysicalName: 0/0/* - egressq
entPhysicalIndex:    2359704 entPhysicalName: 0/0/* - cpu
```

```
entPhysicalIndex:    2469162 entPhysicalName: 0/2/* - egressq - Hotspot0
entPhysicalIndex:    2559937 entPhysicalName: 0/0/* - egressq - 1.2V
entPhysicalIndex:    2577533 entPhysicalName: 0/2/CPU0/0
entPhysicalIndex:    2853020 entPhysicalName: 0/0/* - egressqse - 5V
entPhysicalIndex:    3497583 entPhysicalName: 0/SM1/* - host - brd-ok-led
entPhysicalIndex:    3500791 entPhysicalName: 0/SM1/* - host - Inlet1
 --More—
```

```
RP/0/RSP0/CPU0:router# show snmp entity

Mon Nov 15 11:19:23.609 UTC
entPhysicalIndex:     172193 entPhysicalName: portslot 0/0/CPU0/1
entPhysicalIndex:     322450 entPhysicalName: voltages 0/0/CPU0
entPhysicalIndex:     345071 entPhysicalName: voltages 0/7/CPU0
entPhysicalIndex:     346659 entPhysicalName: voltages 0/7/CPU0
entPhysicalIndex:     349835 entPhysicalName: voltages 0/7/CPU0
entPhysicalIndex:     546880 entPhysicalName: voltages 0/7/CPU0
entPhysicalIndex:     845998 entPhysicalName: voltages 0/7/CPU0
entPhysicalIndex:     847586 entPhysicalName: voltages 0/7/CPU0
entPhysicalIndex:    1192623 entPhysicalName: 0/25/CPU0
entPhysicalIndex:    1227530 entPhysicalName: voltages 0/21/CPU0
entPhysicalIndex:    1460256 entPhysicalName: temperatures 0/18/CPU0
entPhysicalIndex:    1795138 entPhysicalName: temperatures 0/20/CPU0
entPhysicalIndex:    3079213 entPhysicalName: voltages 0/7/CPU0
entPhysicalIndex:    3080801 entPhysicalName: voltages 0/7/CPU0
entPhysicalIndex:    3082421 entPhysicalName: slot 7/0
entPhysicalIndex:    5037675 entPhysicalName: 0/21/CPU0
entPhysicalIndex:    5509481 entPhysicalName: voltages 0/9/CPU0
entPhysicalIndex:    6182130 entPhysicalName: voltages 0/9/CPU0
entPhysicalIndex:    6369487 entPhysicalName: portslot 0/9/CPU0/2
entPhysicalIndex:    8392407 entPhysicalName: temperatures 0/17/CPU0
entPhysicalIndex:    8548798 entPhysicalName: 0/21/CPU0 - host
entPhysicalIndex:   10735504 entPhysicalName: voltages 0/1/CPU0
entPhysicalIndex:   10737188 entPhysicalName: voltages 0/1/CPU0
entPhysicalIndex:   10738808 entPhysicalName: slot 1/1
entPhysicalIndex:   11312388 entPhysicalName: slot 7
entPhysicalIndex:   11314008 entPhysicalName: slot 3
entPhysicalIndex:   12644344 entPhysicalName: voltages 0/19/CPU0
entPhysicalIndex:   12761695 entPhysicalName: slot 24
entPhysicalIndex:   12763283 entPhysicalName: slot 20
entPhysicalIndex:   12907576 entPhysicalName: voltages 0/0/CPU0
entPhysicalIndex:   13262622 entPhysicalName: slot 16
entPhysicalIndex:   13290941 entPhysicalName: temperatures 0/16/CPU0
entPhysicalIndex:   13404457 entPhysicalName: voltages 0/2/CPU0
entPhysicalIndex:   13406077 entPhysicalName: voltages 0/2/CPU0
entPhysicalIndex:   13701859 entPhysicalName: voltages 0/2/CPU0
entPhysicalIndex:   13900492 entPhysicalName: voltages 0/2/CPU0
entPhysicalIndex:   13903700 entPhysicalName: voltages 0/2/CPU0
entPhysicalIndex:   13905384 entPhysicalName: voltages 0/2/CPU0
entPhysicalIndex:   14106204 entPhysicalName: portslot 0/8/CPU0/2
entPhysicalIndex:   14256525 entPhysicalName: voltages 0/8/CPU0
entPhysicalIndex:   14979942 entPhysicalName: slot 2/2
entPhysicalIndex:   14981562 entPhysicalName: voltages 0/2/CPU0
entPhysicalIndex:   15141782 entPhysicalName: 0/19/CPU0
entPhysicalIndex:   15873651 entPhysicalName: temperatures 0/22/CPU0
entPhysicalIndex:   15986678 entPhysicalName: voltages 0/1/CPU0
entPhysicalIndex:   15988234 entPhysicalName: voltages 0/1/CPU0
entPhysicalIndex:   15991442 entPhysicalName: voltages 0/1/CPU0
entPhysicalIndex:   16136999 entPhysicalName: voltages 0/1/CPU0
entPhysicalIndex:   16138619 entPhysicalName: voltages 0/1/CPU0
entPhysicalIndex:   16285636 entPhysicalName: temperatures 0/1/CPU0
entPhysicalIndex:   16287256 entPhysicalName: voltages 0/1/CPU0
entPhysicalIndex:   16606045 entPhysicalName: voltages 0/8/CPU0
```

```
entPhysicalIndex:   16607633 entPhysicalName: voltages 0/8/CPU0
entPhysicalIndex:   16733769 entPhysicalName: 0/2/CPU0 - host
entPhysicalIndex:   16949774 entPhysicalName: portslot 0/0/CPU0/0
entPhysicalIndex:   17098539 entPhysicalName: temperatures 0/0/CPU0
entPhysicalIndex:   17122684 entPhysicalName: voltages 0/7/CPU0
entPhysicalIndex:   17124272 entPhysicalName: voltages 0/7/CPU0
entPhysicalIndex:   17127448 entPhysicalName: voltages 0/7/CPU0
entPhysicalIndex:   17205790 entPhysicalName: 0/2/CPU0
entPhysicalIndex:   17322905 entPhysicalName: temperatures 0/7/CPU0
entPhysicalIndex:   17324589 entPhysicalName: voltages 0/7/CPU0
entPhysicalIndex:   17595466 entPhysicalName: 0/25/CPU0 - host
entPhysicalIndex:   17620307 entPhysicalName: voltages 0/7/CPU0
entPhysicalIndex:   17621991 entPhysicalName: voltages 0/7/CPU0
entPhysicalIndex:   17623611 entPhysicalName: voltages 0/7/CPU0
entPhysicalIndex:   18003523 entPhysicalName: temperatures 0/21/CPU0
entPhysicalIndex:   18237837 entPhysicalName: voltages 0/18/CPU0
entPhysicalIndex:   18571163 entPhysicalName: voltages 0/20/CPU0
---More---
```

show snmp group

To display the names of groups on the router, security model, status of the different views, and storage type of each group, use the **show snmp group** command in

EXEC

mode.

show snmp group

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
snmp	read

This example shows sample output from the **show snmp group** command:

```
RP/0/RSP0/CPU0:router# show snmp group

  groupname: public security model:snmpv1
  readview : v1default writeview: -
  notifyview: v1default
  row status: nonVolatile

  groupname: public security model:snmpv2c
  readview : v1default writeview: -
  notifyview: v1default
  row status: nonVolatile
```

Table 3: show snmp group Field Descriptions

Field	Definition
groupname	Name of the Simple Network Management Protocol (SNMP) group or collection of users that have a common access policy.

Field	Definition
readview	String identifying the read view of the group.
security model	Security model used by the group, either v1, v2c, or v3.
writeview	String identifying the write view of the group.
notifyview	String identifying the notify view of the group.
row status	Settings that are set in volatile or temporary memory on the device, or in nonvolatile or persistent memory where settings remain after the device is turned off and on again.

Related Topics

snmp-server group, on page 98

show snmp host

To display the configured Simple Network Management Protocol (SNMP) notification recipient host, User Datagram Protocol (UDP) port number, user, and security model, use the **show snmp host** command in

EXEC

mode.

show snmp host

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
snmp	read

The following example shows sample output from the **show snmp host** command:

```
RP/0/RSP0/CPU0:router# show snmp host

  Notification host: 10.50.32.170 udp-port: 2345 type: trap
  user: userV3auth security model: v3 auth

  Notification host: 10.50.32.170 udp-port: 2345 type: trap
  user: userV3noauth security model: v3 noauth

  Notification host: 10.50.32.170 udp-port: 2345 type: trap
  user: userV3priv security model: v3 priv

  Notification host: 10.50.32.170 udp-port: 2345 type: trap
  user: userv2c security model: v2c
```

Table 4: show snmp host Field Descriptions

Field	Definition
Notification host	Name or IP address of target host.
udp-port	UDP port number to which notifications are sent.
type	Type of notification configured.
user	Security level of the user.
security model	Version of SNMP used to send the trap, either v1, v2c, or v3.

show snmp interface

To display the interface index identification numbers (ifIndex values) for all the interfaces or a specified interface, use the **show snmp interface** command in the appropriate mode.

show snmp interface [*type interface-path-id* **ifindex**]

Syntax Description

type	(Optional) Interface type. For more information, use the question mark (?) online help function.
interface-path-id	(Optional) Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
ifindex	(Optional) Displays the ifIndex value for the specified interface.

Command Default

Enter the **show snmp interface** command without keywords or arguments to display the ifIndex value for all interfaces.

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
snmp	read

This example displays the ifIndex value for a specific interface:

```
RP/0/RSP0/CPU0:router# show snmp interface pos 0/1/0/1 ifindex

ifName : POS0/1/0/1            ifIndex : 12
```

The following example displays the ifIndex value for all interfaces:

```
RP/0/RSP0/CPU0:router# show snmp interface
```

```
ifName : Loopback0             ifIndex : 1
ifName : POS0/1/0/1            ifIndex : 12
ifName : POS0/1/4/2            ifIndex : 14
ifName : POS0/1/4/3            ifIndex : 15
ifName : POS0/6/0/1            ifIndex : 2
ifName : POS0/6/4/4            ifIndex : 18
ifName : POS0/6/4/5            ifIndex : 19
ifName : POS0/6/4/6            ifIndex : 20
ifName : Bundle-POS24          ifIndex : 4
ifName : Bundle-Ether28        ifIndex : 5
ifName : Bundle-Ether28.1      ifIndex : 7
ifName : Bundle-Ether28.2      ifIndex : 8
ifName : Bundle-Ether28.3      ifIndex : 9
ifName : MgmtEth0/RP0/CPU0/0   ifIndex : 6
ifName : MgmtEth0/RP1/CPU0/0   ifIndex : 10
ifName : GigabitEthernet0/1/5/0  ifIndex : 11
ifName : GigabitEthernet0/1/5/1  ifIndex : 13
ifName : GigabitEthernet0/1/5/2  ifIndex : 3
ifName : GigabitEthernet0/6/5/1  ifIndex : 16
ifName : GigabitEthernet0/6/5/2  ifIndex : 17
ifName : GigabitEthernet0/6/5/7  ifIndex : 21
```

Table 5: show snmp interface Field Descriptions

Field	Definition
ifName	Interface name.
ifIndex	ifIndex value.

Related Topics

snmp-server ifindex persist, on page 105
snmp-server interface, on page 111

show snmp interface notification

To display the linkUp and linkDown notification status for a subset of interfaces, use the **show snmp interface notification** command in EXEC mode.

show snmp interface notification {**subset** *subset-number* | **regular-expression** *expression* | [*type interface-path-id*]}

Syntax Description

subset *subset-number*	Specifies the identifier of the interface subset. The subset-number argument is configured using the **snmp-server interface subset** command.
regular-expression *expression*	Specifies a subset of interfaces matching a regular expression, for which to display information.
type	(Optional) Interface type. For more information, use the question mark (?) online help function.
interface-path-id	(Optional) Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Regular expressions have two constraints:

- Regular expressions must always be entered within double quotes to ensure that the CLI interprets each character correctly.
- All characters that are part of a regular expression are considered regular characters with no special meaning. In order to enter special characters, such as "\" or "?," they must be preceded by the backslash character "\." For example, to enter the regular expression ([A-Z][A-Z0-9]*)\b[^>]*>(.*?)</\1, you would enter ([A-Z][A-Z0-9]*)\\b[^>]*>(.*\?)</\\1.

Refer to the *Understanding Regular Expressions, Special Characters, and Patterns* module in *Cisco ASR 9000 Series Aggregation Services Router Getting Started Guide* for more information regarding regular expressions.

When using the **subset** or **regular-expression** keywords, the actual display might not match the configuration if there are higher priority *subset-number* values that actually apply to the interface. This can happen for a set of interfaces that are included in two or more configured regular expressions or where an individual interface configuration is enabled.

Task ID

Task ID	Operation
snmp	read

The following example illustrates how to display linkUp and linkDown notification status for a subset of interfaces identified by a specific *subset-number* :

```
RP/0/RSP0/CPU0:router# show snmp interface notification subset 3
```

This example illustrates how to display linkUp and linkDown notification status for a subset of interfaces identified by a regular expression:

```
RP/0/RSP0/CPU0:router# show snmp interface notification regular-expression
"^Gig[a-zA-Z]+[0-9/]+\."
```

show snmp interface regular-expression

To display interface names and indices assigned to interfaces that match a regular expression, use the **show snmp interface regular-expression** command in EXEC mode.

show snmp interface regular-expression *expression*

Syntax Description

expression	Specifies a subset of interfaces matching a regular expression, for which to display information.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

All characters that are part of a regular expression are considered regular characters with no special meaning. In order to enter special characters, such as "\" or "?," they must be preceded by the backslash character "\." For example, to enter the regular expression ([A-Z][A-Z0-9]*)\b[^>]*>(.*?)</\1, you would enter ([A-Z][A-Z0-9]*)\\b[^>]*>(.*\?)</\\1.

Refer to the *Understanding Regular Expressions, Special Characters, and Patterns* module in *Cisco ASR 9000 Series Aggregation Services Router Getting Started Guide* for more information regarding regular expressions.

Task ID

Task ID	Operation
snmp	read

This example illustrates how to display information for interfaces that match the given regular expression:

```
RP/0/RSP0/CPU0:router# show snmp interface regular-expression "^Gig[a-zA-Z]+[0-9/]+\."
```

Related Topics

snmp-server interface subset, on page 113

show snmp mib

To display a list of MIB module object identifiers (OIDs) registered on the system, use the **show snmp mib** command in

EXEC

mode.

show snmp mib [*object-name* | **dll**]

Syntax Description

object-name	(Optional) Specific MIB object identifier or object name.
dll	(Optional) Displays a list of all MIB DLL filenames and the OID supported by each DLL filename on the system.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.
Release 3.9.0	The **detailed** keyword was not supported.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **show snmp mib** command to display a list of the MIB module instance identifiers registered on the system.

Although the **show snmp mib** command can be used to display a list of MIB 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 is intended only for network managers who are familiar with Abstract Syntax Notation One (ASN.1) syntax and the Structure of Management Information (SMI) of Open Systems Interconnection (OSI) Reference Model.

SNMP management information is viewed as a collection of managed objects residing in a virtual information store termed the *MIB*. Collections of related objects are defined in MIB modules. These modules are written using a subset of ASN.1 termed the *SMI.*

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.

Use the **detailed** keyword to display a list of the MIB module instance identifiers registered on the system. The output displays additional details, such as DLL and configuration information.

Use the **dll** keyword to display a list of the MIB modules loaded into the agent. This command can be used to find the supported MIBs.



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

Task ID

Task ID	Operations
snmp	read

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

```
RP/0/RSP0/CPU0:router# show snmp mib

1.3.6.1.2.1.47.1.1.1.1.2
1.3.6.1.2.1.47.1.1.1.1.3
1.3.6.1.2.1.47.1.1.1.1.4
1.3.6.1.2.1.47.1.1.1.1.5
1.3.6.1.2.1.47.1.1.1.1.6
1.3.6.1.2.1.47.1.1.1.1.7
1.3.6.1.2.1.47.1.1.1.1.8
1.3.6.1.2.1.47.1.1.1.1.9
1.3.6.1.2.1.47.1.1.1.1.10
1.3.6.1.2.1.47.1.1.1.1.11
1.3.6.1.2.1.47.1.1.1.1.12
1.3.6.1.2.1.47.1.1.1.1.13
1.3.6.1.2.1.47.1.1.1.1.14
1.3.6.1.2.1.47.1.1.1.1.15
1.3.6.1.2.1.47.1.1.1.1.16
1.3.6.1.2.1.47.1.2.1.1.2
1.3.6.1.2.1.47.1.2.1.1.3
1.3.6.1.2.1.47.1.2.1.1.4
1.3.6.1.2.1.47.1.2.1.1.5
1.3.6.1.2.1.47.1.2.1.1.6
1.3.6.1.2.1.47.1.2.1.1.7
1.3.6.1.2.1.47.1.2.1.1.8
1.3.6.1.2.1.47.1.3.1.1.1
--More-
```

This example shows sample output from the **show snmp mib** command with the **detailed** keyword:

```
RP/0/RSP0/CPU0:router# show snmp mib detailed

Entitymib:dll=/pkg/lib/mib/libEntitymib.dll, config=Entity.mib, loaded
1.3.6.1.2.1.47.1.1.1.1.2
1.3.6.1.2.1.47.1.1.1.1.3
1.3.6.1.2.1.47.1.1.1.1.4
1.3.6.1.2.1.47.1.1.1.1.5
1.3.6.1.2.1.47.1.1.1.1.6
1.3.6.1.2.1.47.1.1.1.1.7
1.3.6.1.2.1.47.1.1.1.1.8
1.3.6.1.2.1.47.1.1.1.1.9
1.3.6.1.2.1.47.1.1.1.1.10
1.3.6.1.2.1.47.1.1.1.1.11
```

```
1.3.6.1.2.1.47.1.1.1.1.12
1.3.6.1.2.1.47.1.1.1.1.13
1.3.6.1.2.1.47.1.1.1.1.14
1.3.6.1.2.1.47.1.1.1.1.15
1.3.6.1.2.1.47.1.1.1.1.16
1.3.6.1.2.1.47.1.2.1.1.2
1.3.6.1.2.1.47.1.2.1.1.3
1.3.6.1.2.1.47.1.2.1.1.4
1.3.6.1.2.1.47.1.2.1.1.5
1.3.6.1.2.1.47.1.2.1.1.6
1.3.6.1.2.1.47.1.2.1.1.7
1.3.6.1.2.1.47.1.2.1.1.8
--More--
```

This example shows sample output from the **show snmp mib** command with the **dll** keyword:

```
RP/0/RSP0/CPU0:router# show snmp mib dll

Entitymib:dll=/pkg/lib/mib/libEntitymib.dll, config=Entity.mib, loaded
bgp4mib:dll=/pkg/lib/mib/libbgp4mib.dll, config=bgp4.mib, loaded
cdpmib:dll=/pkg/lib/mib/libcdpmib.dll, config=cdp.mib, loaded
ciscoprocessmib:dll=/pkg/lib/mib/libciscoprocessmib.dll,
 config=ciscoprocess.mib, loaded
ciscosyslogmib:dll=/pkg/lib/mib/libciscosyslogmib.dll,
 config=ciscosyslog.mib, loaded
ciscosystemmib:dll=/pkg/lib/mib/libciscosystemmib.dll,
 config=ciscosystem.mib, loaded
confcopymib:dll=/pkg/lib/mib/libconfcopymib.dll, config=confcopy.mib,
 loaded
configmanmib:dll=/pkg/lib/mib/libconfigmanmib.dll, config=configman.mib,
 loaded
dot3admib:dll=/pkg/lib/mib/libdot3admib.dll, config=dot3ad.mib,
 loaded
fabhfrmib:dll=/pkg/lib/mib/libfabhfrmib.dll, config=fabhfr.mib,
 loaded
fabmcastapplmib:dll=/pkg/lib/mib/libfabmcastapplmib.dll,
 config=fabmcastappl.mib, loaded
fabmcastmib:dll=/pkg/lib/mib/libfabmcastmib.dll, config=fabmcast.mib,
 loaded
flashmib:dll=/pkg/lib/mib/libflashmib.dll, config=flash.mib,
 loaded
hsrpmib:dll=/pkg/lib/mib/libhsrpmib.dll, config=hsrp.mib, loaded
icmpmib:dll=/pkg/lib/mib/libicmpmib.dll, config=icmp.mib, loaded
ifmib:dll=/pkg/lib/mib/libifmib.dll, config=if.mib, loaded
ipmib:dll=/pkg/lib/mib/libipmib.dll, config=ip.mib, loaded
mempoolmib:dll=/pkg/lib/mib/libmempoolmib.dll, config=mempool.mib,
 loaded
mplsldpmib:dll=/pkg/lib/mib/libmplsldpmib.dll, config=mplsldp.mib,
 loaded
.
.
.
```

Related Topics

show snmp, on page 27

show snmp mib bulkstat transfer

To display completed local bulk statistics files, use the **show snmp mib bulkstat transfer** command in EXEC mode.

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

Syntax Description

transfer-name	Specifies a named transfer file to display.

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The **show snmp mib bulkstat transfer** command lists all bulk statistics virtual files (VFiles) on the system that have finished collecting data. (Data files that are not complete are not displayed.)

The output lists all of the completed local bulk statistics files, the remaining time left before the bulk statistics file is deleted (remaining retention period), and the state of the bulk statistics file. The state of the bulk statistics file should be Retry. Retry indicates that one or more transfer attempts have failed and that the file transfer will be attempted again. The number of retry attempts remaining is displayed in parenthesis. After the successful retry or retry attempts, the local files created by the MIB process in the router are deleted and data collection begins again.

To display only the status of a named transfer (as opposed to all configured transfers), specify the name of the transfer in the *transfer-name* argument. The *transfer-name* argument names a file which is supposed to be created even before the retries.

Task ID

Task ID	Operation
snmp	read

```
RP/0/RSP0/CPU0:router# show snmp mib bulkstat transfer

Transfer Name : ifmib
 Retained files

 File Name        : Time Left (in seconds)   :STATE
 ----------------------------------------------------------
```

```
ifmib_Router_020421_100554683 : 173 : Retry (2 Retry attempt(s) Left)
```

show snmp request duplicates

To display the number of duplicate protocol data unit (PDU) requests dropped by the SNMP agent, use the **show snmp request duplicates** command in

EXEC

mode.

show snmp request duplicates

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 4.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
snmp	read

This example illustrates sample output from the **show snmp request duplicates** command:

```
RP/0/RSP0/CPU0:router# show snmp request duplicates

No of Duplicate request received/Dropped : 0
```

show snmp request incoming-queue detail

To show the details of the queue of incoming SNMP requests, use the **show snmp request incoming-queue detail** command in EXEC mode.

show snmp request incoming-queue detail

This command has no keywords or arguments.

Command Modes

Global configuration

Command History

Release	Modification
Release 5.2.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

This command shows an output for maximum of 15 queues and an additional general queue. The entry will be deleted when any queue is not polled for 30 minutes.

This command shows these details:

Field	Description
NMS Address	Source address (IPv4 or IPv6) of network management system (NMS) queue. Specifies the NMS packet requests in this queue.
Q Depth	Number of packets to be processed in the queue.
Deque Count	Number of packets that are processed.
Priority	Priority of queue with packets to be processed. The priority ranges from 1 to 5, 1 indicates low priority and 5 indicates high priority.
Enque time	Time stamp of last request in the queue.

Task ID

Task ID	Operations
snmp	read, write

```
RP/0/RSP0/CPU0:router# show snmp request incoming-queue detail
 Wed Mar 12 05:16:59.505 PDT

NMS ADDRESS          Q Depth      Deque count          Priority             Enque time
```

```
4.5.6.7               0               1223            1                   Wed Mar 12
05:16:25

1.2.3.4               0               1193            1                   Wed Mar 12
05:15:06

General Q             0                0              0                   Wed Mar 12
05:14:49

NMS ADDRESS       : 4:5:6::7

  Q Depth     Deque count           Priority              Enque time

  0               1220               1                    Wed Mar 12 05:16:02

NMS ADDRESS       : 1:2:3::4

  Q Depth     Deque count          Priority              Enque time

  0              1221               1                     Wed Mar 12 05:15:37
```

show snmp request type summary

To show the types of requests sent from each network management system (NMS), use the **show snmp request type summary** command in EXEC mode.

show snmp request type summary

This command has no keywords or arguments.

Command Modes

Global configuration

Command History

Release	Modification
Release 5.2.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The **show snmp request type summary** command shows these details:

Field	Description
NMS address	IP address of the NMS that sent the request.
Get	Number of requests of Get type.
Getnext	Number of requests of Getnext type.
Getbulk	Number of requests of Getbulk type.
Set	Number of requests of Set type.
Test	Number of requests of Test type that is part of Set request.

Task ID

Task ID	Operations
snmp	read, write

```
RP/0/RSP0/CPU0:router# show snmp request type summary
 Wed Mar 12 05:17:14.643 PDT
NMS Address          Get      GetNext      GetBulk      Set      Test
 1.2.3.4             0          1254         0          0         0
 4.5.6.7             0          5101         0          0         0

NMS Address : 1:2:3::4
 Get      GetNext      GetBulk      Set      Test
  0          2536        0          0         0
```

```
NMS Address : 4:5:6::7
 Get       GetNext       GetBulk       Set       Test
  0           3817          0           0          0
```

show snmp request type detail

To shows the group that is polled frequently and from which network management system (NMS), use the **show snmp reqest type detail** command in EXEC mode.

show snmp request type detail

This command has no keywords or arguments.

Command Modes

Global configuration

Command History

Release	Modification
Release 5.2.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The **show snmp request type detail** command shows these details:

Field	Description
NMS Address	Address of Network Management Station from which the request is received.
Request	Number of requests from NMS.
SNMPD	Number of requests to snmpd.
Interface	Number of requests to mibd_interface.
Entity	Number of requests to mibd_entity.
Route	Number of requests to mibd_route.
Infra	Number of requests to mibd_infra.

Task ID

Task ID	Operations
snmp	read, write

```
RP/0/RSP0/CPU0:router# show snmp request type detail
Wed Mar 12 05:17:34.838 PDT
NMS Address      Request    AGENT    INTERFACE    ENTITY    ROUTE    INFRA
1.2.3.4          1193       52         742         70       267        123
4.5.6.7          1223       52         742         100      267        123
1:2:3::4         1221       52         742         100      265        123
4:5:6::7         1220       52         742         100      265        122
```

show snmp request drop summary

To show the summary of overall packet drop, use the **show snmp request drop summary** command in EXEC mode.

show snmp request drop summary

This command has no keywords or arguments.

Command Modes

Global configuration

Command History

Release	Modification
Release 5.2.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The **show snmp request drop summary** command shows these details:

Field	Description
NMS Address	Address of network management station from which request is received.
IN Q	Number of packets dropped in incoming queue as the dropped packets are not processed more than 10 seconds.
Encode	Number of packets dropped because of encode errors.
Duplicate	Number of requests dropped with duplicate request feature.
Stack	Numbers of requests are dropped in stack.
AIPC	Number of packets dropped at AIPC module.
Overload	Number of packets dropped because of overload control notification.
Timeout	Number of packets are dropped because of slow response from MIB.
Internal	Number of packets dropped because of internal failures.

Task ID

Task ID	Operations
snmp	read, write

```
RP/0/RSP0/CPU0:router# show snmp request drop summary
 Fri Mar 14 05:32:31.732 PDT
NMS Address          INQ   Encode    Duplicate   Stack    AIPC   Overload   Timeout
Internal
 1.2.3.4              0     0         0           0      0         218        0         0

NMS Address : 1:2:3::4
INQ      Encode     Duplicate    Stack    AIPC    Overload     Timeout     Internal
0         0           0            0       0       109          0           0
```

show snmp request overload stats

To show the number of packets dropped due to overload feature, use the **snmp request overload stats** command in EXEC mode.

show snmp request overload stats

This command has no keywords or arguments.

Command Modes

Global configuration

Command History

Release	Modification
Release 5.2.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

This command displays the latest 100 entries.

The show snmp request overload stats command shows these details:

Field	Description
StartTime	Time when overload control notification is received.
InQInDrop	Number of packet drops before inserting in incoming queue.
InQOutDrop	Number of packets dropped from incoming queue.
EndTime	Time when overload control notification ends.

Task ID

Task ID	Operations
snmp	read, write

```
RP/0/RSP0/CPU0:router# show snmp request overload stats
Thu Mar 13 07:00:45.575 UTC
StartTime                          InQInDrop        InQOutDrop                EndTime

Thu Mar 13 07:00:28                   1               0                        Thu Mar
13 07:00:38
```

show snmp statistics oid group

To show the statistics of object ID (OID), use the **show snmp statistics oid group** command in EXEC mode.

show snmp statistics oid group {**interface** | **infra** | **route** | **entity**}

Syntax Description

interface	mibd_interface sub-agent process
infra	mibd_infra sub-agent process
route	mibd_route sub-agent process
entity	mibd_entity sub-agent process

Command Modes

Global configuration

Command History

Release	Modification
Release 5.2.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The latest 500 entries for each group is displayed and a maximum of 2000 entries is displayed for four groups.

The **show snmp statistics oid group** command shows these details:

Field	Description
SerNum	Unique serial number for each request processing in sub-agents.
Type	Request type.
NumObj	Number of OIDs processing in this request.
MIBMGR-IN	Time stamp of request received from AIPC.
PDU-IN	Time stamp of request sent to MIB for processing. This will be offset in milli seconds from MIBMGR_IN time stamp.
FROM-MIB	Time stamp of response sent from MIB after processing. This will be offset in milli seconds from MIBMGR_IN time stamp.
PDU-OUT	Time stamp of response sent to SNMP through AIPC . This will be offset in milli seconds from MIBMGR_IN.
OID	OID info processing this request.

Field	Description
MIB-IN	Time stamp of the request sent to MIB for each OID.
MIB-OUT	Time stamp of response sent from MIB after processing. This will be offset in milli seconds from MIB-IN.
ExpNext	Request Exp-Next.

Task ID

Task ID	Operations
snmp	read, write

```
RP/0/RSP0/CPU0:router# show snmp statistics oid group interface
Thu Mar 13 07:10:30.310 UTC
SerNum: 2489   Type: GETNEXT     NumObj: 1
  MIBMGR-IN    PDU-IN[ms]          PDU-OUT[ms]          MIBMGR-OUT[ms]
  Mar 13 07:00:49.933                1030                 1030
    OID: 1.3.6.1.2.1.10.32.4.2.0       Exp-Next: Yes
      MIB-IN : Mar 13 07:00:49.933   MIB-OUT[ms] : 1030
SerNum: 10203    Type: GETNEXT     NumObj: 1
  MIBMGR-IN      PDU-IN[ms]          PDU-OUT[ms]            MIBMGR-OUT[ms]
  Mar 13 06:36:16.976    0             1031                   1031
    OID: 1.3.6.1.2.1.10.32.4.2.0  Exp-Next: Yes
      MIB-IN : Mar 13 06:36:16.976   MIB-OUT[ms] : 1031
```

show snmp statistics pdu

To show if processing time of any protocol data unit (PDU) is more than threshold limit, use the **show snmp statistics pdu nms** command in EXEC mode.

show snmp statistics pdu nms[address]

Syntax Description

nms [address]	Address of Network Management Station from which request has arrived. The PDU statistics is filtered for each NMS.

Command Modes

Global configuration

Command History

Release	Modification
Release 5.2.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The PDU processing time can exceed the threshold limit in these scenarios:

- SNMPD not able to dispatch the request to MIB because of any failures in snmpd.
- MIB response after threshold limit.
- MIB does not respond to SNMPD.

Default threshold limit is 2 seconds. To change the default threshold value, use the command:

```
Snmp-server timeouts pdu stats <1-10>
```

The maximum number of entries per network management system (NMS) is 500 and the maximum number of NMS is 30.

This command shows these details:

Field	Description
NMS	Address of Network Management Station from which request has arrived.
Port	Port number of application that requested the SNMP query.
REQID	Request ID for each PDU.
Type	Type of PDU.
SerNum	The unique number generated for every request and sent to all MIBDs.

Field	Description
Timeout	If the request was timeout out set to TRUE, else set to FALSE.
InputQ-In	Time stamp of the PDU when queued into input Q.
InputQ-Out	Time stamp of the PDU when queued into input Q, This will be in milliseconds, Offset from INPUT-IN time stamp.
ProcQ-In	Time stamp of the PDU when queued into Processing Q. This will be in milliseconds, Offset from INPUT-IN time stamp.
Response	Time stamp in milli seconds of the PDU when response is received from sub agents. Offset from INPUT-IN time stamp.

Task ID

Task ID	Operations
snmp	read, write

```
RP/0/RSP0/CPU0:router# show snmp statistics pdu nms
 Thu Mar 13 08:03:17.322 UTC
NMS: 64.103.222.6   PORT: 35028
  REQID:962974264  TYPE: 161  SerNum: 9428 TIMEOUT: No
  INPUTQ-IN                    INPUTQ-OUT[ms]       PROCQ-IN[ms]        RESPONSE[ms]
 Mar 13 08:03:15.269            0                    0                   1056
```

show snmp statistics slow oid

To show the object ID (OID) that has exceeded beyond the threshold time for processing and the number of times that the threshold limit is exceeded with the latest timestamp, use the **show snmp statistics slow oid** command in EXEC mode.

show snmp statistics slow oid

This command has no keywords or arguments.

Command Modes

Global configuration

Command History

Release	Modification
Release 5.2.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Default threshold limit for this data as 500 milli seconds. To change the default value, use the command:

```
Snmp-server logging threshold oid-processing < <0-20000>
```

The latest 500 entries for each sub agent is displayed and a total of upto 2000 entries is maintained.

The **show snmp statistics slow oid** command shows these details:

Field	Description
Type	Request type for slow OID.
Exact OID	Requested OID from NMS.
Resp OID	Response OID for the Request type and EXACT OID.
Slow Count	Number of times OID is slow.
Slow Time	Time taken for processing the OID in milli seconds.
Time Stamp	Time stamp of the slow OID when MIB responded to MIBD.

Task ID

Task ID	Operations
snmp	read, write

This example shows a slow OIDs that exceeds the specified threshold time.

```
RP/0/RSP0/CPU0:router# show snmp statistics slow oid
```

```
 Group:agent

  TYPE                : GETNEXT
  REQ_OID           : 1.3.6.1.2.1.1.1.0
  RESP_OID         : 1.3.6.1.2.1.1.1.2
  COUNT               : 2
  TIME[ms]            : 0
  TIME_STAMP     : Mar 13 05:36:52.279

Group:infra

Group:route

  TYPE               : GETNEXT
  REQ_OID         :
1.3.6.1.2.1.4.34.1.3.4.20.254.128.0.0.0.0.0.0.254.8.255.254.203.38.197.0.0.0.2
  RESP_OID       :
1.3.6.1.2.1.4.34.1.3.4.20.254.128.0.0.0.0.0.0.254.8.255.254.203.38.197.0.0.0.2
  COUNT            : 4
  TIME[ms]         : 14
  TIME_STAMP   : Mar 13 05:36:52.279
  TYPE               : GET
  REQ_OID         :
1.3.6.1.2.1.4.34.1.3.4.20.254.128.0.0.0.0.0.0.254.8.255.254.203.38.197.0.0.0.2
  RESP_OID       :
1.3.6.1.2.1.4.34.1.3.4.20.254.128.0.0.0.0.0.0.254.8.255.254.203.38.197.0.0.0.2
  COUNT            : 4
  TIME[ms]         : 14
  TIME_STAMP   : Mar 13 05:36:52.279

Group:entity

Group:interface

  TYPE                : GETNEXT
  REQ_OID          : 1.3.6.1.2.1.2.1
  RESP_OID        : 1.3.6.1.2.1.2.1.0
  COUNT             : 1
  TIME[ms]          : 0
  TIME_STAMP    : Mar 13 05:36:52.279
```

show snmp statistics poll oid all

To show all object IDs (OIDs) polled from all network management system (NMS) and how many times it has polled, use the **show snmp statistics poll oid all** command in EXEC mode.

For this command to work, the following configuration has to be committed:

(config)#snmp-server oid-poll-stats

show snmp statistics poll oid all

This command has no keywords or arguments.

Command Modes

Global configuration

Command History

Release	Modification
Release 5.2.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The maximum number of entries equals the number of OIDs that were polled. The maximum number of NMS details for each OID is 15.

The **show snmp statistics poll oid all** command shows these details:

Field	Description
Object ID	OID requested from NMS.
NMS	List of NMS IP address requested for each OID.
Count	Number of times OID is polled for each NMS.

Task ID

Task ID	Operations
snmp	read, write

```
RP/0/RSP0/CPU0:router# show snmp statistics poll oid all
 Object ID   :   1.3.6.1.2.1.1.3
 NMS                  COUNT
 10.2.1.3               10
 10.3.1.2               30
 10.4.1.3               20
 10.12.1.3              5

Object ID    :    1.3.6.1.2.1.1.4
NMS                   COUNT
10.2.1.3                10
```

```
10.3.1.2                5
10.4.1.3                20
10.12.1.3               30

Object ID   :  1.3.6.1.2.1.1.5
NMS                    COUNT
10.2.1.3                10
10.3.1.2                3
10.4.1.3                2
```

Show snmp statistics poll oid nms

To show which object ID (OID) is polled from which network management system (NMS) and how many times it has polled, use the **show snmp statistics poll oid nms** command in EXEC mode.

show snmp statistics poll oid nms<V4 / V6 address>

This command has no keywords or arguments.

Command Modes

Global configuration

Command History

Release	Modification
Release 5.2.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The **show snmp statistics poll oid nms** command shows these details:

Field	Description
Object ID	OID requested from NMS.
NMS	List of NMS IP address requested for each OID.
Count	Number of times OID is polled for each NMS.

Task ID

Task ID	Operations
snmp	read, write

```
RP/0/RSP0/CPU0:router# show snmp statistics poll nms 1.2.3.4
 NMS Address   : 1.2.3.4
Object ID                 Count
1.3.6.1.2.1.2.2.1.2       14
```

show snmp statistics slow oid [after/before] hh:mm:ss day mday year

To show the object ID (OID) that has exceeded beyond the threshold time for processing and the number of times that the threshold limit is exceeded with the latest timestamp, use the **show snmp statistics slow oid [after/before] hh:mm:ss day mday year** command in EXEC mode.

show snmp statistics slow oid[after/before] hh:mm:ss day mday year

This command has no keywords or arguments.

Command Modes

Global configuration

Command History

Release	Modification
Release 5.2.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Default threshold limit for this data as 500 milli seconds. To change the default value, use the command:

```
Snmp-server logging threshold oid-processing < <0-20000>
```

The latest 500 entries for each sub agent is displayed and a total of upto 2000 entries is maintained.

The **show snmp statistics slow oid [after/before] hh:mm:ss day mday year** command shows these details:

Field	Description
Type	Request type for slow OID.
Exact OID	Requested OID from NMS.
Resp OID	Response OID for the Request type and EXACT OID.
Slow Count	Number of times OID is slow.
Slow Time	Time taken for processing the OID in milli seconds.
Time Stamp	Time stamp of the slow OID when MIB responded to MIBD.

Task ID

Task ID	Operations
snmp	read, write

This example shows a slow OIDs that exceeds the specified threshold time.

```
RP/0/RSP0/CPU0:router# show snmp statistics slow oid
Group:agent

  TYPE                : GETNEXT
  REQ_OID          : 1.3.6.1.2.1.1.1.0
  RESP_OID        : 1.3.6.1.2.1.1.1.2
  COUNT             : 2
  TIME[ms]          : 0
  TIME_STAMP    : Mar 13 05:36:52.279

Group:infra
Group:route
  TYPE              : GETNEXT
  REQ_OID        :
1.3.6.1.2.1.4.34.1.3.4.20.254.128.0.0.0.0.0.0.254.8.255.254.203.38.197.0.0.0.2
  RESP_OID      :
1.3.6.1.2.1.4.34.1.3.4.20.254.128.0.0.0.0.0.0.254.8.255.254.203.38.197.0.0.0.2
  COUNT           : 4
  TIME[ms]        : 14
  TIME_STAMP  : Mar 13 05:36:52.279

  TYPE              : GET
  REQ_OID        :
1.3.6.1.2.1.4.34.1.3.4.20.254.128.0.0.0.0.0.0.254.8.255.254.203.38.197.0.0.0.2
  RESP_OID      :
1.3.6.1.2.1.4.34.1.3.4.20.254.128.0.0.0.0.0.0.254.8.255.254.203.38.197.0.0.0.2
  COUNT           : 4
  TIME[ms]        : 14
  TIME_STAMP  : Mar 13 05:36:52.279

Group:entity
Group:interface
  TYPE               : GETNEXT
  REQ_OID         : 1.3.6.1.2.1.2.1
  RESP_OID       : 1.3.6.1.2.1.2.1.0
  COUNT            : 1
  TIME[ms]         : 0
  TIME_STAMP   : Mar 13 05:36:52.279
```

show snmp mib ifmib general

To show how many requests get data from internal cache and how many requests are sent to statsd to get data, use the **show snmp mib ifmib general** command in EXEC mode.

show snmp mib ifmib general

This command has no keywords or arguments.

Command Modes

Global configuration

Command History

Release	Modification
Release 5.2.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Default IFMIB internal cache is 15 seconds. To change the duration, use the command:

```
snmp-server ifmib internal cache max-duration <0-60>
```

The default duration is 15 seconds, 0 seconds to disable the IFMIB internal cache.

To service the requests from Stats cache instead of Drivers, use the command:

```
snmp-server ifmib stats cache
```

The **show snmp mib ifmib general** command shows these details:

Field	Description
Cache Hit	Number of times the request retrieves data from IFMIB internal cache.
Cache Miss	Number of times the request processed from statsd, and not from IFMIB internal cache
Last Access Time	Latest time stamp of corresponding hit or miss.
Count	Number of times the data is retrieved.

The Cache Hit and Cache Miss are 32 bit counters. The maximum value is 2^31 and reset to 0 if the maximum value is exceeded.

Task ID

Task ID	Operations
snmp	read, write

```
RP/0/RSP0/CPU0:router# Show snmp mib ifmib general
```

```
 Fri Mar 14 05:05:50.408 PDT

Type                    Count            Last Access Time

Cache Hit               328              Mar 14 05:05:47.480

Cache Miss               2               Mar 14 05:05:47.386
```

show snmp mib ifmib cache

To show the Ifindex that has exceeded the threshold time for processing, the request type and the time stamp, use the **show snmp mib ifmib cache** command in EXEC mode. The threshold time for the data to create an entry is 500 milli seconds.

show snmp mib ifmib cache

This command has no keywords or arguments.

Command Modes

Global configuration

Command History

Release	Modification
Release 5.2.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

This command displays the latest 500 entries. An entry will be added when the difference between Cache in and Cache out time is more than 500 milli seconds. The timeout value cannot be changed.

The **show snmp mib ifmib cache** command shows these details:

Field	Description
Index	Interface index.
MIB IN	Time stamp of the request when IFMIB starts processing.
Cache In	Time stamp in milli seconds when data retrieval from the cache starts for the request. It is offset from MIB IN time stamp.
Cache Out	Time stamp in milli seconds when data is retrieved from cache. It is offset from MIB IN time stamp.
MIB Out	Time stamp in milli seconds of the response from IF MIB. It is offset from MIB IN time stamp.

Task ID

Task ID	Operations
snmp	read, write

```
RP/0/RSP0/CPU0:router# show snmp mib ifmib cache
IFIndex    Type          MIB IN                    CACHE IN[ms]          CACHE OUT[ms]
```

```
        MIB OUT[ms]

2          NEXT          Mar 18 07:14:41.815           4                    701
           701

2          NEXT          Mar 18 07:15:36.815           0                    679
           679

2          NEXT          Mar 18 07:16:00.735           0                    684
           684
```

show snmp mib ifmib statsd

To show the Ifindex that has exceeded the threshold time for processing, the request type and the time stamp, use the **show snmp mib ifmib statsd** command in EXEC mode. The threshold time for the data to create an entry is 500 milli seconds.

show snmp mib ifmib statsd

This command has no keywords or arguments.

Command Modes

Global configuration

Command History

Release	Modification
Release 5.2.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

This command displays the latest 500 entries. An entry will be added when the difference between Stats in and Stats out time is more than 500 milli seconds. The timeout value cannot be changed.

The **show snmp mib ifmib statsd** command shows these details:

Field	Description
Index	Interface index.
MIB IN	Time stamp of the request when IFMIB starts processing.
Stats In	Time stamp in milli seconds when data retrieval from the Statsd starts for the request. It is offset from MIB IN time stamp.
Stats Out	Time stamp in milli seconds when data is retrieved from Statsd. It is offset from MIB IN time stamp.
MIB Out	Time stamp in milli seconds of the response from IF MIB. It is offset from MIB IN time stamp.

Task ID

Task ID	Operations
snmp	read, write

```
RP/0/RSP0/CPU0:router# show snmp mib ifmib statsd
IFIndex    Type          MIB IN                    STATS IN[ms]      STATS OUT[ms]     MIB
```

```
 OUT[ms]

2           NEXT          Mar 18 07:14:41.815         4                   701
701

2           NEXT          Mar 18 07:15:36.815         0                   679
679

2           NEXT          Mar 18 07:16:00.735         0                   684
684
```

show snmp traps details

To show the details about the traps generated for each host, the sent and drop count and the timestamp, use the **show snmp traps details** command in EXEC mode.

show snmp traps details

This command has no keywords or arguments.

Command Modes

Global configuration

Command History

Release	Modification
Release 5.2.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The **show snmp traps details** command shows these details:

Field	Description
TrapOID	Generated trap.
Sent	Number of times the trap sent from the host and port configured.
Drop	Number of times the trap dropped from the host and port configured.
Last-sent	Time stamp when the last trap was sent from the host and port.
Last-drop	Time stamp when the last trap dropped from the host and port.
Host	Configured address of the host to receive traps
udp-port	Configured port to receive traps

Task ID

Task ID	Operations
snmp	read, write

```
RP/0/RSP0/CPU0:router# show snmp traps details
Mon Apr  7 17:14:07.241 UTC
HOST:9.22.24.150, udp-port:3333
------------------------------
```

```
TrapOID                             Sent    Drop     Last-sent                     Last-drop
ciscoConfigManMIB.2.0.1               2          0      Mon Apr 07 14 17:12:29          ~
ciscoFlashDeviceInsertedNotif         1          0      Mon Apr 07 14 17:12:28          ~
ciscoFlashDeviceRemovedNotif          1          0      Mon Apr 07 14 17:12:28          ~
```

show snmp informs details

To show the details about the informs generated for each host, the drop and retry count and the timestamp, use the **show snmp informs details** command in EXEC mode.

show snmp informs details

This command has no keywords or arguments.

Command Modes

Global configuration

Command History

Release	Modification
Release 5.2.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The **show snmp informs details** command shows these details:

Field	Description
InformOID	Generated inform.
Sent	Number of times the Inform is sent from the inform host and port configiured.
Drop	Number of times the Inform is sent from the inform host and port configiured.
Retry	Number of times the Inform retries from the inform host and port configiured
Last-sent	Time stamp when the last inform was sent from the host and port.
Last-drop	Time stamp when the last inform dropped from the host and port.
Host	Configured address of the host to receive traps.
udp-port	Configured port to receive traps.

Task ID

Task ID	Operations
snmp	read, write

```
RP/0/RSP0/CPU0:router# show snmp informs details
Mon Apr  7 17:14:17.212 UTC
HOST:9.22.24.150, udp-port:5555
------------------------------
InformOID                          Sent    Drop    Retry   Last-sent
Last-drop
ciscoConfigManMIB.2.0.1            8       2       6       Mon Apr 07 14 17:12:54      Mon
 Apr 07 14 17:12:42
ciscoFlashDeviceInsertedNotif      4       1       3       Mon Apr 07 14 17:12:55      Mon
 Apr 07 14 17:12:42
ciscoFlashDeviceRemovedNotif       4       1       3       Mon Apr 07 14 17:12:54      Mon
 Apr 07 14 17:12:42
ciscoMgmt.117.2.0.1                8       2       6       Mon Apr 07 14 17:12:53      Mon
 Apr 07 14 17:12:42
ciscoMgmt.117.2.0.2                4       1       3       Mon Apr 07 14 17:12:52      Mon
 Apr 07 14 17:12:42|
```

show snmp users

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

EXEC

mode.

show snmp users

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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

Use the **show snmp users** command to display information about all configured users.

When configuring SNMP, you may see the logging message "Configuring snmpv3 USM user." USM stands for the User-Based Security Model (USM) for SNMP Version 3 (SNMPv3). For further information about USM, see RFC 3414, *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)*.

Task ID

Task ID	Operations
snmp	read

This example shows sample output from the **show snmp users** command:

```
RP/0/RSP0/CPU0:router# show snmp users

  User name:user1
  Engine ID:localSnmpID
  storage-type:nonvolatile active
```

Table 6: show snmp users Field Descriptions

Field	Definition
User name	String identifying the name of the SNMP user.
Engine ID	String identifying the name of the copy of SNMP on the device.
storage-type	Settings that are set in volatile or temporary memory on the device, or in nonvolatile or persistent memory where settings remain after the device is turned off and on again.

Related Topics

snmp-server group, on page 98
snmp-server user, on page 192

show snmp view

To display the configured views and the associated MIB view family name, storage type, and status, use the **show snmp view** command in

EXEC

mode.

show snmp view

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
snmp	read

This example shows sample output from the **show snmp view** command:

```
RP/0/RSP0/CPU0:router# show snmp view

  view1 1.3 - included nonVolatile active
  v1default 1.3.6.1 - included nonVolatile active
```

Related Topics

snmp-server group, on page 98
snmp-server user, on page 192

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 *serial-number*
no snmp-server chassis-id

Syntax Description

serial-number	Unique identification string to identify the chassis serial number.

Command Default

On hardware platforms, where the serial number can be read by the device, the default is the serial number. For example, some Cisco devices have default chassis ID values of their serial numbers.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **snmp-server chassis-id** command to provide a message line identifying the SNMP server serial number.

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

Task ID

Task ID	Operations
snmp	read, write

The following example shows how to specify the chassis serial number 1234456:

```
RP/0/RSP0/CPU0:router# snmp-server chassis-id 1234456
```

Related Topics

show snmp, on page 27

snmp-server community

To configure 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 [**clear** | **encrypted**] *community-string* [**view** *view-name*] [**RO** | **RW**] [**SDROwner** | **SystemOwner**] [*access-list-name*]
no snmp-server community *community-string*

Syntax Description

clear	(Optional) Specifies that the entered *community-string* is clear text and should be encrypted when displayed by the **show running** command.
encrypted	(Optional) Specifies that the entered *community-string* is encrypted text and should be displayed as such by the **show running** command.
community-string	Community string that acts like a password and permits access to the SNMP protocol. The maximum length of the *community-string* argument is 32 alphabetic characters. If the **clear** keyword was used, *community-string* is assumed to be clear text. If the **encrypted** keyword was used, *community-string* is assumed to be encrypted. If neither was used, *community-string* is assumed to be clear text.
view *view-name*	(Optional) Specifies the name of a previously defined view. The view defines the objects available to the community.
RO	(Optional) Specifies read-only access. Authorized management stations are able only to retrieve MIB objects.
RW	(Optional) Specifies read-write access. Authorized management stations are able both to retrieve and to modify MIB objects.
SDROwner	(Optional) Limits access to the owner service domain router (SDR).
SystemOwner	(Optional) Provides system-wide access.
access-list-name	(Optional) Name of an access list of IP addresses allowed to use the community string to gain access to the SNMP agent.

Command Default

By default, an SNMP community string permits read-only access to all MIB objects.

By default, a community string is assigned to the SDR owner.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **snmp-server community** command to configure the community access string to permit access to SNMP.

To remove the specified community string, use the **no** form of this command.

Use the **clear** keyword to specify that the clear text community string you enter is displayed encrypted in the **show running** command output. To enter an encrypted string, use the **encrypted** keyword. To enter a clear text community string that is not encrypted by the system, use neither of these keywords.

When the **snmp-server community** command is entered with the **SDROwner** keyword, SNMP access is granted only to the MIB object instances in the owner SDR.

When the **snmp-server community** command is entered with the **SystemOwner** keyword, SNMP access is granted to the entire system.

Task ID

Task ID	Operations
snmp	read, write

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

```
RP/0/RSP0/CPU0:router(config)# snmp-server community comaccess ro 4
```

The following example shows how to assign the string mgr to SNMP, allowing read-write access to the objects in the restricted view:

```
RP/0/RSP0/CPU0:router(config)# snmp-server community mgr view restricted rw
```

This example shows how to remove the community comaccess:

```
RP/0/RSP0/CPU0:router(config)#no snmp-server community comaccess
```

Related Topics

snmp-server view, on page 195

snmp-server community-map

To associate a Simple Network Management Protocol (SNMP) community with an SNMP context, security name, or a target-list use the **snmp-server 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-server community-map [**clear** | **encrypted**] *community-string* [**context** *context-name*] [**security-name** *security-name*] [**target-list** *target*]
no snmp-server community-map [**clear** | **encrypted**] *community-string*

Syntax Description

clear	(Optional) Specifies that the *community-string* argument is clear text.
encrypted	(Optional) Specifies that the community-string argument is encrypted text.
community-string	Name of the community.
context *context-name*	(Optional) Name of the SNMP context to which this community name is to be mapped.
security-name *security-name*	(Optional) Security name for this community. By default, the *string* is the security name.
target-list *target*	(Optional) Name of the target list for this community.

Command Default

The value of the *community-string* argument is also the security name.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **snmp-server community-map** command to map an SNMPv1 or SNMPv2c community name to one or more of the following:

- **context name**—Maps a community name to a specific SNMP context name. This allows MIB instances in an SNMP context to be accessed through SNMPv1 or SNMPv2c using this community name.
- **security name**—By default, the community name is used to authenticate SNMPv1 and SNMPv2c. Configure a security name for a community name to override the default and authenticate SNMP with the security name.
- **target**—Target list identifies a list of valid hosts from which SNMP access can be made using a specific security name. When such mapping is done for a particular community name, SNMP access is allowed only from hosts included in the target list.

Use the **clear** keyword to specify that the clear text community string you enter is displayed encrypted in the **show running** command output. To enter an encrypted string, use the **encrypted** keyword. To enter a clear text community string that is not encrypted by the system, use neither of these keywords.

Task ID

Task ID	Operations
snmp	read, write

This example maps the community name “sample 2” to the SNMP context name “sample1”:

```
RP/0/RSP0/CPU0:router(config)# snmp-server community-map sample2 context sample1
```

Related Topics

snmp-server context, on page 90
snmp-server target list, on page 141

snmp-server contact

To set the Simple Network Management Protocol (SNMP) system contact, 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 *system-contact-string*
no snmp-server contact

Syntax Description

system-contact-string	String that describes the system contact information. The maximum string length is 255 alphanumeric characters.

Command Default

No system contact is set.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **snmp-server contact** command to set the system contact string. Use the **no** form of this command to remove the system contact information.

Task ID

Task ID	Operations
snmp	read, write

This example shows how to specify a system contact string:

```
RP/0/RSP0/CPU0:router(config)# snmp-server contact Dial System Operator at beeper # 27345
```

Related Topics

snmp-server location, on page 118

snmp-server context

To create a Simple Network Management Protocol (SNMP) context, use the **snmp-server context** command in

global configuration

mode. To remove 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.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use commands of this module, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using any command, contact your AAA administrator for assistance.

This command creates an SNMP context. By default, all the SNMP MIB instances are in a default context. Create an SNMP context and map it to a particular feature to enable similar instances of the same object to co-exist in different SNMP contexts.

Task ID

Task ID	Operations
snmp	read, write

This example creates a new SNMP context named “sample1:”

```
RP/0/RSP0/CPU0:router(config)# snmp-server context sample1
```

Related Topics

snmp-server community-map, on page 87
snmp-server vrf, on page 197

snmp-server context mapping

To map an SNMP context with a protocol instance, topology or VRF entity, use the **snmp-server context mapping** command in global configuration mode.

snmp-server context mapping *context-name* [**feature** *feature-name*] [**instance** *instance-name*] [**topology** *topology-name*] [**vrf** *vrf-name*]

Syntax Description

context-name	Name of the SNMP context.
feature *feature-name*	Specifies the protocol for which to map the context. Available options are: • **bridge**—Layer 2 VPN bridge • **vrf**—Virtual Routing and Forwarding
instance *instance-name*	Maps the context to the specified protocol instance.
topology *topology-name*	Maps the context to the specified protocol topology.
vrf *vrf-name*	Maps the context to the specified VRF logical entity.

Command Default

No context mappings exist by default.

Command Modes

Global configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

A device can support multiple instances of a logical network entity, such as protocol instances or VRFs. Most existing MIBs cannot distinguish between these multiple logical network entities. For example, the original OSPF-MIB assumes a single protocol instance on a device, but you can now configure multiple OSPF instances on a device.

The **snmp-server context mapping** command maps a context to a protocol instance, topology or VRF logical entity.



Note The snmp-server context mapping command does not work for OSPF and OSPFv3. Refer to the **snmp context** commands.

Task ID

Task ID	Operation
snmp	read, write

This example illustrates how to map an snmp context to an OSPF instance:

```
RP/0/RSP0/CPU0:router(config)# snmp-server context mapping con5 feature ospf instance in1
```

Related Topics

show snmp context, on page 30
snmp context (OSPF)

snmp-server drop report acl

To apply an ACL policy for restricting an SNMPv3 unknown engine-id report to be sent out to NMS, use the **snmp-server drop report acl** command in the configuration mode.

snmp-server drop report acl IPv4 *IPv4-acl-name* **IPv6** *IPv6-acl-name*

Syntax Description

acl	Specifies IP Access Control Lists (ACL) policy
IPv4 *IPv4-acl-name*	Defines an IPv4 ACL name.
IPv6 *IPv6-acl-name*	Defines an IPv6 ACL name.

Command Default

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

Command Modes

Configuration mode

Command History

Release	Modification
Release 6.2.3	This command was introduced.

Usage Guidelines

To drop an unknown engine-id report, you can either configure IPv4/IPv6 ACL name or both. When router is polled with wrong engine-id or no engine-id during a snmpv3 packet exchange, the unknown engine-id report will be sent based on the ACL policy that is configured.

Unknown engine-id 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 engin-id report:

```
RP/0/RSP0/CPU0:router (config) #  snmp-server drop report acl IPv4 nms-block IPv6
nms-block-ipv6
```

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.

Command Modes

XR config

Command History

Release	Modification
Release 6.2.3	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
snmp	read, write

Example

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

```
RP/0/RSP0/CPU0:router (config) #  snmp-sever drop unknown-user
```

snmp-server engineid local

To specify Simple Network Management Protocol (SNMP) engine ID on the local device, use the **snmp-server engineid local** command in

global configuration

mode. To return the engine ID to the default, use the **no** form of this command.

snmp-server engineid local *engine-id*
no snmp-server engineid local *engine-id*

Syntax Description

engine-id	Character string that identifies the engine ID. Consists of up to 24 characters in hexadecimal format. Each hexadecimal number is separated by a colon (:).

Command Default

An SNMP engine ID is generated automatically.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
snmp	read, write

This example shows how to configure the SNMP engine ID on the local device:

```
RP/0/RSP0/CPU0:router(config)# snmp-server engineID local 00:00:00:09:00:00:00:a1:61:6c:20:61
```

Related Topics

show snmp engineid, on page 33

snmp-server engineid remote

To specify a Simple Network Management Protocol (SNMP) engine ID on a remote device, use the **snmp-server engineid remote** command in

global configuration

mode. To return the engine ID to the default, use the **no** form of this command.

snmp-server engineid remote *ip-address engine-id* **udp-port** *port*
no snmp-server engineid remote *ip-address engine-id* **udp-port** *port*

Syntax Description

ip-address	IP address of remote SNMP notification host
engine-id	Character string that identifies the engine ID. Consists of up to 24 characters in hexadecimal format. Each hexadecimal number is separated by a colon (:).
udp-port *port*	(Optional) Specifies the User Datagram Protocol (UDP) port of the host to use. Range is from 1 to 65535. The default UDP port is 161.

Command Default

An SNMP engine ID is generated automatically.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
snmp	read, write

This example shows how to configure the SNMP engine ID on the local device:

```
RP/0/RP0/CPU0:Router(config)# snmp-server engineID remote 172.16.4.1
00:00:00:09:00:00:00:a1:61:6c:20:61
```

Related Topics

show snmp engineid, on page 33
snmp-server engineid local, on page 95

snmp-server entityindex persist

To enable the persistent storage of ENTITY-MIB data across process restarts, switchovers, and device reloads, use the **snmp-server entityindex persist** command in

global configuration

mode. To disable the persistent storage of ENTITY-MIB data, use the **no** form of this command.

snmp-server entityindex persist
no snmp-server entityindex persist

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
snmp	read, write

Example

This example illustrates how to enable persistent storage of ENTITY-MIB indices:

```
RP/0/RSP0/CPU0:router(config)# snmp-server entityindex persist
```

Related Topics

snmp-server mibs cbqosmib persist, on page 127

snmp-server group

To configure a new Simple Network Management Protocol (SNMP) group, or a table that maps SNMP users to SNMP views, use the **snmp-server group** command in

global configuration

mode. To remove a specified SNMP group, use the **no** form of this command.

snmp-server group *name* {**v1** | **v2c** | **v3** {**auth** | **noauth** | **priv**}} [**read** *view*] [**write** *view*] [**notify** *view*] [**context** *context-name*] [*access-list-name*]
no snmp-server group *name*

Syntax Description

name	Name of the group.
v1	Specifies a group that uses the SNMPv1 security model. The SNMP v1 security model is the least secure of the possible security models.
v2c	Specifies a group that uses the SNMPv2c security model. The SNMPv2c security model is the second least secure of the possible security models.
v3	Specifies a group that uses the SNMPv3 security model. The SNMP v3 security is the most secure of the possible security models.
auth	Specifies authentication of a packet without encrypting it.
noauth	Specifies no authentication of a packet.
priv	Specifies authentication of a packet with encryption.
read *view*	(Optional) Specifies a read view string (not to exceed 64 characters) that is the name of the view that allows only the contents of the agent to be viewed.
write *view*	(Optional) Specifies a write view string (not to exceed 64 characters) that is the name of the view used to enter data and configure the contents of the agent.
notify *view*	(Optional) Specifies a notify view string (not to exceed 64 characters) that is the name of the view used to specify a notify or trap.
context *context-name*	(Optional) Specifies the SNMP context to associate with this SNMP group and associated views.
access-list-name	(Optional) Access list string (not to exceed 64 characters) that is the name of the access list.

Command Default

See Table 7: snmp-server group Default Descriptions, on page 99.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

This table describes the default values for the different views:

Table 7: snmp-server group Default Descriptions

Default	Definition
read *view*	Assumed to be every object belonging to the Internet (1.3.6.1) object identifier (OID) space, unless the user uses the **read** option to override this state.
write *view*	Nothing is defined for the write view (that is, the null OID). You must configure write access.
notify *view*	Nothing is defined for the notify view (that is, the null OID). If a view is specified, any notifications in that view that are generated are sent to all users associated with the group (provided an SNMP server host configuration exists for the user).

Configuring Notify Views

Do not specify a notify view when configuring an SNMP group for the following reasons:

- The **snmp-server host** command autogenerates a notify view for the user, and then adds it to the group associated with that user.
- Modifying the notify view of the group affects all users associated with that group.

The notify view option is available for two reasons:

- If a group has a notify view that is set using SNMP, you may need to change the notify view.
- The **snmp-server host** command may have been configured before the **snmp-server group** command. In this case, reconfigure the **snmp-server host** command or specify the appropriate notify view.

Instead of specifying the notify view for a group as part of the **snmp-server group** command, use the following commands in global configuration mode:

- **snmp-server user**—Configures an SNMP user.
- **snmp-server group**—Configures an SNMP group, without adding a notify view.
- **snmp-server host**—Autogenerates the notify view by specifying the recipient of a trap operation.

Working with Passwords and Digests

No default values exist for authentication or privacy algorithms when this command is configured. In addition, no default passwords exist. The minimum length for a password is one character, although we recommend using eight characters for security. A plain-text password or localized Message Digest 5 (MD5) password can be specified. Forgotten passwords cannot be recovered, and the user must be reconfigured.

SNMP Contexts

SNMP contexts provide Virtual Private Network (VPN) users with a secure way of accessing MIB data. When a VPN is associated with a context, that VPN's specific MIB data 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.

Task ID

Task ID	Operations
snmp	read, write

The following example shows how to configure an SNMP version 3 group named group1 that requires the authentication of packets with encryption:

```
RP/0/RSP0/CPU0:router(config)# snmp-server group group1 v3 priv
```

Related Topics

show snmp, on page 27
show snmp group, on page 37
snmp-server host, on page 101
snmp-server view, on page 195

snmp-server host

To specify the recipient of a Simple Network Management Protocol (SNMP) notification operation, use the **snmp-server host** command in

global configuration

mode. To remove the specified host, use the **no** form of this command.

snmp-server host *address* [**clear** | **encrypted**] [**informs**] [**traps**] [**version** {**1** | **2c** | **3** {**auth** | **noauth** | **priv**}}] *community-string* [**udp-port** *port*] [*notification-type*]
nosnmp-server host *address* [**clear** | **encrypted**] [**informs**] [**traps**] [**version** {**1** | **2c** | **3** {**auth** | **noauth** | **priv**}}] *community-string* [**udp-port** *port*] [*notification-type*]

Syntax Description

address	Name or IP address of the host (the targeted recipient).
clear	(Optional) Specifies that the *community-string* argument is clear text.
encrypted	(Optional) Specifies that the *community-string* argument is encrypted text.
informs	(Optional) Specifies to send inform messages to this host.
traps	(Optional) Specifies that notifications should be sent as traps. This is the default.
version	(Optional) Specifies the version of the SNMP used to send the traps.
1	Specifies SNMPv1, the default.
2c	Specifies SNMPv2C.
3	Specifies SNMPv3. Version 3 is the most secure model because it allows packet encryption. If you specify the SNMPv3 keyword, you must specify the security level.
auth	Enables Message Digest 5 (MD5) algorithm and Secure Hash Algorithm (SHA) packet authentication.
noauth	Specifies that the noAuthNoPriv security level applies to this host. This is the default security level for SNMPv3.
priv	Enables Data Encryption Standard (DES) packet encryption (also called "privacy").
community-string	Password-like community string sent with the notification operation. We recommend defining this string using the **snmp-server community** command prior to using the **snmp-server host** command.
udp-port *port*	(Optional) Specifies the User Datagram Protocol (UDP) port of the host to use. Range is from 1 to 65535. The default UDP port is 161.

notification-type	(Optional) Type of notification to be sent to the host. If no type is specified, all available notifications are sent. The notification type can be one or more of these keywords: • **bgp** —Enables SNMP Border Gateway Protocol Version 4 (BGPv4) traps. • **config** —Controls configuration notifications, as defined in the CISCO-CONFIG-MAN-MIB (enterprise 1.3.6.1.4.1.9.9.43.2). The notification type is (1) ciscoConfigManEvent. • **copy-complete** —Enables CISCO-CONFIG-COPY-MIB ccCopyCompletion traps. • **entity** —Controls Entity MIB modification notifications. This notification type is defined in the ENTITY-MIB (enterprise 1.3.6.1.2.1.47.2) as: (1) entConfigChange. • **fabric** —Enables SNMP fabric traps. • **fru-ctrl** —Enables SNMP entity field-replaceable unit (FRU) control traps. • **mpls** —Enables SNMP Multiprotocol Label Switching (MPLS) traps. • **sensor** —Enables SNMP entity sensor traps. • **snmp** —Enables SNMP traps. • **syslog** —Controls error message notifications (Cisco-syslog-MIB). Specify the level of messages to be sent with the **logging history** command.

Command Default

This command is disabled by default. No notifications are sent.

The default UDP port is 161.

When this command is entered without keywords, the default is to send all trap types to the host.

If no version keyword is entered, the default is version 1.

If version 3 is specified, but the security level is not specified, the default security level is noauth.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

SNMP notifications can be sent as traps. Traps are unreliable because the receiver does not send acknowledgments when it receives traps. The sender cannot determine if the traps were received. Traps are discarded as soon as they are sent. Traps are also sent only once.

When the **snmp-server host** command is not entered, no notifications are sent. To configure the device to send SNMP notifications, configure at least one **snmp-server host** command. When the command is entered without keywords, all trap types are enabled for the host.

To enable multiple hosts, issue a separate **snmp-server host** command for each host. You can specify multiple notification types in the command for each host.

When multiple **snmp-server host** commands are given for the same host and kind of notification (trap), each succeeding **snmp-server host** command overwrites the previous command. Only the last **snmp-server host** command is in effect. For example, if an **snmp-server host** command with the **traps** keyword is entered for a host and then another command with the **traps** keyword is entered for the same host, the second command replaces the first.

Either a host name or IP address can be used to specify the host.

The **snmp-server host** command is used with the **snmp-server engineid** command. Use the **snmp-server traps** command to specify which SNMP notifications are sent globally. For a host to receive most notifications, at least one **snmp-server traps** command and the **snmp-server host** command for that host must be enabled.

However, some notification types cannot be controlled with the **snmp-server traps** command. For example, some notification types are always enabled. Other notification types are enabled by a different command.

The availability of a notification-type depends on the device type and Cisco software features supported on the device.

To display which notification types are available on the system, use the question mark (**?**) online help function at the end of the **snmp-server host** command.

Previously, the SNMP agent would drop traps after 5 minutes if the respective hosts were unreachable. In its new behavior, the SNMP agent now sends traps to all unreachable hosts instead of dropping them. There is no change in the trap delay timer behavior.

The **no snmp-server host** command used with no keywords disables traps.

Use the **clear** keyword to specify that the clear text community string you enter is displayed encrypted in the **show running** command output. To enter an encrypted string, use the **encrypted** keyword. To enter a clear text community string that is not encrypted by the system, use neither of these keywords.

Task ID

Task ID	Operations
snmp	read, write

This example shows how to send RFC 1157 SNMP traps to the host specified by the name myhost.cisco.com. Other traps are enabled, but only SNMP traps are sent because only the **snmp** keyword is specified in the **snmp-server host** command. The community string is defined as comaccess.

```
RP/0/RSP0/CPU0:router(config)# snmp-server traps
RP/0/RSP0/CPU0:router(config)# snmp-server host myhost.cisco.com comaccess snmp
```

This example shows how to send the SNMP traps to address 172.30.2.160:

```
RP/0/RSP0/CPU0:router(config)# snmp-server traps snmp
```

```
RP/0/RSP0/CPU0:router(config)# snmp-server host 172.30.2.160 public snmp
```

This example shows how to enable the router to send all traps to the host, myhost.cisco.com, using the community string public:

```
RP/0/RSP0/CPU0:router(config)# snmp-server traps
RP/0/RSP0/CPU0:router(config)# snmp-server host myhost.cisco.com public
```

This example shows how to prevent traps from being sent to any host. The BGP traps are enabled for all hosts, but only the configuration traps are enabled to be sent to a host.

```
RP/0/RSP0/CPU0:router(config)# snmp-server traps bgp
RP/0/RSP0/CPU0:router(config)# snmp-server host hostabc public config
```

Related Topics

snmp-server engineid local, on page 95
snmp-server inform, on page 110
snmp-server traps bgp

snmp-server ifindex persist

To enable ifIndex persistence globally on all Simple Network Management Protocol (SNMP) interfaces, use the **snmp-server ifindex persist** command in global configuration mode. To disable global interface persistence, use the **no** form of this command.

snmp-server ifindex persist
no snmp-server ifindex persist

Syntax Description

This command has no keywords or arguments.

Command Default

Global interface persistence is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **snmp-server ifindex persist** command to enable ifIndex persistence on all interfaces that have entries in the ifIndex table of the IF-MIB. When enabled, this command retains the mapping between the ifName object values and the ifIndex object values (generated from the IF-MIB) persistent during reloads, allowing for consistent identification of specific interfaces using SNMP. Applications such as device inventory, billing, and fault detection depend on this feature.

Task ID

Task ID	Operations
snmp	read, write

This example shows how to enable ifIndex persistence globally:

```
RP/0/RSP0/CPU0:router(config)# snmp-server ifindex persist
```

Related Topics

index persistence, on page 12
notification linkupdown, on page 18
show snmp interface, on page 41

snmp-server ifmib ifalias long

To enable the ifAlias IF-MIB object to accept an interface alias name that exceeds the 64-byte default, use the **snmp-server ifmib ifalias long** command. Use the **no** form of this command to revert to the default length.

snmp-server ifmib ifalias long
no snmp-server ifmib ifalias long

Syntax Description

This command has no keywords or arguments.

Command Default

Global interface persistence is disabled.

The alias name is 64 bytes in length.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **snmp-server ifmib ifalias long** command to enable the IF-MIB object ifAlias to accept an interface alias name that is greater than 64 bytes in length. The default length for the alias name is 64 bytes.

Task ID

Task ID	Operations
snmp	read, write

This example shows how to enable the IF-MIB object ifAlias:

```
RP/0/RSP0/CPU0:router(config)# snmp-server ifmib ifalias long
RP/0/RSP0/CPU0:router(config)# exit

Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:yes
RP/0/RSP0/CPU0:router#
```

snmp-server ifmib internal cache max-duration

To configure the refresh interval for the IF-MIB statistics cache, use the **snmp-server ifmib internal cache max-duration** command in global configuration mode. To revert to the default cache interval, use the **no** form of this command.

snmp-server ifmib internal cache max-duration *timeout*

Syntax Description

timeout	Length of time before the cache is refreshed. Values can range from 0 to 60 seconds. The default is 15.

Command Default

timeout: 15 seconds

Command Modes

Global configuration

Command History

Release	Modification
Release 4.2.3	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The **snmp-server ifmib internal cache max-duration** command controls the refresh interval of the cache. If the *timeout* value in the **snmp-server ifmib internal cache max-duration** command is set to zero, the cache is disabled. By default, the counters are cached for 15 secs in the ifmib internal cache, after which it will be discarded.

Task ID

Task ID	Operation
snmp	read, write

This example shows how to change the refresh interval for the IF-MIB statistics cache.

```
RP/0/RSP0/CPU0:routerrouter(config)# snmp-server ifmib internal cache max-duration 60
```

Related Topics

snmp-server ifmib stats cache, on page 109

snmp-server ifmib ipsubscriber

To enable IP subscriber interfaces in the interfaces MIB (IF-MIB), use the **snmp-server ifmib ipsubscriber** command in global configuration mode. To disable IP subscriber interfaces, use the **no** form of this command.

snmp-server ifmib ipsubscriber
no snmp-server ifmib ipsubscriber

Syntax Description

This command has no keywords or arguments.

Command Default

Ip subscriber interfaces are not enabled.

Command Modes

Global configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
snmp	read, write

This example shows how to enable IP subscriber interfaces in the IF-MIB:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# snmp-server ifmib ipsubscriber
```

snmp-server ifmib stats cache

To enable retrieval of cached statistics instead of real-time statistics, use the **snmp-server ifmib stats cache** command. To revert to the default, use the **no** form of this command.

snmp-server ifmib stats cache
no snmp-server ifmib stats cache

Syntax Description

This command has no keywords or arguments.

Command Default

Cached statistics are not enabled.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Cisco IOS XR statistics infrastructure maintains a cache of statistics for all interfaces. This cache is updated every 30 seconds. Use the **snmp-server ifmib stats cache** command to enable the IF-MIB to retrieve these cached statistics rather than real-time statistics. Accessing cached statistics is less CPU-intensive than accessing real-time statistics.

Task ID

Task ID	Operations
snmp	read, write

This example shows how to enable the IF-MIB caches statistics:

```
RP/0/RSP0/CPU0:router(config)# snmp-server ifmib stats cache
RP/0/RSP0/CPU0:router(config)# exit

Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:yes
RP/0/RSP0/CPU0:router#
```

Related Topics

snmp-server ifmib internal cache max-duration, on page 107

snmp-server inform

To configure Simple Network Management Protocol (SNMP) inform message options, use the **snmp-server inform** command in global configuration mode. To revert to the default informs options, use the **no** form of this command.

snmp-server inform {**pending** *max-no* | **retries** *no-retries* | **timeout** *seconds*}
no snmp-server inform {**pending** *max-no* | **retries** *no-retries* | **timeout** *seconds*}

Syntax Description

pending *max-no*	Specifies the maximum number of inform messages to hold in the queue. The default is 25.
retries *no-retries*	Specifies the retry count for inform messages. Values can be from 1 to 100. The default is three.
timeout *seconds*	Specifies the inform message timeout value in seconds. The default is 15.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

To enable the sending of SNMP inform messages, use the **snmp-server host** command with the **informs** keyword. When SNMP server informs are enabled, the SNMP version can be only SNMPv2C or SNMPv3.

Task ID

Task ID	Operations
snmp	read, write

This example shows how to configure SNMP inform messages:

```
RP/0/RSP0/CPU0:router(config)# snmp-server host myhost.cisco.com informs comaccess
RP/0/RSP0/CPU0:router(config)# snmp-server inform pending 40
RP/0/RSP0/CPU0:router(config)# snmp-server inform retries 10
```

Related Topics

snmp-server host, on page 101

snmp-server interface

To enable an interface to send Simple Network Management Protocol (SNMP) trap notifications and enter SNMP interface configuration mode, use the **snmp-server interface** command in global configuration mode. To disable the sending of SNMP trap notifications on an interface, use the **no** form of this command.

snmp-server interface *type interface-path-id*
no snmp-server interface *type interface-path-id*

Syntax Description

type	Interface type. For more information, use the question mark (**?**) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.

Command Default

Ethernet interfaces are enabled to send SNMP trap notifications. SNMP trap notifications are disabled on all other physical and logical interfaces.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The **snmp-server interface** command enters SNMP interface configuration mode for you to configure the available SNMP options.

Note In references to a Management Ethernet interface located on a route switch processor card, the physical slot number is numeric (0 through n-1 where n is the number of line card slots in the chassis) and the module is CPU0. Example: interface MgmtEth0/1/CPU0/0.

Task ID

Task ID	Operations
snmp	read, write

This example shows how to assign ifIndex persistence on Packet-over-SONET/SDH (POS) interface 0/0/1/0:

```
RP/0/RSP0/CPU0:router(config)# snmp-server interface pos 0/0/1/0
RP/0/RSP0/CPU0:router(config-snmp-if)#
```

Related Topics

show snmp interface, on page 41
snmp-server engineid local, on page 95
snmp-server ifindex persist, on page 105

snmp-server interface subset

To enter snmp-server interface subset configuration mode for a set of interfaces, use the **snmp-server interface subset** command in global configuration mode. To revert to the default interface settings, use the **no** form of this command.

snmp-server interface subset *subset-number* **regular-expression** *expression*
no snmp-server interface subset *subset-number*

Syntax Description

subset-number	Identifying number of the interface subset, which also indicates its relative priority.
regular-expression *expression*	Specifies for which subset of interfaces to enter snmp-server interface subset configuration mode. The *expression* argument must be entered surrounded by double quotes.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The *subset-number* argument is used to set the priority for an interface that matches more than one configured regular expressions. Lower values of the *subset-number* have a higher priority. If a single interface becomes part of a multiple-interface configured regular expression, the configuration with the lower *subset-number* value is applied.

Regular expressions have two constraints:

- Regular expressions must always be entered within double quotes to ensure that the CLI interprets each character correctly.
- All characters that are part of a regular expression are considered regular characters with no special meaning. In order to enter special characters, such as "\" or "?," they must be preceded by the backslash character "\." For example, to enter the regular expression ([A-Z][A-Z0-9]*)\b[^>]*>(.*?)</\1, you would enter ([A-Z][A-Z0-9]*)\\b[^>]*>(.*\?)</\\1.

Refer to the *Understanding Regular Expressions, Special Characters, and Patterns* module in *Cisco ASR 9000 Series Aggregation Services Router Getting Started Guide* for more information regarding regular expressions.

From the snmp-server interface mode of a subset of interfaces, SNMP linkUp and linkDown notifications can be enabled or disabled using the **notification linkupdown disable** command.

Task ID

Task ID	Operation
snmp	read, write

This example illustrates how to configure all Gigabit Ethernet interfaces:

```
RP/0/RSP0/CPU0:router# config
RP/0/RSP0/CPU0:router(config)# snmp-server int subset 2
    regular-expression "^Gig[a-zA-Z]+[0-9/]+\."
RP/0/RSP0/CPU0:router(config-snmp-if-subset)#
```

Related Topics

notification linkupdown, on page 18
show snmp interface notification, on page 43
show snmp interface regular-expression, on page 45

snmp-server ipv4 dscp

To mark packets with a specific differentiated services code point (DSCP) value, use the **snmp-server ipv4 dscp** command in global configuration mode. To remove matching criteria, use the **no** form of this command.

snmp-server ipv4 dscp *value*
no snmp-server ipv4 dscp [*value*]

Syntax Description

value	Value of the DSCP. The DSCP value can be a number from 0 to 63, or it can be one of the following keywords: **default**, **ef**, **af11**, **af12**, **af13**, **af21**, **af22**, **af23**, **af31**, **af32**, **af33**, **af41**, **af42**, **af43**, **cs1**, **cs2**, **cs3**, **cs4**, **cs5**, **cs6**, **cs7**.

Command Default

The IP DSCP default value for SNMP traffic is 0.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **snmp-server ipv4 dscp** command to specify an IP DSCP value to give SNMP traffic higher or lower priority in your network.

Task ID

Task ID	Operations
snmp	read, write

This example shows how to configure the DSCP value to af32:

```
RP/0/RSP0/CPU0:router(config)# snmp-server ipv4 dscp af32
```

snmp-server ipv4 precedence

To mark packets with a specific precedence level to use for packet matching, use the **snmp-server ipv4 precedence** command in global configuration mode. To restore the system to its default interval values, use the **no** form of this command.

snmp-server ipv4 precedence *value*
no snmp-server ipv4 precedence [*value*]

Syntax Description

value Value of the precedence. The precedence value can be a number from 0 to 7, or it can be one of the following keywords:

critical

Set packets with critical precedence (5)

flash

Set packets with flash precedence (3)

flash-override

Set packets with flash override precedence (4)

immediate

Set packets with immediate precedence (2)

internet

Set packets with internetwork control precedence (6)

network

Set packets with network control precedence (7)

priority

Set packets with priority precedence (1)

routine

Set packets with routine precedence (0)

Command Default

The IP Precedence default value for SNMP traffic is 0.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **snmp-server ipv4 precedence** command to specify an IP Precedence value to give SNMP traffic higher or lower priority in your network.

Task ID

Task ID	Operations
snmp	read, write

This example shows how to set the precedence to 2:

```
RP/0/RSP0/CPU0:router(config)# snmp-server ipv4 precedence 2
```

snmp-server location

To specify the system location for Simple Network Management Protocol (SNMP), use the **snmp-server location** command in

global configuration

mode. To remove the location string, use the **no** form of this command.

snmp-server location *system-location*
no snmp-server location

Syntax Description

system-location	String indicating the physical location of this device. The maximum string length is 255 alphanumeric characters.

Command Default

No system location string is set.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
snmp	read, write

This example shows how to specify a system location string:

```
RP/0/RSP0/CPU0:router(config)# snmp-server location Building 3/Room 214
```

Related Topics

snmp-server contact, on page 89

snmp-server mib bulkstat max-procmem-size

To configure the overall per-process memory size limit used by all bulk statistics files in the process, use the **snmp-server mib bulkstat max-procmem-size** command in

global configuration

mode. To remove the overall per-process memory size, use the **no** form of this command.

snmp mib bulkstat max-procmem-size *size*
no snmp mib bulkstat max-procmem-size [*size*]

Syntax Description

size	Overall per-process memory size limit in kilobytes. The valid range is from 100 to 200000. The default is 200000.

Command Default

The maximum process memory size is 200000 KB.

Command Modes

Global configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Currently 300 MB is the maximum process memory available for MIB and SNMP processes.

Task ID

Task ID	Operation
snmp	read, write

This example sets the maximum process memory size to 100000 KB.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# snmp-server mib bulkstat max-procmem-size 100000
```

snmp-server mib bulkstat object-list

To configure a Simple Network Management Protocol (SNMP) bulk statistics object list and enter bulk statistics objects configuration mode, use the **snmp-server mib bulkstat object-list** in

global configuration

mode. To remove an SNMP object list configuration, use the **no** form of this command.

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

Syntax Description

object-list-name	Name or object identifier (OID) of the bulk statistics object list to configure.

Command Default

No SNMP bulk statistics object list is configured.

Command Modes

Global configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The **snmp-server 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.Use the **add** command to add objects to the object list configured with the **snmp-server mib bulkstat object-list** command. Bulk statistics object lists can be reused in multiple schemas.

Task ID

Task ID	Operation
snmp	read, write

In this example, a bulk statistics object list called ifmib is configured to include two objects:

```
RP/0/RSP0/CPU0:router# config
RP/0/RSP0/CPU0:router(config)# snmp-server mib bulkstat object-list ifmib
RP/0/RSP0/CPU0:router(config-bulk-objects)# add ifOutOctets
RP/0/RSP0/CPU0:router(config-bulk-objects)# add ifInOctets
```

Related Topics

add (bulkstat object), on page 5
show snmp mib bulkstat transfer, on page 49

snmp-server mib bulkstat schema

To configure a Simple Network Management Protocol (SNMP) bulk statistics schema and enter bulk statistics schema configuration mode, use the **snmp-server mib bulkstat schema** command in

global configuration

mode. To remove the SNMP bulk statistics schema, use the **no** form of this command.

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

Syntax Description

schema-name	Specifies the name of the schema to configure.

Command Default

No schemas are configured.

Command Modes

Global configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The **snmp-server 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.

Task ID

Task ID	Operation
snmp	read, write

The following example shows how to configure a bulk statistics schema called GigE0/6/5/0:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# snmp-server mib bulkstat schema tengige 0/6/5/0
RP/0/RSP0/CPU0:router(config-bulk-sc)# object-list ifmib
RP/0/RSP0/CPU0:router(config-bulk-sc)# poll-interval 3
RP/0/RSP0/CPU0:router(config-bulk-sc)# instance exact interface tengige 0/6/5/0 subif
```

```
RP/0/RSP0/CPU0:router(config-bulk-sc)# exit
```

Related Topics

instance (bulkstat schema), on page 13
poll-interval, on page 21

snmp-server mib bulkstat transfer-id

To identify the bulk statistics transfer configuration and enter bulk statistics transfer configuration mode, use the **snmp-server mib bulkstat transfer-id** command in

global configuration

mode. To remove a previously configured transfer, use the **no** form of this command

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

Syntax Description

transfer-id	Name of the transfer configuration.

Command Default

Bulk statistics transfer is not configured.

Command Modes

Global configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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.

Task ID

Task ID	Operation
snmp	read, write

In this example, The bulk statistics transfer is given the name bulkstat1 and contains two schemas:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# snmp-server mib bulkstat transfer-id bulkstat1
RP/0/RSP0/CPU0:router(config-bulk-tr)# schema IFMIB
RP/0/RSP0/CPU0:router(config-bulk-tr)# schema CAR
RP/0/RSP0/CPU0:router(config-bulk-tr)# url primary
ftp://user1:pswrd@cbin2-host/users/user1/bulkstat1
RP/0/RSP0/CPU0:router(config-bulk-tr)# url secondary
tftp://user1@10.1.0.1/tftpboot/user1/bulkstat1
RP/0/RSP0/CPU0:router(config-bulk-tr)# format schemaASCII
RP/0/RSP0/CPU0:router(config-bulk-tr)# transfer-interval 30
RP/0/RSP0/CPU0:router(config-bulk-tr)# retry 5
RP/0/RSP0/CPU0:router(config-bulk-tr)# buffer-size 1024
```

```
RP/0/RSP0/CPU0:router(config-bulk-tr)# retain 30
RP/0/RSP0/CPU0:router(config-bulk-tr)# end
```

Related Topics

buffer-size, on page 6
format (bulkstat), on page 10
retain, on page 22
retry, on page 24
schema, on page 26
show snmp mib bulkstat transfer, on page 49
transfer-interval, on page 207
url, on page 209

snmp-server mibs cbqosmib cache

To enable and configure caching of the QoS MIB statistics, use the **snmp-server mibs cbqosmib cache** command in global configuration mode. To disable caching, use the **no** form of this command.

snmp-server mibs cbqosmib cache {**refresh time** *time* | **service-policy count** *count*}
no snmp-server mibs cbqosmib cache [**refresh time** *time* | **service-policy count** *count*]

Syntax Description

refresh	Enables QoS MIB caching with a specified cache refresh time.
time *time*	Specifies the cache refresh time, in seconds. The *time* argument can be between 5 and 60. The default is 30.
service-policy	Enables QoS MIB caching with a limited number of service policies to cache.
count *count*	Specifies the maximum number of service policies to cache. The count argument can be between 1 and 5000.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
snmp	read, write

Example

This example illustrates how to enable QoS MIB caching with a refresh time:

```
RP/0/RSP0/CPU0:router(config)# snmp-server mibs cbqosmib cache refresh time 45
```

This example illustrates how to enable QoS MIB caching with a service policy count limitation:

```
RP/0/RSP0/CPU0:router(config)# snmp-server mibs cbqosmib cache service-policy count 10
```

Related Topics

snmp-server entityindex persist, on page 97
snmp-server mibs cbqosmib persist, on page 127

snmp-server mibs cbqosmib persist

To enable persistent storage of the CISCO-CLASS-BASED-QOS-MIB data across process restarts, switchovers, and device reloads, use the **snmp-server mibs cbqosmib persist** command in global configuration mode. To disable persistent storage of the MIB data, use the **no** form of this command.

snmp-server mibs cbqosmib persist
no snmp-server mibs cbqosmib persist

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
snmp	read, write

Example

This example illustrates how to enable persistent storage of CISCO-CLASS-BASED-QOS-MIB data:

```
RP/0/RSP0/CPU0:router(config)# snmp-server mibs cbqosmib persist
```

Related Topics

snmp-server entityindex persist, on page 97

snmp-server mibs eventmib congestion-control

To configure the generation of SNMP traps when congestion exceeds configured thresholds, use the **snmp-server mibs eventmib congestion-control** command in global configuration mode. To restore the default values, use the **no** form of this command.

snmp-server mibs eventmib congestion-control *type interface-path-id* **falling** *lower-threshold* **interval** *sampling-interval* **rising** *upper-threshold*
no snmp-server mibs eventmib congestion-control *type interface-path-id*

Syntax Description

type	Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the show interfaces command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.
falling *lower-threshold*	Specifies the lower threshold for which to determine whether an mteTriggerFalling SNMP Trap is generated.
interval *sampling-interval*	Specifies how often the congestion statistics are polled. The *interval* argument, in minutes, can be between 5 and 1440; it must be a multiple of 5.
rising *upper-threshold*	Specifies the upper threshold for which to determine whether an mteTriggerRising SNMP Trap is generated.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Note A maximum of 100 interfaces can be monitored for congestion.

Congestion configurations using the **snmp-server mibs eventmib congestion-control** command cannot be modified using SNMP SET and vice versa.

When the congestion between two intervals increases above the *upper-threshold* argument, an mteTriggerRising SNMP trap is generated. This trap is not generated until the congestion drops below the lower threshold and then rises above the upper threshold.

When the congestion between two intervals falls below the *lower-threshold* argument, and an SNMP mteTriggerRising trap was generated previously, an SNMP mteTriggerFalling trap is generated. The mteTriggreRising trap is not generated until the congestion goes above the upper threshold and then falls back below the lower threshold.

The *lower-threshold* value (falling) should be set to a value less than or equal to the *upper-threshold* value (rising).

The **snmp-server mibs eventmib congestion-control** command is configured on a specific interface and is supported on the following cards:

- 8-port 10 Gigabit Ethernet PLIM
- 16-port OC-48c/STM-16 POS/DPT PLIM
- 1-port OC-768c/STM-256 POS PLIM
- 4-port OC-192c/STM-64 POS/DPT PLIM
- All Ethernet SPAs
- 2-port and 4-port OC-3c/STM-1 POS SPAs
- 2-port, 4-port, and 8-port OC-12c/STM-4 POS SPAs
- 2-port and 4-port OC-48c/STM-16 POS/RPR SPAs
- 1-port OC-192c/STM-64 POS/RPR SPA

Task ID

Task ID	Operations
snmp	read, write

This example shows how to configure the generation of SNMP traps in response to congestion:

```
RP/0/RSP0/CPU0:router(config)# snmp-server mibs eventmib congestion-control pos 0/1/0/0
    falling 1 interval 5 rising 2
```

snmp-server mibs eventmib packet-loss

To configure the generation of SNMP traps when packet loss exceeds configured thresholds, use the **snmp-server mibs eventmib packet-loss** command in global configuration mode. To restore the default values, use the **no** form of this command.

snmp-server mibs eventmib packet-loss *type interface-path-id* **falling** *lower-threshold* **interval** *sampling-interval* **rising** *upper-threshold*
no snmp-server mibs eventmib packet-loss *type interface-path-id*

Syntax Description

type	Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the show interfaces command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.
falling *lower-threshold*	Specifies the lower threshold for which to determine whether an mteTriggerFalling SNMP Trap is generated.
interval *sampling-interval*	Specifies how often the packet loss statistics are polled. The *interval* argument, in minutes, can be between 5 and 1440; it must be a multiple of 5.
rising *upper-threshold*	Specifies the upper threshold for which to determine whether an mteTriggerRising SNMP Trap is generated.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Note A maximum of 100 interfaces can be monitored for packet loss.

Packet loss configurations using the **snmp-server mibs eventmib packet-loss** command cannot be modified using SNMP SET and vice versa.

When the packet loss between two intervals increases above the *upper-threshold* argument, an mteTriggerRising SNMP trap is generated. This trap is not generated until the packet loss drops below the lower threshold and then rises above the upper threshold.

When the packet loss between two intervals falls below the *lower-threshold* argument, and an SNMP mteTriggerRising trap was generated previously, an SNMP mteTriggerFalling trap is generated. The mteTriggreRising trap is not generated until the packet loss goes above the upper threshold and then falls back below the lower threshold.

The *lower-threshold* value (falling) should be set to a value less than or equal to the *upper-threshold* value (rising).

The **snmp-server mibs eventmib packet-loss** command is configured on a specific interface and is supported on the following cards:

- 8-port 10 Gigabit Ethernet PLIM
- 16-port OC-48c/STM-16 POS/DPT PLIM
- 1-port OC-768c/STM-256 POS PLIM
- 4-port OC-192c/STM-64 POS/DPT PLIM
- All Ethernet SPAs
- 2-port and 4-port OC-3c/STM-1 POS SPAs
- 2-port, 4-port, and 8-port OC-12c/STM-4 POS SPAs
- 2-port and 4-port OC-48c/STM-16 POS/RPR SPAs
- 1-port OC-192c/STM-64 POS/RPR SPA

Task ID

Task ID

Task ID	Operations
snmp	read, write

This example shows how to configure the generation of SNMP traps in response to packet loss:

```
RP/0/RSP0/CPU0:router(config)# snmp-server mibs eventmib packet-loss pos 0/1/0/0
    falling 1 interval 5 rising 2
```

snmp-server mibs sensormib cache

To enable and configure caching for sensor mib values, use **snmp-server mibs sensormib cache** command in global configuration mode. To restore the default values, use the **no** form of this command.

snmp-server mibs sensormib cache

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Global configuration mode.

Command History

Release	Modification
Release 5.3.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Example

```
RP/0/RSP0/CPU0:router(config)# snmp-server mibs sensormib cache
```

snmp-server mibs subscriber threshold

To set the snmp-server mibs server threshold parameters, use the **snmp-server mibs subscriber threshold** command in the global configuration mode. To delete any of the set parameters, use the **no** form of the command.

snmp-server mibs subscriber threshold [**rising** | **falling** | **delta-loss percent** | **delta-loss evaluation**] [**access-if location** *interface-path-id* **interval** *seconds*] [**session-count**]

nosnmp-server mibs subscriber threshold

Syntax Description

rising	Rising threshold value. The set value triggers the traps. Traps are generated when the number of sessions exceed the rising threshold value.
falling	Falling threshold value. The set value triggers the traps. Traps are generated when the number of sessions are lesser than the falling threshold value.
delta-loss percent	Delta-loss percentage.
delta-loss evaluation	The actual subscriber sessions (after delta-loss) . This is based on the set delta-loss percentage. If the number of sessions exceed the loss percentage, traps are generated.
access-if	Access-interface.
location *name*	Location name.
interval *seconds*	Interval between the rising and the falling thresholds (in seconds).
session-count	Subscriber-session count.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Release 5.1	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The minimum delta loss interval is 30 seconds and can be incremented by 10 seconds till the time period reaches 5 minutes.

Task ID

Task ID	Operation
snmp	read, write

Example

```
RP/0/RSP0/CPU0:router (config) # snmp-server mibs subscriber threshold delta-loss evaluation
 access-if tengige 0/4/0/0 interval 100
```

snmp-server mibs subscriber threshold access-if

To disable the per-session access notifications by the session monitoring process, use the **snmp-server mibs subscriber threshold access-if** in the global configuration mode. To enable notifications, use the **no** form of the command.

snmp-server mibs subscriber threshold access-if subset*number* **regular expression** *word* **notification rising-falling disable**
nosnmp-server mibs subscriber threshold access-if

Syntax Description

subset *number*	Subset number of the subscriber threshold. Lower the subset value, higher is the priority. Range is 1 to 255.
regular expression *word*	Regular expression to match the interface name. Traps on the corresponding access interface(s) are disabled.
notification	Name of the notification.
rising-falling	The rising and falling thresholds.
disable	Disables the access interface notifications.

Command Default

Session monitoring is enabled by default

Command Modes

Global configuration

Command History

Release	Modification
Release 5.1	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The **regular expression** keyword disables notifications of the access-interface.

Task ID

Task ID	Operation
snmp	read, write

Example

```
RP/0/RSP0/CPU0:router (config) # snmp-server mibs subscriber threshold access-if subset 100
 regular expression notification rising-falling disable
```

snmp-server notification-log-mib

To configure the NOTIFICATION-LOG-MIB, use the **snmp-server notification-log-mib** command in global configuration mode. To remove the specified configuration, use the **no** form of this command.

snmp-server notification-log-mib {**globalAgeOut** *time* | **globalSize** *size* | **default** | **disable** | **size** *size*}
no snmp-server notification-log-mib {**globalAgeOut** | **globalSize** | **default** | **disable** | **size**}

Syntax Description

globalAgeOut *time*	Specifies how much time, in minutes, a notification remains in the log. Values for the *time* argument can range from 0 to 4294967295; the default is 15.
globalSize *size*	Specifies the maximum number of notifications that can be logged in all logs. The default is 500.
default	Specifies to create a default log.
disable	Specifies to disable logging to the default log.
size *size*	Specifies the maximum number of notifications that the default log can hold. The default is 500.

Command Default

NOTIFICATION-LOG-MIB notifications are not logged.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Logging of NOTIFICATION-LOG-MIB notifications begins when the default log is created. Named logs are not supported, therefore only the default log can be created.

Task ID

Task ID	Operations
snmp	read, write

The following example creates a default log for notifications:

```
RP/0/RSP0/CPU0:router(config)# snmp-server notification-log-mib default
```

This example removes the default log:

```
RP/0/RSP0/CPU0:router(config)# no snmp-server notification-log-mib default
```

This example configures the size of all logs to be 1500:

```
RP/0/RSP0/CPU0:router(config)# snmp-server notification-log-mib globalSize 1500
```

Related Topics

snmp-server community-map, on page 87

snmp-server packetsize

To establish control over the largest Simple Network Management Protocol (SNMP) packet size permitted when the SNMP server is receiving a request or generating a reply, use the **snmp-server packetsize** command in

global configuration

mode. To restore the default value, use the **no** form of this command.

snmp-server packetsize *size*
no snmp-server packetsize

Syntax Description

size	Packet size, in bytes. Range is from 484 to 65500. The default is 1500.

Command Default

size: 1500

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **snmp-server packetsize** command to establish control over the largest SNMP packet size permitted when the SNMP server is receiving a request or generating a reply.

Task ID

Task ID	Operations
snmp	read, write

This example shows how to set the maximum size of SNMP packets to 1024 bytes:

```
RP/0/RSP0/CPU0:router(config)# snmp-server packetsize 1024
```

snmp-server queue-length

To establish the message queue length for each trap host for Simple Network Management Protocol (SNMP), use the **snmp-server queue-length** command in

global configuration

mode. To restore the default value, use the **no** form of this command.

snmp-server queue-length *length*
no snmp-server queue-length

Syntax Description

length	Integer that specifies the number of trap events that can be held before the queue must be emptied. Range is from 1 to 5000.

Command Default

length : 100

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **snmp-server queue-length** command to define the length of the message queue for each trap host. After a trap message is successfully sent, Cisco IOS XR software continues to empty the queue at a throttled rate to prevent trap flooding.

Task ID

Task ID	Operations
snmp	read, write

This example shows how to set the SNMP notification queue to 20 events:

```
RP/0/RSP0/CPU0:router(config)# snmp-server queue-length 20
```

snmp-server target list

To create a Simple Network Management Protocol (SNMP) target list, use the **snmp-server target list** command in

global configuration

mode. To remove an SNMP target list, use the **no** form of this command.

snmp-server target list *target-list* {**vrf** *vrf-name* | **host** *hostname*}
no snmp-server target list *target-list*

Syntax Description

target-list	Name of the target list.
vrf *vrf-name*	Specifies the name of the VRF hosts included in the target list.
host *hostname*	Assigns a hostname to the target list. The *hostname* variable is a name or IP address.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use this command to create an SNMP target list and assign hosts to the list. When a target list is mapped to a community name using the **snmp-server community-map** command, SNMP access is restricted to the hosts in the target list (for that community name).

Task ID

Task ID	Operations
snmp	read, write

In this example, a new target list “sample3” is created and assigned to the vrf server “server2:”

```
RP/0/RSP0/CPU0:router(config)# snmp-server target list sample3 vrf server2
```

Related Topics

snmp-server community-map, on page 87

snmp-server throttle-time

To specify the throttle time for handling incoming Simple Network Management Protocol (SNMP) messages, use the **snmp-server throttle-time** command in

global configuration

mode. To restore the throttle time to its default value, use the **no** form of this command.

snmp-server throttle-time *time*
no snmp-server throttle-time

Syntax Description

time	Throttle time for the incoming queue, in milliseconds. Values can be from 50 to 1000.

Command Default

time : 0

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
snmp	read, write

In the following example, the throttle time is set to 500 milliseconds:

```
RP/0/RSP0/CPU0:router(config)# snmp-server throttle-time 500
```

Related Topics

snmp-server community-map, on page 87

snmp-server timeouts subagent

To change the timeout used by the SNMP agent while it waits for a response from a subagent, use the **snmp-server timeouts subagent** command in

global configuration

mode. SNMP subagents are feature-specific entities that register with the SNMP agent and implement sets of MIB objects.

snmp-server timeouts subagent *timeout*
no snmp-server timeouts subagent *timeout*

Syntax Description

timeout	The timeout used by the SNMP agent when waiting for a response from a MIB module, in seconds. The default is 10.

Command Default

timeout : 10

Command Modes

Global configuration

Command History

Release	Modification
Release 3.8.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
snmp	read, write

In the following example, the timeout is set to 8 seconds:

```
RP/0/RSP0/CPU0:router(config)# snmp-server timeouts subagent 8
```

snmp-server timeouts duplicate

To set the timeout value for the snmp-sever duplicate request feature, use the **snmp-server timeouts duplicate** command in the appropriate mode. To delete the set value, use the **no** form of the command.

snmp-server timeouts duplicate *timeout-value*
no snmp-server timeouts duplicate *timeout-value*

Syntax Description

timeout-value Timeout value in seconds. Range is 0 to 20 seconds.

- 0- To Remove this feature support. i.e SNMP will process all the packets irrespective of duplicate (retry) Packets.
- 1- This is the default value, i.e if no configuration is present , then, the timeout value is set to 1. If any packet takes more than 1 second for getting processed, then the Duplicate drop feature is enabled.
- 2 to 20 - if the packet processing is done between 2 and 20 seconds, then the Duplicate drop feature is enabled.

Command Default

1 second

Command Modes

Global configuration

Command History

Release	Modification
Release 5.1.1	This feature was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
snmp	read, write

Example

This example shows how to use the **snmp-server timeouts duplicate** command:

```
RP/0/RSP0/CPU0:router (config) #  snmp-server timeouts duplicate 10
```

snmp-server trap authentication vrf disable

To disable authentication traps on VPNs, use the **snmp-server trap authentication vrf disable** command in global configuration mode.

snmp-server trap authentication vrf disable

Syntax Description

This command has no keywords or arguments.

Command Default

Authentication traps are enabled on VPNs by default.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
snmp	read, write

This example illustrates how to disable authentication traps on VPNs:

```
RP/0/RSP0/CPU0:router(config)# snmp-server trap authentication vrf disable
```

Related Topics

snmp-server vrf, on page 197

snmp-server trap link ietf

To enable the varbind used for linkUp and linkDown SNMP traps to utilize the RFC 2863 standard varbind, use the **snmp-server trap link ietf** command in

global configuration

mode. To restore the default value, use the **no** form of this command..

snmp-server trap link ietf
nosnmp-server trap link ietf

Syntax Description

This command has no keywords or arguments.

Command Default

The default varbind used is cisco.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

For more information about linkUP and linkDown notifications, see RFC 2863, *The Interface Group MIB*, and RFC 3418, *Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)*.

Task ID

Task ID	Operations
snmp	read, write

This example shows how to enable the RFC 2863 standard varbind:

```
RP/0/RSP0/CPU0:router# snmp-server trap link ietf
```

Related Topics

snmp-server engineid local, on page 95
snmp-server host, on page 101
snmp-server traps bgp
snmp-server traps snmp, on page 183
snmp-server traps syslog, on page 185

snmp-server trap throttle-time

To specify the throttle time for handling more Simple Network Management Protocol (SNMP) traps, use the **snmp-server trap throttle-time** command in

global configuration

mode. To restore the throttle time to its default value, use the **no** form of this command.

snmp-server trap throttle-time *time*
no snmp-server trap throttle-time

Syntax Description

time	Throttle time in milliseconds. Values can be from 10 to 500.

Command Default

250

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
snmp	read, write

In the following example, the trap throttle time is set to 500 milliseconds:

```
RP/0/RSP0/CPU0:router(config)# snmp-server trap throttle-time 500
```

Related Topics

snmp-server throttle-time, on page 142

snmp-server traps

To enable Simple Network Management Protocol (SNMP) trap notifications, use the **snmp-server traps** command in global configuration mode. To disable SNMP notifications, use the **no** form of this command.

snmp-server traps *notification-type*
no snmp-server traps [*notification-type*]

Syntax Description *notification-type*

(Optional) Type of notification (trap) to enable or disable. If no type is specified, all notifications available on the device are enabled or disabled.

The notification type can be one or more of the following keywords:

bfd

Enables Bidirectional Forwarding Detection (BFD) traps.

bgp

Enables BGP4-MIB and CISCO-BGP4-MIB traps.

bridgemib

Enables SNMP traps for the Bridge MIB.

config

Controls configuration notifications, as defined in the CISCO-CONFIG-MAN-MIB (enterprise 1.3.6.1.4.1.9.9.43.2). The notification type is: (1) ciscoConfigManEvent.

copy-complete

Enables CISCO-CONFIG-COPY-MIB ccCopyCompletion traps.

ds1

Enables SNMP Cisco DS1 traps.

ds2

Enables SNMP Cisco DS2 traps.

entity

Controls Entity MIB modification notifications. This notification type is defined in the ENTITY-MIB (enterprise 1.3.6.1.2.1.47.2) as: (1) entConfigChange.

ethernet

Enables Ethernet link OAM and 802.1ag connectivity fault management traps.

flash insertion

Enables ciscoFlashDeviceInsertedNotif.

flash removal

Enables ciscoFlashDeviceRemovedNotif.

fru-ctrl

Enables SNMP entity field-replaceable unit (FRU) control traps.

hsrp

Enables SNMP HSRP traps.

ipsec tunnel start

Enables SNMP IPsec tunnel start traps.

ipsec tunnel stop

Enables SNMP IPsec tunnel stop traps.

isakmp

Enables ISAKMP traps.

l2vpn all

Enables all Layer 2 VPN traps.

l2vpn vc-down

Enables Layer 2 VPN VC down traps.

l2vpn vc-up

Enables Layer 2 VPN VC up traps.

mpls frr all

Enables all MPLS fast reroute MIB traps.

mpls frr protected

Enables MPLS fast reroute tunnel protected traps.

mpls ldp

Enables SNMP Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP) traps.

mpls traffic-eng

Enables SNMP MPLS traffic engineering traps.

msdp peer-state-change

Enables SNMP MSDP Peer state change traps.

ntp

Enables SNMP Cisco NTP traps.

otn

Enables SNMP Cisco optical transport network (OTN) traps.

pim

Enables SNMP PIM traps.

rf

Enables RF-MIB traps.

sensor

Enables SNMP entity sensor traps.

snmp

Enables SNMP traps.

sonet

Enables SONET traps.

syslog

Controls error message notifications (Cisco-syslog-MIB). Specify the level of messages to be sent with the **logging history** command.

system

Enables SNMP SYSTEMMIB-MIB traps.

vpls

Enables virtual private LAN service (VPLS) traps.

vrrp events

Enables Virtual Router Redundancy Protocol (VRRP) traps.

Note
To display the trap notifications supported on a platform, use the online help (**?**) function.

Command Default

SNMP notifications are disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.
Release 3.9.0	The **bridgemib** , **ds1** , **ds3** , **otn** , , **system** , and **vrrp events** keywords were introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **snmp-server traps** command to enable trap requests for the specified notification types. To configure the router to send SNMP notifications, specify at least one **snmp-server traps** command. When the command is entered with no keyword, all notification types are enabled. When a notification type keyword is specified, only the notification type related to that keyword is enabled. To enable multiple types of notifications, issue a separate **snmp-server traps** command for each notification type.

More information about individual MIBs can be found in the SNMP Object Navigator, available through cisco.com at http://tools.cisco.com/Support/SNMP/do/BrowseMIB.do?local=en&step=2.

The **snmp-server traps** command is used with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications.



Note The use of **flash insertion** and **flash removal** keywords is limited to IOS XR 32-bit OS on ASR 9000.

Task ID

Task ID	Operations
snmp	read, write

Some SNMP trap notifications require additional Task IDs as indicated in the following table:

Notification Type	Task ID	Operations
bfd	bgp	read, write
	ospf	read, write
	isis	read, write
	mpls-te	read, write
	snmp	read, write
bgp	bgp	read, write
copy-complete	config-services	read, write
ipsec	crypto	read, write
isakmp	crypto	read, write
l2vpn	l2vpn	read, write
mpls frr	mpls-ldp	read, write
	mpls-te	read, write
mpls l3vpn	ipv4	read, write
	mpls-ldp	read, write
	mpls-te	read, write
mpls ldp	mpls-ldp	read, write
	mpls-te	read, write
mpls traffic-eng	mpls-ldp	read, write
	mpls-te	read, write
ospf	ospf	read, write
syslog	sysmgr	read, write
vpls	l2vpn	read, write

This example shows how to enable the router to send all traps to the host specified by the name myhost.cisco.com, using the community string defined as public:

```
RP/0/RSP0/CPU0:router(config)# snmp-server traps
RP/0/RSP0/CPU0:router(config)# snmp-server host myhost.cisco.com public
```

Related Topics

snmp-server host, on page 101
snmp-server traps bgp
snmp-server traps snmp, on page 183
snmp-server traps syslog, on page 185

snmp-server traps bgp updown

To enable Border Gateway Protocol (BGP) to receive Simple Network Management Protocol (SNMP) notifications when a BGP peer changes state in IPv4 neighbor sessions, use the **snmp-server traps bgp updown** command in global configuration mode.

snmp-server traps bgp [updown]

Syntax Description

bgp	Specifies IPv4 neighbor sessions.
updown	(Optional) Specifies trap notifications.

Command Default

SNMP notifications are disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
Release 4.3.1	This command was introduced.

Usage Guidelines

SNMP notifications are sent as traps.

BGP generates traps when:

- A neighbor's session state has changed.
- A neighbor prefix limit has exceeded.
- A neighbor prefix count is under the limit.

Multiple traps can be generated when the neighbor is not in steady state.

Configure **snmp-server traps bgp updown** command to prevent the generation multiple traps.

When you configure the **snmp-server traps bgp updown** command, traps are sent out only when the BGP neighbor goes to established state or moves out from the established state. The prefix limit traps remain unaffected.

When you configure the **bgp** keyword, traps are sent for IPv4 neighbor sessions only.

Example

The following example shows how to enable the router to send BGP state-change notifications to the host at the address myhost.cisco.com using the community string defined as public in IPv4 neighbor sessions only:

```
Router(config)# snmp-server traps bgp updown
Router(config)# snmp-server host myhost.cisco.com version 2c public
```

Related References

#unique_448

snmp-server engineid local
snmp-server host
snmp-server traps snmp
snmp-server traps syslog

snmp-server traps cbgp2 updown

To enable Border Gateway Protocol (BGP) to receive Simple Network Management Protocol (SNMP) notifications when a BGP peer changes state in both IPv4 and IPv6 neighbor sessions, use the **snmp-server traps cbgp2 updown** command in global configuration mode.

snmp-server traps cbgp2 [updown]

Syntax Description

cbgp2	Specifies IPv4 and IPv6 neighbor sessions.
updown	(Optional) Specifies trap notifications.

Command Default

SNMP notifications are disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
Release 4.3.1	This command was introduced.

Usage Guidelines

SNMP notifications are sent as traps.

BGP generates traps when:

- A neighbor's session state has changed.
- A neighbor prefix limit has exceeded.
- A neighbor prefix count is under the limit.

Multiple traps can be generated when the neighbor is not in steady state.

Configure **snmp-server traps cbgp2 updown** command to prevent the generation multiple traps.

When you configure the **snmp-server traps cbgp2 updown** command, traps are sent out only when the BGP neighbor goes to established state or moves out from the established state. The prefix limit traps remain unaffected.

When you configure the **cbgp2** keyword, traps are sent for both IPv4 and IPv6 neighbor sessions.

Example

The following example shows how to enable the router to send BGP state-change notifications to the host at the address myhost.cisco.com using the community string defined as public in both IPv4 and IPv6 neighbor sessions:

```
Router(config)# snmp-server traps cbgp2 updown
Router(config)# snmp-server host myhost.cisco.com version 2c public
```

Related References

snmp-server traps bgp updown

snmp-server engineid local
snmp-server host
snmp-server traps snmp
snmp-server traps syslog

snmp-server traps mpls l3vpn

To enable the sending of MPLS Layer 3 VPN Simple Network Management Protocol (SNMP) notifications, use the **snmp-server traps mpls l3vpn** command in global configuration mode. To disable MPLS Layer 3 VPN SNMP notifications, use the **no** form of this command.

snmp-server traps mpls l3vpn {**all** | **max-threshold-cleared** | **max-threshold-exceeded** | **max-threshold-reissue-notif-time** *seconds* | **mid-threshold-exceeded** | **vrf-down** | **vrf-up**}
no snmp-server traps mpls l3vpn

Syntax Description

all	Enables all MPLS Layer 3 VPN traps.
max-threshold-cleared	Enables maximum threshold cleared traps.
max-threshold-exceeded	Enables maximum threshold exceeded traps.
max-threshold-reissue-notif-time *seconds*	Specifies the time interval for reissuing a maximum threshold notification, in seconds.
mid-threshold-exceeded	Enables mid-threshold exceeded traps.
vrf-down	Enables VRF down traps.
vrf-up	Enables VRF up traps.

Command Default

SNMP notifications are disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
snmp	read, write

The following example shows how to enable the device to send MPLS Layer 3 VPN traps:

```
RP/0/RSP0/CPU0:router(config)# snmp-server traps mpls l3vpn all
```

Related Topics

snmp-server traps, on page 148

snmp-server traps ospf errors

To enable Open Shortest Path First (OSPF) error Simple Network Management Protocol (SNMP) notifications, use the **snmp-server traps ospf errors** command in global configuration mode. To disable OSPF error SNMP notifications, use the **no** form of this command.

snmp-server traps ospf errors {**authentication-failure** | **bad-packet** | **config-error** | **virt-authentication-failure** | **virt-bad-packet** | **virt-config-error**}
no snmp-server traps ospf errors {**authentication-failure** | **bad-packet** | **config-error** | **virt-authentication-failure** | **virt-bad-packet** | **virt-config-error**}

Syntax Description

authentication-failure	Enables SNMP traps for authentication failure errors on physical interfaces.
bad-packet	Enables SNMP traps for bad packet errors on physical interfaces.
config-error	Enables SNMP traps for configuration errors on physical interfaces.
virt-authentication-failure	Enables SNMP traps for authentication failure errors on virtual interfaces.
virt-bad-packet	Enables SNMP traps for bad packet errors on virtual interfaces.
virt-config-error	Enables SNMP traps for configuration errors on virtual interfaces.

Command Default

SNMP notifications are disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

SNMP notifications can be sent as traps.

For a complete description of OSPF error notifications and additional MIB functions, see the OSPF-TRAP-MIB in the SNMP Object Navigator, available through cisco.com at http://tools.cisco.com/Support/SNMP/do/BrowseMIB.do?local=en&step=2.

The **snmp-server traps ospf errors** command is used with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications.

Task ID

Task ID	Operations
snmp	read, write

This example shows how to enable the router to send OSPF error notifications to the host at the address myhost.cisco.com using the community string defined as public:

```
RP/0/RSP0/CPU0:router(config)# snmp-server traps ospf errors
RP/0/RSP0/CPU0:router(config)# snmp-server host myhost.cisco.com version 2c public
```

Related Topics

snmp-server engineid local, on page 95
snmp-server host, on page 101
snmp-server traps snmp, on page 183
snmp-server traps syslog, on page 185

snmp-server traps ospf lsa

To enable Open Shortest Path First (OSPF) link-state advertisement Simple Network Management Protocol (SNMP) notifications, use the **snmp-server traps ospf lsa** command in global configuration mode. To disable OSPF link state SNMP notifications, use the **no** form of this command.

snmp-server traps ospf lsa {**lsa-maxage** | **lsa-originate**}
no snmp-server traps ospf lsa {**lsa-maxage** | **lsa-originate**}

Syntax Description

lsa-maxage	Enables SNMP traps for link-state advertisement maxage.
lsa-originate	Enables SNMP traps for new link-state advertisement origination.

Command Default

SNMP notifications are disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

SNMP notifications can be sent as traps.

For a complete description of OSPF link-state advertisement notifications and additional MIB functions, see the OSPF-TRAP-MIB in the SNMP Object Navigator, available through cisco.com at http://tools.cisco.com/Support/SNMP/do/BrowseMIB.do?local=en&step=2.

The **snmp-server traps ospf lsa** command is used with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications.

Task ID

Task ID	Operations
snmp	read, write

This example shows how to enable the router to send OSPF link-state advertisement notifications to the host at the address myhost.cisco.com using the community string defined as public:

```
RP/0/RSP0/CPU0:router(config)# snmp-server traps ospf lsa lsa-maxage
RP/0/RSP0/CPU0:router(config)# snmp-server host myhost.cisco.com version 2c public
```

Related Topics

snmp-server engineid local, on page 95

snmp-server host, on page 101
snmp-server traps snmp, on page 183
snmp-server traps syslog, on page 185

snmp-server traps ospf retransmit

To enable Open Shortest Path First (OSPF) retransmission Simple Network Management Protocol (SNMP) notifications, use the **snmp-server traps ospf retransmit** command in global configuration mode. To disable OSPF retransmission SNMP notifications, use the **no** form of this command.

snmp-server traps ospf retransmit {**packets** | **virt-packets**}
no snmp-server traps ospf retransmit {**packets** | **virt-packets**}

Syntax Description

packets	Enables SNMP traps for packet retransmissions on physical interfaces.
virt-packets	Enables SNMP traps for packet retransmissions on virtual interfaces.

Command Default

SNMP notifications are disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

SNMP notifications can be sent as traps.

For a complete description of OSPF retransmission notifications and additional MIB functions, see the OSPF-TRAP-MIB in the SNMP Object Navigator, available through cisco.com at http://tools.cisco.com/Support/SNMP/do/BrowseMIB.do?local=en&step=2.

The **snmp-server traps ospf retransmit** command is used with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications.

Task ID

Task ID	Operations
snmp	read, write

This example shows how to enable the router to send OSPF retransmission notifications to the host at the address myhost.cisco.com using the community string defined as public:

```
RP/0/RSP0/CPU0:router(config)# snmp-server traps ospf retransmit packets
RP/0/RSP0/CPU0:router(config)# snmp-server host myhost.cisco.com version 2c public
```

Related Topics

snmp-server engineid local, on page 95

snmp-server host, on page 101
snmp-server traps snmp, on page 183
snmp-server traps syslog, on page 185

snmp-server traps ospf state-change

To enable Simple Network Management Protocol (SNMP) notifications for Open Shortest Path First (OSPF) neighbor state change, use the **snmp-server traps ospf state-change** command in global configuration mode. To disable OSPF state-change SNMP notifications, use the **no** form of this command.

snmp-server traps ospf state-change {**if-state-change** | **neighbor-state-change** | **virtif-state-change** | **virtneighbor-state-change**}
no snmp-server traps ospf state-change {**if-state-change** | **neighbor-state-change** | **virtif-state-change** | **virtneighbor-state-change**}

Syntax Description

if-state-change	Enables SNMP traps for OSPF non-virtual interface state chages.
neighbor-state-change	Enables SNMP traps for OSPF neighbor state changes
virtif-state-change	Enables SNMP traps for OSPF virtual interface state changes.
virtneighbor-state-change	Enables SNMP traps for OSPF virtual neighbor state changes.

Command Default

SNMP notifications are disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

SNMP notifications can be sent as traps.

Use the **snmp-server traps ospf state-change** command to enable or disable OSPF server state-change notifications, as defined in the MIB. One notification type is ospfNbrStateChange.

For example, the OSPF ospfNbrStateChange notification is defined in the OSPF MIB as follows:

```
!     ospfNbrStateChange NOTIFICATION-TYPE
!         OBJECTS {
!                     ospfRouterId, -- The originator of the trap
!                     ospfNbrIpAddr,
!                     ospfNbrAddressLessIndex,
!                     ospfNbrRtrId,
!                     ospfNbrState  -- The new state
!                   }
!         STATUS             current
```

For a complete description of these notifications and additional MIB functions, see the OSPF-TRAP-MIB in the SNMP Object Navigator, available through cisco.com at http://tools.cisco.com/Support/SNMP/do/BrowseMIB.do?local=en&step=2.

The **snmp-server traps ospf state-change** command is used with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications.

Task ID

Task ID	Operations
snmp	read, write

The following example shows how to enable the router to send OSPF state-change notifications to the host at the address myhost.cisco.com using the community string defined as public:

```
RP/0/RSP0/CPU0:router(config)# snmp-server traps ospf state-change neighbor-state-change
RP/0/RSP0/CPU0:router(config)# snmp-server host myhost.cisco.com version 2c public
```

Related Topics

snmp-server engineid local, on page 95
snmp-server host, on page 101
snmp-server traps snmp, on page 183
snmp-server traps syslog, on page 185

snmp-server traps ospfv3 errors

To enable Open Shortest Path First (OSPF) Version 3 error Simple Network Management Protocol (SNMP) notifications, use the **snmp-server traps ospfv3 errors** command in global configuration mode. To disable OSPFv3 error SNMP notifications, use the **no** form of this command.

snmp-server traps ospfv3 errors [**bad-packet** | **config-error** | **virt-bad-packet** | **virt-config-error**]
no snmp-server traps ospfv3 errors [**bad-packet** | **config-error** | **virt-bad-packet** | **virt-config-error**]

Syntax Description

bad-packet	Enables SNMP traps for bad packet errors on physical interfaces.
config-error	Enables SNMP traps for configuration errors on physical interfaces.
virt-bad-packet	Enables SNMP traps for bad packet errors on virtual interfaces.
virt-config-error	Enables SNMP traps for configuration errors on virtual interfaces.

Command Default

SNMP notifications are disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
Release 4.2.1	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

SNMP notifications can be sent as traps.

For a complete description of OSPFv3 error notifications and additional MIB functions, see the OSPFV3-MIB in the SNMP Object Navigator, available through cisco.com at http://tools.cisco.com/Support/SNMP/do/BrowseMIB.do?local=en&step=2.

The **snmp-server traps ospfv3 errors** command is used with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications.

Task ID

Task ID	Operations
snmp	read, write

This example shows how to enable the router to send OSPF error notifications to the host at the address myhost.cisco.com using the community string defined as public:

```
RP/0/RSP0/CPU0:router(config)# snmp-server traps ospfv3 errors
RP/0/RSP0/CPU0:router(config)# snmp-server host myhost.cisco.com version 2c public
```

Related Topics

snmp-server engineid local, on page 95
snmp-server host, on page 101
snmp-server traps snmp, on page 183
snmp-server traps syslog, on page 185

snmp-server traps ospfv3 state-change

To enable Simple Network Management Protocol (SNMP) notifications for Open Shortest Path First (OSPF) Version 3 state changes, use the **snmp-server traps ospfv3 state-change** command in global configuration mode. To disable OSPFv3 state-change SNMP notifications, use the **no** form of this command.

snmp-server traps ospfv3 state-change [**if-state-change** | **neighbor-state-change** | **nssa-state-change** | **restart-helper-status-change** | **restart-status-change** | **restart-virtual-helper-status-change** | **virtif-state-change** | **virtneighbor-state-change**]
no snmp-server traps ospfv3 state-change [**if-state-change** | **neighbor-state-change** | **nssa-state-change** | **restart-helper-status-change** | **restart-status-change** | **restart-virtual-helper-status-change** | **virtif-state-change** | **virtneighbor-state-change**]

Syntax Description

if-state-change	Enables SNMP traps for OSPFv3 non-virtual interface state chages.
neighbor-state-change	Enables SNMP traps for OSPFv3 neighbor state changes
nssa-state-change	Enables SNMP traps for OSPFv3 not so stubby area (NSSA) status changes.
restart-helper-status-change	Enables SNMP traps for OSPFv3 restart helper status changes.
restart-status-change	Enables SNMP traps for OSPFv3 restart status changes.
restart-virtual-helper-status-change	Enables SNMP traps for OSPFv3 virtual helper restart status changes.
virtif-state-change	Enables SNMP traps for OSPFv3 virtual interface state changes.
virtneighbor-state-change	Enables SNMP traps for OSPFv3 virtual neighbor state changes.

Command Default

SNMP notifications are disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
Release 4.2.1	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

SNMP notifications can be sent as traps.

Use the **snmp-server traps ospfv3 state-change** command to enable or disable the various OSPFv3 server state-change notifications, as defined in the MIB.

The **snmp-server traps ospfv3 state-change** command is used with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications.

Task ID

Task ID	Operations
snmp	read, write

The following example shows how to enable the router to send OSPFv3 NSSA state-change notifications to the host at the address myhost.cisco.com using the community string defined as public:

```
RP/0/RSP0/CPU0:router(config)# snmp-server traps ospfv3 state-change nssa-state-change
RP/0/RSP0/CPU0:router(config)# snmp-server host myhost.cisco.com version 2c public
```

Related Topics

snmp-server engineid local, on page 95
snmp-server host, on page 101
snmp-server traps snmp, on page 183
snmp-server traps syslog, on page 185

snmp-server traps pim interface-state-change

To enable Protocol Independent Multicast (PIM) interface status notification, use the **snmp-server traps pim interface-state-change** command in global configuration mode. To disable this command so no notification is sent, use the **no** form of this command.

snmp-server traps pim interface-state-change
no snmp-server traps pim interface-state-change

Syntax Description

This command has no keywords or arguments.

Command Default

Simple Network Management Protocol (SNMP) notifications are disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications.

Use the **snmp-server traps pim interface-state-change** command to send notifications when a PIM interface changes status from up to down. When the status is up, the notification signifies the restoration of a PIM interface. When the status is down, the notification signifies the loss of a PIM interface.

PIM notifications are defined in the CISCO-PIM-MIB.my and PIM-MIB.my files that can be accessed from the SNMP Object Navigator, available through cisco.com at http://tools.cisco.com/Support/SNMP/do/BrowseMIB.do?local=en&step=2.

Task ID

Task ID	Operations
snmp	read, write

This example shows how to use the **snmp-server traps pim interface-state-change** command:

```
RP/0/RSP0/CPU0:router(config)# snmp-server traps pim interface-state-change
RP/0/RSP0/CPU0:router(config)# snmp-server host myhost.cisco.com version 2c public
```

Related Topics

snmp-server engineid local, on page 95
snmp-server host, on page 101
snmp-server traps pim invalid-message-received, on page 175

snmp-server traps pim neighbor-change, on page 177
snmp-server traps pim rp-mapping-change, on page 179
snmp-server traps snmp, on page 183
snmp-server traps syslog, on page 185

snmp-server traps pim invalid-message-received

To enable notifications for monitoring invalid Protocol Independent Multicast (PIM) protocol operations, such as invalid register received and invalid join or prune received, use the **snmp-server traps pim invalid-message-received** command in global configuration mode. To disable this command so that no notification is sent, use the **no** form of this command.

snmp-server traps pim invalid-message-received
no snmp-server traps pim invalid-message-received

Syntax Description

This command has no keywords or arguments.

Command Default

Simple Network Management Protocol (SNMP) notifications are disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications.

A router can receive a join or prune message in which the RP specified in the packet is not the RP for the multicast group. Or a router can receive a register message from a multicast group in which it is not the RP.

PIM notifications are defined in the CISCO-PIM-MIB.my and PIM-MIB.my files that can be accessed from the SNMP Object Navigator, available through cisco.com at http://tools.cisco.com/Support/SNMP/do/BrowseMIB.do?local=en&step=2.

Task ID

Task ID	Operations
snmp	read, write

The following example shows how to use the **snmp-server traps pim invalid-message-received** command:

```
RP/0/RSP0/CPU0:router(config)# snmp-server traps pim invalid-message-received
RP/0/RSP0/CPU0:router(config)# snmp-server host myhost.cisco.com version 2c public
```

Related Topics

snmp-server engineid local, on page 95
snmp-server host, on page 101
snmp-server traps pim interface-state-change, on page 173

snmp-server traps pim neighbor-change, on page 177
snmp-server traps pim rp-mapping-change, on page 179
snmp-server traps snmp, on page 183
snmp-server traps syslog, on page 185

snmp-server traps pim neighbor-change

To enable Protocol Independent Multicast (PIM) neighbor status down notifications, use the **snmp-server traps pim neighbor-change** command in global configuration mode. To disable PIM neighbor down notifications, use the **no** form of this command.

snmp-server traps pim neighbor-change
no snmp-server traps pim neighbor-change

Syntax Description

This command has no keywords or arguments.

Command Default

PIM Simple Network Management Protocol (SNMP) notifications are disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **snmp-server traps pim neighbor-change** command to send notifications when a PIM neighbor changes status from up to down on an interface. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications.

PIM notifications are defined in the CISCO-PIM-MIB.my and PIM-MIB.my files that can be accessed from the SNMP Object Navigator, available through cisco.com at http://tools.cisco.com/Support/SNMP/do/BrowseMIB.do?local=en&step=2.

Task ID

Task ID	Operations
snmp	read, write

This example shows how to enable the router to send PIM neighbor status down notifications to the host at the address myhost.cisco.com using the community string defined as public:

```
RP/0/RSP0/CPU0:router(config)# snmp-server traps pim neighbor-change
RP/0/RSP0/CPU0:router(config)# snmp-server host myhost.cisco.com version 2c public
```

Related Topics

snmp-server engineid local, on page 95
snmp-server host, on page 101
snmp-server traps pim interface-state-change, on page 173
snmp-server traps pim invalid-message-received, on page 175

snmp-server traps pim rp-mapping-change, on page 179
snmp-server traps snmp, on page 183
snmp-server traps syslog, on page 185

snmp-server traps pim rp-mapping-change

To enable notifications indicating a change in the rendezvous point (RP) mapping information due to either Auto-RP or bootstrap router (BSR) messages, use the **snmp-server traps pim rp-mapping-change** command in global configuration mode. To disable this command so no notification is sent, use the **no** form of this command.

snmp-server traps pim rp-mapping-change
no snmp-server traps pim rp-mapping-change

Syntax Description

This command has no keywords or arguments.

Command Default

PIM SNMP notifications are disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications.

PIM notifications are defined in the CISCO-PIM-MIB.my and PIM-MIB.my files that can be accessed from the SNMP Object Navigator, available through cisco.com at http://tools.cisco.com/Support/SNMP/do/BrowseMIB.do?local=en&step=2.

Task ID

Task ID	Operations
snmp	read, write

This example shows how to use the **snmp-server traps pim rp-mapping-change** command:

```
RP/0/RSP0/CPU0:router(config)# snmp-server traps pim rp-mapping-change
RP/0/RSP0/CPU0:router(config)# snmp-server host myhost.cisco.com version 2c public
```

Related Topics

snmp-server engineid local, on page 95
snmp-server host, on page 101
snmp-server traps pim interface-state-change, on page 173
snmp-server traps pim neighbor-change, on page 177
snmp-server traps pim invalid-message-received, on page 175
snmp-server traps snmp, on page 183

snmp-server traps syslog, on page 185

snmp-server traps rsvp

To enable the sending of Resource Reservation Protocol (RSVP) notifications, use the **snmp-server traps rsvp** command in global configuration mode. To disable RSVP notifications, use the **no** form of this command.

snmp-server traps rsvp {**all** | **lost-flow** | **new-flow**}

Syntax Description

all	Enables the sending of both new flow lost flow traps.
lost-flow	Enables the sending of traps when a flow is deleted.
new-flow	Enables the sending of traps when a flow is created.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
mpls-te	read, write
ouni	read, write
snmp	read, write

This example illustrates how to enable all SNMP RSVP MIB traps.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# snmp-server traps rsvp all
```

snmp-server traps selective-vrf-download role-change

To attempt to download only those prefixes and labels to a physical entity required to forward traffic through the physical entity, use the **snmp-server trap selective-vrf-download role-change** command in global configuration mode.

snmp-server trap selective-vrf-download role-change

This command has no keywords or arguments.

Command Default

Selective VRF downloads are disabled.

Command Modes

Global configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

The selective VRF download feature makes a best effort to download only those prefixes and labels to a physical entity required to forward traffic through the physical entity. This is accomplished by characterizing roles for physical entities based on their configuration.

From a network management point of view the CISCO-SELECTIVE-VRF-DOWNLOAD-MIB:

- Lists the state relating to the selective VRF download feature for each physical entity capable of forwarding packets.
- Lists the role change history per address family (ipv4 and ipv6) for each physical entity capable of forwarding packets.
- Lists the VRF tables selectively downloaded to each physical entity capable of forwarding packets.

Task ID

Task ID	Operation
snmp	read, write
basic-services	read, write

This example shows how to enable the selective VRF downloads:

```
RP/0/RSP0/CPU0:router(config)# snmp-server traps selective-vrf-download role-change
```

snmp-server traps snmp

To enable the sending of RFC 1157 Simple Network Management Protocol (SNMP) notifications, use the **snmp-server traps snmp** command in the appropriate configuration mode. To disable RFC 1157 SNMP notifications, use the **no** form of this command.

snmp-server traps snmp [**authentication** | **coldstart** | **linkdown** | **linkup** | **warmstart**]
no snmp-server traps snmp [**authentication** | **coldstart** | **linkdown** | **linkup** | **warmstart**]

Syntax Description

authentication	(Optional) Controls the sending of SNMP authentication failure notifications.
linkup	(Optional) Controls the sending of SNMP linkUp notifications
linkdown	(Optional) Controls the sending of SNMP linkDown notifications
coldstart	(Optional) Controls the sending of SNMP coldStart notifications.
warmstart	(Optional) Controls the sending of SNMP warmStart notifications.

Command Default

SNMP notifications are disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.
Release 3.9.0	The **authentication**, **linkup**, **linkdown**, **coldstart**, and **warmstart** keywords were added.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The **snmp-server traps snmp** command is used with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications.

The optional **authentication** keyword controls the sending of SNMP authentication failure notifications. In order to send notifications, you must configure at least one **snmp-server host** command. An authentication Failure (4) trap signifies that the sending device is the addressee of a protocol message that is not properly authenticated. The authentication method depends on the version of SNMP being used. For SNMPv1 or SNMPv2, authentication failure occurs for packets with an incorrect community string. For SNMPv3, authentication failure occurs for packets with an incorrect Secure Hash Algorithm (SHA) or Message Digest 5 (MD5) authentication key or for a packet that is outside the authoritative SNMP engine's window, for

example, the packets that are configured outside access lists or time ranges. In such an instance, only a report Protocol Data Unit (PDU) is generated, and authentication failure traps are not generated.

The optional **linkup** keyword controls the sending of SNMP linkUp notifications. The linkUp(3) trap signifies that the sending device recognizes one of the communication links represented in the agent's configuration coming up.

The optional **linkdown** keyword controls the sending of SNMP linkDown notifications. The linkDown(2) trap signifies that the sending device recognizes a failure in one of the communication links represented in the agent's configuration.

The **snmp-server traps snmp** command with the **linkup** or **linkdown** keywords globally enables or disables SNMP linkUp and linkDown traps. After enabling either of these traps globally, you can enable or disable these traps on specific interfaces using the **no notification linkupdown disable** command in interface configuration mode. According to RFC 2863, linkUp and linkDown traps are enabled for interfaces that do not operate on top of any other interface (as defined in the ifStackTable), and are disabled otherwise. This means that you do not have to enable linkUp and linkdown notifications on such interfaces. However, linkUp and linkDown notifications will not be sent unless you enable them globally using the **snmp-server traps snmp** command.

The optional **coldstart** keyword controls the sending of SNMP coldStart notifications. The coldStart(0) trap signifies that the sending device is reinitializing itself such that the agent's configuration or the protocol entity implementation may be altered.

The optional **warmstart** keyword controls the sending of SNMP coldStart notifications. The warmStart(1) trap signifies that the sending device is reinitializing itself such that neither the agent configuration nor the protocol entity implementation is altered.

Task ID

Task ID	Operations
snmp	read, write

This example shows how to enable the device to send all traps to the host myhost.cisco.com using the community string defined as public:

```
RP/0/RSP0/CPU0:router(config)# snmp-server traps snmp
RP/0/RSP0/CPU0:router(config)# snmp-server host myhost.cisco.com public snmp
```

The following example shows how to enable only linkUp and linkDown traps:

```
RP/0/RSP0/CPU0:router(config)# snmp-server traps snmp linkup
RP/0/RSP0/CPU0:router(config)# snmp-server traps snmp linkdown
```

Related Topics

snmp-server engineid local, on page 95
snmp-server host, on page 101
snmp-server traps bgp
snmp-server traps syslog, on page 185

snmp-server traps syslog

To enable Simple Network Management Protocol (SNMP) notifications of Cisco-syslog-MIB error messages, use the **snmp-server traps syslog** command in the appropriate configuration mode. To disable these types of notifications, use the **no** form of this command.

snmp-server traps syslog
no snmp-server traps syslog

Syntax Description

This command has no keywords or arguments.

Command Default

SNMP notifications are disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The **snmp-server traps syslog** command is used with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications.

Task ID

Task ID	Operations
snmp	read, write

The following example shows how to enable Cisco-syslog-MIB error message notifications to the host at the address myhost.cisco.com, using the community string defined as public:

```
RP/0/RSP0/CPU0:router(config)# snmp-server traps syslog
RP/0/RSP0/CPU0:router(config)# snmp-server host myhost.cisco.com version 2c public
```

Related Topics

snmp-server engineid local, on page 95
snmp-server host, on page 101
snmp-server traps bgp
snmp-server traps snmp, on page 183

snmp-server trap-source

To specify the interface (and hence the corresponding IP address) from which a Simple Network Management Protocol (SNMP) trap should originate, use the **snmp-server trap-source** command in

global configuration

mode. To remove the source designation, use the **no** form of this command.

snmp-server trap-source *type interface-path-id*
no snmp-server trap-source

Syntax Description

type	Interface type. For more information, use the question mark (**?**) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.

Command Default

No interface is specified.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

When an SNMP trap is sent from a Cisco SNMP device, it has a notification address of the interface it happened to exit at that time. Use the **snmp-server trap-source** command to monitor notifications from a particular interface.

Note In references to a Management Ethernet interface located on a route switch processor card, the physical slot number is numeric (0 through n-1 where n is the number of line card slots in the chassis) and the module is CPU0. Example: interface MgmtEth0/1/CPU0/0.

Task ID

Task ID	Operations
snmp	read, write

The following example shows how to specify that the IP address for interface 0/0/1/0 is the source for all SNMP notifications:

```
RP/0/RSP0/CPU0:router(config)# snmp-server trap-source tengige 0/0/1/0
```

Related Topics

snmp-server engineid local, on page 95
snmp-server host, on page 101
snmp-server traps bgp
snmp-server traps snmp, on page 183
snmp-server traps syslog, on page 185

snmp-server traps subscriber session-aggregation

To set the session aggregation parameters, use the **snmp-server traps subscriber session** command in global configuration mode. To delete the set parameters, use the no form of the command.

snmp-server traps subscriber session-agregation [**access-interface** | **node**]

no snmp-server traps subscriber session-agregation [**access-interface** | **node**]

Syntax Description

access-interface	Subscriber notification at access interface level.
node	Subscriber notification at node level.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Release 5.1	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **snmp-server traps subscriber session-agregation** command to enable CISCO-SUBSCRIBER-SESSION-MIB notifications (traps). Notifications will include MIB's asynchronous events.

Task ID

Task ID	Operation
snmp	read, write

Example

```
RP/0/RSP0/CPU0:router (config)# snmp-server traps subscriber session-aggregation node
```

snmp-server traps updown

To enable Border Gateway Protocol (BGP) to receive Simple Network Management Protocol (SNMP) notifications when a BGP peer changes state in IPv4 or both IPv4 and IPv6 neighbor sessions, use the **snmp-server traps updown** command in global configuration mode.

snmp-server traps {bgp | cbgp2} [updown]

Syntax Description

bgp	Specifies IPv4 neighbor sessions.
cbgp2	Specifies IPv4 and IPv6 neighbor sessions.
updown	(Optional) Specifies trap notifications.

Command Default

SNMP notifications are disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
Release 4.3.1	This command was introduced.

Usage Guidelines

SNMP notifications are sent as traps.

BGP generates traps when:

- A neighbor's session state has changed.
- A neighbor prefix limit has exceeded.
- A neighbor prefix count is under the limit.

Multiple traps can be generated when the neighbor is not in steady state.

Configure **snmp-server traps updown** command to prevent the generation multiple traps.

When you configure the **snmp-server traps updown** command, traps are sent out only when the BGP neighbor goes to established state or moves out from the established state. The prefix limit traps remain unaffected.

When you configure the **bgp** keyword, traps are sent for IPv4 neighbor sessions only. When you configure the **cbgp2** keyword, traps are sent for both IPv4 and IPv6 neighbor sessions.

Example

The following example shows how to enable the router to send BGP state-change notifications to the host at the address myhost.cisco.com using the community string defined as public in IPv4 neighbor sessions only:

```
Router(config)# snmp-server traps bgp updown
Router(config)# snmp-server host myhost.cisco.com version 2c public
```

The following example shows how to enable the router to send BGP state-change notifications to the host at the address myhost.cisco.com using the community string defined as public in both IPv4 and IPv6 neighbor sessions:

```
Router(config)# snmp-server traps cbgp2 updown
Router(config)# snmp-server host myhost.cisco.com version 2c public
```

Related References

snmp-server engineid local

snmp-server host

snmp-server traps snmp

snmp-server traps syslog

snmp-server trap-timeout

To define how often to try resending trap messages on the retransmission queue, use the **snmp-server trap-timeout** command in

global configuration

mode. To restore the default value, use the **no** form of this command.

snmp-server trap-timeout *seconds*
no snmp-server trap-timeout *seconds*

Syntax Description

seconds	Integer that sets the interval for resending the messages, in seconds). Value can be from 1 to 1000.

Command Default

seconds : 30

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Before Cisco IOS XR software tries to send a trap, it looks for a route to the destination address. If there is no known route, the trap is saved in a retransmission queue. Use the **snmp-server trap-timeout** command to determine the number of seconds between retransmission attempts.

Task ID

Task ID	Operations
snmp	read, write

The following example shows how to set an interval of 20 seconds to try resending trap messages on the retransmission queue:

```
RP/0/RSP0/CPU0:router(config)# snmp-server trap-timeout 20
```

Related Topics

snmp-server engineid local, on page 95
snmp-server host, on page 101
snmp-server traps bgp
snmp-server traps snmp, on page 183
snmp-server traps syslog, on page 185

snmp-server user

To configure a new user to a Simple Network Management Protocol (SNMP) group, use the **snmp-server user** command in

global configuration

mode. To remove a user from an SNMP group, use the **no** form of this command.

snmp-server user *username groupname* {**v1** | **v2c** | **v3** [**auth** {**md5** | **sha**} {**clear** | **encrypted**} *auth-password* [**priv** {**3des** | **aes** *aes-bit-encryption* | **des56**} {**clear** | **encrypted**} *priv-password*]]} [**SDROwner** | **SystemOwner**] [*access-list-name*]
no snmp-server user *username groupname*

Syntax Description

username	Name of the user on the host that connects to the agent. **Note** The recommended range for a user-defined username is 2-253 characters.
groupname	Name of the group to which the user belongs.
v1	Specifies that the SNMPv1 security model should be used.
v2c	Specifies that the SNMPv2c security model should be used.
v3	Specifies that the SNMPv3 security model should be used.
auth	(Optional) Specifies which authentication level should be used. If this keyword is used, you must specify an authentication level and an authorization password.
md5	Specifies the HMAC-MD5-96 authentication level.
sha	Specifies the HMAC-SHA-96 authentication level.
clear	Specifies that an unencrypted password follows.
encrypted	Specifies that an encrypted password follows.
auth-password	Authentication password, which is a string (not to exceed 64 characters) that enables the agent to receive packets from the host.
priv	(Optional) Specifies that encryption parameters follow.
3des	Specifies the 168-bit Triple Data Encryption Standard (3DES) level of encryption for the user.
aes *aes-bit-encryption*	Specifies the Advanced Encryption Standard (AES) level of encryption for the user. Supported options are 128, 192 and 256 bit encryption.

des56	Specifies the 56-bit Data Encryption Standard (DES) level of encryption for the user.
priv-password	Privacy password, which can be clear or encrypted text, according to what is specified.
SDROwner	(Optional) Limits access to the agents for the owner secure domain router (SDR) only.
SystemOwner	(Optional) Provides system-wide access to the agents for all SDRs.
access-list-name	(Optional) Access list to be associated with this SNMP user. The *access-list-name* argument represents a value from 1 to 99, that is, the identifier of the standard IP access list.

Command Default

By default, access is limited to agents on the owner SDR only.

See also Table 8: snmp-server user Default Descriptions, on page 193.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.
Release 3.9.0	AES and 3DES encryption formats were supported.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

To use 3DES and AES encryption standards, you must have installed the security package (k9sec). For information on installing software packages, see *Upgrading and Managing Cisco IOS XR Software* in *System Management Configuration Guide for Cisco ASR 9000 Series Routers*.

Note Only one remote host can be assigned to the same username for SNMP version 3. If you configure the same username with different remote hosts, only the last username and remote host combination will be accepted and will be seen in the **show running** configuration. In the case of multiple SNMP managers, multiple unique usernames are required.

Table 8: snmp-server user Default Descriptions

Characteristic	Default
passwords	Text strings are assumed.
access lists	Access from all IP access lists is permitted.

SDR and System-wide Access

When the **snmp-server user** command is entered with the **SDROwner** keyword, SNMP access is granted only to the MIB object instances in the owner SDR.

When the **snmp-server user** command is entered with the **SystemOwner** keyword, SNMP access is granted to the entire system.

Task ID

Task ID	Operations
snmp	read, write

The following example shows how to enter a plain-text password for the string *abcd* for user2 in group2:

```
RP/0/RSP0/CPU0:router(config)# snmp-server user user2 group2 v3 auth md5 clear abcd
```

To learn if this user has been added to the configuration, use the **show snmp user** command.

If the localized Message Digest 5 (MD5) or Secure Hash Algorithm (SHA) digest is known, specify that string instead of the plain-text password. The digest should be formatted as AA:BB:CC:DD where AA, BB, CC, and DD are hexadecimal values. The digest should also be exactly 16 octets long.

This example shows how to specify the command with a digest name of 00:11:22:33:44:55:66:77:88:99:AA:BB:CC:DD:EE:FF:

```
RP/0/RSP0/CPU0:router(config)# snmp-server user user2 group2 v3 auth md5 encrypted
     00:11:22:33:44:55:66:77:88:99:AA:BB:CC:DD:EE:FF
```

Related Topics

snmp-server group, on page 98

snmp-server view

To create or update a Simple Network Management Protocol (SNMP) view entry, use the **snmp-server view** command in

global configuration

mode. To remove the specified server view entry, use the **no** form of this command.

snmp-server view *view-name oid-tree* {**excluded** | **included**}
no snmp-server view *view-name oid-tree* {**excluded** | **included**}

Syntax Description

view-name	Label for the view record being updated or created. The name is used to reference the record.
oid-tree	Object identifier (OID) of the ASN.1 subtree to be included or excluded from the view. To identify the subtree, specify a text string consisting of numbers, such as 1.3.6.2.4, or a word, such as *system*. Replace a single subidentifier with the asterisk (*) wildcard to specify a subtree family; for example 1.3.*.4.
excluded	Excludes the MIB family from the view.
included	Includes the MIB family in the view.

Command Default

No view entry exists.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Other SNMP commands require a view as a keyword. Use the **snmp-server view** command to create a view to be used as keywords for other commands that create records including a view.

Instead of defining a view explicitly, you can rely on the following predefined views, which are supported by the SNMP agent:

all

Predefined view indicating that a user can see all objects.

CfgProt

Predefined view indicating that a user can see all objects except the SNMPv3 configuration tables.

vacmViewTreeFamilyEntry

Predefined view indicating that a user can see the default configuration of vacmViewTreeFamilyEntry.

The predefined views supported on Cisco IOS XR software, however, do not match the predefined views specified in RFC 3415.

Task ID

Task ID	Operations
snmp	read, write

This example creates a view that includes all objects in the MIB-II subtree:

```
RP/0/RSP0/CPU0:router(config)# snmp-server view mib2 1.3.6.1.2.1 included
```

This example shows how to create a view that includes all objects in the MIB-II system group and all objects in the Cisco enterprise MIB:

```
RP/0/RSP0/CPU0:router(config)# snmp-server view view1 1.3.6.1.2.1.1 included
RP/0/RSP0/CPU0:router(config)# snmp-server view view1 1.3.6.1.4.1.9 included
```

This example shows how to create a view that includes all objects in the MIB-II system group except for sysServices (System 7) and all objects for interface 1 in the MIB-II interfaces group:

```
RP/0/RSP0/CPU0:router(config)# snmp-server view view1 1.3.6.1.2.1.1 included
RP/0/RSP0/CPU0:router(config)# snmp-server view view1 1.3.6.1.2.1.1.7 excluded
RP/0/RSP0/CPU0:router(config)# snmp-server view view1 1.3.6.1.2.1.2.2.1.*.1 included
```

Related Topics

show snmp view, on page 83
snmp-server group, on page 98

snmp-server vrf

To configure the VPN routing and forwarding (VRF) properties of Simple Network Management Protocol (SNMP), use the **snmp-server vrf** command in

global configuration

mode. To remove the configuration, use the **no** form of this command.

snmp-server vrf *vrf-name*[**host** *address* [**clear** | **encrypted**][**traps**][**version** {**1** | **2c** | **3** *security-level*}] *community-string*[**udp-port** *port*]][**context** *context-name*]
no snmp-server vrf *vrf-name*

Syntax Description

vrf-name	Name of the VRF.
host *address*	(Optional) Specifies the name or IP address of the host (the targeted recipient).
clear	(Optional) Specifies that the *community-string* argument is clear text.
encrypted	(Optional) Specifies that the *community-string* argument is encrypted text.
traps	(Optional) Specifies that notifications should be sent as traps. This is the default.
version {**1** | **2c** | **3**}	(Optional) Specifies the version of the SNMP used to send the traps. The default is SNMPv1. When the **version** keyword is used, one of these keywords must be specified: • **1**—SNMPv1 • **2c**—SNMPv2C • **3**—SNMPv3
security-level	(Optional) Security level for SNMPv3. Options are: • **auth**—authNoPriv • **noauth**—noAuthNoPriv • **priv**—authPriv
community-string	Specifies the community string for SNMPv1 and SNMPv2, or the SNMPv3 user.
udp-port *port*	(Optional) Specifies the UDP port to which notifications should be sent.
context *context-name*	(Optional) Name of the context that must be mapped to VRF identified by value of the *vrf-name* argument.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use this command to enter SNMP VRF configuration mode and configure an SNMP notification recipient on a VRF. You can also map a VRF to an SNMP context.

SNMP notification recipient that is reachable by way of a VRF can be configured. Notification is forwarded to the recipient represented by its address using the routing table instance identified by the VRF name.

The *address* argument can be either a host name or an IP address.

Use the **clear** keyword to specify that the clear text community string you enter is displayed encrypted in the **show running** command output. To enter an encrypted string, use the **encrypted** keyword. To enter a clear text community string that is not encrypted by the system, use neither of these keywords.

An SNMP context identified by the value of the *context-name* argument can be mapped to a VRF in this mode. This context must be created using **snmp-server context** command.

Task ID

Task ID	Operations
snmp	read, write

This example shows how to configure a host IP address for a VRF name:

```
RP/0/RSP0/CPU0:router(config)# snmp-server vrf vrfa
RP/0/RSP0/CPU0:router(config-snmp-vrf)# host 12.21.0.1 traps version
2c public udp-port 2525
```

Related Topics

snmp-server context, on page 90
snmp-server host, on page 101

snmp test trap all

To send a Simple Network Management Protocol (SNMP) trap message to the trap receivers for all supported traps, use the **snmp test trap all** command in

EXEC

mode.

snmp test trap all

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.9.1	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

To use the **snmp test trap** command, SNMP must be configured on the router. This command is not intended for testing scalability, performance, or high availability scenarios.

Use the **snmp test trap all** command to generate test traps for all supported traps. The following traps are supported:

- coldStart—SNMP agent Initializing and its configuration may have changed.
- warmStart—SNMP agent Initializing and its configuration is unaltered.
- linkUp—Interface ifOperStatus is Up.
- linkDown—Interface ifOperStatus is Down.
- clogMessage Generated—Syslog message generated.
- ciscoFlashDeviceInsertedNotif—Flash device inserted.
- ciscoFlashDeviceRemovedNotif—Flash device removed.
- ciscoRFProgressionNotif—RF state change.
- ciscoRFSwactNotif—Switchover.
- ciscoConfigManEvent—Command-line interface (CLI) configuration management event.
- newRoot—SNMP agent is a new root of the spanning tree.
- topologyChange—Bridge port has transitioned to the Forwarding state.
- cefcFanTrayOperStatus—Fan tray cefcFanTrayOperStatus is Up.

- cefcModuleStatusChange—Module cefcModuleOperStatus is OK (module up) or module cefcModuleOperStatus is Failed (module down).
- entSensorThresholdNotification—entSensorValue crossed the entSensorthresholdValue.
- cefcPowerStatusChange—Redundant PowerSupply fails.

Task ID

Task ID	Operation
snmp	read

This example illustrates how to use the **snmp test trap all** command:

```
RP/0/RSP0/CPU0:router# snmp test trap all
```

Related Topics

show snmp entity, on page 34

snmp test trap entity

To send a test SNMP Entity trap message to the trap receivers, use the **snmp test trap entity** command in

EXEC

mode.

snmp test trap entity {**fru** {**power status-change failed** | **module status-change** {**up** | **down**} | **fan-tray oper-status up**} | **sensor threshold-notification**}[**entity-index** *index*]

Syntax Description

fru	Sends a field replacement unit trap.
power status-change failed	Sends a cefcPowerStatusChange trap for the CISCO-ENTITY-FRU-CONTROL-MIB.
module status-change{**up** | **down**}	Sends a cefcModuleStatusChange trap for the CISCO-ENTITY-FRU-CONTROL-MIB.
fan-tray oper-status up	Sends a cefcFanTrayOperStatus trap for the CISCO-ENTITY-FRU-CONTROL-MIB.
sensor	Sends a sensor trap.
threshold-notification	Sends a entSensorThresholdNotification trap for the CISCO-ENTITY-SENSOR-MIB.
entity-index *index*	Specifies the physical index for which to generate the trap.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.9.1	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The **snmp test trap entity** command tests the sending of Entity MIB traps. It is not intended for testing scalability, performance, or high availability scenarios. To use the **snmp test trap** command, SNMP must be configured on the router.

Task ID

Task ID	Operation
snmp	read

This example illustrates how to use the **snmp test trap entity** command:

```
RP/0/RSP0/CPU0:router# snmp test trap entity sensor threshold index
```

Related Topics

show snmp entity, on page 34

snmp test trap infra

To send a test Simple Network Management Protocol (SNMP) Infra trap message to the trap receivers, use the **snmp test trap infra** command in

EXEC

mode.

snmp test trap infra {**bridge** {**new-root** | **topology-change**} | **config event** | **flash** {**device-inserted** | **device-removed**} | **redundancy** {**progression** | **switch**} | **syslog message-generated**}

Syntax Description

bridge	Sends a bridge trap.
new-root	Sends a newRoot trap for the BRIDGE-MIB.
topology-change	Sends a topologyChange trap for the BRIDGE-PORT.
config event	Sends a ciscoConfigManEvent trap for the CISCO-CONFIG-MAN-MIB.
flash	Sends a flash trap.
device-inserted	Sends a ciscoFlashDeviceInsertedNotif trap for the CISCO-FLASH-MIB.
device-removed	Sends a ciscoFlashDeviceRemovedNotif trap for the CISCO-FLASH-MIB.
redundancy	Sends an RF trap.
progression	Sends a ciscoRFProgressionNotif trap for the CISCO-RF-MIB.
switch	Sends a ciscoRFSwactNotif trap for the CISCO-RF-MIB.
syslog message-generated	Sends a clogMessageGenerated for the CISCO-SYSLOG-MIB.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.9.1	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The **snmp test trap infra** command tests the sending of Infra MIB traps. It is not intended for testing scalability, performance, or high availability scenarios. To use this command, SNMP must be configured on the router.

Task ID

Task ID	Operation
snmp	read

This example illustrates how to use the **snmp test trap infra** command:

```
RP/0/RSP0/CPU0:router# snmp test trap infra syslog message-generated
```

snmp test trap interface

To send a test Simple Network Management Protocol (SNMP) interface trap message to the trap receivers, use the **snmp test trap interface** command in

EXEC

mode.

snmp test trap interface {**link-down** | **link-up**}**ifindex** *index*

Syntax Description

link-down	Sends a linkDown trap for the IF-MIB.
link-up	Sends a linkUp trap for the IF-MIB.
ifindex *index*	Specifies the interface index for which to send the IF-MIB trap.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.9.1	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The **snmp test trap interface** command tests the sending of IF-MIB traps. It is not intended for testing scalability, performance, or high availability scenarios. To use this command, SNMP must be configured on the router.

Task ID

Task ID	Operation
snmp	read

This example illustrates how to use the **snmp test trap interface** command:

```
RP/0/RSP0/CPU0:router# snmp test trap interface link-down
```

snmp test trap snmp

To send a test Simple Network Management Protocol (SNMP) trap message to the trap receivers, use the **snmp test trap snmp** command in

EXEC

mode.

snmp test trap snmp {**cold-start** | **warm-start**}

Syntax Description

cold-start	Sends a coldStart trap for the SNMPv2-MIB.
warm-start	Sends a warmStart trap for the SNMPv2-MIB.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.9.1	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The **snmp test trap snmp** command tests the sending of MIB traps. It is not intended for testing scalability, performance, or high availability scenarios. To use this command, SNMP must be configured on the router.

Task ID

Task ID	Operation
snmp	read

The following example illustrates how to use the **snmp test trap snmp** command:

```
RP/0/RSP0/CPU0:router# snmp test trap snmp cold-start
```

transfer-interval

To configure how long bulk statistics should be collected before a bulk statistics transfer is initiated, use the **transfer-interval** command in bulk statistics transfer configuration mode. To remove a previously configured interval from a bulk statistics configuration, use the **no** form of this command.

transfer-interval *minutes*
no transfer-interval *minutes*

Syntax Description

minutes	Length of time, in minutes, that the system should collect MIB data before attempting the transfer operation. The valid range is from 1 to 2147483647. The default is 30.

Command Default

Bulk statistics file transfer operations start 30 minutes after the **enable (bulkstat)** command is used.

Command Modes

Bulk statistics transfer configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Bulk statistics data is collected into a new file when a transfer attempt begins, which means that this command also configures the collection interval.

If the maximum buffer size for a bulk statistics file is reached before the transfer interval time expires, the transfer operation is still initiated, and bulk statistics MIB data are collected into a new file in the system buffer.

Task ID

Task ID	Operation
snmp	read, write

The following example shows how to configure a transfer interval of 20 minutes for the bulk statistics configuration bulkstat1:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# snmp-server mib bulkstat transfer-id bulkstat1
RP/0/RSP0/CPU0:router(config-bulk-tr)# transfer-interval 20
```

Related Topics

enable (bulkstat), on page 8
show snmp mib bulkstat transfer, on page 49

snmp-server mib bulkstat transfer-id, on page 123

url

To specify the host to which bulk statistics files should be transferred, use the **url** command in bulk statistics transfer configuration mode. To remove a previously configured destination host, use the **no** form of this command.

url [**primary** | **secondary**] *url*
no url [**primary** | **secondary**] *url*

Syntax Description

primary	Specifies the URL to be used first for bulk statistics transfer attempts.
secondary	Specifies the URL to be used for bulk statistics transfer attempts if the transfer to the primary URL is not successful.
url	Destination URL address for the bulk statistics file transfer. Use FTP or TFTP. The syntax for these URLs is as follows: • **ftp:**[[[//*username* [:*password*]**@**]*location*]/*directory*]/*filename* • **tftp:**[[/*location*]/*directory*]/*filename* The location argument is typically an IP address.

Command Default

No host is specified.

Command Modes

Bulk statistics transfer configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

For bulk statistics transfer retry attempts, a single retry consists of an attempt to send first to the primary URL, and then to the secondary URL.

Task ID

Task ID	Operation
snmp	read, write

In the following example, an FTP server is used as the primary destination for the bulk statistics file. If a transfer to that address fails, an attempt is made to send the file to the TFTP server at 192.168.10.5. No retry command is specified, which means that only one attempt to each destination will be made.

```
RP/0/RSP0/CPU0:router# configure
```

```
RP/0/RSP0/CPU0:router(config)# snmp-server mib bulkstat transfer ifMibTesting
RP/0/RSP0/CPU0:router(config-bulk-tr)# schema carMibTesting1
RP/0/RSP0/CPU0:router(config-bulk-tr)# schema carMibTesting2
RP/0/RSP0/CPU0:router(config-bulk-tr)# url primary
ftp://user2:pswd@192.168.10.5/functionality/
RP/0/RSP0/CPU0:router(config-bulk-tr)# url secondary tftp://user2@192.168.10.8/tftpboot/
RP/0/RSP0/CPU0:router(config-bulk-tr)# enable
RP/0/RSP0/CPU0:router(config-bulk-tr)# exit
```

Related Topics

show snmp mib bulkstat transfer, on page 49