

Cisco IOS SNMP Support Command Reference

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2013 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1 **action (event) through rising (test threshold) 1**

action (event) 3

add (bulk statistics object) 5

bandwidth (interface) 7

buffer-size (bulk statistics) 10

comparison 12

conditional object 14

context 16

context (bulk statistics) 19

correlate 20

delta (test threshold) 23

delta interval 25

description (event) 26

description (expression) 27

description (trigger) 28

discontinuity object (expression) 29

enable (bulk statistics) 31

enable (event) 33

enable (expression) 35

event owner 36

expression 38

falling (test threshold) 39

format (bulk statistics) 41

frequency (event trigger) 43

id (expression) 44

instance (MIB) 45

instance range 48

instance repetition 50

no snmp-server 52
object (expression) 53
object id 54
object id (event trigger) 56
object list 57
object-list 59
poll-interval 61
prefix object 63
retain 64
retry (bulk statistics) 66
rising (test threshold) 68

CHAPTER 2 **sample (event trigger) through snmp mib event sample 71**

sample (event trigger) 73
sample (expression) 75
schema 77
show management event 79
show management expression 81
show snmp 83
show snmp chassis 87
show snmp community 88
show snmp contact 90
show snmp engineID 91
show snmp group 93
show snmp host 95
show snmp location 97
show snmp mib 98
show snmp mib bulkstat transfer 101
show snmp mib context 104
show snmp mib ifmib traps 106
show snmp mib ifmib ifindex 108
show snmp mib notification-log 113
show snmp pending 115
show snmp sessions 117
show snmp stats oid 120

show snmp sysobjectid 122
show snmp user 124
show snmp view 127
snmp context (VRF) 129
snmp get 131
snmp get-bulk 133
snmp get-next 136
snmp ifmib ifalias long 138
snmp inform 140
snmp mib bulkstat object-list 143
snmp mib bulkstat schema 145
snmp mib bulkstat transfer 147
snmp mib community-map 149
snmp mib event object list 152
snmp mib event owner 154
snmp mib event sample 155

CHAPTER 3 **snmp mib event trigger owner through snmp-server enable informs 157**

snmp mib event trigger owner 158
snmp mib expression delta 160
snmp mib expression owner 162
snmp mib flash cache 164
snmp mib flowmon alarmhistorysize 165
snmp mib notification-log default 166
snmp mib notification-log default disable 168
snmp mib notification-log globalageout 170
snmp mib notification-log globalsize 172
snmp mib persist 174
snmp mib target list 176
snmp trap link-status 178
snmp set 181
snmp-server cache 184
snmp-server chassis-id 186
snmp-server community 188
snmp-server contact 192

snmp-server context 193

snmp-server drop vrf-traffic 195

snmp-server enable informs 196

CHAPTER 4 snmp-server enable traps through snmp-server enable traps ospf cisco-specific retransmit 197

snmp-server enable traps 199

snmp-server enable traps (MPLS) 208

snmp-server enable traps aaa_server 216

snmp-server enable traps atm pvc 218

snmp-server enable traps atm pvc extension 221

snmp-server enable traps atm pvc extension mibversion 226

snmp-server enable traps atm subif 228

snmp-server enable traps bfd 231

snmp-server enable traps bgp 233

snmp-server enable traps bulkstat 236

snmp-server enable traps c6kxbar 238

snmp-server enable traps calltracker 240

snmp-server enable traps cnpd 242

snmp-server enable traps cpu 243

snmp-server enable traps dhcp 245

snmp-server enable traps dhcp-snooping bindings 247

snmp-server enable traps director 248

snmp-server enable traps dlsw 250

snmp-server enable traps eigrp 252

snmp-server enable traps envmon 254

snmp-server enable traps errdisable 257

snmp-server enable traps firewall 258

snmp-server enable traps flash 260

snmp-server enable traps flowmon 262

snmp-server enable traps frame-relay 264

snmp-server enable traps frame-relay multilink bundle-mismatch 266

snmp-server enable traps frame-relay subif 268

snmp-server enable traps if-monitor 270

snmp-server enable traps ip local pool 271

snmp-server enable traps isdn 272

snmp-server enable traps l2tun pseudowire status 275
snmp-server enable traps l2tun session 277
snmp-server enable traps memory 279
snmp-server enable traps ospf cisco-specific errors config-error 281
snmp-server enable traps ospf cisco-specific errors shamlink 283
snmp-server enable traps ospf cisco-specific retransmit 285

CHAPTER 5 **snmp-server enable traps ospf cisco-specific state-change through snmp-server enable traps voice poor-qov** 287

snmp-server enable traps ospf cisco-specific state-change 289
snmp-server enable traps pim 291
snmp-server enable traps power-ethernet group 293
snmp-server enable traps pppoe 295
snmp-server enable traps pppoe per-interface 297
snmp-server enable traps pppoe per-mac 299
snmp-server enable traps pppoe per-vc 301
snmp-server enable traps pppoe per-vlan 303
snmp-server enable traps pppoe system 305
snmp-server enable traps pppoe vc 307
snmp-server enable traps repeater 309
snmp-server enable traps resource-policy 311
snmp-server enable traps rtr 312
snmp-server enable traps snmp 314
snmp-server enable traps srp 317
snmp-server enable traps storm-control 318
snmp-server enable traps syslog 319
snmp-server enable traps transceiver all 321
snmp-server enable traps trustsec 322
snmp-server enable traps trustsec-interface 324
snmp-server enable traps trustsec-policy 326
snmp-server enable traps trustsec-server 328
snmp-server enable traps trustsec-sxp 330
snmp-server enable traps voice 332
snmp-server enable traps voice poor-qov 334
snmp-server enable traps vswitch dual-active 335

CHAPTER 6 **snmp-server engineID local through snmp trap link-status** 337

snmp-server engineID local 339

snmp-server file-transfer access-group 341

snmp-server group 343

snmp-server host 348

snmp-server inform 362

snmp-server ip dscp 364

snmp-server ip precedence 365

snmp-server location 366

snmp-server manager 367

snmp-server manager session-timeout 369

snmp-server packetsize 371

snmp-server queue-length 372

snmp-server queue-limit 374

snmp-server source-interface 376

snmp-server system-shutdown 378

snmp-server tftp-server-list 379

snmp-server trap authentication unknown-context 381

snmp-server trap authentication vrf 382

snmp-server trap link 384

snmp-server trap link switchover 386

snmp-server trap retry 387

snmp-server trap timeout 388

snmp-server trap-authentication 389

snmp-server trap-source 390

snmp-server trap-timeout 392

snmp-server user 394

snmp-server usm cisco 399

snmp-server view 400

snmp trap if-monitor 402

snmp trap link-status 403

CHAPTER 7 **startup (test boolean) through write mib-data** 407

startup (test boolean) 409

startup (test existence) 410
startup (test threshold) 411
test (event trigger) 413
test snmp trap auth-framwork sec-violation 415
test snmp trap bridge 416
test snmp trap c6kxbar 417
test snmp trap call-home 420
test snmp trap config-copy 421
test snmp trap dhcp bindings 423
test snmp trap dhcp-snooping bindings 424
test snmp trap dot1x 425
test snmp trap entity-diag 426
test snmp trap errdisable ifevent 428
test snmp trap flex-links status 429
test snmp trap fru-ctrl 430
test snmp trap l2-control vlan 431
test snmp trap l2tc 432
test snmp trap mac-notification 433
test snmp trap module-auto-shutdown 434
test snmp trap port-security 435
test snmp trap power-ethernet port-on-off 436
test snmp trap snmp 437
test snmp trap stack 439
test snmp trap storm-control 440
test snmp trap stpx 441
test snmp trap syslog 442
test snmp trap trustsec 444
test snmp trap trustsec-interface 446
test snmp trap trustsec-policy 447
test snmp trap trustsec-server 448
test snmp trap trustsec-sxp 449
test snmp trap udld 451
test snmp trap vswitch dual-active 452
test snmp trap vswitch vsl 454
test snmp trap vtp 455

test snmp trap vtp pruning-change 457
type (test existence) 458
url (bulk statistics) 460
value (test boolean) 462
value type 463
wildcard (expression) 466
write mib-data 467



action (event) through rising (test threshold)

- action (event), page 3
- add (bulk statistics object), page 5
- bandwidth (interface), page 7
- buffer-size (bulk statistics), page 10
- comparison, page 12
- conditional object, page 14
- context, page 16
- context (bulk statistics), page 19
- correlate, page 20
- delta (test threshold), page 23
- delta interval, page 25
- description (event), page 26
- description (expression), page 27
- description (trigger), page 28
- discontinuity object (expression), page 29
- enable (bulk statistics), page 31
- enable (event), page 33
- enable (expression), page 35
- event owner, page 36
- expression, page 38
- falling (test threshold), page 39
- format (bulk statistics), page 41
- frequency (event trigger), page 43
- id (expression), page 44

- instance (MIB), page 45
- instance range, page 48
- instance repetition, page 50
- no snmp-server, page 52
- object (expression), page 53
- object id, page 54
- object id (event trigger), page 56
- object list, page 57
- object-list, page 59
- poll-interval, page 61
- prefix object, page 63
- retain, page 64
- retry (bulk statistics), page 66
- rising (test threshold), page 68

action (event)

To set an action for an event, use the **action** command in event configuration mode. To disable the action for an event, use the **no** form of this command.

action {**set**| **notification**}

no action {**set**| **notification**}

Syntax Description

set	Specifies the action for an event.
notification	Enables notifications for events.

Command Default

No action is set for an event.

Command Modes

Event configuration (config-event)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.

Usage Guidelines

While configuring a set of actions for an event, you can specify the object identifier of the object. You can also configure events to perform activities such as sending notifications or setting a MIB object whenever an event is triggered. If notifications are enabled for an event, the system sends a notification to the SNMP manager whenever the object configured for that event is modified.

Examples

The following example shows how to enable notifications for an event:

```
Router(config)# snmp mib event owner owner1 name test
Router(config-event)# action notification
Router(config-event-action-notification)# end
```

Related Commands

Command	Description
object id	Specifies the object identifier of an object.
snmp mib event owner	Specifies the event owner for a management event.

Command	Description
value	Specifies a value for the object configured for an event.
wildcard	Specifies whether an object used for evaluating an expression is to be wildcarded during an event configuration.

add (bulk statistics object)

To add a MIB object to a 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-name*| *oid*}

no add {*object-name*| *oid*}

Syntax Description

object-name	Name of the MIB object to add to the list. Only object names from the Interfaces MIB (IF-MIB.my), Cisco Committed Access Rate MIB (CISCO-CAR-MIB.my) and the MPLS Traffic Engineering MIB (MPLS-TE-MIB.my) may be used.
oid	Object ID (OID) of the MIB object to add to the list.Only OIDs from the Interfaces MIB (IF-MIB.my), Cisco Committed Access Rate MIB (CISCO-CAR-MIB.my) and the MPLS Traffic Engineering MIB (MPLS-TE-MIB.my) may be used.

Command Default

No MIB objects are listed in the bulk statistics object list.

Command Modes

Bulk Statistics Object List configuration (config-bulk-objects)

Command History

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

Usage Guidelines

All the objects in an object list have to be indexed by the same MIB index, but the objects need not belong to the same MIB table. For example, it is possible to group ifInoctets and an Ether MIB object in the same schema because the containing tables are indexed by the ifIndex (in the IF-MIB).

Object names are available in the relevant MIB modules. For example, the input byte count of an interface is defined in the Interfaces Group MIB (IF-MIB.my) as ifInoctets. Complete MIB modules can be downloaded from Cisco.com at http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml.

Examples

In the following example, two bulk statistics object lists are configured: one for IF-MIB objects and one for CISCO-CAR-MIB objects. Because the IF-MIB objects and the CISCO-CAR-MIB objects do not have the same index, they must be defined in separate object lists.

```
Router(config)# snmp mib bulkstat object-list if-Objects

Router(config-bulk-objects)# add ifInoctets
Router(config-bulk-objects)# add ifOutoctets

Router(config-bulk-objects)# add ifInUcastPkts

Router(config-bulk-objects)# add ifInDiscards

Router(config-bulk-objects)# exit

Router(config)# snmp mib bulkstat object-list CAR-Objects
Router(config-bulk-objects)# add CcarStatSwitchedPkts

Router(config-bulk-objects)# add ccarStatSwitchedBytes

Router(config-bulk-objects)# add CcarStatFilteredBytes

Router(config-bulk-objects)# exit

Router(config)#
```

Related Commands

Command	Description
snmp mib bulkstat object-list	Names a bulk statistics object list and enters Bulk Statistics Object List configuration mode.

bandwidth (interface)

To set the inherited and received bandwidth values for an interface, use the **bandwidth** command in interface or virtual network interface config mode. To restore the default values, use the **no** form of this command.

bandwidth [**receive**] {*kbps*| **inherit** [*kbps*]}

no bandwidth [**receive**] {*kbps*| **inherit** [*kbps*]}

Syntax Description

kbps	Intended bandwidth, in kilobits per second. The range is from 1 to 10000000. For a full bandwidth DS3 line, enter the value 44736.
inherit	(Optional) Specifies how a subinterface inherits the bandwidth of its main interface.
receive	(Optional) Enables asymmetric transmit/receive operations so that the transmitted (**inherit** *kbps*) and received bandwidth are different.

Command Default

Default bandwidth values are set during startup. The bandwidth values can be displayed using the **show interfaces** or **show ipv6 interface** command. If the **receive** keyword is not used, by default, the transmit and receive bandwidths will be assigned the same value.

Command Modes

Interface configuration (config-if)

Virtual network interface (config-if-vnet)

Command History

Release	Modification
10.0	This command was introduced.
12.2T	This command was modified. The **inherit** keyword was added.
12.4(6)T	This command was modified. Support for IPv6 was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was implemented on Cisco ASR 1000 Aggregation Services Series Routers.

Release	Modification
Cisco IOS XE Release 3.2S	This command was modified. Support was added for this command in virtual network interface configuration mode.
15.1(03)S	This command was modified. Support was added for the **receive** keyword.

Usage Guidelines

Bandwidth Information

The **bandwidth** command sets an informational parameter to communicate only the current bandwidth to the higher-level protocols; you cannot adjust the actual bandwidth of an interface using this command.

Note This is only a routing parameter. It does not affect the physical interface.

Changing Bandwidth

For some media, such as Ethernet, the bandwidth is fixed; for other media, such as serial lines, you can change the actual bandwidth by adjusting the hardware. For both classes of media, you can use the **bandwidth** command to communicate the current bandwidth to the higher-level protocols.

Bandwidth Inheritance

Before the introduction of the **bandwidth inherit** command option, when the bandwidth value was changed on the main interface, the existing subinterfaces did not inherit the bandwidth value. If the subinterface was created before the bandwidth was changed on the main interface, the subinterface would receive the default bandwidth of the main interface, and not the configured bandwidth. Additionally, if the router was subsequently reloaded, the bandwidth of the subinterface would then change to the bandwidth configured on the main interface.

The **bandwidth inherit** command controls how a subinterface inherits the bandwidth of its main interface. This functionality eliminates inconsistencies related to whether the router has been reloaded and what the order was in entering the commands.

The **no bandwidth inherit** command enables all subinterfaces to inherit the default bandwidth of the main interface, regardless of the configured bandwidth. If the **bandwidth inherit** command is used without configuring a bandwidth on a subinterface, all subinterfaces will inherit the current bandwidth of the main interface. If you configure a new bandwidth on the main interface, all subinterfaces will use this new value.

If you do not configure a bandwidth on the subinterface and you configure the **bandwidth inherit** *kbps* command on the main interface, the subinterfaces will inherit the specified bandwidth.

In all cases, if an explicit bandwidth setting is configured on an interface, the interface will use that setting, regardless of whether the bandwidth inheritance setting is in effect.

Bandwidth Receipt

Some interfaces (such as Asymmetric Digital Subscriber Line (ADSL), V.35, RS-449, and High-Speed Serial Interface (HSSI)) can operate with different transmit and receive bandwidths. The **bandwidth receive** command permits this type of asymmetric operation. For example, for ADSL, the lower layer detects the two bandwidth values and configures the Integrated Data Base (IDB) accordingly. Other interface drivers, particularly serial interface cards on low- and midrange-platforms, can operate in this asymmetric bandwidth mode but cannot measure their clock rates. In these cases, administrative configuration is necessary for asymmetric operations.

Examples

The following example shows how to set the full bandwidth for DS3 transmissions:

```
Router(config)# interface serial 0
Router(config-if)# bandwidth 44736
```

The following example shows how to set the receive bandwidth:

```
Router(config)# interface serial 0
Router(config-if)# bandwidth receive 1000
```

Related Commands

Command	Description
show interfaces	Displays statistics for all interfaces configured on the router.
show ipv6 interface	Displays statistics for all interfaces configured on the IPv6 router.

buffer-size (bulk statistics)

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

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 (config-bulk-tr)

Command History

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

Usage Guidelines

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.

Examples

In the following example, the bulk statistics transfer buffer size is set to 3072 bytes:

```
Router(config)# snmp mib bulkstat transfer bulkstat1
Router(config-bulk-tr)# schema ATM2/0-IFMIB
Router(config-bulk-tr)# url primary ftp://user:pswrd@host/folder/bulkstat1
```

```
Router(config-bulk-tr)# buffer-size 3072
Router(config-bulk-tr)# enable
Router(config-bulk-tr)# exit
Router(config)#
```

Related Commands

Command	Description
snmp mib bulkstat transfer	Identifies the transfer configuration with a name and enters Bulk Statistics Transfer configuration mode.

comparison

To specify the type of Boolean comparison to be performed, use the **comparison** command in event trigger test boolean configuration mode. To disable the specified comparison value, use the **no** form of this command.

comparison {**equal**| **greatOrEqual**| **greater**| **lessOrEqual**| **lesser**| **unequal**}

no comparison

Syntax Description

equal	Specifies the type of Boolean comparison as equal.
greatOrEqual	Specifies the type of Boolean comparison as equal to or greater than.
greater	Specifies the type of Boolean comparison as greater than.
lessOrEqual	Specifies the type of Boolean comparison as equal to or less than.
lesser	Specifies the type of Boolean comparison as lesser than.
unequal	Specifies the type of Boolean comparison as unequal.

Command Default

The default comparison value for Boolean test is unequal.

Command Modes

Event trigger test boolean configuration (config-event-trigger-boolean)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.

Usage Guidelines

The specified value is used for Boolean comparison during trigger tests.

Examples

The following example shows how to specify a comparison value for Boolean test:

```
Router(config)# snmp mib event trigger owner owner1 name triggerA
Router(config-event-trigger)# test boolean
Router(config-event-trigger-boolean)# comparison unequal
Router(config-event-trigger-boolean)# end
```

Related Commands

Command	Description
test boolean	Configures parameters for the Boolean trigger test.

conditional object

To define a conditional object when evaluating an expression, use the **conditional object** command in expression object configuration mode. To disable the configured settings, use the **no** form of this command.

conditional object *conditional-object-id* [**wildcard**]

no conditional object

Syntax Description

conditional-object-id	Conditional object identifier for evaluating the expression. • Conditional object identifiers are specified as numerical value.
wildcard	(Optional) Enables the wildcarded search for conditional object identifiers.

Command Default

By default, the conditional object identifiers are not defined.

Command Modes

Expression object configuration (config-expression-object)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.

Usage Guidelines

The object identifier specifies the instance of the object to consider while evaluating an expression. If the object does not have an instance, the value specified for the object identifier will not be used. Conditional objects determine the use of the value specified for the object identifier.

Examples

The following example shows how to specify a conditional object:

```
Router(config)# snmp mib expression owner owner1 name Expression1
Router(config-expression)# object 32
Router(config-expression-object)# conditional object
mib-2.90.1.3.1.1.2.3.112.99.110.4.101.120.112.53
Router(config-expression-object)# end
```

The following example shows how to enable wildcarded search for conditional object identifiers:

```
Router(config-expression-object)# conditional object mib-2.5 wildcard
Router(config-expression-object)# end
```

Related Commands

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

context

Note Effective with Cisco IOS Release 15.0(1)M, the **context** command is replaced by the **snmp context**command. See the **snmp context** command for more information.

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

context *context-name*

no context

Syntax Description

context-name	Name of the SNMP VPN context. The name can be up to 32 alphanumeric characters.

Command Default

No SNMP contexts are associated with VPNs.

Command Modes

VRF configuration (config-vrf)

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRB	This command was modified. Support for IPv6 was added.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
15.0(1)M	This command was replaced by the **snmp context** command.

Usage Guidelines

Before you use the **context** command to associate an SNMP context with a VPN, you must do the following:

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

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

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

Examples

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

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

Related Commands

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

context (bulk statistics)

To associate a Simple Network Management Protocol (SNMP) context with the bulk statistics schema, use the **context** command in bulk statistics schema configuration mode. To disassociate an SNMP context from the bulk statistics schema, use the **no** form of this command.

context *context-name*

no context

Syntax Description

context-name	Name of the SNMP context that is associated with the bulk statistics schema.

Command Default

No SNMP context is associated with the bulk statistics schema.

Command Modes

Bulk statistics schema configuration (config-bulk-sc)

Command History

Release	Modification
12.2(33)SRC	This command was introduced.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.

Usage Guidelines

Use the **snmp mib bulkstat schema** command to enter bulk statistics schema configuration mode, and then use the **context** command to associate an SNMP context with the bulk statistics schema.

Examples

The following example shows how to create an SNMP context named ctx and associate the context with the bulk statistics schema:

```
Router(config)# snmp mib bulkstat schema sch
Router(config-bulk-sc)# context ctx
```

Related Commands

Command	Description
snmp mib bulkstat schema	Names an SNMP bulk statistics schema and enters bulk statistics schema configuration mode.

correlate

To build a single complex event, use the correlate command in trigger applet configuration mode. To disable the complex event, use the **no** form of this command.

correlate {**event** *event-tag*| **track** *track-object-number*}[**andor**| **and**| **or**]{**event** *event-tag*| **track** *track-object-number*}

no correlate {**event** *event-tag*| **track** *track-object-number*}[**andor**| **and**| **or**]{**event** *event-tag*| **track** *track-object-number*}

Syntax Description

event *event-tag*	Specifies the event that can be used with the **trigger** command to support multiple event statements within an applet. If the event associated with the event-tag argument occurs for the number of times specified by the **trigger** command, the result is true. If not, the result is false.
track *track-object-number*	Specifies the event object number for tracking. The range is from 1 to 500. If the tracked object is set, the result of the evaluation is true. If the tracked object is not set or is undefined, the result of the evaluation is false. This result is regardless of the state of the object.
andnot	(Optional) Specifies that if event 1 occurs the action is executed, and if event 2 and event 3 occur together the action is not executed.
and	(Optional) Specifies that if event 1 occurs the action is executed, and if event 2 and event 3 occur together the action is executed.
or	(Optional) Specifies that if event 1 occurs the action is executed, or else if event 2 and event 3 occur together the action is executed.

Command Default

The event detector counter is triggered when the specified counter crosses the threshold.

Command Modes

Trigger applet configuration (config-applet-trigger)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.

Usage Guidelines

After you enter the trigger statement, the router enters trigger applet configuration mode. The correlate statement and up to eight attribute statements can be specified in trigger applet configuration mode. These statements are used to create a complex event correlation using the participating event statements to a maximum of eight statements. The correlate statement allows Boolean logic to be used to relate events and tracked objects. When the result of the correlate evaluation is true, the trigger criteria are applied. The correlation occurs from left to right taking into account the attribute statement conditions for the event.

Examples

The following example, shows how to configure a correlate statement after entering trigger applet configuration mode. This applet will run if the write memory or copy run start command occurs within 60 seconds of CRON specified time.

```
Router(config)# event manager applet trigger
Router(config-applet)# event tag e1 cli pattern "write mem.*" sync yes
Router(config-applet)# event tag e2 cli pattern "copy run start" sync yes
Router(config-applet)# trigger occurs 1 period-start 0-59/1 0-23/1 * * 0-7 period 60
Router(config-applet-trigger)# correlate event e1 or event e2
Router(config-applet-trigger)# attribute tag e1 occurs 1
Router(config-applet-trigger)# attribute tag e2 occurs 1
Router(config-applet-trigger)# action 1.0 syslog msg "$_cli_msg Command Executed"
Router(config-applet-trigger)# set 2.0 _exit_status 1
```

In the following example, the applet will run if either the write memory or copy run start command occurs and any syslog message that contains the string “hello” occurs within 60 seconds of any valid CRON specified time.

```
Router(config)# event manager applet trigger
Router(config-applet)# event tag e1 cli pattern "write mem.*" sync yes
Router(config-applet)# event tag e2 cli pattern "copy run start" sync yes
Router(config-applet)# event tag e3 syslog pattern "hello"
Router(config-applet)# trigger occurs 1 period-start 0-59/1 0-23/1 * * 0-7 period 60
Router(config-applet-trigger)# correlate event e1 or event e2 and event e3
Router(config-applet-trigger)# attribute tag e1 occurs 1
Router(config-applet-trigger)# attribute tag e2 occurs 1
Router(config-applet-trigger)# attribute tag e3 occurs 1
Router(config-applet-trigger)# action 1.0 syslog msg "$_cli_msg Command Executed"
Router(config-applet-trigger)# set 2.0 _exit_status 1
```

In the following example, the applet will run when the write memory command is entered and the tracked object 10 is set:

```
Router(config)# event manager applet trigger
Router(config)# event tag e1 cli pattern "write mem.*" sync yes
Router(config)# trigger occurs 1
Router(config-applet-trigger)# correlate event e1 and track 10
Router(config-applet-trigger)# attribute tag e1 occurs 1
Router(config-applet-trigger)# action 1.0 syslog msg "$_cli_msg Command Executed"
Router(config-applet-trigger)# set 2.0 _exit_status 1
```

Related Commands

Command	Description
action syslog	Specifies the action of writing a message to a syslog when an EEM applet is triggered.
attribute	Configures an attribute in a local service profile.
event manager applet	Registers an applet with the EEM and enters applet configuration mode.
trigger (EEM)	Enters the trigger applet configuration mode and specifies the multiple event configuration statements for an EEM applet.

delta (test threshold)

To specify a delta value for the threshold trigger test, use the **delta** command in event trigger threshold configuration mode. To disable the configured settings, use the **no** form of this command.

delta {**falling**| **rising**} {*threshold-value*| **event owner** *event-owner* **name** *event-name*}

no delta {**falling**| **rising**}

Syntax Description

falling	Specifies the delta value for the falling threshold.
rising	Specifies the delta value for the rising threshold.
threshold-value	Delta value for thresholds. The default value is 0.
event	Specifies the event.
owner	Specifies the event owner.
event-owner	Name of the event owner.
name	Specifies the name of an event.
event-name	Name of the event.

Command Default

The delta threshold value is set to 0 and no event is invoked by default.

Command Modes

Event trigger threshold configuration (config-event-trigger-threshold)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.

Usage Guidelines

The **delta** command sets the delta falling or rising threshold to the specified value when the object sampling method is delta. The **delta rising event owner** command specifies the event to be invoked when the delta rising threshold is triggered. Similarly, the **delta falling event owner** specifies the event to be invoked when the delta falling threshold is triggered.

Examples

The following example shows how to specify a delta falling threshold:

```
Router(config)# snmp mib event trigger owner owner1 name triggerA
Router(config-event-trigger)# test threshold
Router(config-event-trigger-threshold)# delta falling 20
Router(config-event-trigger-threshold)# end
```

Related Commands

Command	Description
test	Specifies the type of test to perform during an event trigger.

delta interval

To specify an interval for the delta sampling of objects used while evaluating an expression, use the **delta interval** command in expression configuration mode. To disable the configured settings, use the **no** form of this command.

delta interval *seconds*

no delta interval

Syntax Description

seconds	Number of seconds for the delta sampling interval. The default is 0.

Command Default

The default delta sampling interval is 0.

Command Modes

Expression configuration (config-expression)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.

Usage Guidelines

If there are no objects configured for the delta sampling method, the **delta interval** command does not configure the interval.

Examples

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

```
Router(config)# snmp mib expression owner owner1 name expressionA
Router(config-expression)# delta interval 60
Router(config-expression)# end
```

Related Commands

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

description (event)

To describe the function and use of an event, use the **description** command in event configuration mode. To remove the description, use the **no** form of this command.

description *event-description*

no description

Syntax Description

event-description	Description of the function and use of an event. • The description text string can be up to 256 characters in length. If the string contains embedded blanks, enclose it in double quotation marks.

Command Default

By default, events are not described.

Command Modes

Event configuration (config-event)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.

Usage Guidelines

The **description** command configures a free-text description of the function and use of an event.

Examples

The following example shows how to describe an event:

```
Router(config)# snmp mib event owner owner1 name EventA
Router(config-event)# description "EventA is an RMON event"
Router(config-event)# end
```

Related Commands

Command	Description
snmp mib event owner	Specifies an event owner for a management event.

description (expression)

To provide a description of the use of an expression, use the **description** command in expression configuration mode. To remove the description, use the **no** form of this command.

description *expression-description*

no description

Syntax Description

expression-description	Description of the function and use of an expression. The description text string can be up to 256 characters in length.

Command Default

By default, no expression is described.

Command Modes

Expression configuration (config-expression)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.

Usage Guidelines

The **description** command configures a free-text description of the function and use of an expression.

Examples

The following example shows how to describe an expression:

```
Router(config)# snmp mib expression owner owner1 name expressionA
Router(config-expression)# description expressionA is created for the sysLocation MIB object
Router(config-expression)# end
```

Related Commands

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

description (trigger)

To provide a description of the function and use of an event trigger, use the **description** command in the event trigger configuration mode. To remove the description, use the **no** form of this command.

description *trigger-description*

no description

Syntax Description

trigger-description	Description of the function and use of a trigger. • The description text string can be up to 256 characters in length.

Command Default

By default, no trigger is described.

Command Modes

Event trigger configuration (config-event-trigger)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.

Usage Guidelines

The **description** command configures a free-text description of the function and use of an event trigger.

Examples

The following example shows how to describe an event trigger:

```
Router(config)# snmp mib event trigger owner owner1 name triggerA
Router(config-event-trigger)# description triggerA is configured for network management
events
Router(config-event-trigger)# end
```

Related Commands

Command	Description
snmp mib event trigger owner	Specifies the event trigger owner while configuring management event trigger information.

discontinuity object (expression)

To define the discontinuity properties for an object, use the **discontinuity object** command in expression object configuration mode. To disable the configuration settings, use the **no** form of this command.

discontinuity object *discontinuity-object-id* **[wildcard]** [**type** {**timeticks**| **timestamp**| **date-and-time**}]

no discontinuity object

Syntax Description

discontinuity-object-id	Discontinuity object identifier to identify discontinuity in a counter. • The default object identifier is sysUpTime.0.
wildcard	(Optional) Specifies whether an object identifier is to be wildcarded or fully specified. • By default, the object identifier is fully specified.
type	(Optional) Specifies the type of discontinuity in a counter. • The default value for the discontinuity type is timeticks.
timeticks	(Optional) Specifies timeticks for discontinuity in a counter.
timestamp	(Optional) Specifies the time stamp for discontinuity in a counter.
date-and-time	(Optional) Specifies the date and time of discontinuity in a counter.

Command Default

The default discontinuity object identifier is sysUpTime.0.

Command Modes

Expression object configuration (config-expression)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Release	Modification
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.

Usage Guidelines

The **discontinuity object** command configures discontinuity properties of an object when the object sampling type is delta or changed.

Examples

The following example shows how to configure discontinuity properties for an object:

```
Router(config)# snmp mib expression owner owner1 name ExpressionA
Router(config-expression)# object 43
Router(config-expression-object)# discontinuity object 0.7
Router(config-expression-object)# end
```

The following example shows how to enable wildcarded search for discontinuity object identifiers:

```
Router(config-expression-object)# discontinuity object 0.7 wildcard
Router(config-expression-object)# end
```

The following example shows how to specify the type for discontinuity in a counter:

```
Router(config-expression-object)# discontinuity object 0.7 type timeticks
Router(config-expression-object)# end
```

Related Commands

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

enable (bulk statistics)

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 arguments or keywords.

Command Default

Bulk statistics transfer is disabled.

Command Modes

Bulk Statistics Transfer configuration (config-bulk-tr)

Command History

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

Usage Guidelines

Specific bulk statistics configurations are identified with a name, as specified in the **snmp mib bulkstat transfer** command. The **enable** command (in Bulk Statistics Transfer configuration mode) begins the periodic MIB data collection and transfer process.

Collection (and subsequent file transfer) will start only if this command is used. Conversely, the **no enable**command will stop the collection process. Subsequently, issuing the **enable**command will start 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 will immediately begin (in other words, the existing bulk statistics file will be 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.

Examples

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

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

Related Commands

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

enable (event)

To enable an event or event trigger, use the **enable** command in event or event trigger configuration mode, respectively. To disable the event, use the **no** form of this command.

enable

no enable

Syntax Description

This command has no arguments or keywords.

Command Default

No event is enabled by default.

Command Modes

Event configuration (config-event)

Event trigger configuration (config-event-trigger)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.

Usage Guidelines

If an event is not enabled, it is not executed when triggered.

Examples

The following example shows how to enable an event:

```
Router(config)# snmp mib event owner owner1 name EventA
Router(config-event)# enable
Router(config-event)# end
```

The following example shows how to enable an event trigger:

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

Related Commands

Command	Description
snmp mib event owner	Specifies an owner for a management event.
snmp mib event trigger owner	Specifies an event trigger owner while configuring management event trigger information.

enable (expression)

To enable an expression, use the **enable** command in expression configuration mode. To disable an expression, use the **no** form of this command.

enable

no enable

Syntax Description

This command has no arguments or keywords.

Command Default

No expression is enabled by default.

Command Modes

Expression configuration (config-expression)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.

Usage Guidelines

The **enable** command enables the expression for evaluation.

Examples

The following example shows how to enable an expression:

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

Related Commands

Command	Description
snmp mib expression owner	Specifies an expression.

event owner

To specify the event owner for an event trigger according to the trigger type and status of the trigger, use the **event owner** command in event trigger existence or event trigger boolean configuration mode. To disable the configuration and set default parameters, use the **no** form of this command.

event owner *event-owner* **name** *event-name*

no event owner

Syntax Description

event-owner	Owner of the event.
name	Indicates the name of the event.
event-name	Unique name of the event.

Command Default

The event owner and event name are not specified.

Command Modes

Event trigger existence configuration (config-event-trigger-existence)

Event trigger boolean configuration (config-event-trigger-boolean)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.

Usage Guidelines

The event is identified by *event-owner* and *event-name* values and is configured by using the **snmp mib event** command. Events are enabled by using the **enable** command.

Examples

The following example shows how to specify an event owner for the existence trigger test:

```
Router(config)# snmp mib event trigger owner owner1 name triggerA
Router(config-event-trigger)# test existence
Router(config-event-trigger-existence)# event owner owner2 name event2
Router(config-event-trigger-existence)# end
```

The following example shows how to specify an event owner for the Boolean trigger test:

```
Router(config)# snmp mib event trigger owner owner1 name triggerA
Router(config-event-trigger)# test boolean
Router(config-event-trigger-boolean)# event owner owner2 name event2
Router(config-event-trigger-boolean)# end
```

Related Commands

Command	Description
snmp mib event trigger owner	Specifies an event trigger owner while configuring management event trigger information.
test boolean	Configures parameters for the Boolean trigger test.
test existence	Configures parameters for the existence trigger test.

expression

To specify an expression for evaluation, use the **expression** command in expression configuration mode. To disable the configured settings, use the **no** form of this command.

expression *expression*

no expression

Syntax Description

expression	Expression to be evaluated.

Command Default

By default, no expression is configured.

Command Modes

Expression configuration (config-expression)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.

Usage Guidelines

The expressions are in the ANSI C syntax except for the variable names. Variables are expressed as $ (dollar sign) and integers that correspond to the object number. An example of an expression is ($1-$5)*100.

Examples

The following example shows how to specify an expression:

```
Router(config)# snmp mib expression owner owner1 name expressionA
Router(config-expression)# expression ($1+$2)*800/$3
Router(config-expression)# end
```

Related Commands

Command	Description
snmp mib expression owner	Specifies an expression owner.

falling (test threshold)

To specify a falling threshold value for the threshold trigger test, use the **falling** command in event trigger threshold configuration mode. To disable the specified threshold, use the **no** form of this command.

falling {*threshold-value* | **event owner** *event-owner* **name** *event-name*}

no falling

Syntax Description

threshold-value	Numerical value for falling threshold. The default value is 0.
event	Specifies the event.
owner	Specifies the event owner.
event-owner	Name of the event owner.
name	Indicates the name of an event.
event-name	Name of an event.

Command Default

The default falling threshold value is 0. No event is invoked by default.

Command Modes

Event trigger threshold configuration (config-event-trigger-threshold)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.

Usage Guidelines

The falling threshold value you specify is verified when the threshold trigger is active. If the sample value is equal to or less than the value you specify and greater than the value at the last sampling interval, a corresponding trigger is generated.

The **falling event owner** command specifies the event to be invoked when the falling threshold is triggered. An event is identified by the owner and name and is configured by using the **snmp mib event owner** command.

Examples

The following example shows how to specify a falling threshold value of 12:

```
Router(config)# snmp mib event trigger owner owner1 name triggerA
Router(config-event-trigger)# test threshold
Router(config-event-trigger-threshold)#  falling 12
Router(config-event-trigger-threshold)# end
```

Related Commands

Command	Description
test	Enables a trigger test.

format (bulk statistics)

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

Syntax Description

bulkBinary	Binary format.
bulkASCII	ASCII (human-readable) format.
schemaASCII	ASCII format with 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 (config-bulk-tr)

Command History

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

Usage Guidelin

Note In Cisco IOS Release 12.0(24)S, only the schemaASCII format is supported. This command will not change the file format in that release.

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.

For the bulkASCII and bulkBinary formats, periodic polling enables data for a single data group (object list) to be collected more than once in the same VFile. Each such instance of a data group can be treated as a different “table” type.

Every object and table tag contains an additional sysUpTime field. Similarly each row tag contains the value of the sysUpTime when the data for that row was collected. The sysUpTime provides a time stamp for the data.

For additional information about the structures of the bulk statistics data file formats, see the definitions in the CISCO-DATA-COLLECTION-MIB.

Examples

In the following example, the bulk statistics data file is set to schemaASCII:

```
Router(config)# snmp mib bulkstat transfer bulkstat1
Router(config-bulk-tr)# schema ATM2/0-IFMIB
Router(config-bulk-tr)# url primary ftp://user:pswrd@host/folder/bulkstat1
Router(config-bulk-tr)# format schemaASCII
Router(config-bulk-tr)# exit
```

Related Commands

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

frequency (event trigger)

To specify an interval between trigger samples, use the **frequency** command in event trigger configuration mode. To disable the configured interval, use the **no** form of this command.

frequency *seconds*

no frequency

Syntax Description

seconds	Number of seconds between two trigger samples. The default is 600.

Command Default

The interval between the trigger samples is set to the default value.

Command Modes

Event trigger configuration (config-event-trigger)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.

Usage Guidelines

The **frequency** command configures the waiting time between trigger samples. By default, the frequency of object sampling is 600 seconds.

Examples

The following example shows how to specify an interval of 360 seconds for sampling:

```
Router(config)# snmp mib event trigger owner owner1 name triggerA
Router(config-event-trigger)# frequency 360
Router(config-event-trigger)# end
```

Related Commands

Command	Description
snmp mib event trigger owner	Specifies an event trigger owner while configuring management event trigger information.

id (expression)

To configure the object identifier, use the **id** command in expression object configuration mode. To disable the configuration, use the **no** form of this command.

id *object-oid*

no id

Syntax Description

object-oid	Object identifier of an object. The default is 0.0.

Command Default

By default, the object identifier for an object is not configured.

Command Modes

Expression object configuration mode (config-expression-object)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Examples

The following example shows how to set the object identifier to 2.2 in expression object configuration mode:

```
Router(config)# snmp mib expression owner owner1 name expressionA
Router(config-expression)# object 3
Router(config-expression-object)# id 2.2
```

instance (MIB)

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

instance {**exact**| **wild**} {**interface** *interface-id* **[sub-if]**| **oid** *oid*}

no instance

Syntax Description

exact	Indicates that the specified instance (interface, controller, or object identifier [OID]), when appended to the object list, is the complete OID to be used in this schema.
wild	Indicates that all instances that fall within the specified interface, controller, or OID range should be included in this schema.
interface	Specifies a specific interface or group of interfaces for the schema.
interface-id	Interface name and number for a specific interface or group of interfaces.
sub-if	(Optional) Specifies that the object instances should be polled for all subinterfaces of the specified interface or controller in addition to the object instances for the main interface.
oid	Indicates that an OID is specified.
oid	Object ID that, when appended to the object list, specifies the complete (or wildcarded) OID for the objects to be monitored.

Command Default

By default, MIB object instances to be used in bulk statistics schema are not configured.

Command Modes

Bulk Statistics Schema configuration (config-bulk-sc)

Command History

Release	Modification
12.0(24)S	This command was introduced.

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

Usage Guidelines

The **instance** command specifies the instance information for objects in the schema being configured. 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 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. In other words, the **wild** keyword allows you to specify a partial, wildcarded instance.

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, FastEthernet 0) instead of specifying the ifIndex OID for the interface.

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

Only one **instance** command can be configured per schema.

Examples

The following example shows how to configure the router to collect bulk statistics for the ifInOctets object (from the IF-MIB) for Fast Ethernet interface 3/0. In this example, 3 is the ifIndex instance for Fast Ethernet interface 3/0. The instance (3) when combined with the object list (ifIndex; 1.3.6.1.2.1.2.2.1.1) translates to the OID 1.3.6.1.2.1.2.2.1.1.3.

```
Router# configure terminal
Router(config)# snmp mib bulkstat object-list E0InOctets
! The following command specifies the object 1.3.6.1.2.1.2.2.1.1.3 (ifIndex)
Router(config-bulk-objects)# add ifIndex
Router(config-bulk-objects)# exit
Router(config)# snmp mib bulkstat schema E0
Router(config-bulk-sc)# object-list E0InOctets
! The following command is equivalent to “instance exact oid 3”.
Router(config-bulk-sc)# instance exact interface FastEthernet 3/0
Router(config-bulk-sc)# exit
Router(config)# snmp mib bulkstat transfer bulkstat1
Router(config-bulk-tr)# schema E0
Router(config-bulk-tr)# url primary ftp://user:password@host/ftp/user/bulkstat1
Router(config-bulk-tr)# url secondary tftp://user@host/tftp/user/bulkstat1
Router(config-bulk-tr)# format schemaASCII
Router(config-bulk-tr)# transfer-interval 30
```

```
Router(config-bulk-tr)# retry 5
Router(config-bulk-tr)# enable
Router(config-bulk-tr)# exit
Router(config)# do copy running-config startup-config
```

Related Commands

Command	Description
object-list	Configures the bulk statistics object list to be used in the bulk statistics schema.
snmp mib bulkstat schema	Names an SNMP bulk statistics schema and enters Bulk Statistics Schema configuration mode.

instance range

To specify the range of instances to collect for a given data group, use the **instance range**command in Bulk Statistics Schema configuration mode. To delete a previously configured instance range, use the **no** form of this command.

instance range start *oid* **end** *oid*

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

Syntax Description

start	Indicates the beginning of the range.
oid	The object ID to be monitored for the specific range.
end	Indicates the end of the range.

Command Default

No instance range is configured.

Command Modes

Bulk Statistics Schema configuration (config-bulk-sc)

Command History

Release	Modification
12.2(33)SRC	This command was introduced.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS Release XE 2.1.

Usage Guidelines

When used in conjunction with the **snmp mib bulkstat schema** command, the **instance range** command can be used to configure a range of instances on which to collect data.

Examples

The following example shows the collection of data for all instances starting with instance 1 and ending with instance 2:

```
snmp mib bulkstat object-list ifmib
  add ifInOctets
  add ifOutOctets
  exit
!
snmp mib bulkstat schema IFMIB
 object-list ifmib
 poll-interval 1
 instance range start 1 end 2
 exit
```

```
!
snmp mib bulkstat transfer bulkstat1
 schema IFMIB
 url primary tftp://202.153.144.25/pcn/bulkstat1
 format schemaASCII
 transfer-interval 5
 retry 5
 buffer-size 1024
 retain 30
 enable
 end
```

Related Commands

Command	Description
instance	Specifies the instance that, when appended to the object list, gives the OID of the object instance to be monitored in the bulk statistics schema.
snmp mib bulkstat schema	Names a bulk statistics schema and enters Bulk Statistics Schema configuration mode.

instance repetition

To configure 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 repetition

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 (config-bulk-sc)

Command History

Release	Modification
12.2(33)SRC	This command was introduced.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS Release XE 2.1.

Usage Guidelines

When used in conjunction with the **snmp mib bulkstat schema** command, the **instance repetition** command can be used to configure data collection to repeat for a certain number of instances of a MIB object.

Examples

The following example shows how to start data collection at the first instance and repeat for four instances of the indicated MIB object:

```
snmp mib bulkstat object-list ifmib
 add ifOutOctets
 add ifInOctets
snmp mib bulkstat schema IFMIB
 object-list ifmib
 poll-interval 1
 instance repetition 1 max 4
snmp mib bulkstat transfer bulkstat1
```

```
schema IFMIB
transfer-interval 5
retain 30
retry 5
buffer-size 1024
enable
```

Related Commands

Command	Description
instance	Specifies the instance that, when appended to the object list, gives the OID of the object instance to be monitored in the bulk statistics schema.
snmp mib bulkstat schema	Names a bulk statistics schema and enters Bulk Statistics Schema configuration mode.

no snmp-server

To disable Simple Network Management Protocol (SNMP) agent operation, use the **no snmp-server** command in global configuration mode.

no snmp-server

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

This command disables all running versions of SNMP (SNMPv1, SNMPv2C, and SNMPv3) on the device.

Examples

The following example disables the current running version of SNMP:

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

object (expression)

To specify the objects to be used while evaluating an expression, use the **object** command in expression configuration mode. To disable the configured settings, use the **no** form of this command.

object *object-number*

no object *object-number*

Syntax Description

object-number	The object number, which is associated with variables while evaluating an expression.

Command Default

No object is configured for evaluating an expression by default.

Command Modes

Expression configuration (config-expression)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.

Usage Guidelines

The *object-number* argument associates objects with variables in an expression. The variable corresponding to an object contains $ (dollar sign) and the object number. For example, the object number is 1, and the variable is $1. The **object** command can be used multiple times to define multiple objects or variables in an expression.

Examples

The following example shows how to specify objects used in expressions:

```
Router(config)# snmp mib expression owner owner1 name expression1
Router(config-expression)# object 10
Router(config-expression)# end
```

Related Commands

Command	Description
snmp mib expression owner	Specifies an expression.

object id

To specify the object identifier of an object associated with an event, use the **object id** command in event object list, event action notification, event action set, or event trigger configuration mode. To disable the configured settings, use the **no** form of this command.

object id *object-identifier*

no object id

Syntax Description

object-identifier	Object identifier of an object. The default is 0.0.

Command Default

By default the object identifier is not specified.

Command Modes

Event object list configuration (config-event-objlist)

Event action notification configuration (config-event-action-notification)

Event action set configuration (config-event-action-set)

Event trigger configuration (config-event-trigger)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.

Usage Guidelines

The **object id** command specifies the object identifier of the object associated with an event. If notifications are enabled for an event, the system sends a notification whenever the object is modified.

Examples

The following example shows how to set the object identifier to 2.2 in event object list configuration mode:

```
Router(config)# snmp mib event owner owner1 name eventA
Router(config-event)# snmp mib event object list owner owner1 name objectA 10
Router(config-event-objlist)# object id 2.2
Router(config-event-objlist)# end
```

The following example shows how to set the object identifier to 2.2 in event action notification configuration mode:

```
Router(config)# snmp mib event owner owner1 name eventA
Router(config-event)# action notification
Router(config-event-action-notification)# object id 2.2
Router(config-event-action-notification)# end
```

The following example shows how to set the object identifier to 2.2 in event action set configuration mode:

```
Router(config)# snmp mib event owner owner1 name eventA
Router(config-event)# action set
Router(config-event-action-set)# object id 2.2
Router(config-event-action-set)# end
```

The following example shows how to set the object identifier to 2.2 in event trigger configuration mode:

```
Router(config)# snmp mib event trigger owner owner1 name triggerA
Router(config-event-trigger)# object id 2.2
Router(config-event-trigger)# end
```

Related Commands

Command	Description
action	Configures actions for an event.
snmp mib event object list	Configures a list of objects.
snmp mib event trigger owner	Specifies the owner for an event trigger.

object id (event trigger)

To specify the object identifier of an object, use the **object id** command in event trigger configuration mode.

object id *object-identifier*

Syntax Description

object-identifier	Object identifier of an object.

Command Default

This command is enabled by default.

Command Modes

Event trigger configuration (config-event-trigger).

Command History

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

Usage Guidelines

The **object id** command specifies object identifier of the object configured for an event trigger. The default value of the object identifier is **0.0**.

Examples

The following example shows how to specify the object identifier by using the **object id** command:

```
Router(config)# snmp mib event trigger owner John name triggerA
Router(config-event-trigger)# object id 2.2
Router(config-event-trigger)#
```

Related Commands

Command	Description
snmp mib event trigger owner	Specifies the name of the event trigger owner. This command also enables the event trigger configuration mode.

object list

To configure a list of objects during an event, use the **object list** command in event trigger, event action notification, event trigger existence, event trigger boolean, or event trigger threshold configuration mode. To disable the configured settings, use the **no** form of this command.

object list owner *object-list-owner* **name** *object-list-name*

no object list

Syntax Description

owner	Indicates the owner of the object list.
object-list-owner	Name of the object list owner.
name	Indicates the name of the object list.
object-list-name	Unique name that identifies the object list.

Command Default

Object lists are not configured.

Command Modes

Event trigger configuration (config-event-trigger)

Event action notification configuration (config-event-action-notification)

Event trigger existence configuration (config-event-trigger-existence)

Event trigger boolean configuration (config-event-trigger-boolean)

Event trigger threshold configuration (config-event-trigger-threshold)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.

Examples

The following example shows how to specify the object list for an event trigger:

```
Router(config)# snmp mib event trigger owner owner1 name triggerA
Router(config-event-trigger)# object list owner owner1 name objectA
Router(config-event-trigger)# end
```

The following example shows how to specify the object list for an action notification:

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

```
Router(config-event-action-notification)# object list owner owner1 name objectA
Router(config-event-action-notification)# end
```

The following example shows how to specify the object list for an existence trigger test:

```
Router(config-event-trigger)# test existence
Router(config-event-trigger-existence)# object list owner owner1 name objectA
Router(config-event-trigger-existence)# end
```

The following example shows how to specify the object list for a Boolean trigger test:

```
Router(config-event-trigger)# test boolean
Router(config-event-trigger-boolean)# object list owner owner1 name objectA
Router(config-event-trigger-boolean)# end
```

The following example shows how to specify the object list for a threshold trigger test:

```
Router(config-event-trigger)# test threshold
Router(config-event-trigger-threshold)# object list owner owner1 name objectA
Router(config-event-trigger-threshold)# end
```

Related Commands

Command	Description
snmp mib event trigger owner	Specifies an event trigger owner while configuring management event trigger information.
test	Enables a trigger test.

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

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 (config-bulk-sc)

Command History

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

Usage Guidelines

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.

Examples

In the following example, the object list named E0InOctets is associated with the schema named E0:

```
Router(config)# snmp mib bulkstat schema E0
Router(config-bulk-sc)# object-list EOInOctets
```

```
Router(config-bulk-sc)# instance exact interface FastEthernet 3/0
Router(config-bulk-sc)# exit
```

Related Commands

Command	Description
instance	Specifies the instance that, when appended to the object list, gives the OID of the object instance to be monitored in the bulk statistics schema.
snmp mib bulkstat schema	Names a bulk statistics schema and enters Bulk Statistics Schema configuration mode.

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 (config-bulk-sc)

Command History

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

Usage Guidelines

The **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.

Examples

In the following example, the polling interval for bulk statistics collection is set to once every 3 minutes in the schema called FastEthernet2/1-CAR:

```
Router(config)# snmp mib bulkstat schema FastEthernet2/1-CAR
```

```
Router(config-bulk-sc)# object-list CAR-mib
Router(config-bulk-sc)# poll-interval 3
Router(config-bulk-sc)# instance wildcard oid 3.1
Router(config-bulk-sc)# exit
```

Related Commands

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

prefix object

To enable the application to determine the object based on instance indexing, use the **prefix object**command in the expression object configuration mode.

prefix object *object-id*

Syntax Description

object-id	Object identifier of an object.

Command Default

No object is prefixed by default.

Command Modes

Expression object configuration (config-expression-object)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

The **prefix object**command enables the application to determine an object according to the instance indexing. The instance index is used in expValueTable. The **prefix object** command eliminates the need to scan expObjectTable to determine a prefix, thereby easing the burden of an application.

Examples

The following example shows how to specify a prefix object:

```
Router(config)# snmp mib expression owner John name ExpressionA
Router(config-expression)# object
Router(config-expression-object)# prefix object 0.0.6
Router(config-expression-object)#
```

Related Commands

Command	Description
snmp mib expression owner	Specifies an expression owner.

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

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 (config-bulk-tr)

Command History

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

Usage Guidelines

This 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 will be 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 will be attempted once every 5 minutes. Therefore, if the **retain** command is not configured (retain default is 0), no retries will be attempted.

Examples

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

```
Router(config)# snmp mib bulkstat transfer bulkstat1
Router(config-bulk-tr)# schema ATM2/0-IFMIB
Router(config-bulk-tr)# url primary ftp://user:pswrd@host/folder/bulkstat1
Router(config-bulk-tr)# retry 2
Router(config-bulk-tr)# retain 10
Router(config-bulk-tr)# exit
```

Related Commands

Command	Description
retry	Configures the number of retries that should be attempted for sending bulk statistics files.
snmp mib bulkstat transfer	Identifies the transfer configuration with a name and enters Bulk Statistics Transfer configuration mode.

retry (bulk statistics)

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

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 (config-bulk-tr)

Command History

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

Usage Guidelines

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 will be attempted once every 5 minutes. Therefore, if the **retain** command is not configured (or the **retain 0** command is used) no retries will be attempted.

Examples

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

```
Router(config)# snmp mib bulkstat transfer bulkstat1
Router(config-bulk-tr)# schema ATM2/0-IFMIB
Router(config-bulk-tr)# url primary ftp://user:pswrd@host/folder/bulkstat1
Router(config-bulk-tr)# retry 2
Router(config-bulk-tr)# retain 10
Router(config-bulk-tr)# exit
```

Related Commands

Command	Description
retain	Configures the retention interval in local system memory (NVRAM) for bulk statistics files.
snmp mib bulkstat transfer	Identifies the transfer configuration with a name and enters Bulk Statistics Transfer configuration mode.

rising (test threshold)

To specify an event owner for the rising threshold trigger, use the **rising event owner** command in event trigger threshold configuration mode. To disable the configured settings, use the **no** form of this command.

rising {*threshold-value*| **event owner** *event-owner* **name** *event-name*}

no rising

Syntax Description

threshold-value	Numerical value to specify the rising threshold. The default value is 0.
event	Specifies the event.
owner	Specifies the owner of the event.
event-owner	Owner of an event.
name	Specifies the name of an event.
event-name	Unique name of an event.

Command Default

The default rising threshold value is 0. No event is invoked by default.

Command Modes

Event trigger threshold configuration (config-event-trigger-threshold)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.

Usage Guidelines

The **rising** command specifies the event to be invoked when the rising threshold is triggered. An event is identified by the owner and name and is configured using the **snmp mib event owner** command.

Examples

The following example shows how to specify an event owner for the rising threshold trigger:

```
Router(config)# snmp mib event trigger owner owner1 name triggerA
Router(config-event-trigger)# test threshold
```

```
Router(config-event-trigger-threshold)# rising event owner owner1 name event5
Router(config-event-trigger-threshold)# end
```

Related Commands

Command	Description
test	Enables a trigger test.



sample (event trigger) through snmp mib event sample

- sample (event trigger), page 73
- sample (expression), page 75
- schema, page 77
- show management event, page 79
- show management expression, page 81
- show snmp, page 83
- show snmp chassis, page 87
- show snmp community, page 88
- show snmp contact, page 90
- show snmp engineID, page 91
- show snmp group, page 93
- show snmp host, page 95
- show snmp location, page 97
- show snmp mib, page 98
- show snmp mib bulkstat transfer, page 101
- show snmp mib context, page 104
- show snmp mib ifmib traps, page 106
- show snmp mib ifmib ifindex, page 108
- show snmp mib notification-log, page 113
- show snmp pending, page 115
- show snmp sessions, page 117
- show snmp stats oid, page 120
- show snmp sysobjectid, page 122

- show snmp user, page 124
- show snmp view, page 127
- snmp context (VRF), page 129
- snmp get, page 131
- snmp get-bulk, page 133
- snmp get-next, page 136
- snmp ifmib ifalias long, page 138
- snmp inform, page 140
- snmp mib bulkstat object-list, page 143
- snmp mib bulkstat schema, page 145
- snmp mib bulkstat transfer, page 147
- snmp mib community-map, page 149
- snmp mib event object list, page 152
- snmp mib event owner, page 154
- snmp mib event sample, page 155

sample (event trigger)

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

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

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

Syntax Description

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

Command Default

The default sampling method is absolute.

Command Modes

Event trigger configuration (config-event-trigger)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.

Usage Guidelines

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

- Absolute
- Delta
- Changed

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

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

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

Examples

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

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

Related Commands

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

sample (expression)

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

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

no sample

Syntax Description

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

Command Default

The default sampling method is absolute.

Command Modes

Expression object configuration (config-expression-object)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.

Usage Guidelines

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

- Absolute
- Delta
- Changed

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

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

Examples

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

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

Related Commands

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

schema

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

schema *schema-name*

no schema *schema-name*

Syntax Description

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

Command Default

No bulk statistics schema is specified.

Command Modes

Bulk Statistics Transfer configuration (config-bulk-tr)

Command History

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

Usage Guidelines

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

Examples

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

```
Router(config)# snmp mib bulkstat transfer bulkstat1
```

```
Router(config-bulk-tr)# schema ATM2/0-IFMIB
Router(config-bulk-tr)# schema ATM2/0-CAR
Router(config-bulk-tr)# url primary ftp://user:pswrd@host/folder/bulkstat1
Router(config-bulk-tr)# retry 2
Router(config-bulk-tr)# retain 10
Router(config-bulk-tr)# exit
```

Related Commands

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

show management event

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

show management event

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

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

Examples

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

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

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

Related Commands

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

show management expression

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

show management expression

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC Privileged EXEC (#)

Command History

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

Examples

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

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

The output is self-explanatory.

Related Commands

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

show snmp

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

show snmp

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

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

Usage Guidelines

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

Examples

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

```
Router# show snmp
Chassis: 12161083
0 SNMP packets input
    0 Bad SNMP version errors
    0 Unknown community name
    0 Illegal operation for community name supplied
    0 Encoding errors
    0 Number of requested variables
    0 Number of altered variables
    0 Get-request PDUs
    0 Get-next PDUs
    0 Set-request PDUs
    0 Input queue packet drops (Maximum queue size 1000)
0 SNMP packets output
    0 Too big errors (Maximum packet size 1500)
    0 No such name errors
    0 Bad values errors
    0 General errors
    0 Response PDUs
    0 Trap PDUs
SNMP logging: enabled
    SNMP Trap Queue: 0 dropped due to resource failure.
```

```
    Logging to 202.153.144.25.162, 0/10, 0 sent, 0 dropped.
SNMP Manager-role output packets
    4 Get-request PDUs
    4 Get-next PDUs
    6 Get-bulk PDUs
    4 Set-request PDUs
    23 Inform-request PDUs
    30 Timeouts
    0 Drops
SNMP Manager-role input packets
    0 Inform response PDUs
    2 Trap PDUs
    7 Response PDUs
    1 Responses with errors
SNMP informs: enabled
    Informs in flight 0/25 (current/max)
    Logging to 171.69.217.141.162
        4 sent, 0 in-flight, 1 retries, 0 failed, 0 dropped
    Logging to 171.69.58.33.162
        0 sent, 0 in-flight, 0 retries, 0 failed, 0 dropped
```

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

Table 1: show snmp Field Descriptions

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

Field	Description
No such name errors	Number of SNMP requests that specified a MIB object that does not exist.
Bad values errors	Number of SNMP set requests that specified an invalid value for a MIB object.
General errors	Number of SNMP set requests that failed due to some other error. (It was not a noSuchName error, badValue error, or any of the other specific errors.)
Response PDUs	Number of responses sent in reply to requests.
Trap PDUs	Number of SNMP traps sent.
SNMP logging	Indicates whether logging is enabled or disabled.
sent	Number of traps sent.
dropped	Number of traps dropped. Traps are dropped when the trap queue for a destination exceeds the maximum length of the queue, as set by the **snmp-server queue-length** global configuration command.
SNMP Trap Queue	Number of traps that are getting dropped due to memory resource failure.
SNMP Manager-role output packets	Information related to packets sent by the router as an SNMP manager.
Get-request PDUs	Number of get requests sent.
Get-next PDUs	Number of get-next requests sent.
Get-bulk PDUs	Number of get-bulk requests sent.
Set-request PDUs	Number of set requests sent.
Inform-request PDUs	Number of inform requests sent.
Timeouts	Number of request timeouts.
Drops	Number of requests dropped. Reasons for drops include no memory, a bad destination address, or an unreasonable destination address.
SNMP Manager-role input packets	Information related to packets received by the router as an SNMP manager.
Inform response PDUs	Number of inform request responses received.

Field	Description
Trap PDUs	Number of SNMP traps received.
Response PDUs	Number of responses received.
Responses with errors	Number of responses containing errors.
SNMP informs	Indicates whether SNMP informs are enabled.
Informs in flight	Current and maximum possible number of informs waiting to be acknowledged.
Logging to	Destination of the following informs.
sent	Number of informs sent to this host.
in-flight	Number of informs currently waiting to be acknowledged.
retries	Number of inform retries sent.
failed	Number of informs that were never acknowledged.
dropped	Number of unacknowledged informs that were discarded to make room for new informs.

Related Commands

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

show snmp chassis

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

show snmp chassis

Syntax Description

This command has no arguments or keywords.

Command Default

The system serial number will be displayed.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

Command	Description
show snmp	Displays SNMP communication details.
snmp-server chassis-id	Configures a message line identifying the SNMP server serial number.

show snmp community

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

show snmp community

Syntax Description

This command has no arguments or keywords.

Command Default

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

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

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

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

Examples

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

```
Router# show snmp community
Community name: ILMI
Community Index: ILMI
Community SecurityName: ILMI
storage-type: read-only  active
Community name: private
Community Index: private
Community SecurityName: private
storage-type: nonvolatile        active
Community name: private@1
Community Index: private@1
Community SecurityName: private
storage-type: read-only  active
Community name: public
Community Index: public
Community SecurityName: public
storage-type: nonvolatile        active
```

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

Table 2: show snmp community Field Descriptions

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

Related Commands

Command	Description
snmp-server community	Sets up the community string to permit access to SNMP entities.

show snmp contact

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

show snmp contact

Syntax Description

This command has no arguments or keywords.

Command Default

The SNMP system contact information is displayed.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

Command	Description
snmp-server contact	Sets the system contact information.

show snmp engineID

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

show snmp engineID

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

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

Usage Guidelines

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

Examples

The following example specifies 00000090200000000C025808 as the local engineID and 123456789ABCDEF000000000 as the remote engine ID, 172.16.37.61 as the IP address of the remote engine (copy of SNMP) and 162 as the port from which the remote device is connected to the local device:

```
Router# show snmp engineID
Local SNMP engineID: 00000090200000000C025808
Remote Engine ID           IP-addr          Port
123456789ABCDEF000000000   172.16.37.61     162
```

The table below describes the fields shown in the display.

Table 3: show snmp engineID Field Descriptions

Field	Definition
Local SNMP engine ID	A string that identifies the copy of SNMP on the local device.
Remote Engine ID	A string that identifies the copy of SNMP on the remote device.
IP-addr	The IP address of the remote device.

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

Related Commands

Command	Description
snmp-server engineID local	Configures a name for either the local or remote SNMP engine on the router.

show snmp group

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

show snmp group

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

SNMP groups are configured using the snmp-server group command.

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

Examples

The following example specifies the group name as public, the security model as v1, the read view name as v1default, the notify view name as *tv.FFFFFFFF, and the storage type as volatile:

```
Router# show snmp group
groupname: V1                             security model:v1
readview : v1default                      writeview: <no writeview specified>
notifyview: <no notifyview specified>
row status: active
groupname: ILMI                           security model:v1
readview : *ilmi                          writeview: *ilmi
notifyview: <no notifyview specified>
row status: active
groupname: ILMI                           security model:v2c
readview : *ilmi                          writeview: *ilmi
notifyview: <no notifyview specified>
row status: active
groupname: group1                         security model:v1
readview : v1default                      writeview: <no writeview specified>
notifyview: <no notifyview specified>
row status: active
```

The table below describes the fields shown in the example.

Table 4: show snmp group Field Descriptions

Field	Definition
groupname	The name of the SNMP group, or collection of users that have a common access policy.
security model	The security model used by the group, either v1, v2c, or v3.
readview	A string identifying the read view of the group. • For further information on the SNMP views, use the **show snmp view** command.
writeview	A string identifying the write view of the group.
notifyview	A string identifying the notify view of the group. The notify view indicates the group for SNMP notifications, and corresponds to the setting of the **snmp-server group** *group-name version* **notify** *notify-view* command.

Related Commands

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

show snmp host

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

show snmp host

Syntax Description

This command has no arguments or keywords.

Command Default

The information configured for SNMP notification operation is displayed.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

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

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

Examples

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

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

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

Table 5: show snmp host Field Descriptions

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

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

Related Commands

Command	Description
snmp-server host	Configures the recipient details for SNMP notification operations.

show snmp location

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

show snmp location

Syntax Description

This command has no arguments or keywords.

Command Default

The SNMP system location information is displayed.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

Command	Description
snmp-server location	Configures SNMP system location details.

show snmp mib

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

show snmp mib

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

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

Usage Guidelines

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

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

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

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

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



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

Examples

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

```
Router# show snmp mib
system.1
system.2
sysUpTime
system.4
system.5
system.6
system.7
system.8
sysOREntry.2
sysOREntry.3
sysOREntry.4
interfaces.1
ifEntry.1
ifEntry.2
ifEntry.3
ifEntry.4
ifEntry.5
ifEntry.6
ifEntry.7
ifEntry.8
ifEntry.9
ifEntry.10
ifEntry.11
 --More--
 .
 .
 .
captureBufferEntry.2
captureBufferEntry.3
captureBufferEntry.4
captureBufferEntry.5
captureBufferEntry.6
captureBufferEntry.7
capture.3.1.1
eventEntry.1
eventEntry.2
eventEntry.3
eventEntry.4
eventEntry.5
eventEntry.6
eventEntry.7
logEntry.1
logEntry.2
logEntry.3
logEntry.4
rmon.10.1.1.2
rmon.10.1.1.3
rmon.10.1.1.4
rmon.10.1.1.5
rmon.10.1.1.6
rmon.10.1.1.7
rmon.10.2.1.2
rmon.10.2.1.3
rmon.10.3.1.2
--More--
 .
 .
 .
rmon.192.168.1.1
rmon.192.168.1.2
rmon.192.168.1.3
rmon.192.168.1.2
rmon.192.168.1.3
rmon.192.168.1.4
rmon.192.168.1.5
rmon.192.168.1.6
```

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

Related Commands

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

show snmp mib bulkstat transfer

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

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

Syntax Description

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

Command Default

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

Command Modes

Privileged EXEC (#)

Command History

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

Examples

In the following example, the initial transfer attempt and the first retry for the file IfMIB_objects_Router_030307_102519739 to the primary and secondary URL have failed, and four additional retry attempts will be made. The time stamp for this file indicates the file was created on March 7, 2003, at 10:25:19 a.m.

```
Router# show snmp mib bulkstat transfer
Transfer Name : IfMIB_objects
Primary URL ftp://user:XXXXXXXX@192.168.1.229/
Secondary ftp://user:XXXXXXXX@192.168.1.230/
   Retained files
```

```
File Name                          :Time Left (in seconds)     : STATE
-------------------------------------------------------------------------
IfMIB_objects_Router_030307_102519739 :  1196   :Retry(5 Retry attempt(s) Left)
IfMIB_objects_Router_030307_102219739 :  1016   :Retained
IfMIB_objects_Router_030307_101919739 :   836   :Retained
IfMIB_objects_Router_030307_101619739 :   656   :Retained
IfMIB_objects_Router_030307_101319739 :   475   :Retained
IfMIB_objects_Router_030307_101119739 :   295   :Retained
```

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

Table 6: show snmp mib bulkstat transfer Field Descriptions

Field	Description
Transfer Name	The name of the transfer configuration, specified in the **snmp mib bulkstat transfer** global configuration command.
Retained files	Indicates that the following output shows the status of files that are in system memory (retained), as opposed to files that have already been set.
File Name	The name of the bulk statistics file as it will appear after transfer. The filename of the file is generated using the following components: *transfer-name _device-name _date _time-stamp* The *transfer-name* is the name *s* pecified by the corresponding **snmp mib bulkstat transfer** command. The *device-name* is the name used in the command-line interface (CLI) router prompt. The format of the *date* and *time-stamp* depends on your system configuration, but is typically YYMMDD and HHMMSSmmm, where HH is hour, MM is minutes, SS is seconds and mmm is milliseconds.
Time Left (in seconds)	Indicates how much time is left before the specified file will be deleted (retention period), as specified with the **retain** Bulk Statistics Transfer configuration command. **Note** Regardless of the configured retention period, all retry attempts will be made before the file is deleted.

Field	Description
STATE	The state of the local bulk statistics file will be one of the following: • Queued--Collection time for this file is completed and the file is waiting for transfer to configured primary and secondary URL. • Retained--The file has been either successfully transferred to its destination or, if all transfer attempts have failed, all retry attempts have been completed. • Retry--The local bulk statistics file will be in this state if an attempt to transfer it to its configured destination fails and one or more retries are pending. The number of retries left will also be displayed in parenthesis.

Related Commands

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

show snmp mib context

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

show snmp mib context

Syntax Description

This command has no arguments or keywords.

Command Default

The list of VPN-aware MIBs is displayed.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

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

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

Examples

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

```
Router# show snmp mib context
dot1dBridge
ciscoPingMIB
ciscoStpExtensionsMIB
ciscoIpSecFlowMonitorMIB
ciscoCat6kCrossbarMIB
ciscoIPsecMIB
mplsLdpMIB
```

Related Commands

Command	Description
context	Associates an SNMP context with a particular VRF.
snmp-server context	Configures SNMP context.

show snmp mib ifmib traps

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

show snmp mib ifmib traps

Syntax Description

This command has no arguments or keywords.

Command Default

By default, trap status for all interfaces is displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SXI	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

The **show snmp mib ifmib traps**command displays information about the status of linkUp and linkDown traps for a particular interface.

Examples

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

```
Router# show snmp mib ifmib traps
ifDescr                  ifindex    TrapStatus
-----------------------------------------------------
FastEthernet3/6                14     enabled
FastEthernet3/19               27     enabled
GigabitEthernet5/1             57     enabled
unrouted VLAN 1005             73     disabled
FastEthernet3/4                12     enabled
FastEthernet3/39               47     enabled
FastEthernet3/28               36     enabled
FastEthernet3/48               56     enabled
unrouted VLAN 1003             74     disabled
FastEthernet3/2                10     enabled
Tunnel0                        66     enabled
SPAN RP Interface              64     disabled
Tunnel10                       67     enabled
FastEthernet3/44               52     enabled
GigabitEthernet1/3             3      enabled
FastEthernet3/11               19     enabled
FastEthernet3/46               54     enabled
GigabitEthernet1/1             1      enabled
FastEthernet3/13               21     enabled
```

The table below describes the fields shown in the display.

Table 7: show snmp mib ifmib traps Field Descriptions

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

Related Commands

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

show snmp mib ifmib ifindex

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

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

Syntax Description

type number	(Optional) Interface type and number. The table below lists the valid values for interface type and number.
detail	(Optional) Displays the trap status for all SNMP ifIndex identification numbers for the specified system interfaces.
free-list	(Optional) Displays information about the ifIndex values that are not yet assigned.

Command Default

The ifIndex values for all interfaces are displayed.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

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

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

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

Table 8: show snmp mib ifmib ifindex type and number

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

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

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

Examples

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

```
Router# show snmp mib ifmib ifindex Ethernet2/0
Ethernet2/0: Ifindex = 2
```

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

```
Router# show snmp mib ifmib ifindex

ATM1/0: Ifindex = 1
ATM1/0-aal5 layer: Ifindex = 12
ATM1/0-atm layer: Ifindex = 10
ATM1/0.0-aal5 layer: Ifindex = 13
ATM1/0.0-atm subif: Ifindex = 11
```

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

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

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

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

The table below describes the fields shown in the display.

Table 9: show snmp mib ifmib ifindex Field Descriptions

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

The following example shows sample output for unassigned ifIndexes:

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

```
ifIndex range
-----------------------------------
 75 - 2147483647
```

```
-----------------------------------
Total free ifIndex : 2147483573
```

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

Related Commands

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

show snmp mib notification-log

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

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

Syntax Description

all	(Optional) Displays all notification log entries stored in the local Notification Log MIB database.
default	(Optional) Displays summary information for the default (unnamed) SNMP Notification Log.

Command Modes

EXEC

Command History

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

Usage Guidelines

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

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

Examples

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

```
Router# show snmp mib notification-log

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

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

Related Commands

Command	Description
snmp mib notification-log default	Creates and activates an SNMP Notification Log.
snmp mib notification-log globalageout	Sets the maximum age for a notification.
snmp mib notification-log globalsize	Sets the maximum number of notifications allowed in all logs.

show snmp pending

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

show snmp pending

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

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

Usage Guidelines

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

Examples

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

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

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

Table 10: show snmp pending Field Descriptions

Field	Description
req id	ID number of the pending request.
dest	IP address of the intended receiver of the request.
V2C community	SNMP version 2C community string sent with the request.

Field	Description
Expires in	Remaining time before request timeout expires.

Related Commands

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

show snmp sessions

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

show snmp sessions [brief]

Syntax Description

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

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

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

Usage Guidelines

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

Examples

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

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

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

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

```
Router# show snmp sessions brief
Destination: 171.69.58.33.161, V2C community: public, Expires in 55 secs
```

Table 11: show snmp sessions Field Descriptions

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

Related Commands

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

show snmp stats oid

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

show snmp stats oid

Syntax Description

This command has no arguments or keywords.

Command Default

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

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.

Usage Guidelines

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

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

Examples

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

```
Router# show snmp stats oid

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

```
02:57:57 UTC Jul 7 2008         1                   cpmCPUTotalTable.1.9
02:57:57 UTC Jul 7 2008         1                   cpmCPUTotalTable.1.8
```

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

Table 12: show snmp stats oid Field Descriptions

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

show snmp sysobjectid

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

Cisco IOS Release 12.4(10) and Later Releases

show snmp sysobjectid

Cisco IOS Release 12.2(44)SE and Later Releases

show snmp sysobjectid type

Syntax Description

type	Displays the system object ID type.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

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

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

Examples

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

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

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

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

Related Commands

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

show snmp user

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

show snmp user [*username*]

Syntax Description

username	(Optional) Name of a specific user or users about which to display SNMP information.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

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

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

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

Examples

The following is sample output from the **show snmp user** command. The output indicates the username as authuser, the engine ID string as 00000090200000000C025808, and the storage type as nonvolatile:

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

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

Table 13: show snmp user Field Descriptions

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

show snmp view

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

show snmp view

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

Use this command to display the SNMP view configuration.

Examples

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

```
Router# show snmp view
View Family Name/View Family Subtree/View Family Mask/View Family Type/storage/status
myview              mib-2                -          included         nonvolatile active
myview              cisco                -          included         nonvolatile active
myview              atEntry              -          excluded         nonvolatile active
v1default           iso                  -          included         permanent   active
v1default           internet             -          included         volatile    active
v1default           internet.6.3.15      -          excluded         volatile    active
v1default           internet.6.3.16      -          excluded         volatile    active
v1default           internet.6.3.18      -          excluded         volatile    active
```

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

Table 14: show snmp view Field Descriptions

Field	Description
View Family Name	Family name.
View Family Subtree	MIB name.
View Family Mask	Family mask. A hyphen (-) appears in this column when no mask is associated.
View Family Type	Type of family, either included or excluded.

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

snmp context (VRF)

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

snmp context *context-name*

no snmp context

Syntax Description

context-name	Name of the SNMP VPN context. The name can be up to 32 alphanumeric characters.

Command Default

No SNMP contexts are associated with VPNs.

Command Modes

VRF configuration (config-vrf)

Command History

Release	Modification
15.0(1)M	This command was introduced. This command replaces the **context** command.

Usage Guidelines

Before you use the **snmp context**command to associate an SNMP context with a VPN, you must do the following:

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

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

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

Examples

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

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

Related Commands

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

snmp get

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

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

Syntax Description

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

Command Default

No variables are retrieved by default.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

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

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

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

Examples

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

```
Router# snmp get v1 10.16.2.8 public retry 2 timeout 60 oid sysName.0
SNMP Response: reqid 3, errstat 0, erridx 0
 system.1.0
```

Related Commands

Command	Description
snmp get-bulk	Retrieves variables in bulk.
snmp get-next	Retrieves data about the lexicographical successor to the specified variable.

snmp get-bulk

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

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

Syntax Description

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

oid-value	The object identifier value. For example, sysName.0 or 1.3.6.1.4.1.9.9.10.1.3.0.5.
oid-1 oid-n	(Optional) The object identifier values for which the getNext attempts can be repeated.

Command Default

Variables are not retrieved in bulk by default.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

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

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

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

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

Examples

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

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

Related Commands

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

snmp get-next

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

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

Syntax Description

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

Command Default

No variables are retrieved by default.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

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

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

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

Examples

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

```
Router# snmp get-next v2c 10.16.2.8 public retry 2 timeout 60 oid ifStackStatus.0
SNMP Response: reqid 11, errstat 0, erridx 0
 ifStackStatus.0.1 = 1
```

Related Commands

Command	Description
snmp get	Retrieves SNMP object variables.
snmp get-bulk	Retrieves SNMP object variables in bulk.

snmp ifmib ifalias long

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

snmp ifmib ifalias long

no snmp ifmib ifalias long

Syntax Description

This command has no arguments or keywords.

Command Default

The ifAlias description is limited to 64 characters.

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

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

Examples

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

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

Related Commands

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

snmp inform

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

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

Syntax Description

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

oid-value	The object identifier value. For example, sysName.0 or 1.3.6.1.4.1.9.9.10.1.3.0.5.
oid-type	The type of OID. The following values are valid: • **counter** --A 32-bit number with a minimum value of 0. When the maximum value is reached, the counter resets to 0. • **gauge** --A 32-bit number with a minimum value of 0. For example, the interface speed on a router is measured using a gauge object type. • **integer** --A 32-bit number used to specify a numbered type within the context of a managed object. For example, to set the operational status of a router interface, 1 represents up and 2 represents down. • **ip-address** --IP address. • **string** --An octet string in text notation used to represent text strings. • **timeticks** --Specifies a value based on time ticks. Time ticks represents an integer value that specifies the elapsed time between two events, in units of hundredth of a second.
oid-type-value	Integer or text string value of the OID type specified for the SNMP set operation. The following list describes the integer or text string values that are valid with each *oid-type* argument value: • **counter** --Integer value in the range from 0 to 4294967295. • **gauge** --Integer value in the range from 0 to 4294967295. • **integer** --Integer value in the range from 0 to 4294967295. • **ip-address** --IP address in dotted decimal notation. • **string** --Text string. • **timeticks** --Integer value in the range from 0 to 4294967295.

Command Default No SNMP inform requests are sent by default.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

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

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

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

Examples

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

```
Router# snmp inform v2c 10.16.2.8 public retry 2 timeout 60 trap-oid system.2.0 oid
sysUpTime.0 counter 20
SNMP: Inform request, reqid 24, errstat 0, erridx 0
sysUpTime.0 = 10244391
snmpTrapOID.0 = ciscoConfigManMIB.2.0.1
ccmHistoryEventEntry.3.40 = 1
```

Related Commands

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

snmp mib bulkstat object-list

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

snmp mib bulkstat object-list *name*

no snmp mib bulkstat object-list *name*

Syntax Description

name	Name of the object list to be configured.

Command Default

No SNMP bulk statistics object list is configured.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

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

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

Bulk statistics object lists can be reused in multiple schemas.

Examples

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

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

Related Commands

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

snmp mib bulkstat schema

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

snmp mib bulkstat schema *schema-name*

no snmp mib bulkstat schema *schema-name*

Syntax Description

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

Command Default

No schemas are defined.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

The **snmp mib bulkstat schema** command names the schema and enters Bulk Statistics Schema configuration mode. Bulk Statistics Schema configuration mode is used to configure the object list, instance, and polling interval to be used in the schema.

The specific instances of MIB objects for which data should be collected are determined by appending the value of the **instance** command to the objects specified in the object list.

Multiple schemas can be associated with a single bulk statistics file when configuring the bulk statistics transfer options.

Examples

The following example shows the configuration of a bulk statistics schema called ATM2/0-IFMIB:

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

Related Commands

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

snmp mib bulkstat transfer

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

snmp mib bulkstat transfer *transfer-id*

no snmp mib bulkstat transfer *transfer-id*

Syntax Description

transfer-id	Name of the transfer configuration.

Command Default

No bulk statistics transfer configuration exists.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

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

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

Examples

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

```
Router(config)# snmp mib bulkstat transfer bulkstat1
```

```
Router(config-bulk-tr)# schema ATM2/0-IFMIB
Router(config-bulk-tr)# schema ATM2/0-CAR
Router(config-bulk-tr)# url primary ftp://user1:pswrd@cbin2-host/users/user1/bulkstat1
Router(config-bulk-tr)# url secondary tftp://user1@10.1.0.1/tftpboot/user1/bulkstat1
Router(config-bulk-tr)# format schemaASCII
Router(config-bulk-tr)# transfer-interval 30
Router(config-bulk-tr)# retry 5
Router(config-bulk-tr)# buffer-size 1024
Router(config-bulk-tr)# retain 30
Router(config-bulk-tr)# end
Router# copy running-config startup-config
```

Related Commands

Command	Description
show snmp mib bulkstat transfer	Displays the transfer status of files generated by the Periodic MIB Data Collection and Transfer Mechanism.

snmp mib community-map

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

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

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

Syntax Description

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

Command Default

No SNMP communities and contexts are associated.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

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

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

Examples

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

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

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

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

Related Commands

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

Command	Description
snmp-server community	Sets up the community access string to permit access to the SNMP.

snmp mib event object list

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

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

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

Syntax Description

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

Command Default

No object list is configured for an event.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.

Examples

The following example shows how to configure an object list:

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

Related Commands

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

Command	Description
test	Enables a trigger test.

snmp mib event owner

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

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

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

Syntax Description

event-owner	Name of the event owner.
name	Indicates the name of an event.
event-name	Name of an event.

Command Default

By default, no event is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.

Usage Guidelines

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

Examples

The following example shows how to specify an event owner:

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

snmp mib event sample

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

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

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

Syntax Description

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

Command Default

No value is set for scalar object sampling.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.

Examples

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

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



snmp mib event trigger owner through snmp-server enable informs

- snmp mib event trigger owner, page 158
- snmp mib expression delta, page 160
- snmp mib expression owner, page 162
- snmp mib flash cache, page 164
- snmp mib flowmon alarmhistorysize, page 165
- snmp mib notification-log default, page 166
- snmp mib notification-log default disable, page 168
- snmp mib notification-log globalageout, page 170
- snmp mib notification-log globalsize, page 172
- snmp mib persist, page 174
- snmp mib target list, page 176
- snmp trap link-status, page 178
- snmp set, page 181
- snmp-server cache, page 184
- snmp-server chassis-id, page 186
- snmp-server community, page 188
- snmp-server contact, page 192
- snmp-server context, page 193
- snmp-server drop vrf-traffic, page 195
- snmp-server enable informs, page 196

snmp mib event trigger owner

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

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

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

Syntax Description

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

Command Default

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

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

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

Examples

The following example shows how to specify a trigger owner:

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

Related Commands

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

snmp mib expression delta

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

snmp mib expression delta {**minimum** {*delta-value*| *seconds*}| **wildcard maximum** *wildcard-instance*}

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

Syntax Description

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

Command Default

The default value for minimum delta interval is 1 second.

The default wildcard maximum value is 0.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.

Usage Guidelines

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

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

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

Examples

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

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

Related Commands

Command	Description
sample	Specifies the method of sampling an object.

snmp mib expression owner

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

snmp mib expression owner *expr-owner* **name** *expr-name*

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

Syntax Description

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

Command Default

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

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.

Usage Guidelines

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

Examples

The following example shows how to specify an expression owner:

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

Related Commands

Command	Description
delta interval	Specifies an interval for the delta sampling of objects used while evaluating an expression.

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

snmp mib flash cache

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

snmp mib flash cache [**interval** *minutes*]

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

Syntax Description

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

Command Default

The Flash MIB data collection process is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SXI	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.

Usage Guidelines

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

Examples

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

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

snmp mib flowmon alarmhistorysize

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

snmp mib flowmon alarmhistorysize *num*

no snmp mib flowmon alarmhistorysize *num*

Syntax Description

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

Command Default

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

Command Modes

Global configuration (config)

Command History

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

Examples

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

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

Related Commands

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

snmp mib notification-log default

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

snmp mib notification-log default [**size** *number*]

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

Syntax Description

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

Command Default

500 entries

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

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

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

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

Examples

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

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

Related Commands

Command	Description
show snmp mib notification-log	Displays information about the state of local SNMP notification logging.
snmp mib notification-log globalageout	Sets the maximum age for a notification.
snmp mib notification-log globalsize	Sets the maximum number of notifications allowed in all logs.

snmp mib notification-log default disable

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

snmp mib notification-log default disable

no snmp mib notification-log default disable

Syntax Description

This command has no arguments or keywords

Command Default

Logging is enabled.

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

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

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

Examples

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

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

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

Router(config)#
```

Related Commands

Command	Description
show snmp mib notification-log	Displays information about the state of local SNMP notification logging.
snmp mib notification-log default	Creates an SNMP notification log.
snmp mib notification-log globalageout	Sets the maximum age for a notification.
snmp mib notification-log globalsize	Sets the maximum number of notifications allowed in all logs.

snmp mib notification-log globalageout

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

snmp mib notification-log globalageout minutes

no snmp mib notification-log globalageout minutes

Syntax Description

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

Command Default

The default global ageout value is 15 minutes.

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

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

Examples

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

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

Related Commands

Command	Description
show snmp mib notification-log	Provides a summary of logs.
snmp mib notification-log default	Creates the default log in the MIB.

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

snmp mib notification-log globalsize

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

snmp mib notification-log globalsize *number*

no snmp mib notification-log globalsize *number*

Syntax Description

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

Command Default

The default global log size is 500 entries.

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

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

Examples

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

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

Related Commands

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

snmp mib persist

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

snmp mib persist [**event**| **expression**| **circuit**| **cbqos**| **v3mibs**]

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

Syntax Description

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

Command Default

MIB persistence is disabled.

Command Modes

Global configuration (config)

Command History

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

T Release	Modification
SX Release	Modification
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI. The **cbqos** keyword was added.
SR Release	Modification
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB. The **cbqos** keyword was added.
12.2(33)SRC	The **v3mibs** keyword was added.

Usage Guidelines

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

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

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

Examples

The following example shows how to enable Event MIB persistence:

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

Router# write mib-data
```

Related Commands

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

snmp mib target list

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

snmp mib target list *vpn-list-name* {**vrf** *vrf-name*| **host** *ip-address*}

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

Syntax Description

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

Command Default

No target list is created.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31) SB2.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

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

- Only the following MIBs are context aware and all the tables in these MIBs can be polled:
  - CISCO-IPSEC-FLOW-MONITOR-MIB (Cisco IOS Release 12.4T and later)
  - CISCO-IPSEC-MIB (Cisco IOS Release 12.4T and later)
  - CISCO-PING-MIB
  - IP-FORWARD-MIB
  - MPLS-LDP-MIB
- Currently, two SNMP variables in the IP-FORWARD-MIB can be polled: 1.3.6.1.2.1.4.24.3 (ipCidrRouteNumber - Scalar) and 1.3.6.1.2.1.4.24.4.1 (ipCidrRouteEntry - Table).



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

Examples

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

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

Related Commands

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

snmp trap link-status

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

snmp trap link-status [**permit duplicates**]

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

Syntax Description

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

Command Default

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

Command Modes

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

Command History

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

Usage Guidelines

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

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

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

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

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

Cisco 10000 Series Router

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

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

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

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

Examples

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

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

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

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

Related Commands

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

snmp set

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

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

Syntax Description

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

oid-type	The type of OID. The following values are valid: • **counter** --A 32-bit number with a minimum value of 0. When the maximum value is reached, the counter resets to 0. • **gauge** --A 32-bit number with a minimum value of 0. For example, the interface speed on a router is measured using a gauge object type. • **integer** --A 32-bit number used to specify a numbered type within the context of a managed object. For example, to set the operational status of a router interface, 1 represents up and 2 represents down. • **ip-address** --IP address. • **string** --An octet string in text notation used to represent text strings. • **timeticks** --Specifies a value based on time ticks. Time ticks represents an integer value that specifies the elapsed time between two events, in units of hundredth of a second.
oid-type-value	Integer or text string value of the OID type specified for the SNMP set operation. The following list describes the integer or text string values that are valid with each *oid-type* argument value: • **counter** --Integer value in the range from 0 to 4294967295. • **gauge** --Integer value in the range from 0 to 4294967295. • **integer** --Integer value in the range from 0 to 4294967295. • **ip-address** --IP address in dotted decimal notation. • **string** --Text string. • **timeticks** --Integer value in the range from 0 to 4294967295.

Command Default No variable is set by default.

Command Modes Privileged EXEC (#)

Command History

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

Usage Guidelines

The SNMP set operation modifies the individual variables in the SNMP entity.

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

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

Examples

The following example shows how to set the variable using SNMPv2c:

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

Related Commands

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

snmp-server cache

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

snmp-server cache [**interval** *seconds*]

no snmp-server cache

Syntax Description

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

Command Default

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

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

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

Examples

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

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

This example shows how to disable the SNMP cache:

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

Related Commands

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

snmp-server chassis-id

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

snmp-server chassis-id *text*

no snmp-server chassis-id

Syntax Description

text	Message that identifies the chassis serial number.

Command Default

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

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

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

Examples

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

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

Related Commands

Command	Description
show snmp	Checks the status of SNMP communications.
show snmp chassis	Displays the SNMP server serial number.

snmp-server community

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

snmp-server community *string* [**view** *view-name*] [**ro**| **rw**] [**ipv6** *nacl*] [*access-list-number*| *extended-access-list-number*| *access-list-name*]

no snmp-server community *string*

Syntax Description

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

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

Command Modes Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.
12.0(14)ST	This command was integrated into Cisco IOS Release 12.0(14)ST.
12.0(17)S	This command was integrated into Cisco IOS Release 12.0(17)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.3(2)T	The access list values were enhanced to support the expanded range of standard access list values and to support named standard access lists.
12.0(27)S	The **ipv6** *nacl* keyword and argument pair was added to support assignment of IPv6 named access lists. This keyword and argument pair is not supported in Cisco IOS 12.2S releases.
12.3(14)T	The **ipv6** *nacl* keyword and argument pair was integrated into Cisco IOS Release 12.3(14)T to support assignment of IPv6 named access lists. This keyword and argument pair is not supported in Cisco IOS 12.2S releases.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Aggregation Series Routers.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SRE	This command was modified. The automatic insertion of the **snmp-server community** command into the configuration, along with the community string specified in the **snmp-server host** command, is changed. The **snmp-server community** command has to be manually configured.

Release	Modification
15.1(0)M	This command was modified. The automatic insertion of the **snmp-server community** command into the configuration, along with the community string specified in the **snmp-server host** command, is changed. The **snmp-server community** command has to be manually configured.

Usage Guidelines

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

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

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



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

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



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

Examples

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

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

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

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

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

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

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

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

The following example shows how to remove the community comaccess:

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

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

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

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

```
Router(config)# ipv6 access-list list1
Router(config-ipv6-acl)# permit ipv6 any any
Router(config-ipv6-acl)# exit
Router(config)# snmp-server community comaccess rw ipv6 list1
```

Related Commands

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

snmp-server contact

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

snmp-server contact *text*

no snmp-server contact

Syntax Description

text	String that describes the system contact information.

Command Default

No system contact string is set.

Command Modes

Global configuration

Command History

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

Examples

The following is an example of a system contact string:

```
Router(config)# snmp-server contact Dial System Operator at beeper # 27345
```

Related Commands

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

snmp-server context

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

snmp-server context *context-name*

no snmp-server context *context-name*

Syntax Description

context-name	Name of the SNMP context being created.

Command Default

No SNMP contexts are configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

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

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

autonomous system number and an arbitrary number, or it is IP address relative and composed of an IP address and an arbitrary number.

Examples

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

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

Related Commands

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

snmp-server drop vrf-traffic

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

snmp-server drop vrf-traffic

no snmp-server drop vrf-traffic

Syntax Description

This command has no arguments or keywords.

Command Default

SNMP packets are not dropped from VRF interfaces.

Command Modes

Global configuration (config)

Command History

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

Examples

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

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

Related Commands

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

snmp-server enable informs

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

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

Command History

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



snmp-server enable traps through snmp-server enable traps ospf cisco-specific retransmit

- snmp-server enable traps, page 199
- snmp-server enable traps (MPLS), page 208
- snmp-server enable traps aaa_server, page 216
- snmp-server enable traps atm pvc, page 218
- snmp-server enable traps atm pvc extension, page 221
- snmp-server enable traps atm pvc extension mibversion, page 226
- snmp-server enable traps atm subif, page 228
- snmp-server enable traps bfd, page 231
- snmp-server enable traps bgp, page 233
- snmp-server enable traps bulkstat, page 236
- snmp-server enable traps c6kxbar, page 238
- snmp-server enable traps calltracker, page 240
- snmp-server enable traps cnpd, page 242
- snmp-server enable traps cpu, page 243
- snmp-server enable traps dhcp, page 245
- snmp-server enable traps dhcp-snooping bindings, page 247
- snmp-server enable traps director, page 248
- snmp-server enable traps dlsw, page 250
- snmp-server enable traps eigrp, page 252
- snmp-server enable traps envmon, page 254
- snmp-server enable traps errdisable, page 257
- snmp-server enable traps firewall, page 258
- snmp-server enable traps flash, page 260

- snmp-server enable traps flowmon, page 262
- snmp-server enable traps frame-relay, page 264
- snmp-server enable traps frame-relay multilink bundle-mismatch, page 266
- snmp-server enable traps frame-relay subif, page 268
- snmp-server enable traps if-monitor, page 270
- snmp-server enable traps ip local pool, page 271
- snmp-server enable traps isdn, page 272
- snmp-server enable traps l2tun pseudowire status, page 275
- snmp-server enable traps l2tun session, page 277
- snmp-server enable traps memory, page 279
- snmp-server enable traps ospf cisco-specific errors config-error, page 281
- snmp-server enable traps ospf cisco-specific errors shamlink, page 283
- snmp-server enable traps ospf cisco-specific retransmit, page 285

snmp-server enable traps

To enable all Simple Network Management Protocol (SNMP) notification types that are available on your system, use the **snmp-server enable traps**command in global configuration mode. To disable all available SNMP notifications, use the **no**form of this command.

snmp-server enable traps [*notification-type*] **[vrrp]**

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

Syntax Description

notification-type	(Optional) Type of notification (trap or inform) to enable or disable. If no type is specified, all notifications available on your device are enabled or disabled (if the **no** form is used). The notification type can be one of the following keywords: **alarms** --Enables alarm filtering to limit the number of syslog messages generated. Alarms are generated for the severity configured as well as for the higher severity values. • The *severity*argument is an integer or string value that identifies the severity of an alarm. Integer values are from 1 to 4. String values are critical, major, minor, and informational. The default is 4 (informational). Severity levels are defined as follows: • 1--Critical. The condition affects service. • 2--Major. Immediate action is needed. • 3--Minor. Minor warning conditions. • 4--Informational. No action is required. This is the default.
	• **auth-framework** [**sec-violation**]--Enables the SNMP CISCO-AUTH-FRAMEWORK-MIB traps. The optional **sec-violation** keyword enables the SNMP camSecurityViolationNotif notification. 1
	• **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.

	• **dot1x** --Enables IEEE 802.1X traps. This notification type is defined in the CISCO PAE MIB. **Catalyst 6500 Series Switches** The following keywords are available under the **dot1x** keyword: • • **auth-fail-vlan** --Enables the SNMP cpaeAuthFailVlanNotif notification. • **no-auth-fail-vlan** --Enables the SNMP cpaeNoAuthFailVlanNotif notification. • **guest-vlan** --Enables the SNMP cpaeGuestVlanNotif notification. • **no-guest-vlan** --Enables the SNMP cpaeNoGuestVlanNotif notification.
	• **ds0-busyout** --Sends notification when the busyout of a DS0 interface changes state (Cisco AS5300 platform only). This notification is defined in the CISCO-POP-MGMT-MIB (enterprise 1.3.6.1.4.1.9.10.19.2), and the notification type is (1) cpmDS0BusyoutNotification. • **ds1-loopback** --Sends notification when the DS1 interface goes into loopback mode (Cisco AS5300 platform only). This notification type is defined in the CISCO-POP-MGMT-MIB (enterprise 1.3.6.1.4.1.9.10.19.2) as (2) cpmDS1LoopbackNotification. • **dsp** --Enables SNMP digital signal processing (DSP) traps. This notification type is defined in the CISCO-DSP-MGMT-MIB. • **dsp oper-state** --Sends a DSP notification made up of both a DSP ID that indicates which DSP is affected and an operational state that indicates whether the DSP has failed or recovered.
	• **l2tc** --Enable the SNMP Layer 2 tunnel configuration traps. This notification type is defined in CISCO-L2-TUNNEL-CONFIG-MIB.[1]

	• **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.
	• **entity-diag** *type* -- Enables the SNMP CISCO-ENTITY-DIAG-MIB traps. The valid *type*values are as follows: 1 • **boot-up-fail**--(Optional) Enables the SNMP ceDiagBootUpFailedNotif traps. 1 • **hm-test-recover**--(Optional) Enables the SNMP ceDiagHMTestRecoverNotif traps. 1 • **hm-thresh-reached**--(Optional) Enables the SNMP ceDiagHMThresholdReachedNotif traps. 1 • **scheduled-fail**--(Optional) Enables the SNMP ceDiagScheduledJobFailedNotif traps. 1
	• **flowmon** --Controls flow monitoring notifications.
	• **hsrp** --Controls Hot Standby Routing Protocol (HSRP) notifications, as defined in the CISCO-HSRP-MIB (enterprise 1.3.6.1.4.1.9.9.106.2). The notification type is (1) cHsrpStateChange.
	• **ipmulticast** --Controls IP multicast notifications.

	• **license** --Enables licensing notifications as traps or informs. The notifications are grouped into categories that can be individually controlled by combining the keywords with the **license** keyword, or as a group by using the **license** keyword by itself. • **deploy**--Controls notifications generated as a result of install, clear, or revoke license events. • **error**--Controls notifications generated as a result of a problem with the license or with the usage of the license. • **imagelevel**--Controls notifications related to the image level of the license. • **usage**--Controls usage notifications related to the license.
	• **modem-health** --Controls modem-health notifications.
	• **module-auto-shutdown** [**status**]--Enables the SNMP CISCO-MODULE-AUTO-SHUTDOWN-MIB traps. The optional **status** keyword enables the SNMP Module Auto Shutdown status change traps. 1
	• **rsvp** --Controls Resource Reservation Protocol (RSVP) flow change notifications.
	• **sys-threshold** --(Optional) Enables the SNMP cltcTunnelSysDropThresholdExceeded notification. This notification type is an enhancement to the CISCO-L2-TUNNEL-CONFIG-MIB. 1
	• **tty** --Controls TCP connection notifications.

	• **xgcp** --Sends External Media Gateway Control Protocol (XGCP) notifications. This notification is from the XGCP-MIB-V1SMI.my, and the notification is enterprise 1.3.6.1.3.90.2 (1) xgcpUpDownNotification. **Note** For additional notification types, see the Related Commands table.
vrrp	(Optional) Specifies the Virtual Router Redundancy Protocol (VRRP).

[1] Supported on the Catalyst 6500 series switches.

Command Default No notifications controlled by this command are sent.

Command Modes Global configuration (config)

Command History

Release	Modification
10.3	This command was introduced.
12.0(2)T	The **rsvp** notification type was added in Cisco IOS Release 12.0(2)T.
12.0(3)T	The **hsrp** notification type was added in Cisco IOS Release 12.0(3)T.
12.0(24)S	This command was integrated into Cisco IOS Release 12.0(24)S.
12.2(14)SX	Support for this command was implemented on the Supervisor Engine 720.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was integrated into Cisco IOS Release 12.2(17d)SXB.
12.3(11)T	The **vrrp**notification type was added in Cisco IOS Release 12.3(11)T.
12.4(4)T	Support for the **alarms**notification type and *severity* argument was added in Cisco IOS Release 12.4(4)T. Support for the **dsp** and **dsp oper-state**notification types was added in Cisco IOS Release 12.4(4)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
12.4(11)T	The **dot1x** notification type was added in Cisco IOS Release 12.4(11)T.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(20)T	The **license**notification type keyword was added.
12.2(33)SXH	The **l2tc** keyword was added and supported on the Catalyst 6500 series switch.
12.2(33)SXI	The following keywords were added and supported on the Catalyst 6500 series switch: • **auth-fail-vlan** • **entity-diag** • **guest-vlan** • **module-auto-shutdown** • **no-auth-fail-vlan** • **no-guest-vlan** • **sys-threshold**
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.
15.0(1)S	This command was modified. The **flowmon** notification type was added in Cisco IOS Release 15.0(1)S.
Cisco IOS XE 3.1.0SG	This command was modified. Licensing SNMP traps are enabled by default on Catalyst 4500 series switches.

Usage Guidelines

For additional notification types, see the Related Commands table for this command.

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests for the specified notification types. To specify whether the notifications should be sent as traps or informs, use the **snmp-server host** [**traps** | **informs**] command.

To configure the router to send these SNMP notifications, you must enter at least one **snmp-server enable traps**command. If you enter the command with no keywords, all notification types are enabled. If you enter the command with a keyword, only the notification type related to that keyword is enabled. To enable multiple types of notifications, you must issue a separate **snmp-server enable traps** command for each notification type and notification option.

Most notification types are disabled by default but some cannot be controlled with the **snmp-server enable traps** command.

The **snmp-server enable traps**command is used in conjunction with the **snmp-server host**command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send notifications, you must configure at least one **snmp-server host** command.

Catalyst 6500 Series Switches

The following MIBs were enhanced or supported in Cisco IOS Release 12.2(33)SXI and later releases on the Catalyst 6500 series switch:

- CISCO-L2-TUNNEL-CONFIG-MIB-LLDP--Enhancement. The CISCO-L2-TUNNEL-CONFIG-MIB provides SNMP access to the Layer 2 tunneling-related configurations.
- CISCO-PAE-MIB--Enhancement for critical condition and includes traps when the port goes into the Guest Vlan or AuthFail VLAN.
- CISCO-MODULE-AUTO-SHUTDOWN-MIB--Supported. The CISCO-MODULE-AUTO-SHUTDOWN-MIB provides SNMP access to the Catalyst 6500 series switch Module Automatic Shutdown component.
- CISCO-AUTH-FRAMEWORK-MIB--Supported. The CISCO-AUTH-FRAMEWORK-MIB provides SNMP access to the Authentication Manager component.
- CISCO-ENTITY-DIAG-MIB--The CISCO-ENTITY-DIAG-MIB provides SNMP traps for generic online diagnostics (GOLD) notification enhancements.

Examples

The following 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:

```
Router(config)# snmp-server enable traps

Router(config)# snmp-server host myhost.cisco.com public
```

The following example shows how to configure an alarm severity threshold of 3:

```
Router# snmp-server enable traps alarms 3
```

The following example shows how to enable the generation of a DSP operational state notification from from the command-line interface (CLI):

```
Router(config)# snmp-server enable traps dsp oper-state
```

The following example shows how to enable the generation of a DSP operational state notification from a network management device:

```
setany -v2c 1.4.198.75 test cdspEnableOperStateNotification.0 -i 1
cdspEnableOperStateNotification.0=true(1)
```

The following example shows how to send no traps to any host. The Border Gateway Protocol (BGP) traps are enabled for all hosts, but the only traps enabled to be sent to a host are ISDN traps (which are not enabled in this example).

```
Router(config)# snmp-server enable traps bgp

Router(config)# snmp-server host user1 public isdn
```

The following example shows how to enable the router to send all inform requests to the host at the address myhost.cisco.com, using the community string defined as public:

```
Router(config)# snmp-server enable traps

Router(config)# snmp-server host myhost.cisco.com informs version 2c public
```

The following example shows how to send HSRP MIB traps to the host myhost.cisco.com using the community string public:

```
Router(config)# snmp-server enable traps hsrp

Router(config)# snmp-server host myhost.cisco.com traps version 2c public hsrp
```

The following example shows that VRRP will be used as the protocol to enable the traps:

```
Router(config)# snmp-server enable traps vrrp
Router(config)# snmp-server host myhost.cisco.com traps version 2c vrrp
```

The following example shows how to send IEEE 802.1X MIB traps to the host “myhost.example.com” using the community string defined as public:

```
Router(config)# snmp-server enable traps dot1x
Router(config)# snmp-server host myhost.example.com traps public
```

Related Commands

Command	Description
snmp-server enable traps atm pvc	Enables ATM PVC SNMP notifications.
snmp-server enable traps atm pvc extension	Enables extended ATM PVC SNMP notifications.
snmp-server enable traps bgp	Enables BGP server state change SNMP notifications.
snmp-server enable traps calltracker	Enables Call Tracker callSetup and callTerminate SNMP notifications.
snmp-server enable traps envmon	Enables environmental monitor SNMP notifications.
snmp-server enable traps frame-relay	Enables Frame Relay DLCI link status change SNMP notifications.
snmp-server enable traps ipsec	Enables IPsec SNMP notifications.
snmp-server enable traps isakmp	Enables IPsec ISAKMP SNMP notifications.
snmp-server enable traps isdn	Enables ISDN SNMP notifications.
snmp-server enable traps memory	Enables memory pool and buffer pool SNMP notifications.
snmp-server enable traps mpls ldp	Enables MPLS LDP SNMP notifications.
snmp-server enable traps mpls traffic-eng	Enables MPLS TE tunnel state-change SNMP notifications.
snmp-server enable traps mpls vpn	Enables MPLS VPN specific SNMP notifications.
snmp-server enable traps repeater	Enables RFC 1516 hub notifications.
snmp-server enable traps snmp	Enables RFC 1157 SNMP notifications.

Command	Description
snmp-server enable traps syslog	Enables the sending of system logging messages via SNMP.
snmp-server host	Specifies whether you want the SNMP notifications sent as traps or informs, the version of SNMP to use, the security level of the notifications (for SNMPv3), and the destination host (recipient) for the notifications.
snmp-server informs	Specifies inform request options.
snmp-server trap-source	Specifies the interface (and the corresponding IP address) from which an SNMP trap should originate.
snmp trap illegal-address	Issues an SNMP trap when a MAC address violation is detected on an Ethernet hub port of a Cisco 2505, Cisco 2507, or Cisco 2516 router.
vrrp shutdown	Disables a VRRP group.

snmp-server enable traps (MPLS)

To enable a label switch router (LSR) to send Simple Network Management Protocol (SNMP) notifications or informs to an SNMP host, use the **snmp-server enable traps**command in global configuration mode. To disable notifications or informs, use the **no**form of this command.

snmp-server enable traps [*notification-type*] [*notification-option*]

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

Syntax Description

notification-type	

		(Optional) Specifies the particular type of SNMP notification(s) to be enabled on the LSR. If a notification type is not specified, all SNMP notifications applicable to the LSR are enabled and sent to the SNMP host. Any one or all of the following keywords can be specified in any combination as the *notification-type* (family name) in the **snmp-server enable traps**command: • **bgp** --Sends Border Gateway Protocol (BGP) state change notifications. • **config** --Sends configuration notifications. • **entity** --Sends entity MIB modification notifications. • envmon--Sends Cisco enterprise-specific environmental monitor notifications whenever certain environmental thresholds are exceeded. *Notification-option* arguments (below) can be specified in combination with thiskeyword. • **frame-relay** --Sends Frame Relay notifications. • **hsrp** --Sends Hot Standby Routing Protocol (HSRP) notifications. • isdn--Sends ISDN notifications. *Notification-option* arguments (see examples below) can be specified in combination with thiskeyword. • repeater--Sends Ethernet repeater (hub) notifications. *Notification-option* arguments (see examples below) can be specified in combination with thiskeyword. • **rsvp** --Sends Resource Reservation Protocol (RSVP) notifications. • **rtr** --Sends Service Assurance Agent/Response Time Reporter (RTR) notifications. • **snmp** [**authentication**]--Sends RFC 1157 SNMP notifications. Using the **authentication** keyword produces the same effect as not using it. Both the **snmp-server enable traps snmp** and the **snmp-server enable traps snmp authentication**forms of this command globally enable the following SNMP notifications (or, if you are using the **no** form of the command, disables such notifications): **authenticationFailure**, **linkUp**, **linkDown**, and **warmstart**.

	• **syslog** --Sends system error message (syslog) notifications. You can specify the level of messages to be sent using the **logging history level** command.
notification-type (continued)	• **mpls ldp** --Sends notifications about status changes in LDP sessions. Note that this keyword is specified as *mpls ldp* . This syntax, which the CLI interprets as a two-word construct, has been implemented in this manner to maintain consistency with other MPLS commands. *Notification-option* arguments (below) can be specified in combination with thiskeyword. • **mpls traffic-eng** --Sends notifications about status changes in MPLS label distribution tunnels. This keyword is specified as *mpls traffic-eng* . This syntax, which the CLI interprets as a two-word construct, has been implemented in this manner to maintain consistency with other MPLS commands. *Notification-option* arguments (below) can be specified in combination with thiskeyword.

notification-option	

(Optional) Defines the particular options associated with the specified *notification-type* that are to be enabled on the LSR.

- **envmon** [**voltage** | **shutdown** | **supply** | **fan** | **temperature**]

When you specify the **envmon** keyword, you can enable any one or all of the following environmental notifications in any combination: **voltage**, **shutdown**, **supply**, **fan**, or **temperature**. If you do not specify an argument with the **envmon** keyword, all types of system environmental notifications are enabled on the LSR.

- **isdn** [**call-information** | **isdn u-interface**]

When you specify the **isdn** keyword , you can use either the **call-information** argument (to enable an SNMP ISDN call information option for the ISDN MIB subsystem) or the **isdn u-interface** argument (to enable an SNMP ISDN U interface option for the ISDN U Interfaces MIB subsystem), or both. If you do not specify an argument with the **isdn** keyword, both types of isdn notifications are enabled on the LSR.

- **repeater** [**health** | **reset**]

When you specify the **repeater** keyword, you can use either the **health** argument or the **reset** argument, or both (to enable the IETF Repeater Hub MIB [RFC 1516] notification). If you do not specify an argument with the **repeater** keyword, both types of notifications are enabled on the LSR.

- **mpls ldp** [**session-up** | **session-down** | **pv-limit** | **threshold**]

When you specify the **mpls ldp** keyword, you can use any one or all of the following arguments in any combination to indicate status changes in LDP sessions: **session-up**, session-down, pv-limit, or threshold. If you do not specify an argument with the **mpls ldp** keyword, all four types of LDP session notifications are enabled on the LSR.

- **mpls traffic-eng** [**up** | **down** | **reroute**]

When you specify the **mpls traffic-eng** keyword, you can use any one or all of the following arguments in any combination to enable the sending of notifications regarding status changes in MPLS label distribution

	tunnels: **up**, **down**, or **reroute**. If you do not specify an argument with the **mpls traffic-eng** keyword, all three types of tunnel notifications are enabled on the LSR.

Command Default

If you issue this command on an LSR without specifying any *notification-type* keywords, the default behavior of the LSR is to enable all notification types controlled by the command (some notification types cannot be controlled by means of this command).

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.
11.3	The **snmp-server enable traps snmp authentication** form of this command was introduced to replace the **snmp-server trap-authentication** command.
12.0(17)ST	The **mpls traffic-eng**keyword was added to define a class or family of specific SNMP notifications for use with the *notification-type*and *notification-option*parameters of the **snmp-server enable traps**command.
12.0(21)ST	The **mpls ldp** keyword was added to define a class or family of specific SNMP notifications for use with the *notification-type*and *notification-option*parameters of the **snmp-server enable traps**command.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

To configure an LSR to send SNMP LDP notifications, you must issue at least one **snmp-server enable traps**command on the router.

To configure an LSR to send either notifications (traps) or informs to a designated network management station (NMS), you must issue the **snmp-server host**command on that device, usingthe keyword (**traps** or **informs**) that suits your purposes.

If you issue the **snmp-server enable traps**command without keywords, all SNMP notification types are enabled on the LSR. If you issue this command with specific keywords, only the notification types associated with those particular keywords are enabled on the LSR.

The **snmp-server enable traps**command is used in conjunction with the **snmp-server host**command. You use the latter command to specify the NMS host (or hosts) targeted as the recipient(s) of the SNMP notifications generated by SNMP-enabled LSRs in the network. To enable an LSR to send such notifications, you must issue at least one **snmp-server host** command on the LSR.

Examples

In the following example, the router is enabled to send all notifications to the host specified as myhost.cisco.com. The community string is defined as public.

```
Router(config)# snmp-server enable traps
Router(config)# snmp-server host myhost.cisco.com public
```

In the following example, the router is enabled to send Frame Relay and environmental monitor notifications to the host specified as myhost.cisco.com. The community string is defined as public:

```
Router(config)# snmp-server enable traps frame-relay
Router(config)# snmp-server enable traps envmon temperature
Router(config)# snmp-server host myhost.cisco.com public
```

In the following example, notifications are not sent to any host. BGP notifications are enabled for all hosts, but the only notifications enabled to be sent to a host are ISDN notifications (which are not enabled in this example).

```
Router(config)# snmp-server enable traps bgp
Router(config)# snmp-server host host1 public isdn
```

In the following example, the router is enabled to send all inform requests to the host specified as myhost.cisco.com. The community string is defined as public.

```
Router(config)# snmp-server enable traps
Router(config)# snmp-server host myhost.cisco.com informs version 2c public
```

In the following example, HSRP MIB notifications are sent to the host specified as myhost.cisco.com. The community string is defined as public.

```
Router(config)# snmp-server enable hsrp
Router(config)# snmp-server host myhost.cisco.com traps version 2c public hsrp
```

Related Commands

Command	Description
snmp-server host	Specifies the intended recipient of an SNMP notification (that is, the designated NMS workstation in the network).

snmp-server enable traps aaa_server

To enable authentication, authorization, and accounting (AAA) server state-change Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps aaa_server**command in global configuration mode. To disable AAA server state-change SNMP notifications, use the **no**form of this command.

snmp-server enable traps aaa_server

no snmp-server enable traps aaa_server

Syntax Description

This command has no arguments or keywords.

Command Default

SNMP notifications are disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced for the Cisco AS5300 and Cisco AS5800.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests.

This command controls (enables or disables) AAA Server state change (casServerStateChange) notifications. ServerStateChange notifications, when enabled, will be sent when the server moves from an “up” to “dead” state or when a server moves from a “dead” to “up” state.

The Cisco AAA Server State is defined by the casState object in the Cisco AAA Server MIB. The possible values are as follows:

- up(1)--Server is responding to requests.
- dead(2)--Server failed to respond to requests.

A server is marked "dead" if it does not respond after maximum retransmissions. A server is marked "up" again either after a waiting period or if some response is received from it. The initial value of casState is "up(1)" at system startup. This will only transition to "dead(2)" if an attempt to communicate fails.

For a complete description of this notification and additional MIB functions, see the CISCO-AAA-SERVER-MIB.my file, available on Cisco.com at http://www.cisco.com/public/mibs/v2/.

The **snmp-server enable traps aaa_sever**command is used in conjunction with the **snmp-server host**command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send SNMP notifications, you must configure at least one **snmp-server host**command.

Examples

The following example enables the router to send AAA server up/down informs to the host at the address myhost.cisco.com using the community string defined as public:

```
Router(config)# snmp-server enable traps aaa_server
Router(config)# snmp-server host myhost.cisco.com informs version 2c public
```

Related Commands

Command	Description
aaa session-mib disconnect	Allows a remote network management system to perform Set operations and disconnect users on the configured device using SNMP.
show caller	Displays caller information for async, dialer, and serial interfaces.
show radius statistics	Displays AAA server MIB statistics for AAA functions.
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server trap-source	Specifies the interface that an SNMP trap should originate from.

snmp-server enable traps atm pvc

To enable the sending of ATM permanent virtual circuit (PVC) Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps atm pvc**command in global configuration mode. To disable ATM PVC-specific SNMP notifications, use the **no**form of this command.

snmp-server enable traps atm pvc [**interval** *seconds*] [**fail-interval** *seconds*]

no snmp-server enable traps atm pvc [**interval** *seconds*] [**fail-interval** *seconds*]

Syntax Description

interval *seconds*	(Optional) Specifies a minimum period between successive traps. Generation of PVC traps is dampened by the notification interval to prevent trap storms. No traps are sent until the interval lapses. The *seconds* argument is an integer in the range from 1 to 3600. The default is 30.
fail-interval *seconds*	(Optional) Specifies a minimum period for storing the failed time stamp. The *seconds* argument is an integer in the range from 0 to 3600. The default is 0.

Command Default

SNMP notifications are disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(1)T	This command was introduced for the platforms that support ATM PVC Management.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.3	This command was integrated into Cisco IOS XE Software Release 2.3 and implemented on the Cisco ASR 1000 series routers.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests for the specified notification types. ATM notifications are defined in the CISCO-IETF-ATM2-PVCTRAP-MIB.my file, available from the Cisco FTP site at ftp://ftp.cisco.com/pub/mibs/v2/

ATM PVC failure notifications are sent when a PVC on an ATM interface fails or leaves the UP operational state. Only one trap is generated per hardware interface, within the specified interval defined by the **interval** keyword (stored as the atmIntfPvcNotificationInterval in the MIB). If other PVCs on the same interface go DOWN during this interval, traps are generated and held until the fail interval has elapsed. When the interval has elapsed, the traps are sent if the PVCs are still DOWN.

No notifications are generated when a PVC returns to the UP state after having been in the DOWN state. If you need to detect the recovery of PVCs, you must use the SNMP management application to regularly poll your router.

The **snmp-server enable traps atm pvc**command is used in conjunction with the **snmp-server host**command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send notifications, you must configure at least one **snmp-server host**command.

Examples

The following example shows the enabling of ATM PVC traps on a router, so that if PVC 0/1 goes down, host 172.16.61.90 will receive the notifications:

```
!For ATM PVC Trap Support to work on your router, you must first have SNMP support and
!an IP routing protocol configured on your router:
Router(config)# snmp-server community public ro

Router(config)# snmp-server host 172.16.61.90 public

Router(config)# ip routing

Router(config)# router igrp 109

Router(config-router)# network 172.16.0.0

!
!Enable ATM PVC Trap Support and OAM management:
Router(config)# snmp-server enable traps atm pvc interval 40 fail-interval 10

Router(config)# interface atm 1/0.1

Router(config-if)# pvc 0/1

Router(config-if-atm-vc)# oam-pvc manage
```

Related Commands

Command	Description
show atm pvc	Displays all ATM PVCs and traffic information.
snmp-server enable traps	Enables all available SNMP notifications on your system.
snmp-server host	Specifies the recipient of an SNMP notification operation.

Command	Description
snmp-server trap-source	Specifies the interface from which an SNMP trap should originate.

snmp-server enable traps atm pvc extension

To enable the sending of extended ATM permanent virtual circuit (PVC) SNMP notifications and SNMP notifications for ATM Operation, Administration, and Maintenance (OAM) F5 continuity check (CC), ATM OAM F5 alarm indication signals/remote defect indications (AIS/RDI), and loopback failures, use the **snmp-server enable traps atm pvc extension**command in global configuration mode. To disable these SNMP notifications, use the **no**form of this command.

snmp-server enable traps atm pvc extension {**up**| **down**| **oam failure** [**aisrdi**| **endCC**| **loopback**| **segmentCC**]}

no snmp-server enable traps atm pvc extension {**up**| **down**| **oam failure** [**aisrdi**| **endCC**| **loopback**| **segmentCC**]}

Syntax Description

up	Enables ATM PVC up traps. These notifications are generated when a PVC changes from the DOWN to the UP state.
down	Enables ATM PVC failure traps. These notifications are generated when a PVC changes from the UP to the DOWN state.
oam failure	Enables ATM PVC OAM failure traps. These notifications are generated when any type of OAM failure occurs on the PVC.
aisrdi	(Optional) Enables AIS/RDI OAM failure traps. These notifications are generated when AIS/RDI OAM failure occurs on the PVC.
endCC	(Optional) Enables end-to-end OAM CC failure traps. These notifications are generated when end-to-end CC failures occur on the PVC.
loopback	(Optional) Enables OAM failure loopback traps. These notifications are generated when OAM loopback failure occurs on the PVC.
segmentCC	(Optional) Enables segment OAM CC failure traps. These notifications are generated when segment CC failures occur on the PVC.

Command Default

SNMP notifications are disabled. The interval between successive traps is 30 seconds.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(4)T	This command was introduced for those platforms that support ATM PVC management.
12.2(13)T	This command was modified to configure SNMP notification support for ATM OAM F5 CC and ATM OAM F5 AIS/RDI failures.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
Cisco IOS XE Release 2.3	This command was integrated into Cisco IOS XE Software Release 2.3 and implemented on the Cisco ASR 1000 series routers.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.

Usage Guidelines

For PVCs that are not part of a range, extended ATM PVC traps include virtual path identifier/virtual channel identifier (VPI/ VCI) information, the number of state transitions a PVC goes through in an interval, and the timestamp for the start and end of the transitions. For PVCs that are part of a range, extended ATM PVC traps include the first and last VPI/VCI of the range and the timestamp for the first failure and the last failure within the same range.

Extended ATM PVC and ATM OAM F5 CC traps cannot be used at the same time as the legacy ATM PVC trap. The legacy ATM PVC trap must be disabled by using the **no snmp-server enable traps atm pvc** command before extended ATM PVC traps can be configured.

The extended ATM PVC failure trap (which is enabled by the **snmp-server enable traps atm pvc extension down** command) is the same trap as the legacy ATM PVC failure trap (which is enabled by the **snmp-server enable traps atm pvc** command), but with the following differences:

- The extended ATM PVC failure trap contains information in the form of VPI/VCI ranges.
- The extended ATM PVC failure trap contains timestamps for when PVCs go down.
- The legacy ATM PVC failure trap contains only one VPI/VCI per trap.



Note You must configure the **snmp-server enable traps atm pvc extension mibversion 2**command before you can enable the ATM OAM F5 AIS/RDI failure traps, the end-to-end ATM OAM F5 CC failure traps, the OAM failure loopback traps, and the segment ATM OAM F5 CC failure traps. This command enables the MIB that supports these traps.

OAM management must be enabled on the PVC before you can use ATM PVC traps. To generate F5 loopback failure traps, enable OAM management using the **oam-pvc manage** command. To generate segment F5 CC failure traps, enable segment OAM CC management by using the **oam-pvc manage cc segment** command. To generate end-to-end F5 CC failure traps, enable end-to-end OAM CC management by using the **oam-pvc manage cc end** command. To generate OAM F5 AIS/RDI failure traps, enable any of the three types of OAM management listed above.

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests for the specified notification types. The interval between successive traps is 30 seconds.

The extended ATM PVC notifications for MIB version 1 are defined in the CISCO-IETF-ATM2-PVCTRAP-MIB.my file.The extended ATM PVC notifications for MIB version 2 are defined in the CISCO-ATM-PVCTRAP-EXTN-MIB.my file. Both of these MIB files are available from the Cisco FTP site at ftp://ftp.cisco.com/pub/mibs/v2/ .

ATM PVC traps are generated at the end of the notification interval. It is possible to generate all three types of ATM PVC traps (the ATM PVC failure trap, ATM PVC up trap, and ATM PVC OAM failure trap) at the end of the same notification interval; however, only one type of trap will be generated for each PVC.

The **snmp-server enable traps atm pvc extension**command is used in conjunction with the **snmp-server host**command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. In order to send notifications, you must configure at least one **snmp-server host**command.

When the ATM OAM F5 loopback, AIS/RDI, or CC failure trap is enabled, the PVC remains in the UP state when an OAM loopback, AIS/RDI, or CC failure is detected, so that the flow of data will still be possible. If one of these traps is not enabled, the PVC will be placed in the DOWN state when an OAM loopback, AIS/RDI, or CC failure is detected.

Examples

Examples

The following example shows all three of the extended ATM PVC traps enabled on a router. If PVC 0/1 leaves the UP state, leaves the DOWN state, or has an OAM loopback failure, host 172.16.61.90 will receive the SNMP notifications:

```
! Configure SNMP support and an IP routing protocol on your router:
Router(config)# snmp-server community public ro
Router(config)# snmp-server host 172.16.61.90 public
Router(config)# ip routing
Router(config)# router igrp 109
Router(config-router)# network 172.16.0.0
!
! Enable extended ATM PVC trap support and OAM management:
Router(config)# snmp-server enable traps atm pvc extension down
Router(config)# snmp-server enable traps atm pvc extension up
Router(config)# snmp-server enable traps atm pvc extension oam failure loopback
Router(config)# interface atm 1/0.1
Router(config-if)# pvc 0/1
Router(config-if-atm-vc)# oam-pvc manage
```

Examples

The following example shows output for extended ATM PVC failure trap for PVCs 1/100, 1/102, and 1/103. Note that only one trap is generated for all the PVCs associated with the same interface or subinterface (in contrast to the legacy ATM PVC failure trap, which generates a separate trap for each PVC). The VPI/VCI information and timing information are located in the objects associated with the trap.

```
00:23:56:SNMP:Queuing packet to 10.1.1.1
00:23:56:SNMP:V2 Trap, reqid 2, errstat 0, erridx 0
sysUpTime.0 = 143636
snmpTrapOID.0 = atmIntfPvcFailuresTrap
ifEntry.1.19 = 19
atmIntfPvcFailures.2 = 7
atmIntfCurrentlyFailingPVcls.2 = 3
atmPVclLowerRangeValue.19.1.2 = 102
atmPVclHigherRangeValue.19.1.2 = 103
atmPVclRangeStatusChangeStart.19.1.2 = 140643
atmPVclRangeStatusChangeEnd.19.1.2 = 140698
atmPVclStatusTransition.19.1.100 = 1
```

```
atmPVclStatusChangeStart.19.1.100 = 140636
atmPVclStatusChangeEnd.19.1.100 = 140636
00:23:56:SNMP:Packet sent via UDP to 10.1.1.1
```

Examples

The following example shows output for the extended ATM PVC up trap for PVCs 1/100, 1/102, and 1/103:

```
00:31:29:SNMP:Queuing packet to 10.1.1.1
00:31:29:SNMP:V2 Trap, reqid 2, errstat 0, erridx 0
sysUpTime.0 = 188990
snmpTrapOID.0 = atmIntfPvcUpTrap
ifEntry.1.19 = 19
atmIntfCurrentlyDownToUpPVcls.2 = 3
atmPVclLowerRangeValue.19.1.2 = 102
atmPVclHigherRangeValue.19.1.2 = 103
atmPVclRangeStatusChangeStart.19.1.2 = 186005
atmPVclRangeStatusChangeEnd.19.1.2 = 186053
atmPVclStatusTransition.19.1.100 = 1
atmPVclStatusChangeStart.19.1.100 = 185990
atmPVclStatusChangeEnd.19.1.100 = 185990
00:31:30:SNMP:Packet sent via UDP to 10.1.1.1
```

Examples

In the following example, the ATM OAM CC notifications and an extended ATM PVC notification are enabled. If connectivity failures are detected on PVC 0/1, host 172.16.61.90 will receive the SNMP notifications:

```
! Configure SNMP support and an IP routing protocol on your router:
Router(config)# snmp-server community public ro
Router(config)# snmp-server host 172.16.61.90 public
Router(config)# ip routing
Router(config)# router igrp 109
Router(config-router)# network 172.16.0.0
!
! Enable extended ATM PVC trap support and OAM management:
Router(config)# snmp-server enable traps atm pvc extension mibversion 2
Router(config)# snmp-server enable traps atm pvc extension oam failure aisrdi
Router(config)# snmp-server enable traps atm pvc extension oam failure endcc
Router(config)# snmp-server enable traps atm pvc extension oam failure segmentcc
Router(config)# snmp-server enable traps atm pvc extension oam failure loopback
Router(config)# snmp-server enable traps atm pvc extension up
Router(config)# interface atm 0
Router(config-if)# pvc 0/1
Router(config-if-atm-vc)# oam-pvc manage cc end
```

Related Commands

Command	Description
oam-pvc manage	Enables end-to-end F5 OAM loopback cell generation and OAM management.
oam-pvc manage cc	Configures ATM OAM F5 CC management.
show atm pvc	Displays all ATM PVCs and traffic information.
snmp-server enable traps	Enables all available SNMP notifications on your system.
snmp-server enable traps atm pvc	Enables the sending of legacy ATM PVC failure traps.

Command	Description
snmp-server enable traps atm pvc extension mibversion	Specifies the MIB that supports extended ATM PVC SNMP notifications or the MIB that supports SNMP notifications for ATM OAM F5 CC, F5 AIS/RDI, and F5 loopback failures.
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server trap-source	Specifies the interface from which an SNMP trap should originate.

snmp-server enable traps atm pvc extension mibversion

To specify the MIB that supports extended ATM permanent virtual circuit (PVC) Simple Network Management Protocol (SNMP) notifications or the MIB that supports SNMP notifications for ATM Operation, Administration, and Maintenance (OAM) F5 continuity check (CC) management, ATM OAM F5 AIS/RDI management, and F5 loopback failure management, use the **snmp-server enable traps atm pvc extension mibversion**command in global configuration mode. To remove the MIB specification, use the **no**form of this command.

snmp-server enable traps atm pvc extension mibversion {**1**| **2**}

no snmp-server enable traps atm pvc extension mibversion {**1**| **2**}

Syntax Description

1	Specifies the MIB that supports the extended ATM permanent virtual circuit (PVC) SNMP notifications. This is the default.
2	Specifies the MIB that supports ATM OAM F5 CC and ATM OAM F5 AIS/RDI SNMP notifications, in addition to the notifications supported by MIB version 1.

Command Default

SNMP notifications **are disabled.**

Command Modes

Global configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

MIB version 1 specifies the MIB that supports legacy extended ATM PVC traps and is defined in the file CISCO-IETF-ATM2-PVCTRAP-MIB-EXTN.my. MIB version 1 is implemented by default. Use the **snmp-server enable traps atm pvc extension mibversion 1**command or the **no snmp-server enable traps atm pvc** extens**ion mibversion 2**command to reenable this MIB if it was previously disabled with the **snmp-server enable traps atm pvc extension mibversion 2**command.

Use the **snmp-server enable traps atm pvc** extens**ion mibversion 2**command to specify the MIB that supports ATM OAM F5 CC and ATM OAM AID/RDI failure notifications. This MIB is defined in the file CISCO-ATM-PVCTRAP-EXTN-MIB.my.

To enable the SNMP notifications that support ATM OAM F5 continuity checking, use the **snmp-server enable traps atm pvc** extens**ion**command in global configuration mode. These SNMP notifications are defined in the file CISCO-ATM-PVCTRAP-EXTN-MIB.my, available from the Cisco FTP site at ftp://ftp.cisco.com/pub/mibs/v2/

OAM management and support for OAM F5 continuity checking must be enabled on the PVC by using the oam-pvc manage cc command before you can use the ATM OAM continuity check SNMP notifications.

Examples

In the following example, the MIB that supports the SNMP notifications for ATM OAM continuity checking is implemented, and the ATM OAM continuity checking notifications are enabled. Support for end-to-end OAM F5 continuity checking is enabled on PVC 0/1:

```
Router(config)# snmp-server enable traps atm pvc extension mibversion 2
Router(config)# snmp-server enable traps atm pvc extension oam failure aisrdi
Router(config)# snmp-server enable traps atm pvc extension oam failure endcc
Router(config)# snmp-server enable traps atm pvc extension oam failure segmentcc
Router(config)# snmp-server enable traps atm pvc extension oam failure loopback
Router(config)# snmp-server enable traps atm pvc extension up
Router(config)# interface atm 0
Router(config-if)# pvc 0/40
Router(config-if-atm-vc)# oam-pvc manage cc end
```

Related Commands

Command	Description
debug atm oam cc	Displays ATM OAM F5 CC management activity.
oam-pvc manage cc	Configures ATM OAM F5 CC management.
snmp-server enable traps	Enables all available SNMP notifications on your system.
snmp-server enable traps atm pvc	Enables the sending of legacy ATM PVC DOWN traps.
snmp-server enable traps atm pvc extension	Enables the sending of extended ATM PVC SNMP notifications and SNMP notifications for ATM OAM F5 CC, ATM OAM F5 AIS/RDI, and loopback failures.

snmp-server enable traps atm subif

To enable Simple Network Management Protocol (SNMP) traps (notifications) for ATM subinterfaces, use the **snmp-server enable traps atm subif** command in global configuration mode. To disable ATM subinterface-specific SNMP traps, use the **no** form of this command.

snmp-server enable traps atm subif [**count max-traps**] [**interval** *seconds*]

no snmp-server enable traps atm subif [**count max-traps**] [**interval** *seconds*]

Syntax Description

count	(Optional) Specifies the maximum number of traps that will be sent in the specified interval.
max-traps	(Optional) Number of traps. The range is from 1 to 1000. The default is 10.
interval	(Optional) Specifies the minimum period between successive traps.
seconds	(Optional) Interval, in seconds. The range is from 0 to 3600. The default is 10.

Command Default

ATM subinterface SNMP traps are disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SRE6	This command was modified. To enable the sending of ATM subinterface SNMP notifications, after this command is configured in global configuration mode, the **snmp trap link-status** command must be configured on each ATM subinterface.
15.1(3)S3	This command was integrated in Cisco IOS Release 15.1(3)S3.

Usage Guidelines

The **snmp-server trap link ietf** command must be configured in order to use the **snmp-server enable traps atm subif** command. The **snmp-server trap link ietf** command is used to configure a router to use the RFC 2233 IETF standards-based implementation of linkUp/linkDown traps. The default Cisco object definitions do not generate linkUp/linkDown traps correctly for subinterfaces.

In order to enable SNMP notifications for ATM subinterfaces, after the **snmp-server enable traps atm subif** command has been configured in global configuration mode, the **snmp trap link-status** command must be configured on each ATM subinterface for which you want to enable SNMP notifications.

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests for the specified notification types.

ATM subinterface traps are sent to the network management system (NMS) when a subinterface enters or leaves the down state.

To prevent trap storms, the **count** and **interval** keywords can be configured to limit the number of traps and the frequency at which they are sent. Configuring an interval of 0 seconds causes all ATM subinterface traps to be sent.

You can disable ATM subinterface traps by using the **no snmp-server enable traps atm subif** command. When traps are disabled, you can use the SNMP management application to poll your router for subinterface status information.

The **snmp-server enable traps atm subif** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send notifications, you must configure at least one **snmp-server host** command.

By default (when the **snmp-server enable traps atm subif** command is not configured), the ifLinkUpDownTrapEnable object returns disabled(2), and no traps are generated for the subinterfaces.

When the **snmp-server enable traps atm subif** command is configured, the ifLinkUpDownTrapEnable object is set to enabled(1) for all the ATM AAL5 layers of the subinterfaces. To verify that the traps are generated (with the **debug snmp packets** command enabled), enter the **shutdown** or **no shutdown** commands to display the traps.

Configuring the **snmp trap link-status** command on a subinterface generates the traps and sets the ifLinkUpDownTrapEnable object to enabled(1). If the **snmp trap link-status** command is not configured on the subinterface, the ifLinkUpDownTrapEnable object is set to disabled(2) for that subinterface, and the **shutdown** or **no shutdown** commands no longer generate traps for that subinterface.

Examples

The following example shows how to enable ATM subinterface traps on a device. If an ATM subinterface on this device changes state, host 172.16.61.90 will receive the notifications.

```
! For ATM subinterface trap to work on your router, you must first have SNMP support and
! an IP routing protocol configured on your router.
Device(config)# snmp-server community public ro

Device(config)# snmp-server host 172.16.61.90 public
Device(config)# snmp-server trap link ietf
Device(config)# snmp-server enable traps snmp
Device(config)# ip routing

Device(config)# router igrp 109

Device(config-router)# network 172.16.0.0

! Enable ATM subinterface trap support.
Device(config)# snmp-server enable traps atm subif count 5 interval 60
```

Related Commands

Command	Description
snmp-server enable traps	Enables all available SNMP traps on your system.
snmp-server enable traps atm pvc	Enables the sending of ATM PVC SNMP notifications.
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server trap link ietf	Enables linkUp/linkDown SNMP traps that are compliant with RFC 2233.
snmp-server trap-source	Specifies the interface from which an SNMP trap should originate.
snmp trap link-status	Enables SNMP link trap generation.

snmp-server enable traps bfd

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

snmp-server enable traps bfd [session-down] [session-up]

no snmp-server enable traps bfd [session-down] [session-up]

Syntax Description

session-down	(Optional) Enables or disables BFD session down notifications (bfdSessDown).
session-up	(Optional) Enables or disables BFD session up notifications (bfdSessUp).

Command Default

The sending of SNMP notifications is disabled. If you do not specify an optional keyword, all types of BFD notifications are enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SRE	This command was introduced.
15.1(1)SG	This command was integrated into Cisco IOS Release 15.1(1)SG.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

The **snmp-server enable traps bfd** command is used with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send SNMP notifications, you must configure at least one **snmp-server host** command.

If the **session-down** keyword is used with the **snmp-server enable traps bfd** command, a session-down message is generated when a BFD session between the router and its adjacent peer is terminated.

If the **session-up** keyword is used with the **snmp-server enable traps bfd** command, a message is generated when the router establishes a BFD session.

Examples

In the following example, BFD-specific informs are enabled and will be sent to the host myhost.cisco.com through use of community string defined as public:

```
Router(config)# snmp-server enable traps bfd
Router(config)# snmp-server host myhost.cisco.com informs version 2c public bfd
```

Related Commands

Command	Description
snmp-server host	Specifies whether you want the SNMP notifications sent as traps or informs, the version of SNMP to use, the security level of the notifications (for SNMPv3), and the recipient (host) of the notifications.

snmp-server enable traps bgp

To enable Border Gateway Protocol (BGP) support for Simple Network Management Protocol (SNMP) operations on a router, use the **snmp-server enable traps bgp** command in global configuration mode. To disable BGP support for SNMP operations, use the **no** form of this command.

snmp-server enable traps bgp [cbgp2] [**state-changes [all] [backward-trans] [limited]**| **threshold prefix**]

no snmp-server enable traps bgp [cbgp2][**state-changes [all] [backward-trans] [limited]**| **threshold prefix**]

Syntax Description

cbgp2	(Optional) Enables generation of the CISCO-BGP-MIBv8.1 traps.
state-changes	(Optional) Enables traps for finite state machine (FSM) state changes.
all	(Optional) Enables Cisco specific traps for all FSM state changes
backward-trans	(Optional) Enables Cisco specific traps for backward transition events.
limited	(Optional) Enables traps for standard backward transition and established events.
threshold prefix	(Optional) Enables Cisco-specific trap for prefix threshold events.

Command Default

SNMP notifications are disabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(3)T	This command was introduced for the Cisco AS5300 and Cisco AS5800.
12.0(26)S	This command was modified. The **state-changes**, **all**, **backward-trans**, **limited**, and **threshold prefix** keywords were added.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.

Release	Modification
12.2(27)SBC	This command was implemented on the Cisco 7304.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was implemented on the following platforms: Cisco 7301, Cisco 7200 series, and Cisco 10000 series.
15.2(3)T	This command was modified. The **cbgp2** keyword was added.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests and this command enables both notification types. If this command is entered with no keywords specified, support for all configurable options is enabled.

Use this command to enable or disable BGP server state change notifications for the BGP4-MIB (enterprise 1.3.6.1.2.1.15.7). The notifications types are:

- bgpEstablished
- bgpBackwardsTransition

For a complete description of BGP notifications and additional MIB functions, see the BGP4-MIB.my file, available through the Cisco FTP site at ftp://ftp.cisco.com/pub/mibs/v2/.

Note You may notice incorrect BGP trap object ID (OID) output when using the SNMP version 1 BGP4-MIB that is available for download at ftp://ftp.cisco.com/pub/mibs/v1/BGP4-MIB-V1SMI.my. When a router sends out BGP traps (notifications) about state changes on an SNMP version 1 monitored BGP peer, the enterprise OID is incorrectly displayed as .1.3.6.1.2.1.15 (bgp) instead of .1.3.6.1.2.1.15.7 (bgpTraps). This problem occurs because the BGP4-MIB does not follow RFC 1908 rules for version 1 and version 2 trap compliance. The problem is not due to an error in Cisco IOS software. This MIB is controlled by IANA under the guidance of the IETF, and work is currently in progress by the IETF to replace this MIB with a new version that represents the current state of the BGP protocol. In the meantime, we recommend that you use the SNMP version 2 BGP4-MIB or the CISCO-BGP4-MIB to avoid an incorrect trap OID.

The **snmp-server enable traps bgp** command also can be enabled to control BGP server state change notifications for the CISCO-BGP4-MIB. This MIB contains support the following SNMP operations:

- Notification for all BGP FSM transition changes.
- Notifications to query for total number of routes received by a BGP peer.
- Notifications for the maximum prefix-limit threshold on a BGP peer.
- GET operations for VPNv4 unicast routes.

For a complete description of BGP notifications and additional MIB functions, see the CISCO-BGP4-MIB.my file, available through the Cisco FTP site at ftp://www.cisco.com/public/mibs/v2/.

The **snmp-server enable traps bgp** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send SNMP notifications, you must configure at least one **snmp-server host** command.

You may enable or disable the **snmp-server enable traps bgp** command and the **snmp-server enable traps bgp cbgp2** command independently of each other. If both commands are enabled, both traps are generated. If only one of the two commands is enabled, only that version of traps is generated.

Examples

The following example shows how to enable the router to send BGP state change informs to the host at the address myhost.cisco.com using the community string defined as public:

```
Router(config)# snmp-server enable traps bgp
Router(config)# snmp-server host myhost.cisco.com informs version 2c public
```

The following example shows how to enable generation of the CISCO-BGP-MIBv8.1 traps:

```
Router(config)# snmp-server enable traps bgp cbgp2
```

Related Commands

Command	Description
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server trap-source	Specifies the interface from which an SNMP trap should originate.

snmp-server enable traps bulkstat

To enable the sending of Simple Network Management Protocol (SNMP) bulk statistics collection and transfer SNMP notifications, use the **snmp-server enable traps bulkstat**command in global configuration mode. To disable bulk statistics SNMP notifications, use the **no**form of this command.

snmp-server enable traps bulkstat [collection] [transfer]

no snmp-server enable traps bulkstat [collection] [transfer]

Syntax Description

collection	(Optional) Controls bulk statistics collection notifications, which are sent when data collection cannot be carried out successfully. (Defined as cdcVFileCollectionError in the CISCO-DATA-COLLECTION-MIB.)
transfer	(Optional) Controls bulk statistics transfer notifications, which are sent when a transfer attempt is successful or when a transfer attempt fails. (Defined as cdcFileXferComplete in the CISCO-DATA-COLLECTION-MIB. The varbind cdcFilXferStatus object in the trap indicates if the transfer is successful or not.)

Command Default

SNMP notifications are disabled.

Command Modes

Global configuration (config)#

Command History

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

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. The **snmp-server enable traps bulkstat**command enables both traps and inform requests for the specified notification types. Use this command with the **snmp-server host** [**bulkstat**] command.

The optional **collection** keyword controls bulk statistics collection notifications that are sent when data collection cannot be carried out successfully. One possible reason for this condition is insufficient memory on the device.

If the optional keywords are not used, all bulk statistics notification types are enabled (or disabled, if the **no** form of the command is used).

Examples

In the following example, bulk statistics collection and transfer notifications are configured to be sent to the host myhost.cisco.com using the community string public:

```
Device> enable
Device(config)# snmp-server enable traps bulkstat
Device(config)# snmp-server host myhost.cisco.com traps version 2c public bulkstat
```

Related Commands

Command	Description
snmp mib bulkstat transfer	Names a bulk statistics transfer configuration and enters Bulk Statistics Transfer configuration mode.
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server trap-source	Specifies the interface from which an SNMP trap should originate.

snmp-server enable traps c6kxbar

To enable CISCO-CAT6K-CROSSBAR-MIB Simple Network Management Protocol (SNMP) notifications (traps and informs), use the **snmp-server enable traps c6kxbar**command in global configuration mode. To disable cc6kxbar notifications, use the **no** form of this command.

snmp-server enable traps c6kxbar [**flowctrl-bus**| **intbus-crccvrd**| **intbus-crcexcd**| **swbus**| **tm-channel**| **tm-swbus**]

no snmp-server enable traps c6kxbar [**flowctrl-bus**| **intbus-crcexcd**| **intbus-crccvrd**| **swbus**| **tm-channel**| **tm-swbus**]

Syntax Description

flowctrl-bus	(Optional) Enables SNMP cc6kxbarFlowCtrlBusThrExcdNotif notifications.
intbus-crcvrd	(Optional) Enables SNMP cc6kxbarIntBusCRCErrRcvrdNotif notifications.
intbus-crcexcd	(Optional) Enables SNMP cc6kxbarIntBusCRCErrExcdNotif notifications.
swbus	(Optional) Enables SNMP cc6kxbarSwBusStatusChangeNotif notifications.
tm-channel	(Optional) Enables cc6kxbarTMChUtilAboveNotif and cc6kxbarTMChUtilBelowNotif notifications.
tm-swbus	(Optional) Enables cc6kxbarTMSwBusUtilAboveNotif and cc6kxbarTMSwBusUtilBelowNotif notifications.

Command Default

SNMP notifications are disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(14)SX	This command was introduced on the Supervisor Engine 720.
12.2(18)SXF	Added **intbus-crcexce** and **intbus-crcrcvrd** keywords.
12.2(33)SXH	Added **flowctrl-bus** keyword for Supervisor Engine 32 only.

Release	Modification
12.2(33)SXI4	Added **tm-channel** for Supervisor Engine 720 only and **tm-swbus** keywords.

Usage Guidelines

The **flowctrl-bus** keyword is supported on the Supervisor Engine 32 only.

The **tm-channel** keyword is not supported on the Supervisor Engine 32.

Examples

This example shows how to enable SNMP cc6kxbarFlowCtrlBusThrExcdNotif notifications:

```
Router(config)# snmp-server enable traps c6kxbar flowctrl-bus
Router(config)#
```

This example shows how to enable SNMP cc6kxbarIntBusCRCErrExcdNotif notifications:

```
Router(config)# snmp-server enable traps c6kxbar intbus-crcexcd
Router(config)#
```

This example shows how to enable SNMP cc6kxbarIntBusCRCErrRcvrdNotif notifications:

```
Router(config)# snmp-server enable traps c6kxbar intbus-crcvrd
Router(config)#
```

This example shows how to enable SNMP cc6kxbarSwBusStatusChangeNotif notifications:

```
Router(config)# snmp-server enable traps c6kxbar swbus
Router(config)#
```

This example shows how to enable SNMP cc6kxbarTMChUtilAboveNotif and cc6kxbarTMChUtilBelowNotif notifications:

```
Router(config)# snmp-server enable traps c6kxbar tm-channel
Router(config)#
```

This example shows how to enable SNMP cc6kxbarTMSwBusUtilAboveNotif and cc6kxbarTMSwBusUtilBelowNotif notifications:

```
Router(config)# snmp-server enable traps c6kxbar tm-swbus
Router(config)#
```

Related Commands

Command	Description
test snmp trap c6kxbar	Tests the SNMP c6kxbar notification traps.

snmp-server enable traps calltracker

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

snmp-server enable traps calltracker

no snmp-server enable traps calltracker

Syntax Description

This command has no arguments or keywords.

Command Default

SNMP notifications are disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced for the Cisco AS5300 and Cisco AS580 access servers.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests.

This command controls (enables or disables) Call Tracker CallSetup and CallTerminate notifications. CallSetup notifications are generated at the start of each call, when an entry is created in the active table (cctActiveTable), and CallTerminate notifications are generated at the end of each call, when an entry is created in the history table (cctHistoryTable).

For a complete description of these notifications and additional MIB functions, refer to the CISCO-CALL-TRACKER-MIB.my file, available on Cisco.com at http://www.cisco.com/public/mibs/v2/.

The **snmp-server enable traps calltracker**command is used in conjunction with the **snmp-server host**global configurationcommand. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send SNMP notifications, you must configure at least one **snmp-server host**command.

Examples

The following example enables the router to send call-start and call-stop informs to the host at the address myhost.cisco.com using the community string defined as public:

```
Router(config)# snmp-server enable traps calltracker
Router(config)# snmp-server host myhost.cisco.com informs version 2c public calltracker
```

Related Commands

Command	Description
calltracker call-record	Enables call record SYSLOG generation for the purpose of debugging, monitoring, or externally saving detailed call record information.
calltracker enable	Enables the Call Tracker feature on an access server.
isdn snmp busyout b-channel	Enables PRI B channels to be busied out via SNMP.
show call calltracker	Displays Call Tracker activity and configuration information such as the number of active calls and the history table attributes.
show modem calltracker	Displays all of the information stored within the Call Tracker Active or History Database for the latest call assigned to specified modem.
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server trap-source	Specifies the interface that an SNMP trap should originate from.

snmp-server enable traps cnpd

To enable Cisco Network-Based Application Recognition (NBAR) Protocol Discovery (CNPD) MIB notifications, use the **snmp-server enable traps cnpd** command in global configuration mode. To disable CNPD MIB notifications, use the **no** form of this command.

snmp-server enable traps cnpd

no snmp-server enable traps cnpd

Syntax Description

This command has no arguments or keywords.

Command Default

CNPD MIB notifications are disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

CNPD notifications are used with the CNPD MIB to provide information related to protocol discovery. The **snmp-server enable traps cnpd** command enables these notifications. It also enables SNMP notifications as either traps or inform requests.

The **snmp-server enable traps cnpd** command is used in conjunction with the **snmp-server host** command, which specifies the host or hosts that will receive SNMP notifications. To send SNMP notifications, you must configure at least one **snmp-server host** command. The default action is to send notifications to the default port, but you can specify a port by configuring the **udp-port** option of the **snmp-server host**command.

Examples

The following example shows how to enable CNPD notifications:

```
Router(config)# snmp-server enable traps cnpd
```

Related Commands

Command	Description
snmp-server host	Specifies the recipient of SNMP notifications.

snmp-server enable traps cpu

To enable a device to send CPU thresholding violation notifications, use the **snmp-server enable traps cpu**command in global configuration mode. To stop a device from sending CPU thresholding notifications, use the **no**form of this command.

snmp-server enable traps cpu threshold

no snmp-server enable traps cpu

Syntax Description

threshold	Enables notifications of CPU threshold violations.

Command Default

SNMP notifications are disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests and controls CPU thresholding notifications, as defined in the Process MIB (CISCO-PROCESS-MIB).

This command enables the following notifications:

- cpmCPURisingThreshold--Indicates that CPU usage has risen and remains above the configured CPU threshold settings.
- cpmCPUFallingThreshold--Indicates that CPU usage has fallen and remains below the configured CPU threshold settings.

For a complete description of these notification types, and for information about the other MIB functions, see the CISCO-PROCESS-MIB.my file available from Cisco.com at http://www.cisco.com/go/mibs .

The **snmp-server enable traps cpu**command is used in conjunction with the **snmp-server host**command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send SNMP notifications, you must configure at least one **snmp-server host** command.

Examples

The following example shows how to enable the router to send CPU threshold related informs to the host at the address myhost.cisco.com using the community string defined as public:

```
Router(config)# snmp-server enable traps cpu threshold
Router(config)# snmp-server host myhost.cisco.com informs version 2c public cpu
```

Related Commands

Command	Description
snmp-server host	Specifies the destination NMS and transfer parameters for SNMP notifications.
snmp-server trap-source	Specifies the interface from which an SNMP trap should originate.

snmp-server enable traps dhcp

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

snmp-server enable traps dhcp [duplicate] [interface] [pool] [subnet] [time]

no snmp-server enable traps dhcp [duplicate] [interface] [pool] [subnet] [time]

Syntax Description

duplicate	(Optional) Sends notification about duplicate IP addresses.
interface	(Optional) Sends notification that a per interface lease limit is exceeded.
pool	(Optional) Sends notification when address utilization for an address pool has risen above or fallen below a configurable threshold.
subnet	(Optional) Sends notification when address utilization for a subnet has risen above or fallen below a configurable threshold.
time	(Optional) Sends notification that the DHCP server has started or stopped.

Command Default

DHCP trap notifications are not sent.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

If you do not specify any of the optional keywords, all DHCP trap notifications are enabled.

Examples

The following example shows how to send SNMP trap notifications to the SNMP manager when the secondary subnet utilization falls below or exceeds the configured threshold:

```
Router(config)# ip dhcp pool pool2
```

```
Router(dhcp-config)# utilization mark high 80 log
Router(dhcp-config)# utilization mark low 70 log
Router(dhcp-config)# network 192.0.2.0 255.255.255.0
Router(dhcp-config)# network 192.0.4.0 255.255.255.252 secondary
Router(config-dhcp-subnet-secondary)# override utilization high 40
Router(config-dhcp-subnet-secondary)# override utilization low 30
!
Router(config)# snmp-server enable traps dhcp subnet
```

In the following example, all DHCP trap notifications will be sent to the SNMP manager in response to DHCP server events:

```
Router(config)# snmp-server enable traps dhcp
```

snmp-server enable traps dhcp-snooping bindings

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

snmp-server enable traps dhcp-snooping bindings

no snmp-server enable traps dhcp-snooping bindings

Syntax Description

This command has no keywords or arguments.

Command Default

SNMP notifications are disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(33)SXI4	This command was introduced on the Supervisor Engine 720.

Usage Guidelines

This command controls (enables or disables) SNMP notifications for DHCP-snooping binding activity.

Examples

This example shows how to enable DHCP-snooping bindings SNMP notifications:

```
Router(config)# snmp-server enable traps dhcp-snooping bindings
Router(config)#
```

snmp-server enable traps director



Note Effective with Cisco IOS Release 12.4(24)T, the **snmp-server enable traps director**command is not available in Cisco IOS software.

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

snmp-server enable traps director [**server-up**| **server-down**]

no snmp-server enable traps director [**server-up**| **server-down**]

Syntax Description

server-up	(Optional) Enables the DistributedDirector notification that the server has changed to the “up” state.
server-down	(Optional) Enables the DistributedDirector notification that the server has changed to the “down” state.

Command Default

SNMP notifications are disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.4(24)T	This command was removed.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests.

This command controls (enables or disables) DistributedDirector status notifications for systems. If none of the optional keywords is specified, all available environmental notifications are enabled.

Examples

In the following example, both ciscoDistDirEventServerUp and ciscoDistDirEventServerDown notifications are enabled:

```
Router(config)# snmp-server enable traps director
Router# show running-config
ip host myhost 172.20.2.10 172.20.2.20 172.20.2.30
.
.
.
ip director host myhost
ip dns primary myhost soa myhost myhost@com
ip director host myhost priority boomerang 1
no ip director drp synchronized
snmp-server enable traps director server-up server-down
```

Related Commands

Command	Description
snmp-server enable traps	Enables the router to send SNMP traps.
snmp-server host	Specifies the recipient of an SNMP notification.
snmp-server informs	Specifies inform request options.
snmp-server trap-source	Specifies the interface (and hence the corresponding IP address) from which an SNMP trap should originate.
snmp-server trap-timeout	Defines how often to try resending trap messages on the retransmission queue.
snmp trap link-status	Enables SNMP trap notifications to be generated when a specific port is brought up or down.

snmp-server enable traps dlsw

To enable the sending of Data Link Switch (DLSw) circuit and peer connection Simple Network Management Protocol (SNMP) notifications (traps and informs), use the **snmp-server enable traps dlsw** command in global configuration mode. To disable DLSw notifications, use the **no** form of this command.

snmp-server enable traps dlsw [**circuit**| **tconn**]

no snmp-server enable traps dlsw [**circuit**| **tconn**]

Syntax Description

circuit	(Optional) Enables DLSw circuit traps: • (5) ciscoDlswTrapCircuitUp • (6) ciscoDlswTrapCircuitDown
tconn	(Optional) Enables DLSw peer transport connection traps: • (1) ciscoDlswTrapTConnPartnerReject • (2) ciscoDlswTrapTConnProtViolation • (3) ciscoDlswTrapTConnUp • (4) ciscoDlswTrapTConnDown

Command Default

SNMP notifications are disabled.

If the optional keywords are not used, all DLSw notification types are enabled (or disabled, if the **no** form of the command is used).

Command Modes

Global configuration

Command History

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

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests. Use this command in conjunction with the **snmp-server host** command.

This command controls (enables or disables) SNMP notifications for Data Link Switch (DLSw) circuit and connection activity. DLSw objects are defined in the Cisco DLSw MIB module (CISCO-DLSW-MIB.my) and the DLSw+ (Cisco Specific Features) MIB module (CISCO-DLSW-EXT-MIB.my), available through Cisco.com at http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml.

Examples

In the following example the device is configured to send DLSw circuit state change informs to the host at the address myhost.cisco.com using the community string defined as public:

```
Router(config)# snmp-server enable traps dlsw circuit
Router(config)# snmp-server host myhost.cisco.com informs version 2c public
```

Related Commands

Command	Description
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server trap-source	Specifies the interface that an SNMP trap should originate from.

snmp-server enable traps eigrp

To enable support for Enhanced Interior Gateway Routing Protocol (EIGRP) notifications on a Cisco router, use the snmp-server enable traps eigrp command in global configuration mode. To disable EIGRP notification support, use the **no** form of this command.

snmp-server enable traps eigrp

no snmp-server enable traps eigrp

Syntax Description

This command has no keywords or arguments.

Command Default

EIGRP notification support is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.
12.2(33)SXI4	This command was integrated into Cisco IOS Release 12.2(33)SXI4.

Usage Guidelines

The snmp-server enable traps eigrp command is used to enable notifications (traps) for stuck-in-active (SIA) and neighbor authentication failure events. Support for trap events is not activated until a trap destination is configured with the snmp-server host command and until a community string is defined with the snmp-server community command.

Examples

In the following example, an SNMP server host is specified, a community string is configured, and support for EIGRP notifications is enabled:

```
Router(config)# snmp-server host 10.0.0.1 traps version 2c NETMANAGER eigrp
Router(config)# snmp-server community EIGRP1NET1A
Router(config)# snmp-server enable traps eigrp
```

Related Commands

Command	Description
snmp-server community	Configures a community access string to permit SNMP access to the local router by the remote SNMP software client.
snmp-server host	Specifies the destination host or address for SNMP notifications.

snmp-server enable traps envmon

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

snmp-server enable traps envmon [shutdown] [voltage] [temperature] [fan] [supply]

no snmp-server enable traps envmon [shutdown] [voltage] [temperature] [fan] [supply]

Syntax Description

shutdown	(Optional) Controls shutdown notifications.
voltage	(Optional) Controls voltage notifications.
temperature	(Optional) Controls temperature notifications.
fan	(Optional) Controls fan failure notifications.
supply	(Optional) Controls redundant power supply (RPS) failure notifications.

Command Default

SNMP notifications are disabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.3	This command was introduced.
11.3(6)AA	This command is supported on the Cisco AS5300 access server.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.0(1)SE	This command was modified. The following notifications were added: ciscoEnvMonVoltStatusChangeNotif, ciscoEnvMonTempStatusChangeNotif, ciscoEnvMonFanStatusChangeNotif, and ciscoEnvMonSuppStatusChangeNotif.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests.

This command enables or disables Environmental Monitor (EnvMon) status notifications for supported systems. The Cisco enterprise EnvMon notifications that are listed in the table below are triggered when an environmental threshold is exceeded. If none of the optional keywords are specified, all available environmental notifications are enabled.

Keyword Enabled	EnvMon Notification Sent	Trigger
shutdown	ciscoEnvMonShutdownNotification (enterprise MIB OID 1.3.6.1.4.1.9.9.13.3.1)	The environmental monitor detects a testpoint that is reaching a critical state and is about to initiate a shutdown.
voltage	ciscoEnvMonVoltageNotification (enterprise MIB OID 1.3.6.1.4.1.9.9.13.3.2)	The voltage measured at a given testpoint is outside the normal range for the testpoint (that is, the voltage is at the warning, critical, or shutdown stage). For access servers, this notification is defined as caemVoltageNotification (enterprise MIB OID 1.3.6.1.4.1.9.9.61.2.2).
temperature	ciscoEnvMonTemperatureNotification (enterprise MIB OID 1.3.6.1.4.1.9.9.13.3.3)	The temperature measured at a given testpoint is outside the normal range for the testpoint (that is, the temperature is at the warning, critical, or shutdown stage). For access servers, this notification is defined as caemTemperatureNotification (enterprise MIB OID 1.3.6.1.4.1.9.9.61.2.1).
fan	ciscoEnvMonFanNotification (enterprise MIB OID 1.3.6.1.4.1.9.9.13.3.4)	A fan in a fan array fails.
supply	ciscoEnvMonRedundantSupplyNotification (enterprise MIB OID 1.3.6.1.4.1.9.9.13.2.5)	A redundant power supply fails.

The Cisco enterprise EnvMon notifications that are listed in the table below are triggered when there is a change in the state of a device being monitored. If none of the optional keywords are specified, all available environmental notifications are enabled.

Keyword Enabled	EnvMon Notification Sent	Trigger
voltage	ciscoEnvMonVoltStatusChangeNotif (enterprise MIB OID 1.3.6.1.4.1.9.9.13.3.0.6)	There is a change in the state of a device being monitored by ciscoEnvMonVoltageState.
temperature	ciscoEnvMonTempStatusChangeNotif (enterprise MIB OID 1.3.6.1.4.1.9.9.13.3.0.7)	There is a change in the state of a device being monitored by ciscoEnvMonTemperatureState.
fan	ciscoEnvMonFanStatusChangeNotif (enterprise MIB OID 1.3.6.1.4.1.9.9.13.3.0.8)	There is a change in the state of a device being monitored by ciscoEnvMonFanState.
supply	ciscoEnvMonSuppStatusChangeNotif (enterprise MIB OID 1.3.6.1.4.1.9.9.13.3.0.9)	There is a change in the state of a device being monitored by ciscoEnvMonSupplyState.

For a complete description of these notifications and additional MIB functions, see the CISCO-ENVMON-MIB.my and CISCO-ACCESS-ENVMON-MIB.my files available on Cisco.com at http://www.cisco.com/public/mibs/v2/.

You can view the status of EnvMon by using the **show environment** command.

The **snmp-server enable traps envmon** command is used in combination with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send SNMP notifications, you must configure at least one **snmp-server host** command.

Examples

The following example shows how to enable a Cisco 12000 Gigabit Switch Router (GSR) to send environmental failure informs to the host at the address myhost.cisco.com by using the community string defined as public:

```
Device# configure terminal
Device(config)# snmp-server enable traps envmon
Device(config)# snmp-server host myhost.cisco.com informs version 2c public envmon
```

Related Commands

Command	Description
show environment	Displays environmental conditions on the system.
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server trap-source	Specifies the interface that an SNMP trap should originate from.

snmp-server enable traps errdisable

To enable the CISCO-ERR-DISABLE-MIB Simple Network Management Protocol (SNMP) notification for traps and informs, use the **snmp-server enable traps errdisable**command in global configuration mode. To disable errdisable notifications, use the **no** form of this command.

snmp-server enable traps errdisable [**notification-rate** *rate*]

no snmp-server enable traps [**notification-rate** *rate*]

Syntax Description

notification-rate *rate*	(Optional) Sets the number of notifications per minute.

Command Default

SNMP notifications are disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(33)SXI4	This command was introduced on the Supervisor Engine 720 and Supervisor Engine 32.

Examples

This example shows how to enable the SNMP errdisable notifications:

```
Router(config)# snmp-server enable traps errdisable
Router(config)#
```

This example shows how to set the SNMP errdisable notification rate to 500 per minute:

```
Router(config)# snmp-server enable traps errdisable notification-rate 500
Router(config)#
```

Related Commands

Command	Description
test snmp trap errdisable ifevent	Tests the cErrDisableInterfaceEventRev1 trap.

snmp-server enable traps firewall

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

snmp-server enable traps firewall serverstatus

no snmp-server enable traps firewall serverstatus

Syntax Description

serverstatus	Displays the status of configured servers.

Command Default

SNMP notifications are disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

SNMP notifications are sent as traps by the agent. Currently, only one URL filtering trap is generated.

For a complete description of the notification types and additional MIB functions, refer to the CISCO-UNIFIED-FIREWALL-MIB.my and CISCO-FIREWALL-TC.my files, available on Cisco.com through:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

The **snmp-server enable traps firewall** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send SNMP notifications, you must configure at least one **snmp-server host** command.

Examples

In the following example, the router is configured to send firewall MIB inform notifications to the host nms.cisco.com using the community string named “public”:

```
snmp-server enable traps firewall serverstatus
snmp-server host nms.cisco.com informs public firewall
```

Related Commands

Command	Description
snmp-server host	Specifies the recipient of an SNMP notification operation.

snmp-server enable traps flash

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

snmp-server enable traps flash [insertion] [removal]

no snmp-server enable traps flash [insertion] [removal]

Syntax Description

insertion	(Optional) Controls Flash card insertion notifications.
removal	(Optional) Controls Flash card removal notifications.

Command Default

SNMP notifications are disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.0(23)S	This command was integrated in Cisco IOS Release 12.0 S.
12.1(13)E4	This command was implemented on the Cisco Catalyst 6000 Series.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests.

This command enables or disables Flash card insertion and removal notifications, as defined by the ciscoFlashDeviceInsertedNotif and ciscoFlashDeviceRemovedNotif objects in the Cisco Flash MIB.

When the **insertion** keyword is used, a ciscoFlashDeviceInsertedNotif (OID 1.3.6.1.4.1.9.9.10.1.3.0.5) is sent whenever a removable Flash device is inserted.

When the **removal** keyword is used, a ciscoFlashDeviceRemovedNotif (OID 1.3.6.1.4.1.9.9.10.1.3.0.6) notification is sent whenever a removable Flash device is removed.

For a complete description of these notifications and additional MIB functions, see the CISCO-FLASH-MIB.my file, available on Cisco.com at http://www.cisco.com/go/mibs .

The **snmp-server enable traps flash**command is used in conjunction with the **snmp-server host**command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send SNMP notifications, you must configure at least one **snmp-server host**command.

Examples

The following example shows how to enable the router to send Flash card insertion and removal informs to the host at the address myhost.cisco.com using the community string defined as public:

```
Router(config)# snmp-server enable traps flash insertion removal
Router(config)# snmp-server host myhost.cisco.com informs version 2c public flash
```

Related Commands

Command	Description
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server trap-source	Specifies the interface that an SNMP trap should originate from.

snmp-server enable traps flowmon

To enable flow monitoring SNMP trap notifications, use the **snmp-server enable traps flowmon** command in global configuration mode. To disable flow monitoring trap notifications, use the **no** form of this command.

snmp-server enable traps flowmon

no snmp-server enable traps flowmon

Syntax Description

This command has no arguments or keywords.

Command Default

Flow monitoring trap notifications are disabled.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

SNMP notifications can be sent as traps or informs. This command enables trap notification requests only.

By default all notifications (traps) are disabled. You must explicitly enable any notifications that you need in your system. The **snmp-server enable traps flowmon** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send SNMP notifications, you must configure at least one **snmp-server host** command.

Note For a complete description of the MIB tables for flow monitoring, see the appropriate CISCO_MIB.my file, available on Cisco.com at http://www.cisco.com/go/mibs .

Examples

The following example shows how to enable flow monitoring traps:

```
Router(config)# snmp-server enable traps flowmon
```

Related Commands

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

snmp-server enable traps frame-relay

To enable Frame Relay Data Link Connection Identifier (DLCI) and subinterface Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps frame-relay** command in global configuration mode. To disable Frame Relay DLCI and subinterface SNMP notifications, use the **no** form of this command.

snmp-server enable traps frame-relay

no snmp-server enable traps frame-relay

Syntax Description

This command has no arguments or keywords.

Command Default

SNMP notifications are disabled.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(13)T	This command was modified to enable Frame Relay subinterface traps in addition to DLCI traps.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests.

This command controls (enables or disables) DLCI Frame Relay notifications, as defined in the RFC1315-MIB (enterprise 1.3.6.1.2.1.10.32).

This trap indicates that the indicated virtual circuit (VC) or subinterface has changed state, meaning that the VC or subinterface has either been created or invalidated, or has toggled between the active and inactive states.

To enable only Frame Relay subinterface traps, use the **snmp-server enable traps frame-relay subif** command.

Note For large scale configurations (systems containing hundreds of Frame Relay point-to-point subinterfaces), note that having Frame Relay notifications enabled could potentially have a negative impact on network performance when there are line status changes.

For a complete description of this notification and additional MIB functions, see the RFC1315-MIB.my file and the CISCO-FRAME-RELAY-MIB.my file, available in the "v1" and "v2" directories, respectively, at the Cisco.com MIB web site at http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml .

The **snmp-server enable traps frame-relay**command is used in conjunction with the **snmp-server host**command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send SNMP notifications, you must configure at least one **snmp-server host**command.

Examples

In the following example, the router is configured to send Frame Relay DLCI and subinterface state change informs to the host at the address myhost.cisco.com using the community string defined as public:

```
Router(config)# snmp-server enable traps frame-relay
Router(config)# snmp-server host myhost.cisco.com informs version 2c public
```

Related Commands

Command	Description
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server trap-source	Specifies the interface that an SNMP trap should originate from.

snmp-server enable traps frame-relay multilink bundle-mismatch

To enable multilink Frame Relay Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps frame-relay multilink bundle-mismatch**command in global configuration mode. To disable these notifications, use the **no** form of this command.

snmp-server enable traps frame-relay multilink bundle-mismatch

no snmp-server enable traps frame-relay multilink bundle-mismatch

Syntax Description

This command has no arguments or keywords.

Command Default

SNMP notifications are disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

Use the multilink Frame Relay MIB to manage devices that are configured with multilink Frame Relay.

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests.

Although the bundle-mismatch trap is one of five traps defined in RFC 3020, Cisco IOS supports only the bundle-mismatch trap.

For a complete description of MIB functions, see the CISCO-FRAME-RELAY-MIB.my file, which is available in the “SNMP v2 MIBs” directory found at the following URL:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

Examples

In the following example, multilink Frame Relay is configured on the host router with one bundle, and the peer router is configured with zero bundle links.

On the host router:

```
Router(config)# interface MFR1
Router(config)# ip address 209.165.200.225 255.255.255.224
```

```
Router(config)# frame-relay multilink bid UUT_BUNDLE_ONE
Router(config)# frame-relay interface-dlci 100
!
Router(config)# snmp-server community public RW
Router(config)# snmp-server enable traps frame-relay multilink bundle-mismatch
Router(config)# snmp-server host 10.0.47.4 public
```

On the peer router:

```
Router(config)# interface MFR1
Router(config)# ip address 209.165.200.226 255.255.255.224
Router(config)# frame-relay multilink bid PEER_BUNDLE_ONE
Router(config)# frame-relay interface-dlci 100
Router(config)# frame-relay intf-type dce
Router(config)# snmp-server enable traps frame-relay multilink bundle-mismatch
Router(config)# snmp-server host myhost.cisco.com informs version 2c public
```

Related Commands

Command	Description
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server trap-source	Specifies the interface from which an SNMP trap should originate.

snmp-server enable traps frame-relay subif

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

snmp-server enable traps frame-relay subif [[**interval** *seconds*] **count** *number-of-traps*]

no snmp-server enable traps frame-relay subif [[**interval** *seconds*] **count** *number-of-traps*]

Syntax Description

interval	(Optional) Specifies a minimum period between successive traps,
seconds	(Optional) Integer in the range from 0 to 3600. The default is 10.
count	(Optional) Specifies a maximum number of traps that will be sent in the specified interval.
number-of-traps	(Optional) Integer in the range from 1 to 1000. The default is 10.

Command Default

Frame Relay subinterface SNMP notifications are disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests.

Frame Relay subinterface traps are sent to the network management system (NMS) when a subinterface enters or leaves the down state.

To prevent trap storms, the **count** and **interval** keywords can be configured to limit the number of traps and the frequency at which they are sent. Configuring an interval of 0 seconds causes all Frame Relay subinterface traps to be sent.

Note The **snmp-server enable traps frame-relay** command enables both Frame Relay data-link connection identifier (DLCI) and subinterface traps. The **snmp-server enable traps frame-relay subif**command enables only Frame Relay subinterface traps.

You can disable Frame Relay subinterface traps by using the **no snmp-server enable traps frame-relay subif**command. When traps are disabled, you can use the SNMP management application to poll your router for subinterface status information.

The **snmp-server enable traps frame-relay subif**command is used in conjunction with the **snmp-server host**command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. In order to send notifications, you must configure at least one **snmp-server host**command.

The **snmp-server trap link ietf** command must be configured in order to use the **snmp-server enable traps frame-relay subif**command. The **snmp-server trap link ietf** command is used to configure your router to use the RFC 2233 IETF standards-based implementation of linkUp/linkDown traps. The default Cisco object definitions do not generate linkUp/linkDown traps correctly for subinterfaces.

Examples

The following example shows how to enable Frame Relay subinterface traps on a router. If a Frame Relay subinterface on this router changes state, host 172.16.61.90 will receive the notifications:

```
! For Frame Relay subinterface traps to work on your router, you must first have SNMP !
support and an IP routing protocol configured on your router:
Router(config)# snmp-server community public ro

Router(config)# snmp-server host 172.16.61.90 public
Router(config)# snmp-server trap link ietf
Router(config)# snmp-server enable traps snmp
Router(config)# ip routing

Router(config)# router igrp 109

Router(config-router)# network 172.16.0.0

!Enable Frame Relay subinterface trap support:
Router(config)# snmp-server enable traps frame-relay subif interval 60 count 5
```

Related Commands

Command	Description
snmp-server enable traps frame-relay	Enables Frame Relay DLCI link status SNMP notifications.
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server trap link ietf	Enables linkUp/linkDown SNMP traps that are compliant with RFC 2233.
snmp-server trap-source	Specifies the interface from which an SNMP trap should originate.

snmp-server enable traps if-monitor

To globally enable if-monitor traps, use the **snmp-server enable traps if-monitor** command in global configuration mode. To disable if-monitor traps, use the **no** form of this command.

snmp-server enable traps if-monitor

no snmp-server enable traps if-monitor

Syntax Description

This command has no arguments or keywords.

Command Default

Traps are not generated.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

The **snmp-server enable traps if-monitor** command enables the if-monitor threshold traps for link monitoring. To enable traps for a particular interface, you must enable them globally using the **snmp-server enable traps if-monitor** command and then explicitly on that interface using the **snmp trap if-monitor** command.

A high threshold limit is the highest value for a parameter on a specific link. If that value is reached or exceeded in the configured major monitoring interval, a trap is sent and a message is logged. The link is brought down if the restart mechanism is enabled.

A low threshold limit is the lowest value for a parameter on a specified link. If that value is reached or exceeded in the major monitoring interval, a trap is sent and a message is logged.

Examples

The following example shows how to enable if-monitor traps on all interfaces:

```
Router(config)# snmp-server enable traps if-monitor
```

Related Commands

Command	Description
snmp trap if-monitor	Enables if-monitor traps for a particular interface.

snmp-server enable traps ip local pool

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

snmp-server enable traps ip local pool

no snmp-server enable traps ip local pool

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled; no notifications are sent.

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Examples

The following example shows how to enable the sending of local IP SNMP notifications:

```
Router(config)# snmp-server enable traps ip local pool
```

Related Commands

Command	Description
snmp-server host	Specifies the recipient of an SNMP notification operation.

snmp-server enable traps isdn

To enable the sending of Integrated Services Digital Network (ISDN)-specific Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps isdn**command in global configuration mode. To disable ISDN-specific SNMP notifications, use the **no**form of this command.

snmp-server enable traps isdn [call-information] [chan-not-avail] [ietf] [isdnu-interface] [layer2]

no snmp-server enable traps isdn [call-information] [chan-not-avail] [ietf] [isdnu-interface] [layer2]

Syntax Description

call-information	(Optional) Controls SNMP ISDN call information notifications, as defined in the CISCO-ISDN-MIB (enterprise 1.3.6.1.4.1.9.9.26.2). Notification types are: • demandNbrCallInformation (1) This notification is sent to the manager whenever a successful call clears, or a failed call attempt is determined to have ultimately failed. In the event that call retry is active, then this is after all retry attempts have failed. However, only one such notification is sent in between successful call attempts; subsequent call attempts do not generate notifications of this type. • demandNbrCallDetails (2) This notification is sent to the manager whenever a call connects, or clears, or a failed call attempt is determined to have ultimately failed. In the event that call retry is active, then this is after all retry attempts have failed. However, only one such notification is sent in between successful call attempts; subsequent call attempts do not generate notifications of this type.
chan-not-avail	(Optional) Controls SNMP ISDN channel-not-available notifications. ISDN PRI channel-not-available traps are generated when a requested DS-0 channel is not available, or when there is no modem available to take the incoming call. These notifications are available only for ISDN PRI interfaces.
ietf	(Optional) Controls the SNMP ISDN IETF traps.
isdnu-interface	(Optional) Controls SNMP ISDN U interface notifications.

layer2	(Optional) Controls SNMP ISDN Layer 2 transition notifications.

Command Default

SNMP notifications are disabled by default.

If you enter this command with none of the optional keywords, all available notifications are enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.3	This command was introduced.
11.3	This command was modified. The **call-information** and **isdnu-interface** keywords were added for the Cisco 1600 series router.
12.0	This command was modified. Support for the **call-information** and **isdnu-interface** keywords was introduced for most voice platforms.
12.1(5)T	This command was modified. Support for the **chan-not-available** keyword was added for the Cisco AS5300, Cisco AS5400, and Cisco AS5800 access servers only.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests for the specified notification types. ISDN notifications are defined in the CISCO-ISDN-MIB.my and CISCO-ISDNU-IF-MIB.my files, available on Cisco.com at http://www.cisco.com/public/mibs/v2/.

Availability of notifications will depend on your platform. To see what notifications are available, use the **snmp-server enable traps isdn ?** command.

If you do not enter an **snmp-server enable traps isdn**command, no notifications controlled by this command are sent. In order to configure the router to send these SNMP notifications, you must enter at least one **snmp-server enable traps isdn**command. If you enter the command with no keywords, all notification types are enabled. If you enter the command with a keyword, only the notification type related to that keyword is enabled.

The **snmp-server enable traps snmp**command is used in conjunction with the **snmp-server host**command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send SNMP notifications, you must configure at least one **snmp-server host**command.

Examples

The following example shows how to determine what notification types are available on a Cisco AS5300 and then shows how to enable channel-not-available and Layer 2 informs:

```
NAS(config)# snmp-server enable traps isdn ?
  call-information  Enable SNMP isdn call information traps
  chan-not-avail    Enable SNMP isdn channel not avail traps
  ietf              Enable SNMP isdn ietf traps
  layer2            Enable SNMP isdn layer2 transition traps
```

```
  <cr>
NAS(config)# snmp-server enable traps isdn chan-not-avail layer2
NAS(config)# snmp-server host myhost.cisco.com informs version 2c public isdn
```

Related Commands

Command	Description
snmp-server enable traps	Enables all available SNMP notifications on your system.
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server informs	Specifies inform request options.
snmp-server trap-source	Specifies the interface that an SNMP trap should originate from.

snmp-server enable traps l2tun pseudowire status

To enable the sending of Simple Network Management Protocol (SNMP) notifications when a pseudowire changes state, use the **snmp-server enable traps l2tun pseudowire status**command in global configuration mode. To disable SNMP notifications of pseudowire state changes, use the **no** form of this command.

snmp-server enable traps l2tun pseudowire status

no snmp-server enable traps l2tun pseudowire statuszo

Syntax Description

This command has no arguments or keywords.

Command Default

SNMP notifications are disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.0(31)S	This command was introduced.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
Cisco IOS XE Release 2.4	This command was integrated into Cisco IOS XE Release 2.4.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests.

This command controls (enables or disables) notification of pseudowire state changes. For a complete description of these notification types, and for information about the other MIB functions, see the VPDN MIB, available through the Cisco Technical Assistance Center (TAC) SNMP Object Navigator tool at http://www.cisco.com/go/mibs.

The **snmp-server enable traps l2tun pseudowire status**command is used in conjunction with the **snmp-server host**command. Use the **snmp-server host**command to specify which host or hosts receive SNMP notifications. To send SNMP notifications, you must configure at least one **snmp-server host**command.

Use the **snmp-server enable traps** command without any additional syntax to disable all SNMP notification types supported on your system.

Examples

The following example enables the router to send pseudowire state change informs to the host at the address myhost.cisco.com using the community string defined as public:

```
Router(config)# snmp-server enable traps l2tun pseudowire status
Router(config)# snmp-server host myhost.cisco.com informs version 2c public
```

Related Commands

Command	Description
snmp-server enable traps	Enables all SNMP notifications (traps or informs) available on your system.
snmp-server host	Specifies the recipient of an SNMP notification operation.
xconnect logging pseudowire status	Enables syslog reporting of pseudowire status events.

snmp-server enable traps l2tun session

To enable Simple Network Management Protocol (SNMP) notifications (traps or inform requests) for Layer 2 Tunnel Protocol Version 3 (L2TPv3) sessions, use the **snmp-server enable traps l2tun session**command in global configuration mode. To disable SNMP notifications, use the **no**form of this command.

snmp-server enable traps l2tun session

no snmp-server enable traps l2tun session

Syntax Description

This command has no arguments or keywords.

Command Default

No SNMP notifications for L2TPv3 sessions are sent.

Command Modes

Global configuration

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.3(2)T	This command was integrated into Cisco IOS Release 12.3T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(27)SBC	Support for this command was integrated into Cisco IOS Release 12.2(27)SBC.

Usage Guidelines

In this command **l2tun** indicates “layer 2 tunneling.” Layer 2 tunneling session notifications are defined by the cvpdnNotifSession object { ciscoVpdnMgmtMIBNotifs 3 } in the Cisco VPDN Management MIB (CISCO-VPDN-MGMT-MIB.my). MIB files are available from Cisco.com at http://www.cisco.com/go/mibs .

SNMP notifications can be sent as traps or inform requests and this command enables both types of notifications for L2TP sessions. To specify whether the notifications should be sent as traps or informs, and to specify which host or hosts receive SNMP notifications, use the **snmp-server host** [**traps** | **informs**] command.

Use the **snmp-server enable traps** command without any additional syntax to disable all SNMP notification types supported on your system.

Examples

The following example shows how to enable a router to send L2TP session traps to the host specified by the name myhost.example.com, using the community string defined as public:

```
Router(config)# snmp-server enable traps l2tun session
Router(config)# snmp-server host myhost.example.com public l2tun-session
```

Related Commands

Command	Description
snmp-server enable traps	Enables all SNMP notifications available on your system.
snmp-server host	Specifies whether you want the SNMP notifications sent as traps or informs, the version of SNMP to use, the security level of the notifications (for SNMPv3), and the recipient (host) of the notifications.

snmp-server enable traps memory

To enable a device to send Simple Network Management Protocol (SNMP) notifications when memory pool buffer usage reaches a new peak, use the **snmp-server enable traps memory** command in global configuration mode. To stop notifications from being generated, use the **no** form of this command.

snmp-server enable traps memory [bufferpeak]

no snmp-server enable traps memory [bufferpeak]

Syntax Description

bufferpeak	(Optional) Specifies memory buffer peak notifications.

Command Default

SNMP notifications in the MEMPOOL-MIB are not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests.

This command enables or disables memory buffer peak (cempMemBufferNotify) notifications.When they are enabled, these notifications are sent when the value of the maximum number of buffer objects changes.

In current releases of Cisco IOS software, this command has the same behavior whether you use or omit the **bufferpeak** keyword.

The cempMemBufferNotify notification type is defined as {cempMIBNotifications 1} in the CISCO-ENHANCED-MEMPOOL-MIB. For a complete description of this notification and additional MIB functions, see the CISCO-ENHANCED-MEMPOOL-MIB.my file, available on Cisco.com at http://www.cisco.com/go/mibs/ .

Examples

In the following example all available memory related SNMP notifications are enabled and configured to be sent as informs to the host myhost.cisco.com using the community string public:

```
Router(config)# snmp-server enable traps memory
Router(config)# snmp-server host myhost.cisco.com informs version 3 public memory
```

Related Commands

Command	Description
show buffers	Displays memory buffer pool related information.
show memory	Displays memory pool related information.
snmp-server host	Specifies whether you want the SNMP notifications sent as traps or informs, the version of SNMP to use, the security level of the notifications (for SNMPv3), and the recipient (host) of the notifications.

snmp-serverenabletrapsospfcisco-specificerrorsconfig-error

To e nable Simple Network Management Protocol (SNMP) notifications for Open Shortest Path First (OSPF) nonvirtual interface mismatch errors, use the **snmp-server enable traps ospf cisco-specific errors config-error**command in global configuration mode. To disable OSPF nonvirtual interface mismatch error SNMP notifications, use the **no** form of this command.

snmp-server enable traps ospf cisco-specific errors config-error

no snmp-server enable traps ospf cisco-specific errors config-error

Syntax Description

This command has no keywords or arguments.

Command Default

This command is disabled by default; therefore, SNMP notifications for OSPF nonvirtual interface mismatch errors are not created.

Command Modes

Global configuration

Command History

Release	Modification
12.3(5)	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

To enable the cospfShamLinkConfigError trap, you must first enter the **snmp-server enable traps ospf cisco-specific errors config-error** command in global configuration mode. The **snmp-server enable traps ospf cisco-specific errors config-error** command enables the cospfConfigError trap, so that both traps can be generated at the same place and maintain consistency with a similar case for configuration errors across virtual links.

If you try to enable the cospfShamLinkConfigError trap before configuring the cospfospfConfigError trap you will receive an error message stating you must first configure the cospfConfigError trap.

Examples

The following example enables the router to send nonvirtual interface mismatch error notifications to the host at the address myhost.cisco.com using the community string defined as public:

```
Router(config)# snmp-server enable traps ospf cisco-specific errors config-error
Router(config)# snmp-server host myhost.cisco.com informs version 2c public
```

Related Commands

Command	Description
snmp-server enable traps ospf cisco-specific errors shamlink	Enables SNMP notifications for OSPF sham-link errors.
snmp-server enable traps ospf cisco-specific retransmit	Enables SNMP notifications for OSPF retransmission errors.
snmp-server enable traps ospf cisco-specific state-change	Enables SNMP notifications for OSPF transition state changes.

snmp-server enable traps ospf cisco-specific errors shamlink

T o enable Simple Network Management Protocol (SNMP) notifications for Open Shortest Path First (OSPF) sham-link errors, use the **snmp-server enable traps ospf cisco-specific errors shamlink**command in global configuration mode. To disable OSPF sham-link error SNMP notifications, use the **no**form of this command.

snmp-server enable traps ospf cisco-specific errors shamlink [**authentication [bad-packet]** [**[config]**| **config [bad-packet]**]]

no snmp-server enable traps ospf cisco-specific errors shamlink [**authentication [bad-packet]** [**[config]**| **config [bad-packet]**]]

Syntax Description

authentication	(Optional) Enables SNMP notifications only for authentication failures on OSPF sham-link interfaces.
bad-packet	(Optional) Enables SNMP notifications only for packet parsing failures on OSPF sham-link interfaces.
config	(Optional) Enables SNMP notifications only for configuration mismatch errors on OSPF sham-link interfaces.

Command Default

This command is disabled by default; therefore, SNMP notifications for OSPF sham-link errors are not created.

Command Modes

Global configuration

Command History

Release	Modification
12.0(30)S	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

To enable the cospfShamLinkConfigError trap, you must first enter the **snmp-server enable traps ospf cisco-specific errors config-error** command in global configuration mode. The **snmp-server enable traps ospf cisco-specific errors config-error** command enables the cospfConfigError trap, so that both traps can

be generated at the same place and maintain consistency with a similar case for configuration errors across virtual links.

If you try to enable the cospfShamLinkConfigError trap before configuring the cospfospfConfigError trap you will receive an error message stating you must first configure the cospfConfigError trap.

Examples

The following example enables the router to send OSPF sham-link error notifications to the host at the address myhost.cisco.com using the community string defined as public:

```
Router(config)# snmp-server enable traps ospf cisco-specific errors config-error
Router(config)# snmp-server enable traps ospf cisco-specific errors shamlink
Router(config)# snmp-server host myhost.cisco.com informs version 2c public
```

Related Commands

Command	Description
snmp-server enable traps ospf cisco-specific errors config-error	Enables SNMP notifications for OSPF nonvirtual interface mismatch errors.
snmp-server enable traps ospf cisco-specific retransmit	Enables SNMP notifications for OSPF retransmission errors.
snmp-server enable traps ospf cisco-specific state-change	Enables SNMP notifications for OSPF transition state changes.

snmp-server enable traps ospf cisco-specific retransmit

T o enable Simple Network Management Protocol (SNMP) notifications for Open Shortest Path First (OSPF) retransmission errors, use the **snmp-server enable traps ospf cisco-specific retransmit**command in global configuration mode. To disable OSPF sham-link error SNMP notifications, use the **no**form of this command.

snmp-server enable traps ospf cisco-specific retransmit [**packets** [**shamlink**| **virt-packets**]| **shamlink** [**packets**| **virt-packets**]| **virt-packets [shamlink]**]

no snmp-server enable traps ospf cisco-specific retransmit [**packets** [**shamlink**| **virt-packets**]| **shamlink** [**packets**| **virt-packets**]| **virt-packets [shamlink]**]

Syntax Description

packets	(Optional) Enables SNMP notifications only for packet retransmissions on nonvirtual interfaces.
shamlink	(Optional) Enables SNMP notifications only for sham-link retransmission notifications.
virt-packets	(Optional) Enables SNMP notifications only for packet retransmissions on virtual interfaces.

Command Default

This command is disabled by default; therefore, SNMP notifications for OSPF retransmission errors are not created.

Command Modes

Global configuration

Command History

Release	Modification
12.3(5)	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.0(30)S	The **shamlink** keyword and related options were added.
12.3(14)T	Support was added for the **shamlink** keyword and related options.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

Release	Modification
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Examples

The following example enables the router to send OSPF sham-link retransmission notifications:

```
Router(config)# snmp-server enable traps ospf cisco-specific retransmit shamlink
```

Related Commands

Command	Description
snmp-server enable traps ospf cisco-specific errors config-error	Enables SNMP notifications for OSPF nonvirtual interface mismatch errors.
snmp-server enable traps ospf cisco-specific errors shamlink	Enables SNMP notifications for OSPF sham-link errors.
snmp-server enable traps ospf cisco-specific state-change	Enables SNMP notifications for OSPF transition state changes.



snmp-server enable traps ospf cisco-specific state-change through snmp-server enable traps voice poor-qov

- snmp-server enable traps ospf cisco-specific state-change, page 289
- snmp-server enable traps pim, page 291
- snmp-server enable traps power-ethernet group, page 293
- snmp-server enable traps pppoe, page 295
- snmp-server enable traps pppoe per-interface, page 297
- snmp-server enable traps pppoe per-mac, page 299
- snmp-server enable traps pppoe per-vc, page 301
- snmp-server enable traps pppoe per-vlan, page 303
- snmp-server enable traps pppoe system, page 305
- snmp-server enable traps pppoe vc, page 307
- snmp-server enable traps repeater, page 309
- snmp-server enable traps resource-policy, page 311
- snmp-server enable traps rtr, page 312
- snmp-server enable traps snmp, page 314
- snmp-server enable traps srp, page 317
- snmp-server enable traps storm-control, page 318
- snmp-server enable traps syslog, page 319
- snmp-server enable traps transceiver all, page 321
- snmp-server enable traps trustsec, page 322
- snmp-server enable traps trustsec-interface, page 324
- snmp-server enable traps trustsec-policy, page 326

- snmp-server enable traps trustsec-server, page 328
- snmp-server enable traps trustsec-sxp, page 330
- snmp-server enable traps voice, page 332
- snmp-server enable traps voice poor-qov, page 334
- snmp-server enable traps vswitch dual-active, page 335

snmp-server enable traps ospf cisco-specific state-change

T o enable Simple Network Management Protocol (SNMP) notifications for Open Shortest Path First (OSPF) transition state changes, use the **snmp-server enable traps ospf cisco-specific state-change**command in global configuration mode. To disable OSPF transition state change SNMP notifications, use the **no**form of this command.

snmp-server enable traps ospf cisco-specific state-change [**nssa-trans-change**| **shamlink** [**interface**| **interface-old**| **neighbor**]]

no snmp-server enable traps ospf cisco-specific state-change [**nssa-trans-change**| **shamlink** [**interface**| **interface-old**| **neighbor**]]

Syntax Description

nssa-trans-change	(Optional) Enables only not-so-stubby area (NSSA) translator state changes trap for the OSPF area.
shamlink	(Optional) Enables only the sham-link transition state changes trap for the OSPF area.
interface	(Optional) Enables only the sham-link interface state changes trap for the OSPF area.
interface -old	(Optional) Enables only the replaced interface transition state changes trap for the OSPF area.
neighbor	(Optional) Enables only the sham-link neighbor transition state changes trap for the OSPF area.

Command Default

This command is disabled by default; therefore, SNMP notifications for OSPF transition state changes are not created.

Command Modes

Global configuration

Command History

Release	Modification
12.3(5)	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.0(30)S	The **shamlink**, **interface-old**, and **neighbor** keywords were added.

Release	Modification
12.3(14)T	Support was added for the **shamlink**, **interface-old**, and **neighbor** keywords.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

You cannot enter both the **interface** and **interface-old** keywords because you cannot enable both the new and replaced sham-link interface transition state change traps. You can configure only one of the two traps, but not both.

Examples

The following example enables the router to send OSPF sham-link transition state change notifications to the host at the address myhost.cisco.com using the community string defined as public:

```
Router(config)# snmp-server enable traps ospf cisco-specific state-change shamlink
Router(config)# snmp-server host myhost.cisco.com informs version 2c public
```

Related Commands

Command	Description
snmp-server enable traps ospf cisco-specific errors config-error	Enables SNMP notifications for OSPF nonvirtual interface mismatch errors.
snmp-server enable traps ospf cisco-specific errors shamlink	Enables SNMP notifications for OSPF sham-link errors.
snmp-server enable traps ospf cisco-specific retransmit	Enables SNMP notifications for OSPF retransmission errors.

snmp-server enable traps pim

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

snmp-server enable traps pim [**neighbor-change**| **rp-mapping-change**| **invalid-pim-message**]

no snmp-server enable traps pim

Syntax Description

neighbor-change	(Optional) Enables notifications indicating when a router's PIM interface is disabled or enabled, or when a router's PIM neighbor adjacency expires.
rp-mapping-change	(Optional) Enables notifications indicating a change in the rendezvous point (RP) mapping information due to either Auto-RP or bootstrap router (BSR) messages.
invalid-pim-message	(Optional) Enables invalid PIM message traps. For example, an invalid PIM message could result when a router receives a join or prune message for which the RP specified in the packet is not the RP for the multicast group.

Command Default

SNMP notifications are disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests for the specified notification types. PIM notifications are defined in the CISCO-PIM-MIB.my and PIM-MIB.my files, available from Cisco.com at http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml .

Examples

The following example shows how to configure a router to generate notifications indicating that a PIM interface on the router has been enabled:

```
! Configure PIM traps to be sent as SNMPv2c traps to host with IP address 10.0.0.1.
Router(config)# snmp-server host 10.0.0.1 traps version 2c public pim

! Configure router to send the neighbor-change class of notifications to host.
Router(config)# snmp-server enable traps pim neighbor-change

! Enable PIM sparse-dense mode on Ethernet interface 0/0.
Router(config)# interface ethernet0/0

Router(config-if)# ip pim sparse-dense-mode
```

Related Commands

Command	Description
snmp-server enable traps	Enables all available SNMP notifications on your system.
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server trap-source	Specifies the interface from which an SNMP trap should originate.

snmp-server enable traps power-ethernet group

To configure the group containing the slot that is connected to a power Ethernet power source entity (PSE), use the **snmp-server enable traps power-ethernet group** command in global configuration mode. To disable the group, use the **no** form of this command.

snmp-server enable traps power-ethernet group *slot-number*

no snmp-server enable traps power-ethernet group *slot-number*

Syntax Description

slot-number	Integer that specifies the number of the group that contains the slot that is connected to a power Ethernet PSE. The range is from 1 to 4.

Command Default

Groups containing a slot that is connected to a PSE are not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(1)SY	This command was introduced.

Usage Guidelines

Enable the trap for the group to receive the trap generated from the interface of the slot.

Examples

The following example shows how to configure a group for the Ethernet PSE device:

```
Device> enable
Device# configure terminal
Device(config)# snmp-server enable traps power-ethernet group 2
Device(config)# end
```

Related Commands

Command	Description
power inline	Determines how inline power is applied to a device on the specified switch port.
show power inline	Displays the power status for a specified port or for all ports.

Command	Description
snmp-server trap-source	Specifies the interface (and hence the corresponding IP address) from which an SNMP trap originates.

snmp-server enable traps pppoe

To enable Point-to-Point Protocol over Ethernet (PPPoE) session count Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps pppoe**command in global configuration mode. To disable PPPoE session count SNMP notifications, use the **no**form of this command.

snmp-server enable traps pppoe

no snmp-server enable traps pppoe

Syntax Description

This command has no arguments or keywords.

Command Default

SNMP notifications are disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(1)DC	This command was introduced.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
Cisco IOS XE Release 2.5	This command was implemented on Cisco ASR 1000 series routers.

Usage Guidelines

This command enables SNMP traps only. It does not support inform requests.

To configure the PPPoE session-count thresholds at which SNMP notifications will be sent, use the **pppoe limit max-sessions** or **pppoe max-sessions** commands.

For a complete description of the SNMP notifications and additional MIB functions, see the CISCO-PPPOE-MIB.my file, available on Cisco.com at http://www.cisco.com/go/mibs

Examples

The following example enables the router to send PPPoE session-count SNMP notifications to the host at the address 192.0.2.0:

```
snmp-server community public RW
snmp-server enable traps pppoe
snmp-server host 192.0.2.0 version 2c public udp-port 1717
```

Related Commands

Command	Description
pppoe limit max-sessions	Sets the maximum number of PPPoE sessions that will be permitted on a router, and sets the PPPoE session-count threshold at which an SNMP trap will be generated.
pppoe max-sessions	Sets the maximum number of PPPoE sessions that will be permitted on an ATM PVC, PVC range, VC class, or VLAN, and sets the PPPoE session-count threshold at which an SNMP trap will be generated.
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server trap-source	Specifies the interface from which an SNMP trap should originate.

snmp-server enable traps pppoe per-interface

To enable PPP over Ethernet (PPPoE) session count Simple Network Management Protocol (SNMP) notifications on an interface trap, use the **snmp-server enable traps pppoe per-interface** command in global configuration mode. To disable PPPoE session count SNMP notifications on an interface trap, use the **no** form of this command.

snmp-server enable traps pppoe per-interface [loss-percent | loss-threshold]

no snmp-server enable traps pppoe per-interface [loss-percent | loss-threshold]

Syntax Description

loss-percent	(Optional) Enables the per-interface loss-percent trap.
loss-threshold	(Optional) Enables the per-interface loss-threshold trap.

Command Default

PPPoE session count SNMP notifications are disabled on an interface trap.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(2)S	This command was introduced.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. The **snmp-server enable traps pppoe per-interface** command enables traps and inform requests for the specified notification types. A notification for this command indicates that the percentage of PPPoE sessions lost has crossed the configured threshold value for a particular interface.

Examples

The following example shows how to enable PPPoE session count SNMP notifications on a per-interace loss-percent trap:

```
Device(config)# snmp-server enable traps pppoe per-interface loss-percent
```

Related Commands

Command	Description
snmp-server enable traps pppoe per-mac	Enables PPPoE session count SNMP notifications for a node with MAC address traps.

Command	Description
snmp-server enable traps pppoe per-vc	Enables PPPoE session count SNMP notifications for a VC trap.
snmp-server enable traps pppoe per-vlan	Enables PPPoE session count SNMP notifications on a VLAN trap.
snmp-server enable traps pppoe session	Enables PPPoE session count SNMP notifications for a session trap.
snmp-server enable traps pppoe vc	Enables PPPoE session count SNMP notifications for all VC traps between nodes.

snmp-server enable traps pppoe per-mac

To enable PPP over Ethernet (PPPoE) session count Simple Network Management Protocol (SNMP) notifications for a node with MAC address traps, use the **snmp-server enable traps pppoe per-mac** command in global configuration mode. To disable PPPoE session count SNMP notifications for a node with MAC address traps, use the **no** form of this command.

snmp-server enable traps pppoe per-mac [limit | throttle]

no snmp-server enable traps pppoe per-mac [limit | throttle]

Syntax Description

limit	(Optional) Enables the per-MAC limit trap.
throttle	(Optional) Enables the per-MAC throttle trap.

Command Default

PPPoE session count SNMP notifications are disabled for a node with MAC address traps.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(2)S	This command was introduced.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. The **snmp-server enable traps pppoe per-mac** command enables both traps and inform requests for the specified notification types. A notification for this command indicates that the number of active sessions from a particular client Ethernet MAC address has reached the configured per-MAC limit.

Examples

The following example shows how to enable PPPoE session count SNMP notifications for a node with per-MAC limit traps:

```
Device(config)# snmp-server enable traps pppoe per-mac limit
```

Related Commands

Command	Description
snmp-server enable traps pppoe per-interface	Enables PPPoE session count SNMP notifications on an interface trap.
snmp-server enable traps pppoe per-vc	Enables PPPoE session count SNMP notifications for a VC trap.

Command	Description
snmp-server enable traps pppoe per-vlan	Enables PPPoE session count SNMP notifications on a VLAN trap.
snmp-server enable traps pppoe session	Enables PPPoE session count SNMP notifications for a session trap.
snmp-server enable traps pppoe vc	Enables PPPoE session count SNMP notifications for all VC traps between nodes.

snmp-server enable traps pppoe per-vc

To enable PPP over Ethernet (PPPoE) session count Simple Network Management Protocol (SNMP) notifications for a virtual connection (VC) trap, use the **snmp-server enable traps pppoe per-vc** command in global configuration mode. To disable PPPoE session count SNMP notifications for a VC trap, use the **no** form of this command.

snmp-server enable traps pppoe per-vc [limit | throttle]

no snmp-server enable traps pppoe per-vc [limit | throttle]

Syntax Description

limit	(Optional) Enables a per-VC limit trap.
throttle	(Optional) Enables a per-VC throttle trap.

Command Default

PPPoE session count SNMP notifications are disabled for a VC trap.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(2)S	This command was introduced.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. The **snmp-server enable traps pppoe per-vc** command enables traps and inform requests for the specified notification types. A notification for this command indicates the number of active sessions for a ATM VCI/VPI that has crossed the configured maximum limit.

Examples

The following example shows how to enable PPPoE session count SNMP notifications on a per-VC limit trap:

```
Device(config)# snmp-server enable traps pppoe per-vc limit
```

Related Commands

Command	Description
snmp-server enable traps pppoe per-interface	Enables PPPoE session count SNMP notifications on an interface trap.
snmp-server enable traps pppoe per-mac	Enables PPPoE session count SNMP notifications for a node with MAC address traps.

Command	Description
snmp-server enable traps pppoe per-vlan	Enables PPPoE session count SNMP notifications on a VLAN trap.
snmp-server enable traps pppoe session	Enables PPPoE session count SNMP notifications for a session trap.
snmp-server enable traps pppoe vc	Enables PPPoE session count SNMP notifications for all VC traps between nodes.

snmp-server enable traps pppoe per-vlan

To enable PPP over Ethernet (PPPoE) session count Simple Network Management Protocol (SNMP) notifications on a VLAN trap, use the **snmp-server enable traps pppoe per-vlan** command in global configuration mode. To disable PPPoE session count SNMP notifications on a VLAN trap, use the **no** form of this command.

snmp-server enable traps pppoe per-vlan [limit | throttle]

no snmp-server enable traps pppoe per-vlan [limit | throttle]

Syntax Description

limit	(Optional) Enables a per-VLAN limit trap.
throttle	(Optional) Enables a per-VLAN throttle trap.

Command Default

PPPoE session count SNMP notifications are disabled on a VLAN trap.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(2)S	This command was introduced.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. The **snmp-server enable traps pppoe per-vlan** command enables traps and inform requests for the specified notification types. A notification for this command indicates the number of new PPPoE session requests coming on a particular VLAN over a configured time interval that has reached the rate limit.

Examples

The following example shows how to enable PPPoE session count SNMP notifications on a per-VLAN limit trap:

```
Device(config)# snmp-server enable traps pppoe per-vlan limit
```

Related Commands

Command	Description
snmp-server enable traps pppoe per-interface	Enables PPPoE session count SNMP notifications on an interface trap.
snmp-server enable traps pppoe per-mac	Enables PPPoE session count SNMP notifications for a node with MAC address traps.

Command	Description
snmp-server enable traps pppoe per-vc	Enables PPPoE session count SNMP notifications for a VC trap.
snmp-server enable traps pppoe session	Enables PPPoE session count SNMP notifications for a system trap.
snmp-server enable traps pppoe vc	Enables PPPoE session count SNMP notifications for all VC traps between nodes.

snmp-server enable traps pppoe system

To enable PPP over Ethernet (PPPoE) session count Simple Network Management Protocol (SNMP) notifications on a system trap, use the **snmp-server enable traps pppoe system** command in global configuration mode. To disable PPPoE session count SNMP notifications on a system trap, use the **no** form of this command.

snmp-server enable traps pppoe system [loss-percent | loss-threshold | threshold]

no snmp-server enable traps pppoe system [loss-percent | loss-threshold | threshold]

Syntax Description

loss-percent	(Optional) Enables the session loss-percent trap.
loss-threshold	(Optional) Enables the session loss-threshold trap.
threshold	(Optional) Enables the session threshold trap.

Command Default

PPPoE session count SNMP notifications are disabled on a system trap.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(2)S	This command was introduced.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. The **snmp-server enable traps pppoe system** command enables traps and inform requests for the specified notification types. A notification for this command indicates the percentage of PPPoE session lost globally over a period of time that has crossed the configured threshold.

Examples

The following example shows how to enable PPPoE session count SNMP notifications on a system loss-percent trap:

```
Device(config)# snmp-server enable traps pppoe system loss-percent
```

Related Commands

Command	Description
snmp-server enable traps pppoe per-interface	Enables PPPoE session count SNMP notifications on an interface trap.

Command	Description
snmp-server enable traps pppoe per-mac	Enables PPPoE session count SNMP notifications for a node with MAC address traps.
snmp-server enable traps pppoe per-vc	Enables PPPoE session count SNMP notifications for a VC trap.
snmp-server enable traps pppoe per-vlan	Enables PPPoE session count SNMP notifications on a VLAN trap.
snmp-server enable traps pppoe vc	Enables PPPoE session count SNMP notifications for all VC traps between nodes.

snmp-server enable traps pppoe vc

To enable PPP over Ethernet (PPPoE) session count Simple Network Management Protocol (SNMP) notifications on all virtual connection (VC) traps between nodes, use the **snmp-server enable traps pppoe vc** command in global configuration mode. To disable PPPoE session count SNMP notifications on all VC traps between nodes, use the **no** form of this command.

snmp-server enable traps pppoe vc [threshold]

no snmp-server enable traps pppoe vc [threshold]

Syntax Description

threshold	(Optional) Enables a VC threshold trap.

Command Default

PPPoE session count SNMP notifications are disabled on all VC traps between nodes.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(2)S	This command was introduced.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. The **snmp-server enable traps pppoe vc** command enables traps and inform requests for the specified notification types. A notification for this command indicates the number of active sessions for a ATM VCI/VPI that has crossed the configured maximum limit on a VC interface.

Examples

The following example shows how to enable PPPoE session count SNMP notifications on a VC threshold trap:

```
Device(config)# snmp-server enable traps pppoe vc threshold
```

Related Commands

Command	Description
snmp-server enable traps pppoe per-interface	Enables PPPoE session count SNMP notifications for an interface trap.
snmp-server enable traps pppoe per-mac	Enables PPPoE session count SNMP notifications for a node with MAC address traps.

Command	Description
snmp-server enable traps pppoe per-vc	Enables PPPoE session count SNMP notifications for a VC trap.
snmp-server enable traps pppoe per-vlan	Enables PPPoE session count SNMP notifications on a VLAN trap.
s**nmp-server enable traps pppoe per-system**	Enables PPPoE session count SNMP notifications for a session trap.

snmp-server enable traps repeater

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

snmp-server enable traps repeater [health] [reset]

no snmp-server enable traps repeater [health] [reset]

Syntax Description

health	(Optional) Enables the rptrHealth trap, which conveys information related to the operational status of the repeater.
reset	(Optional) Sends the rptrResetEvent trap on completion of a repeater reset action (triggered by the transition to a START state by a manual command).

Command Default

SNMP notifications are disabled.

If no option keywords are specified when entering this command, all repeater notifications available on your system are enabled or disabled.

Command Modes

Global configuration

Command History

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

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests.

This command enables or disables Repeater MIB notifications, as defined in RFC 1516. RFC 1516 defines objects for managing IEEE 802.3 10 Mbps baseband repeaters, also known as hubs.

Two sets of notifications are available for this command. The following notification is defined in the CISCO-REPEATER-MIB (enterprise 1.3.6.1.4.1.9.9.22.3):

- 1 ciscoRptrIllegalSrcAddrTrap (illegal source address trap)

The following notifications are defined in the CISCO-REPEATER-MIB-V1SMI (enterprise 1.3.6.1.2.1.22):

- 1 rptrHealth
- 2 rptrGroupChange
- 3 rptrResetEvent

For a complete description of the repeater notifications and additional MIB functions, refer to the CISCO-REPEATER-MIB.my and CISCO-REPEATER-MIB-V1SMI.my files, available on Cisco.com at

http://www.cisco.com/public/mibs/ .

When the optional **health** keyword is used, the rptrHealth trap is sent when the value of rptrOperStatus changes, or upon completion of a nondisruptive test.

The rptrOperStatus object indicates the operational state of the repeater. Status values are as follows:

- other(1)--undefined or unknown status
- ok(2)--no known failures
- rptrFailure(3)--repeater-related failure
- groupFailure(4)--group-related failure
- portFailure(5)--port-related failure
- generalFailure(6)--failure, unspecified type

When the optional **reset** keyword is used, the rptrResetEvent trap is not sent when the agent restarts and sends an SNMP coldStart or warmStart trap.

The **snmp-server enable traps repeater**command is used in conjunction with the **snmp-server host**command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send SNMP notifications, you must configure at least one **snmp-server host**command.

Examples

The following example shows how to enable the router to send repeater inform notifications to the host at the address myhost.cisco.com using the community string defined as public:

```
Router(config)# snmp-server enable traps repeater
Router(config)# snmp-server host myhost.cisco.com informs version 2c public
```

Related Commands

Command	Description
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server trap-source	Specifies the interface that an SNMP trap should originate from.

snmp-server enable traps resource-policy

To enable Embedded Resource Manager (ERM)-MIB notification traps, use the **snmp-server enable traps resource-policy** command in global configuration mode. To disable the ERM-MIB notification traps, use the **no** form of this command.

snmp-server enable traps resource-policy

no snmp-server enable traps resource-policy

Syntax Description

This command has no arguments or keywords.

Command Default

Notification traps will be sent to the host that is configured to receive traps.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Examples

The following example shows how to configure the router to send SNMP notifications for ERM to a host:

```
Router(config)# snmp-server enable traps resource policy
```

Related Commands

Command	Description
snmp-server community	Permits access to SNMP by setting up the community access string.
snmp-server host	Specifies the recipient of an SNMP notification message.

snmp-server enable traps rtr

To enable the sending of Cisco IOS IP Service Level Agreements (SLAs) Simple Network Management Protocol (SNMP) trap notifications, use the **snmp-server enable traps rtr**command in global configuration mode. To disable IP SLAs SNMP notifications, use the **no**form of this command.

snmp-server enable traps rtr

no snmp-server enable traps rtr

Syntax Description

This command has no arguments or keywords.

Command Default

SNMP notifications are disabled by default.

Command Modes

Global configuration

Command History

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

Usage Guidelines

This command controls (enables or disables) Cisco IOS IP SLAs notifications, as defined in the Response Time Monitor MIB (CISCO-RTTMON-MIB).

The **snmp-server enable traps rtr**command is used in conjunction with the **snmp-server host**command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send SNMP notifications, you must configure at least one **snmp-server host** command.

Examples

The following example shows how to enable the router to send IP SLAs SNMP traps to the host at the address myhost.cisco.com using the community string defined as public:

```
snmp-server enable traps rtr
snmp-server host myhost.cisco.com informs version 2c public rtr
```

Related Commands

Command	Description
ip sla monitor	Begins configuration for an IP SLAs operation and enters IP SLA monitor configuration mode.

Command	Description
ip sla	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.
snmp-server host	Specifies the destination NMS and transfer parameters for SNMP notifications.
snmp-server trap-source	Specifies the interface that an SNMP trap should originate from.

snmp-server enable traps snmp

To enable the RFC 1157 Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps snmp**command in global configuration mode. To disable RFC 1157 SNMP notifications, use the **no**form of this command.

snmp-server enable traps snmp [authentication] [linkup] [linkdown] [coldstart] [warmstart]

no snmp-server enable traps snmp [authentication] [linkup] [linkdown] [coldstart] [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.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.3	The **snmp-server enable traps snmp authentication** command was introduced. This command replaced the **snmp-server trap-authentication** command.
12.1(3)T	The following keywords were added: • **linkup** • **linkdown** • **coldstart**
12.1(5)T	The **warmstart** keyword was added.

Release	Modification
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests for the specified notification types.

If you do not enter an **snmp-server enable traps snmp**command, no notifications controlled by this command are sent. To configure the router to send these SNMP notifications, you must enter at least one **snmp-server enable traps snmp**command. When you enter the command with no keywords, all notification types are enabled. When you enter the command with a keyword, only the types of notifications related to that keyword are enabled.

When you use the optional **authentication**keyword, the authenticationFailure(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 SNMPv2c, authentication failure occurs for packets with an incorrect community string and the SNMP traps are generated. For SNMPv3, authentication failure occurs for packets with an incorrect SHA/MD5 authentication key or for a packet that is outside the authoritative SNMP engine's window (for example, packets that are configured outside access lists or time ranges) and a report PDU is generated, however authentication failure traps are not generated.

When you use the optional **linkup**keyword, the linkUp(3) trap signifies that the sending device recognizes one of the communication links represented in the agent's configuration coming up.

When you use the optional **linkdown**keyword, 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 enable traps snmp** [**linkup**] [**linkdown**] form of this command globally enables or disables SNMP linkUp and linkDown traps. After enabling either of these traps globally, you can disable them on specific interfaces using the **no snmp trap link-status** command in interface configuration mode. On the interface level, linkUp and linkDown traps are enabled by default, which means that these notifications do not have to be enabled on a per-interface basis. However, linkUp and linkDown notifications will not be sent unless you enable them globally using the **snmp-server enable traps snmp** command.

When you use the optional **coldstart**keyword, 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.

When you use the optional **warmstart**keyword, 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.

The **snmp-server enable traps snmp**command is used in conjunction with the **snmp-server host**command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. In order to send notifications, you must configure at least one **snmp-server host**command.

For a host to receive a notification controlled by this command, you must enable both the **snmp-server enable traps** command and the **snmp-server host**command for that host. If the notification type is not controlled by this command, you must enable the appropriate **snmp-server host** command only.

Examples

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

```
Router(config)# snmp-server enable traps snmp
Router(config)# snmp-server host myhost.cisco.com public snmp
```

The following example shows how to enable the router to send all inform notifications to the host myhost.cisco.com using the community string public:

```
Router(config)# snmp-server enable traps snmp
Router(config)# snmp-server host myhost.cisco.com informs version 2c public snmp
```

The following example shows how to enable all SNMP trap types, and then disable only the linkUp and linkDown traps:

```
Router> enable
Router# configure terminal
Router(config)# snmp-server enable traps snmp
Router(config)# end
Router# more system:running-config | include traps snmp
snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart
Router# configure terminal
Router(config)# no snmp-server enable traps snmp linkup linkdown
Router(config)# end
Router# more system:running-config | include traps snmp
snmp-server enable traps snmp authentication coldstart warmstart
```

Related Commands

Command	Description
snmp-server enable traps	Enables all available SNMP notifications on your system.
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server informs	Specifies inform request options.
snmp-server trap authentication vrf	Disables or reenables SNMP authentication notifications specific to VPN context mismatches.
snmp-server trap-source	Specifies the interface that an SNMP trap should originate from.

snmp-server enable traps srp

To enable the sending of Intelligent Protection Switching (IPS) Spatial Reuse Protocol (SRP) Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps srp** command in global configuration mode. To disable SRP notifications, use the **no** form of this command.

snmp-server enable traps srp

no snmp-server enable traps srp

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.2(13)T	This command was introduced to support DPT-OC12 Port Adapters.

Usage Guidelines

The Cisco SRP MIB module (CISCO-SRP-MIB.my) provides objects for monitoring IP-over-SONET IPS SRP traffic using the SNMP. When IPS is enabled, if a node or fiber facility failure is detected, traffic going toward or coming from the failure direction is wrapped (looped) back to go in opposite direction on the other ring.

The **snmp-server enable traps srp** command enables SRP state change notifications (traps or informs). SRP state change notifications are generated whenever one of the two sides of an SRP interface ring enters or leaves the wrapped state (when a ring wraps, or when a ring is restored).

Specifically, the srpMACIpsWrapCounter object in the CISCO-SRP-MIB increments when a Ring wraps, and the value of the rpMACIpsLastUnWrapTimeStamp object changes when a ring unwraps. (An “unwrap” event happens when the original ring is restored.)

The **snmp-server enable traps srp** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send SNMP notifications, you must configure at least one **snmp-server host** command.

Examples

In the following example, SRP-specific informs are enabled and will be sent to the host “myhost.cisco.com” using the community string defined as public:

```
Router(config)# snmp-server enable traps srp
Router(config)# snmp-server host myhost.cisco.com informs version 2c public srp
```

snmp-server enable traps storm-control

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

snmp-server enable traps storm-control traps-rate num

no snmp-server enable traps storm-control traps-rate num

Syntax Description

traps-rate *num*	Number of traps per minute; valid values are 0 through 1000.

Command Default

Storm-control traps are disabled.

Command Modes

Configuration mode (config)

Command History

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

Examples

This example shows how to enable the storm-control trap notification trap rate to 250:

```
Router# snmp-server enable traps storm control traps-rate 250
Router#
```

Related Commands

Command	Description
snmp-server enable traps storm-control	Enables SNMP storm-control trap notifications.
snmp-server host	Specifies the recipient of an SNMP notification operation.
test snmp trap storm-control	Tests the SNMP CISCO-PORT-STORM-CONTROL-MIB traps.

snmp-server enable traps syslog

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

snmp-server enable traps syslog

no snmp-server enable traps syslog

Syntax Description

This command has no arguments or keywords.

Command Default

SNMP notifications are disabled.

Command Modes

Global configuration

Command History

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

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests.

This command controls (enables or disables) system logging message notifications. System logging messages (also called system error messages, or syslog messages) are status notification messages that are generated by the routing device during operation. These messages are typically logged to a destination (such as the terminal screen, to a system buffer, or to a remote “syslog” host).

If your software image supports the Cisco Syslog MIB, these messages can also be sent via SNMP to a network management station (NMS). To determine which software images support the Cisco Syslog MIB, used the Cisco MIB Locator tool at http://www.cisco.com/go/mibs/ .(At the time of writing, the Cisco Syslog MIB is only supported in “Enterprise” images.)

Unlike other logging processes on the system, debug messages (enabled using CLI debug commands) are not included with the logging messages sent via SNMP.

To specify the severity level at which notifications should be generated, use the **logging history** global configuration command. For additional information about the system logging process and severity levels, see the description of the **logging** commands.

The syslog notification is defined by the clogMessageGenerated NOTIFICATION-TYPE object in the Cisco Syslog MIB (CISCO-SYSLOG-MIB.my). When a syslog message is generated by the device a clogMessageGenerated notification is sent to the designated NMS. The clogMessageGenerated notification includes the following objects: clogHistFacility, clogHistSeverity, clogHistMsgName, clogHistMsgText, clogHistTimestamp.

For a complete description of these objects and additional MIB information, see the text of CISCO-SYSLOG-MIB.my, available on Cisco.com using the SNMP Object Navigator tool at http://www.cisco.com/go/mibs . See also the CISCO-SYSLOG-EXT-MIB and the CISCO-SYSLOG-EVENT-EXT-MIB.

The **snmp-server enable traps syslog**command is used in conjunction with the **snmp-server host**command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send SNMP notifications, you must configure at least one **snmp-server host** command.

Examples

The following example enables the router to send system logging messages at severity levels 0 (emergencies) through 2 (critical) to the host at the address myhost.cisco.com using the community string defined as public:

```
Router(config)# snmp-server enable traps syslog
Router(config)# logging history 2
Router(config)# snmp-server host myhost.cisco.com traps version 2c public
```

Related Commands

Command	Description
logging history	Limits syslog messages sent to the router's history table and to an SNMP NMS based on severity.
snmp-server host	Specifies the destination NMS and transfer parameters for SNMP notifications.
snmp-server trap-source	Specifies the interface that an SNMP trap should originate from.

snmp-server enable traps transceiver all

To enable all supported SNMP transceiver traps for all transceiver types in the global configuration mode, use the **snmp-server enable traps transceiver all**command. Use the **no** form of this command to disable the transceiver SNMP trap notifications.

snmp-server enable traps transceiver all

no snmp-server enable traps transceiver all

Syntax Description

The command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXE	Support for this command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The **snmp-server enable 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. To send notifications, you must configure at least one **snmp-server host** command.

Examples

This example shows how to enable all supported SNMP transceiver traps for all transceiver types:

```
Router(config)# snmp-server enable traps
 transceiver all
Router(config)#
```

Related Commands

Command	Description
show interfaces transceiver	Displays information about the optical transceivers that have DOM enabled.

snmp-server enable traps trustsec

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

snmp-server enable traps trustsec [**authz-file-error**| **cache-file-error**| **keystore-file-error**| **keystore-sync-fail**| **random-number-fail**| **src-entropy-fail**]

no snmp-server enable traps trustsec [**authz-file-error**| **cache-file-error**| **keystore-file-error**| **keystore-sync-fail**| **random-number-fail**| **src-entropy-fail**]

Syntax Description

authz-file-error	(Optional) Enables SNMP ctsAuthzCacheFileErrNotif notifications.
cache-file-error	(Optional) Enables SNMP ctsCacheFileAccessErrNotif notifications.
keystore-file-error	(Optional) Enables SNMP ctsSwKeystoreFileErrNotif notifications.
keystore-sync-fail	(Optional) Enables SNMP ctsSwKeystoreSyncFailNotif notifications.
random-number-fail	(Optional) Enables SNMP ctsSapRandomNumberFailNotif notifications.
src-entropy-fail	(Optional) Enables SNMP ctsSrcEntropyFailNotif notifications.

Command Default

SNMP notifications are disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(1)SY	This command was introduced.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. The **snmp-server enable traps trustsec** command enables both traps and inform requests.

This command enables or disables CISCO-TRUSTSEC-MIB notifications.

Examples

This example shows how to enable SNMP ctsAuthzCacheFileErrNotif notifications:

```
Device(config)# snmp-server enable traps trustsec authz-file-error
```

This example shows how to enable SNMP ctsCacheFileAccessErrNotif notifications;

```
Device(config)# snmp-server enable traps trustsec cache-file-error
```

This example shows how to enable SNMP ctsSwKeystoreFileErrNotif notifications:

```
Device(config)# snmp-server enable traps trustsec keystore-file-error
```

This example shows how to enable SNMP ctsSwKeystoreSyncFailNotif notifications;

```
Device(config)# snmp-server enable traps trustsec keystore-sync-fail
```

This example shows how to enable SNMP ctsSapRandomNumberFailNotif notifications:

```
Device(config)# snmp-server enable traps trustsec random-number-fail
```

This example shows how to enable SNMP ctsSrcEntropyFailNotif notifications:

```
Device(config)# snmp-server enable traps trustsec src-entropy-fail
```

Related Commands

Command	Description
test snmp trap trustsec	Tests SNMP trustsec notification traps and informs.

snmp-server enable traps trustsec-interface

To enable CISCO-TRUSTSEC-INTERFACE-MIB Simple Network Management Protocol (SNMP) notifications (traps and informs), use the **snmp-server enable traps trustsec-interface** command in global configuration mode. To disable trustsec-interface notifications, use the **no** form of this command.

snmp-server enable traps trustsec-interface [**authc-fail**| **authz-fail**| **sap-fail**| **supplicant-fail**| **unauthorized**]

no snmp-server enable traps trustsec-interface [**authc-fail**| **authz-fail**| **sap-fail**| **supplicant-fail**| **unauthorized**]

Syntax Description

authc-fail	(Optional) Enables SNMP ctsiIfAuthenticationFailNotif notifications.
authz-fail	(Optional) Enables SNMP ctsiAuthorizationFailNotif notifications.
sap-fail	(Optional) Enables SNMP ctsiIfSapNegotiationFailNotif notifications.
supplicant-fail	(Optional) Enables SNMP ctsiIfAddSupplicantFailNotif notifications.
unauthorized	(Optional) Enables SNMP ctsiIfUnauthorizedNotifEnable notifications.

Command Default

SNMP notifications are disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(1)SY	This command was introduced.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. The **snmp-server enable traps trustsec-interface** command enables both traps and inform requests.

This command enables or disables CISCO-TRUSTSEC-INTERFACE-MIB notifications.

Examples

This example shows how to enable SNMP ctsiIfAuthenticationFailNotif notifications:

```
Device(config)# snmp-server enable traps trustsec-interface authc-fail
```

This example shows how to enable SNMP ctsiAuthorizationFailNotif notifications:

```
Device(config)# snmp-server enable traps trustsec-interface authz-fail
```

This example shows how to enable SNMP ctsiIfSapNegotiationFailNotif notifications:

```
Device(config)# snmp-server enable traps trustsec-interface sap-fail
```

This example shows how to enable SNMP ctsiIfAddSupplicantFailNotif notifications:

```
Device(config)# snmp-server enable traps trustsec-interface supplicant-fail
```

This example shows how to enable SNMP ctsiIfUnauthorizedNotifEnable notifications:

```
Device(config)# snmp-server enable traps trustsec-interface unauthorized
```

Related Commands

Command	Description
test snmp trap trustsec-interface	Tests SNMP trustsec-interface notification traps and informs.

snmp-server enable traps trustsec-policy

To enable CISCO-TRUSTSEC-POLICY-MIB Simple Network Management Protocol (SNMP) notifications (traps and informs), use the **snmp-server enable traps trustsec-policy** command in global configuration mode. To disable trustsec-policy notifications, use the **no** form of this command.

snmp-server enable traps trustsec-policy [**authz-sgacl-fail**| **peer-policy-updated**]

no snmp-server enable traps trustsec-policy [**authz-sgacl-fail**| **peer-policy-updated**]

Syntax Description

authz-sgacl-fail	(Optional) Enables SNMP ctspAuthorizationSgaclFailNotif notifications.
peer-policy-updated	(Optional) Enables SNMP ctspPeerPolicyUpdatedNotif notifications.

Command Default

SNMP notifications are disabled.

Command Modes

Global configuration(config)

Command History

Release	Modification
15.1(1)SY	This command was introduced.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. The **snmp-server enable traps trustsec-policy** command enables both traps and inform requests.

This command enables or disables CISCO-TRUSTSEC-POLICY-MIB notifications.

Examples

This example shows how to enable SNMP ctspAuthorizationSgaclFailNotif notifications:

```
Device(config)# snmp-server enable traps trustsec-policy authz-sgacl-fail
```

This example shows how to enable SNMP ctspPeerPolicyUpdatedNotif notifications:

```
Device(config)# snmp-server enable traps trustsec-policy peer-policy-updated
```

Related Commands

Command	Description
test snmp trap trustsec-policy	Tests SNMP trustsec-policy notification traps and informs.

snmp-server enable traps trustsec-server

To enable CISCO-TRUSTSEC-SERVER-MIB Simple Network Management Protocol (SNMP) notifications (traps and informs), use the **snmp-server enable traps trustsec-server** command in global configuration mode. To disable trustsec-server notifications, use the **no** form of this command.

snmp-server enable traps trustsec-server [**provision-secret**| **radius-server**]

no snmp-server enable traps trustsec-server [**provision-secret**| **radius-server**]

Syntax Description

provision-secret	(Optional) Enables SNMP ctsvNoProvisionSecretNotif notifications.
radius-server	(Optional) Enables SNMP ctsvNoRadiusServerNotif notifications.

Command Default

SNMP notifications are disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(1)SY	This command was introduced.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. The **snmp-server enable traps trustsec-server** command enables both traps and inform requests.

This command enables or disables CISCO-TRUSTSEC-SERVER-MIB notifications.

Examples

This example shows how to enable SNMP ctsvNoProvisionSecretNotif notifications:

```
Device(config)# snmp-server enable traps trustsec-server provision-secret
```

This example shows how to enable SNMP ctsvNoRadiusServerNotif notifications:

```
Device(config)# snmp-server enable traps trustsec-server radius-server
```

Related Commands

Command	Description
test snmp trap trustsec-server	Tests SNMP trustsec-server notification traps and informs.

snmp-server enable traps trustsec-sxp

To enable CISCO-TRUSTSEC-SXP-MIB Simple Network Management Protocol (SNMP) notifications (traps and informs), use the **snmp-server enable traps trustsec-sxp** command in global configuration mode. To disable trustsec-sxp notifications, use the **no** form of this command.

snmp-server enable traps trustsec-sxp [**binding-conflict**| **binding-err**| **binding-expn-fail**| **conn-config-err**| **conn-down**| **conn-srcaddr-err**| **conn-up**| **msg-parse-err**| **oper-nodeid-change**]

no snmp-server enable traps trustsec-sxp [**binding-conflict**| **binding-err**| **binding-expn-fail**| **conn-config-err**| **conn-down**| **conn-srcaddr-err**| **conn-up**| **msg-parse-err**| **oper-nodeid-change**]

Syntax Description

binding-conflict	(Optional) Enables SNMP ctsxSxpBindingConflictNotif notifications.
binding-err	(Optional) Enables SNMP ctsxSxpBindingErrNotif notifications.
binding-expn-fail	(Optional) Enables SNMP ctsxSxpBindingExpnFailNotif notifications.
conn-config-err	(Optional) Enables SNMP ctsxSxpConnConfigErrNotif notifications.
conn-down	(Optional) Enables SNMP ctsxSxpConnDownNotif notifications.
conn-srcaddr-err	(Optional) Enables SNMP ctsxSxpConnSourceAddrErrNotif notifications.
conn-up	(Optional) Enables SNMP ctsxSxpConnUpNotif notifications.
msg-parse-err	(Optional) Enables SNMP ctsxSxpMsgParseErrNotif notifications.
oper-nodeid-change	(Optional) Enables SNMP ctsxSxpOperNodeIdChangeNotif notifications.

Command Default

SNMP notifications are disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(1)SY	This command was introduced.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. The **snmp-server enable traps trustsec-sxp** command enables both traps and inform requests.

This command enables or disables CISCO-TRUSTSEC-SXP-MIB notifications.

Examples

This example shows how to enable SNMP ctsxSxpBindingConflictNotif notifications:

```
Device(config)# snmp-server enable traps trustsec-sxp binding-conflict
```

This example shows how to enable SNMP ctsxSxpBindingErrNotif notifications:

```
Device(config)# snmp-server enable traps trustsec-sxp binding-err
```

This example shows how to enable SNMP ctsxSxpBindingExpnFailNotif notifications:

```
Device(config)# snmp-server enable traps trustsec-sxp binding-expn-fail
```

This example shows how to enable SNMP ctsxSxpConnConfigErrNotif notifications:

```
Device(config)# snmp-server enable traps trustsec-sxp conn-config-err
```

This example shows how to enable SNMP ctsxSxpConnDownNotif notifications:

```
Device(config)# snmp-server enable traps trustsec-sxp conn-down
```

This example shows how to enable SNMP ctsxSxpConnSourceAddrErrNotif notifications:

```
Device(config)# snmp-server enable traps trustsec-sxp conn-srcaddr-err
```

This example shows how to enable SNMP ctsxSxpConnUpNotif notifications:

```
Device(config)# snmp-server enable traps trustsec-sxp conn-up
```

This example shows how to enable SNMP ctsxSxpMsgParseErrNotif notifications:

```
Device(config)# snmp-server enable traps trustsec-sxp msg-parse-err
```

This example shows how to enable SNMP ctsxSxpOperNodeIdChangeNotif notifications:

```
Device(config)# snmp-server enable traps trustsec oper-nodeid-change
```

Related Commands

Command	Description
test snmp trap trustsec-sxp	Tests SNMP trustsec-sxp notification traps and informs.

snmp-server enable traps voice

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

snmp-server enable traps voice [poor-qov] [fallback]

no snmp-server enable traps voice

Syntax Description

poor-qov	(Optional) Enables poor-quality-of-voice SNMP notifications.
fallback	(Optional) Enables SNMP fallback voice notifications.

Command Default

If you enter this command without any of the optional keywords, both available notifications are enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.3(14)T	The **fallback** keyword was added.

Usage Guidelines

SNMP notifications can be sent as traps (notifications) or inform requests. This command enables both traps and inform requests.

The **poor-qov** keyword enables or disables poor-quality-of-voice notifications. The poor quality-of-voice notification is defined in CISCO-VOICE-DIAL-CONTROL-MIB as follows:

enterprise 1.3.6.1.4.1.9.9.63.2

(1) cvdcPoorQoVNotification

The **fallback** keyword enables or disables public switched telephone network (PSTN) fallback notifications. The fallback notification is defined in CISCO-VOICE-DIAL-CONTROL-MIB as follows:

(1) cvVoIPCallHistoryConnectionId

(2) cvVoIPCallHistoryFallbackIcpif

(2) cvVoIPCallHistoryFallbackLoss

(3) cvVoIPCallHistoryFallbackDelay

(4) cvVoIPCallHistoryRemSigIPAddrT

(5) cvVoIPCallHistoryRemSigIPAddr

(6) cvVoIPCallHistoryRemMediaIPAddrT

(7) cvVoIPCallHistoryRemMediaIPAddr

(8) cCallHistoryCallOrigin

(9) cvCommonDcCallHistoryCoderTypeRate

For a complete description of these notifications and additional MIB functions, see the CISCO-VOICE-DIAL-CONTROL-MIB.my file, available on Cisco.com at http://www.cisco.com/go/mibs .

The **snmp-server enable traps voice**command is used in conjunction with the **snmp-server host**command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send SNMP notifications, you must configure at least one **snmp-server host**command.

Examples

The following example shows how to enable the router to send poor-quality-of-voice informs to the host at the address myhost.cisco.com using the community string defined as public:

```
Router(config)# snmp-server enable traps voice poor-qov
Router(config)# snmp-server host myhost.cisco.com informs version 2c public
```

The following example shows how to enable the router to send PSTN fallback messages at the address myhost.cisco.com using the community string defined as public:

```
Router(config)# snmp-server enable traps voice fallback
Router(config)# snmp-server host myhost.cisco.com informs version 2c public
```

Related Commands

Command	Description
snmp-server enable traps voice poor-qov	Enables poor quality-of-voice SNMP notifications.
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server trap-source	Specifies the interface which an SNMP trap should originate from.

snmp-server enable traps voice poor-qov

The **snmp-server enable traps voice poor-qov** command is replaced by the **snmp-server enable traps voice** command. See the **snmp-server enable traps voice** command for more information.

snmp-server enable traps vswitch dual-active

To enable the CISCO-VIRTUAL-SWITCH-MIB Simple Network Management Protocol (SNMP) notification (trap) when the dual-active state is detected, use the **snmp-server enable traps vswitch dual-active** command in global configuration mode. To disable the CISCO-VIRTUAL-SWITCH-MIB SNMP notification (trap), use the **no** form of this command.

snmp-server enable traps vswitch dual-active

no snmp-server enable traps vswitch dual-active

Syntax Description

This command has no arguments or keywords.

Command Default

The CISCO-VIRTUAL-SWITCH-MIB SNMP notification is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(1)SY	This command was introduced.

Usage Guidelines

The virtual switch link (VSL) is a special link that carries control and data traffic between the two chassis of a virtual switching system (VSS). The VSL is implemented as an EtherChannel with up to eight links. The VSL gives control traffic higher priority than data traffic so that control messages are never discarded. The SNMP agent runs on the VSS active supervisor engine. CISCO-VIRTUAL-SWITCH-MIB is the MIB for virtual switch mode.

If the VSL fails, the VSS standby chassis cannot determine the state of the VSS active chassis. To ensure that switchover occurs without delay, the VSS standby chassis assumes that the VSS active chassis has failed and initiates switchover to take over the VSS active role.

If the original VSS active chassis is still operational, both chassis are now VSS active. This situation is called a dual-active scenario. A dual-active scenario can have adverse effects on network stability because both chassis use the same IP addresses, Secure Shell (SSH) keys, and Spanning Tree Protocol (STP) bridge ID. The VSS must detect a dual-active scenario and take recovery action.

The **snmp-server enable traps vswitch dual-active** command enables the dual-active state change notification. When the VSS changes state to dual-active, SNMP sends the cvsDualActiveDetectionNotif notification. To receive this message from SNMP, enable this command.

This command enables both trap and inform requests.

Examples

The following example shows how to enable the cvsDualActiveDetectionNotif notification:

```
Device(config)# snmp-server enable traps vswitch dual-active
```

```
Device(config)# exit
Device# test snmp trap vswitch dual-active

cvsDualActiveDetectionNotif notification was sent.
Device# show running-config all

.
.
.
snmp-server enable traps vswitch dual-active
.
.
.
```

The following example shows how to disable the cvsDualActiveDetectionNotif notification:

```
Device(config)# no snmp-server enable traps vswitch dual-active
Device(config)# exit
Device# test snmp trap vswitch dual-active

cvsDualActiveDetectionNotif notification is disabled.
```

Related Commands

Command	Description
show running-config all	Displays the contents of the current running configuration file for a specific module, Layer 2 VLAN, class map, interface, map class, policy map, or virtual circuit (VC) class configuration file of SNMP trap in dual-active state.
test snmp trap vswitch dual-active	Tests the CISCO-VIRTUAL-SWITCH-MIB SNMP notification (trap and inform) in the dual-active state.



snmp-server engineID local through snmp trap link-status

- snmp-server engineID local, page 339
- snmp-server file-transfer access-group, page 341
- snmp-server group, page 343
- snmp-server host, page 348
- snmp-server inform, page 362
- snmp-server ip dscp, page 364
- snmp-server ip precedence, page 365
- snmp-server location, page 366
- snmp-server manager, page 367
- snmp-server manager session-timeout, page 369
- snmp-server packetsize, page 371
- snmp-server queue-length, page 372
- snmp-server queue-limit, page 374
- snmp-server source-interface, page 376
- snmp-server system-shutdown, page 378
- snmp-server tftp-server-list, page 379
- snmp-server trap authentication unknown-context, page 381
- snmp-server trap authentication vrf, page 382
- snmp-server trap link, page 384
- snmp-server trap link switchover, page 386
- snmp-server trap retry, page 387
- snmp-server trap timeout, page 388
- snmp-server trap-authentication, page 389

- snmp-server trap-source, page 390
- snmp-server trap-timeout, page 392
- snmp-server user, page 394
- snmp-server usm cisco, page 399
- snmp-server view, page 400
- snmp trap if-monitor, page 402
- snmp trap link-status, page 403

snmp-server engineID local

To specify the Simple Network Management Protocol (SNMP) engine ID on the local device, use the **snmp-server engineID local** command in global configuration mode. To remove the configured engine ID, use the **no** form of this command.

snmp-server engineID local *engineid-string*

no snmp-server engineID local *engineid-string*

Syntax Description

engineid-string	String of a maximum of 24 characters that identifies the engine ID.

Command Default

An SNMP engine ID is generated automatically but is not displayed or stored in the running configuration. You can display the default or configured engine ID by using the **show snmp engineID** command.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

The SNMP engine ID is a unique string used to identify the device for administrative purposes. You do not need to specify an engine ID for the device; a default string is generated using Cisco's enterprise number (1.3.6.1.4.1.9) and the MAC address of the first interface on the device. For further details on the SNMP engine ID, see RFC 2571.

If you specify your own ID, note that the entire 24-character engine ID is not needed if it contains trailing zeros. Specify only the portion of the engine ID up until the point where only zeros remain in the value. For example, to configure an engine ID of 123400000000000000000000, you can specify **snmp-server engineID local 1234**.

The value for the engine ID is displayed in hexadecimal value pairs. If the length of the input is an odd number, the last digit will be prepended with a zero ("0"). For example, if the engine ID is 12345, the ID is treated as 12:34:05 internally. Hence, the engine ID is displayed as 123405 in the **show running configuration** command output.

Changing the value of the SNMP engine ID has significant effects. A user's password (entered on the command line) is converted to a message digest5 algorithm (MD5) or Secure Hash Algorithm (SHA) security digest. This digest is based on both the password and the local engine ID. The command line password is then destroyed, as required by RFC 2274. Because of this deletion, if the local value of the engineID changes, the security digests of SNMPv3 users will become invalid, and the users will have to be reconfigured.

Similar restrictions require the reconfiguration of community strings when the engine ID changes. A remote engine ID is required when an SNMPv3 inform is configured. The remote engine ID is used to compute the security digest for authenticating and encrypting packets sent to a user on the remote host.

Examples

The following example specifies the local SNMP engine ID:

```
Router(config)# snmp-server engineID local
```

Related Commands

Command	Description
show snmp engineID	Displays the identification of the local SNMP engine and all remote engines that have been configured on the router.
snmp-server host	Specifies the recipient (SNMP manager) of an SNMP trap notification.

snmp-server file-transfer access-group

To associate an access list to the transfer protocols TFTP, FTP, Remote Copy Protocol (RCP), Secure Copy Protocol (SCP), and Secured File Transfer Protocol (SFTP), use the **snmp-server file-transfer access-group** command in global configuration mode. To disassociate an access list, use **no** form of this command.

snmp-server file-transfer access-group {*acl-number*| *acl-name*} [**protocol** *p-name*]

no snmp-server file-transfer access-group {*acl-number*| *acl-name*}

Syntax Description

acl-number	Integer from 1 to 99 that specifies a standard ACL.
acl-name	String that specifies a standard ACL.
protocol	(Optional) Enables the user to associate a named protocol with an access group.
p-name	(Optional) Name of a transfer protocol. Valid values are: **ftp**, **rcp**, **scp**, **sftp**, and **tftp**.

Command Default

If a protocol is not specified, all protocols are associated with the access list.

Command Modes

Global configuration

Command History

Release	Modification
12.4(12)	This command was introduced. This command replaces the **snmp-server tftp-server-list** command.

Usage Guidelines

The **snmp-server tftp-server-list** command is still supported in Cisco IOS software, but if it is configured as **snmp-server tftp-server-list 10**, it will be substituted with the **snmp-server file-transfer access-group 10 protocol tftp**command.

Use the **snmp-server file-transfer access-group**command to restrict configuration transfers that are initiated via Simple Network Management Protocol (SNMP). You can restrict transfers for specific transfer protocols by associating an access list to the protocol.

Examples

The following example associates access group 10 to the transfer protocols FTP and RCP:

```
Router(config)# snmp-server file-transfer access-group 10 protocol ftp
Router(config)# snmp-server file-transfer access-group 10 protocol rcp
```

Related Commands

Command	Description
snmp-server tftp-server-list	Associates TFTP servers used via SNMP controlled TFTP operations to the servers specified in an access list.

snmp-server group

To configure a new Simple Network Management Protocol (SNMP) group, 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 *group-name* {**v1**| **v2c**| **v3** {**auth**| **noauth**| **priv**}} [**context** *context-name*] [**read** *read-view*] [**write** *write-view*] [**notify** *notify-view*] [**access** [**ipv6** *named-access-list*] [*acl-number*| *acl-name*]]

no snmp-server group *group-name* {**v1**| **v2c**| **v3** {**auth**| **noauth**| **priv**}} [**context** *context-name*]

Syntax Description

group-name	Name of the group.
v1	Specifies that the group is using the SNMPv1 security model. SNMPv1 is the least secure of the possible SNMP security models.
v2c	Specifies that the group is using the SNMPv2c security model. The SNMPv2c security model allows informs to be transmitted and supports 64-character strings.
v3	Specifies that the group is using the SNMPv3 security model. SMNPv3 is the most secure of the supported security models. It allows you to explicitly configure authentication characteristics.
auth	Specifies authentication of a packet without encrypting it.
noauth	Specifies no authentication of a packet.
priv	Specifies authentication of a packet with encryption.
context	(Optional) Specifies the SNMP context to associate with this SNMP group and its views.
context-name	(Optional) Context name.
read	(Optional) Specifies a read view for the SNMP group. This view enables you to view only the contents of the agent.

read-view	(Optional) String of a maximum of 64 characters that is the name of the view. The default is that the read-view is assumed to be every object belonging to the Internet object identifier (OID) space (1.3.6.1), unless the **read** option is used to override this state.
write	(Optional) Specifies a write view for the SNMP group. This view enables you to enter data and configure the contents of the agent.
write-view	(Optional) String of a maximum of 64 characters that is the name of the view. The default is that nothing is defined for the write view (that is, the null OID). You must configure write access.
notify	(Optional) Specifies a notify view for the SNMP group. This view enables you to specify a notify, inform, or trap.
notify-view	(Optional) String of a maximum of 64 characters that is the name of the view. By default, nothing is defined for the notify view (that is, the null OID) until the **snmp-server host** command is configured. If a view is specified in the **snmp-server group** command, any notifications in that view that are generated will be sent to all users associated with the group (provided a SNMP server host configuration exists for the user). Cisco recommends that you let the software autogenerate the notify view. See the "Configuring Notify Views" section in this document.
access	(Optional) Specifies a standard access control list (ACL) to associate with the group.
ipv6	(Optional) Specifies an IPv6 named access list. If both IPv6 and IPv4 access lists are indicated, the IPv6 named access list must appear first in the list.
named-access-list	(Optional) Name of the IPv6 access list.
acl-number	(Optional) The *acl-number*argument is an integer from 1 to 99 that identifies a previously configured standard access list.

acl-name	(Optional) The *acl-name* argument is a string of a maximum of 64 characters that is the name of a previously configured standard access list.

Command Default No SNMP server groups are configured.

Command Modes Global configuration (config)

Command History

Release	Modification
11.(3)T	This command was introduced.
12.0(23)S	The **context** *context-name* keyword and argument pair was added.
12.3(2)T	The **context** *context-name* keyword and argument pair was integrated into Cisco IOS Release 12.3(2)T, and support for standard named access lists (acl-name) was added.
12.0(27)S	The **ipv6** *named-access-list* keyword and argument pair was added.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.3(14)T	The **ipv6** *named-access-list* keyword and argument pair was integrated into Cisco IOS Release 12.3(14)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines When a community string is configured internally, two groups with the name public are autogenerated, one for the v1 security model and the other for the v2c security model. Similarly, deleting a community string will delete a v1 group with the name public and a v2c group with the name public.

No default values exist for authentication or privacy algorithms when you configure the **snmp-server group** command. Also, no default passwords exist. For information about specifying a Message Digest 5 (MD5) password, see the documentation of the **snmp-server user** command.

Configuring Notify Views

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, you must either reconfigure the **snmp-server host** command, or specify the appropriate notify view.

Specifying a notify view when configuring an SNMP group is not recommended, 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 group's notify view will affect all users associated with that group.

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

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

SNMP Contexts

SNMP contexts provide 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.

Use this command with the **context** *context-name* keyword and argument to associate a read, write, or notify SNMP view with an SNMP context.

Examples

Examples

The following example shows how to create the SNMP server group "public," allowing read-only access for all objects to members of the standard named access list "lmnop":

```
Router(config)# snmp-server group public v2c access lmnop
```

Examples

The following example shows how to remove the SNMP server group "public" from the configuration:

```
Router(config)# no snmp-server group public v2c
```

Examples

The following example shows SNMP context "A" associated with the views in SNMPv2c group "GROUP1":

```
Router(config)# snmp-server context A
Router(config)# snmp mib community commA
Router(config)# snmp mib community-map commA context A target-list commAVpn
Router(config)# snmp-server group GROUP1 v2c context A read viewA write viewA notify viewB
```

Related Commands

Command	Description
show snmp group	Displays the names of groups on the router and the security model, the status of the different views, and the storage type of each group.
snmp mib community-map	Associates a SNMP community with an SNMP context, engine ID, security name, or VPN target list.
snmp-server host	Specifies the recipient of a SNMP notification operation.
snmp-server user	Configures a new user to a SNMP group.

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 from the configuration, use the **no** form of this command.

snmp-server host {*hostname*| *ip-address*} [**vrf** *vrf-name*| **informs**| **traps**| **version** {**1**| **2c**| **3** [**auth**| **noauth**| **priv**]}] *community-string* [**udp-port** *port* [*notification-type*]| *notification-type*]

no snmp-server host {*hostname*| *ip-address*} [**vrf** *vrf-name*| **informs**| **traps**| **version** {**1**| **2c**| **3** [**auth**| **noauth**| **priv**]}] *community-string* [**udp-port** *port* [*notification-type*]| *notification-type*]

Command Syntax on Cisco ME 3400, ME 3400E, and Catalyst 3750 Metro Switches

snmp-server host *ip-address* {*community-string*| **informs**| **traps**} {*community-string*| **version** {**1**| **2c**| **3** {**auth**| **noauth**}}} {*community-string*| **vrf** *vrf-name* {**informs**| **traps**}} [*notification-type*]

no snmp-server host *ip-address* {*community-string*| **informs**| **traps**} {*community-string*| **version** {**1**| **2c**| **3** {**auth**| **noauth**}}} {*community-string*| **vrf** *vrf-name* {**informs**| **traps**}} [*notification-type*]

Command Syntax on Cisco 7600 Series Router

snmp-server host *ip-address* {*community-string*| {**informs**| **traps**} {*community-string*| **version** {**1**| **2c**| **3** {**auth**| **noauth**| **priv**}} *community-string*| **version** {**1**| **2c**| **3** {**auth**| **noauth**| **priv**}} *community-string*| **vrf** *vrf-name* {**informs**| **traps**} {*community-string*| **version** {**1**| **2c**| **3** {**auth**| **noauth**| **priv**}} *community-string*}}} [*notification-type*]

no snmp-server host *ip-address* {*community-string*| {**informs**| **traps**} {*community-string*| **version** {**1**| **2c**| **3** {**auth**| **noauth**| **priv**}} *community-string*| **version** {**1**| **2c**| **3** {**auth**| **noauth**| **priv**}} *community-string*| **vrf** *vrf-name* {**informs**| **traps**} {*community-string*| **version** {**1**| **2c**| **3** {**auth**| **noauth**| **priv**}} *community-string*}}} [*notification-type*]

Syntax Description

hostname	Name of the host. The SNMP notification host is typically a network management station (NMS) or SNMP manager. This host is the recipient of the SNMP traps or informs.
ip-address	IPv4 address or IPv6 address of the SNMP notification host.
vrf	(Optional) Specifies that a VPN routing and forwarding (VRF) instance should be used to send SNMP notifications. • In Cisco IOS Release 12.2(54)SE, the **vrf** keyword is required.

vrf-name	(Optional) VPN VRF instance used to send SNMP notifications. • In Cisco IOS Release 12.2(54)SE, the *vrf-name* argument is required.
informs	(Optional) Specifies that notifications should be sent as informs. • In Cisco IOS Release 12.2(54)SE, the **informs** keyword is required.
traps	(Optional) Specifies that notifications should be sent as traps. This is the default. • In Cisco IOS Release 12.2(54)SE, the **traps** keyword is required.
version	(Optional) Specifies the version of the SNMP that is used to send the traps or informs. The default is 1. • In Cisco IOS Release 12.2(54)SE, the **version** keyword is required and the **priv** keyword is not supported. If you use the **version** keyword, one of the following keywords must be specified: • **1** --SNMPv1. • **2c** --SNMPv2C. • **3** --SNMPv3. The most secure model because it allows packet encryption with the **priv** keyword. The default is **noauth**. One of the following three optional security level keywords can follow the **3** keyword: • • **auth** --Enables message digest algorithm 5 (MD5) 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. **Note** You can set this string using the **snmp-server host** command by itself, but Cisco recommends that you define the string using the **snmp-server community** command prior to using the **snmp-server host** command. **Note** The "at" sign (@) is used for delimiting the context information.
udp-port	(Optional) Specifies that SNMP traps or informs are to be sent to an network management system (NMS) host. • In Cisco IOS Release 12.2(54)SE, the **udp-port** keyword is not supported.
port	(Optional) User Datagram Protocol (UDP) port number of the NMS host. The default is 162. • In Cisco IOS Release 12.2(54)SE, the *port* argument is not supported.
notification-type	(Optional) Type of notification to be sent to the host. If no type is specified, all available notifications are sent. See the "Usage Guidelines" section for more information about the keywords available.

Command Default

This command behavior is disabled by default. A recipient is not specified to receive notifications.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.
Cisco IOS Release 12 and 15 Mainline/T Train	

Release	Modification
12.0(3)T	This command was modified. • The **version 3** [**auth** | **noauth** | **priv**] syntax was added as part of the SNMPv3 Support feature. • The **hsrp** notification-type keyword was added. • The **voice** notification-type keyword was added.
12.1(3)T	This command was modified. The **calltracker** notification-type keyword was added for the Cisco AS5300 and AS5800 platforms.
12.2(2)T	This command was modified. • The **vrf** *vrf-name* keyword-argument pair was added. • The **ipmobile** notification-type keyword was added. • Support for the **vsimaster** notification-type keyword was added for the Cisco 7200 and Cisco 7500 series routers.
12.2(4)T	This command was modified. • The **pim** notification-type keyword was added. • The **ipsec** notification-type keyword was added.
12.2(8)T	This command was modified. • The **mpls-traffic-eng** notification-type keyword was added. • The **director** notification-type keyword was added.
12.2(13)T	This command was modified. • The **srp** notification-type keyword was added. • The **mpls-ldp** notification-type keyword was added.
12.3(2)T	This command was modified. • The **flash** notification-type keyword was added. • The **l2tun-session** notification-type keyword was added.
12.3(4)T	This command was modified. • The **cpu** notification-type keyword was added. • The **memory** notification-type keyword was added. • The **ospf notification-type** keyword was added.

Release	Modification
12.3(8)T	This command was modified. The **iplocalpool notification-type** keyword was added for the Cisco 7200 and 7301 series routers.
12.3(11)T	This command was modified. The **vrrp** keyword was added.
12.3(14)T	This command was modified. • Support for SNMP over IPv6 transport was integrated into Cisco IOS Release 12.3(14)T. Either an IP or IPv6 Internet address can be specified as the *hostname* argument. • The **eigrp** notification-type keyword was added.
12.4(20)T	This command was modified. The **license** notification-type keyword was added.
15.0(1)M	This command was modified. • The **nhrp** notification-type keyword was added. • The automatic insertion of the **snmp-server community** command into the configuration, along with the community string specified in the **snmp-server host** command, was changed. The **snmp-server community** command must be manually configured.
Cisco IOS Release 12.0S	
12.0(17)ST	This command was modified. The **mpls-traffic-eng** notification-type keyword was added.
12.0(21)ST	This command was modified. The **mpls-ldp notification-type** keyword was added.
12.0(22)S	This command was modified. • All features in Cisco IOS Release 12.0ST were integrated into Cisco IOS Release 12.0(22)S. • The **mpls-vpn** notification-type keyword was added.
12.0(23)S	This command was modified. The **l2tun-session** notification-type keyword was added.
12.0(26)S	This command was modified. The **memory** notification-type keyword was added.

Release	Modification
12.0(27)S	This command was modified. • Support for SNMP over IPv6 transport was added. Either an IP or IPv6 Internet address can be specified as the *hostname* argument. • The **vrf** *vrf-name* keyword and argument combination was added to support multiple Lightweight Directory Protocol (LDP) contexts for VPNs.
12.0(31)S	This command was modified. The **l2tun-pseudowire-status** notification-type keyword was added.
Cisco IOS Release 12.2S	
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(25)S	This command was modified. • The **cpu** notification-type keyword was added. • The **memory** notification-type keyword was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	The **cef** notification-type keyword was added.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI5	This command was modified. • The **dhcp-snooping** notification-type keyword was added. • The **errdisable** notification-type keyword was added.
12.2(54)SE	This command was modified. See the snmp-server host, on page 348 for the command syntax for these switches.
12.2(33)SXJ	This command was integrated into Cisco IOS Release 12.2(33)SXJ. The **public storm-control** notification-type keyword was added.
Cisco IOS Release 15S	
15.0(1)S	This command was modified. The **flowmon notification-type** keyword was added.
Cisco IOS XE Releases	

Release	Modification
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.2(1)S	This command was modified. The **p2mp-traffic-eng** notification-type keyword was added.

Usage Guidelines

If you enter this command with no optional keywords, the default is to send all notification-type traps to the host. No informs will be sent to the host.

The **no snmp-server host** command with no keywords disables traps, but not informs, to the host. To disable informs, use the **no snmp-server host informs** command.



Note If a community string is not defined using the **snmp-server community** command prior to using this command, the default form of the **snmp-server community** command will automatically be inserted into the configuration. The password (community string) used for this automatic configuration of the **snmp-server community** command will be the same as that specified in the **snmp-server host** command. This automatic command insertion and use of passwords is the default behavior for Cisco IOS Release 12.0(3) and later releases. However, in Cisco IOS Release 12.2(33)SRE and later releases, you must manually configure the **snmp-server community** command. That is, the **snmp-server community** command will not be seen in the configuration.

SNMP notifications can be sent as traps or inform requests. Traps are unreliable because the receiver does not send acknowledgments when it receives traps. The sender cannot determine if the traps were received. However, an SNMP entity that receives an inform request acknowledges the message with an SNMP response protocol data unit (PDU). If the sender never receives the response, the inform request can be sent again. Thus, informs are more likely to reach their intended destination than traps.

Compared to traps, informs consume more resources in the agent and in the network. Unlike a trap, which is discarded as soon as it is sent, an inform request must be held in memory until a response is received or the request times out. Also, traps are sent only once; an inform may be tried several times. The retries increase traffic and contribute to a higher overhead on the network.

If you do not enter an **snmp-server host** command, no notifications are sent. To configure the router to send SNMP notifications, you must enter at least one **snmp-server host** command. If you enter the command with no optional keywords, all trap types are enabled for the host.

To enable multiple hosts, you must 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 or inform), each succeeding command overwrites the previous command. Only the last **snmp-server host** command will be in effect. For example, if you enter an **snmp-server host inform** command for a host and then enter another **snmp-server host inform** command for the same host, the second command will replace the first.

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

Some notification types cannot be controlled with the **snmp-server enable** command. Some notification types are always enabled, and others are enabled by a different command. For example, the **linkUpDown** notifications are controlled by the **snmp trap link-status** command. These notification types do not require an **snmp-server enable** command.

The availability of notification-type options depends on the router type and the Cisco IOS software features supported on the router. For example, the **envmon** notification type is available only if the environmental monitor is part of the system. To see what notification types are available on your system, use the command help **?** at the end of the **snmp-server host** command.

The **vrf** keyword allows you to specify the notifications being sent to a specified IP address over a specific VRF VPN. The VRF defines a VPN membership of a user so that data is stored using the VPN.

In the case of the NMS sending the query having a correct SNMP community but not having a read or a write view, the SNMP agent returns the following error values:

- For a get or a getnext query, returns GEN_ERROR for SNMPv1 and AUTHORIZATION_ERROR for SNMPv2C.
- For a set query, returns NO_ACCESS_ERROR.

Notification-Type Keywords

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



Note The available notification types differ based on the platform and Cisco IOS release. For a complete list of available notification types, use the question mark (?) online help function.

- **aaa server** --Sends SNMP authentication, authorization, and accounting (AAA) traps.
- **adslline** --Sends Asymmetric Digital Subscriber Line (ADSL) LINE-MIB traps.
- **atm** --Sends ATM notifications.
- **authenticate-fail** --Sends an SNMP 802.11 Authentication Fail trap.
- **auth-framework** --Sends SNMP CISCO-AUTH-FRAMEWORK-MIB notifications.
- **bgp** --Sends Border Gateway Protocol (BGP) state change notifications.
- **bridge** --Sends SNMP STP Bridge MIB notifications.
- **bstun** --Sends Block Serial Tunneling (BSTUN) event notifications.
- **bulkstat** --Sends Data-Collection-MIB notifications.
- **c6kxbar** --Sends SNMP crossbar notifications.
- **callhome** --Sends Call Home MIB notifications.
- **calltracker** -- Sends Call Tracker call-start/call-end notifications.
- **casa** --Sends Cisco Appliances Services Architecture (CASA) event notifications.
- **ccme** --Sends SNMP Cisco netManager Event (CCME) traps.
- **cef** --Sends notifications related to Cisco Express Forwarding.
- **chassis** --Sends SNMP chassis notifications.

- **cnpd** --Sends Cisco Network-based Application Recognition (NBAR) Protocol Discovery (CNPD) traps.
- **config** --Sends configuration change notifications.
- **config-copy** --Sends SNMP config-copy notifications.
- **config-ctid** --Sends SNMP config-ctid notifications.
- **cpu** --Sends CPU-related notifications.
- **csg** --Sends SNMP Content Services Gateway (CSG) notifications.
- **deauthenticate** --Sends an SNMP 802.11 Deauthentication trap.
- **dhcp-snooping** --Sends DHCP snooping MIB notifications.
- **director** --Sends notifications related to DistributedDirector.
- **disassociate** --Sends an SNMP 802.11 Disassociation trap.
- **dlsw** --Sends data-link switching (DLSW) notifications.
- **dnis** --Sends SNMP Dialed Number Identification Service (DNIS) traps.
- **dot1x** --Sends 802.1X notifications.
- **dot11-mibs** --Sends dot11 traps.
- **dot11-qos** --Sends SNMP 802.11 QoS Change trap.
- **ds1** --Sends SNMP digital signaling 1 (DS1) notifications.
- **ds1-loopback** --Sends ds1-loopback traps.
- **dspu** --Sends downstream physical unit (DSPU) notifications.
- **eigrp** --Sends Enhanced Interior Gateway Routing Protocol (EIGRP) stuck-in-active (SIA) and neighbor authentication failure notifications.
- **energywise** --Sends SNMP energywise notifications.
- **entity** --Sends Entity MIB modification notifications.
- **entity-diag** --Sends SNMP entity diagnostic MIB notifications.
- **envmon** --Sends Cisco enterprise-specific environmental monitor notifications when an environmental threshold is exceeded.
- **errdisable** --Sends error disable notifications.
- **ethernet-cfm** --Sends SNMP Ethernet Connectivity Fault Management (CFM) notifications.
- **event-manager** --Sends SNMP Embedded Event Manager notifications.
- **firewall** --Sends SNMP Firewall traps.
- **flash** --Sends flash media insertion and removal notifications.
- **flexlinks** --Sends FLEX links notifications.
- **flowmon** --Sends flow monitoring notifications.
- **frame-relay** --Sends Frame Relay notifications.

- **fru-ctrl** --Sends entity field-replaceable unit (FRU) control notifications.
- **hsrp** --Sends Hot Standby Routing Protocol (HSRP) notifications.
- **icsudsu** --Sends SNMP ICSUDSU traps.
- **iplocalpool** --Sends IP local pool notifications.
- **ipmobile** --Sends Mobile IP notifications.
- **ipmulticast** --Sends IP multicast notifications.
- **ipsec** --Sends IP Security (IPsec) notifications.
- **isakmp** --Sends SNMP ISAKMP notifications.
- **isdn** --Sends ISDN notifications.
- **l2tc** --Sends SNMP L2 tunnel configuration notifications.
- **l2tun-pseudowire-status** --Sends pseudowire state change notifications.
- **l2tun-session** --Sends Layer 2 tunneling session notifications.
- **license** --Sends licensing notifications as traps or informs.
- **llc2** --Sends Logical Link Control, type 2 (LLC2) notifications.
- **mac-notification** --Sends SNMP MAC notifications.
- **memory** --Sends memory pool and memory buffer pool notifications.
- **module** --Sends SNMP module notifications.
- **module-auto-shutdown** --Sends SNMP module autoshutdown MIB notifications.
- **mpls-fast-reroute** --Sends SNMP Multiprotocol Label Switching (MPLS) traffic engineering fast reroute notifications.
- **mpls-ldp** --Sends MPLS Label Distribution Protocol (LDP) notifications indicating status changes in LDP sessions.
- **mpls-traffic-eng** --Sends MPLS traffic engineering notifications, indicating changes in the status of MPLS traffic engineering tunnels.
- **mpls-vpn** --Sends MPLS VPN notifications.
- **msdp** --Sends SNMP Multicast Source Discovery Protocol (MSDP) notifications.
- **mvpn** --Sends multicast VPN notifications.
- **nhrp** --Sends Next Hop Resolution Protocol (NHRP) notifications.
- **ospf** --Sends Open Shortest Path First (OSPF) sham-link notifications.
- **pim** --Sends Protocol Independent Multicast (PIM) notifications.
- **port-security** --Sends SNMP port-security notifications.
- **power-ethernet** --Sends SNMP power Ethernet notifications.
- **public storm-control** --Sends SNMP public storm-control notifications.
- **pw-vc** --Sends SNMP pseudowire virtual circuit (VC) notifications.

- **p2mp-traffic-eng**--Sends SNMP MPLS Point to Multi-Point MPLS-TE notifications.
- **repeater** --Sends standard repeater (hub) notifications.
- **resource-policy** --Sends CISCO-ERM-MIB notifications.
- **rf** --Sends SNMP RF MIB notifications.
- **rogue-ap** --Sends an SNMP 802.11 Rogue AP trap.
- **rsrb** --Sends remote source-route bridging (RSRB) notifications.
- **rsvp** --Sends Resource Reservation Protocol (RSVP) notifications.
- **rtr** --Sends Response Time Reporter (RTR) notifications.
- **sdlc** --Sends Synchronous Data Link Control (SDLC) notifications.
- **sdllc** --Sends SDLC Logical Link Control (SDLLC) notifications.
- **slb** --Sends SNMP server load balancer (SLB) notifications.
- **snmp** --Sends any enabled RFC 1157 SNMP linkUp, linkDown, authenticationFailure, warmStart, and coldStart notifications.



Note To enable RFC-2233-compliant link up/down notifications, you should use the **snmp server link trap** command.

- **sonet** --Sends SNMP SONET notifications.
- **srp** --Sends Spatial Reuse Protocol (SRP) notifications.
- **stpx** --Sends SNMP STPX MIB notifications.
- **srst** --Sends SNMP Survivable Remote Site Telephony (SRST) traps.
- **stun** --Sends serial tunnel (STUN) notifications.
- **switch-over** --Sends an SNMP 802.11 Standby Switchover trap.
- **syslog** --Sends error message notifications (Cisco Syslog MIB). Use the **logging history level** command to specify the level of messages to be sent.
- **syslog** --Sends error message notifications (Cisco Syslog MIB). Use the **logging history level** command to specify the level of messages to be sent.
- **tty** --Sends Cisco enterprise-specific notifications when a TCP connection closes.
- **udp-port** --Sends the notification host's UDP port number.
- **vlan-mac-limit** --Sends SNMP L2 control VLAN MAC limit notifications.
- **vlancreate** --Sends SNMP VLAN created notifications.
- **vlandelete** --Sends SNMP VLAN deleted notifications.
- **voice** --Sends SNMP voice traps.
- **vrrp** --Sends Virtual Router Redundancy Protocol (VRRP) notifications.
- **vsimaster** --Sends Virtual Switch Interface (VSI) Master notifications.

- **vswitch** --Sends SNMP virtual switch notifications.
- **vtp** --Sends SNMP VLAN Trunking Protocol (VTP) notifications.
- **wlan-wep** --Sends an SNMP 802.11 Wireless LAN (WLAN) Wired Equivalent Privacy (WEP) trap.
- **x25** --Sends X.25 event notifications.
- **xgcp** --Sends External Media Gateway Control Protocol (XGCP) traps.

SNMP-Related Notification-Type Keywords

The *notification-type* argument used in the **snmp-server host** command do not always match the keywords used in the corresponding **snmp-server enable traps** command. For example, the *notification-type* argument applicable to Multiprotocol Label Switching Protocol (MPLS) traffic engineering tunnels is specified as **mpls-traffic-eng** (containing two hyphens and no embedded spaces). The corresponding parameter in the **snmp-server enable traps** command is specified as **mpls traffic-eng** (containing an embedded space and a hyphen).

This syntax difference is necessary to ensure that the CLI interprets the *notification-type* keyword of the **snmp-server host** command as a unified, single-word construct, which preserves the capability of the **snmp-server host** command to accept multiple *notification-type* keywords in the command line. The **snmp-server enable traps** commands, however, often use two-word constructs to provide hierarchical configuration options and to maintain consistency with the command syntax of related commands. The table below maps some examples of **snmp-server enable traps** commands to the keywords used in the **snmp-server host** command.

Table 15: snmp-server enable traps Commands and Corresponding Notification Keywords

snmp-server enable traps Command	snmp-server host Command Keyword
snmp-server enable traps l2tun session	**l2tun-session**
snmp-server enable traps mpls ldp	**mpls-ldp**
snmp-server enable traps mpls traffic-eng [2]	**mpls-traffic-eng**
snmp-server enable traps mpls vpn	**mpls-vpn**
snmp-server host *host-address community-string* **udp-port** *port* **p2mp-traffic-eng**	**snmp-server enable traps mpls p2mp-traffic-eng** [**down** | **up**]

2 See the *Cisco IOS Multiprotocol Label Switching Command Reference* for documentation of this command.

Examples

If you want to configure a unique SNMP community string for traps but prevent SNMP polling access with this string, the configuration should include an access list. The following example shows how to name a community string comaccess and number an access list 10:

```
Router(config)# snmp-server community comaccess ro 10
Router(config)# snmp-server host 10.0.0.0 comaccess
Router(config)# access-list 10 deny any
```

Note The "at" sign (@) is used as a delimiter between the community string and the context in which it is used. For example, specific VLAN information in BRIDGE-MIB may be polled using *community @VLAN-ID* (for example, public@100), where 100 is the VLAN number.

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

```
Router(config)# snmp-server enable traps
Router(config)# snmp-server host myhost.cisco.com comaccess snmp
```

The following example shows how to send the SNMP and Cisco environmental monitor enterprise-specific traps to address 10.0.0.0 using the community string public:

```
Router(config)# snmp-server enable traps snmp
Router(config)# snmp-server enable traps envmon
Router(config)# snmp-server host 10.0.0.0 public snmp envmon
```

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

```
Router(config)# snmp-server enable traps
Router(config)# snmp-server host myhost.cisco.com public
```

The following example will not send traps to any host. The BGP traps are enabled for all hosts, but only the ISDN traps are enabled to be sent to a host. The community string is defined as public.

```
Router(config)# snmp-server enable traps bgp
Router(config)# snmp-server host myhost.cisco.com public isdn
```

The following example shows how to enable the router to send all inform requests to the host myhost.cisco.com using the community string public:

```
Router(config)# snmp-server enable traps
Router(config)# snmp-server host myhost.cisco.com informs version 2c public
```

The following example shows how to send HSRP MIB informs to the host specified by the name myhost.cisco.com. The community string is defined as public.

```
Router(config)# snmp-server enable traps hsrp
Router(config)# snmp-server host myhost.cisco.com informs version 2c public hsrp
```

The following example shows how to send all SNMP notifications to example.com over the VRF named trap-vrf using the community string public:

```
Router(config)# snmp-server host example.com vrf trap-vrf public
```

The following example shows how to configure an IPv6 SNMP notification server with the IPv6 address 2001:0DB8:0000:ABCD:1 using the community string public:

```
Router(config)# snmp-server host 2001:0DB8:0000:ABCD:1 version 2c public udp-port 2012
```

The following example shows how to specify VRRP as the protocol using the community string public:

```
Router(config)# snmp-server enable traps vrrp
Router(config)# snmp-server host myhost.cisco.com traps version 2c public vrrp
```

The following example shows how to send all Cisco Express Forwarding informs to the notification receiver with the IP address 10.0.1.1 using the community string public:

```
Router(config)# snmp-server enable traps cef
Router(config)# snmp-server host 10.0.1.1 informs version 2c public cef
```

The following example shows how to enable all NHRP traps, and how to send all NHRP traps to the notification receiver with the IP address 10.0.0.0 using the community string public:

```
Router(config)# snmp-server enable traps nhrp
Router(config)# snmp-server host 10.0.0.0 traps version 2c public nhrp
```

The following example shows how to enable all P2MP MPLS-TE SNMP traps, and send them to the notification receiver with the IP address 172.20.2.160 using the community string "comp2mppublic":

```
Router(config)# snmp-server enable traps mpls p2mp-traffic-eng
Router(config)# snmp-server host 172.20.2.160 comp2mppublic udp-port 162 p2mp-traffic-eng
```

Related Commands

Command	Description
show snmp host	Displays recipient details configured for SNMP notifications.
snmp-server enable peer-trap poor qov	Enables poor quality of voice notifications for applicable calls associated with a specific voice dial peer.
snmp-server enable traps	Enables SNMP notifications (traps and informs).
snmp-server enable traps nhrp	Enables SNMP notifications (traps) for NHRP.
snmp-server informs	Specifies inform request options.
snmp-server link trap	Enables linkUp/linkDown SNMP traps that are compliant with RFC 2233.
snmp-server trap-source	Specifies the interface from which an SNMP trap should originate.
snmp-server trap-timeout	Defines how often to try resending trap messages on the retransmission queue.
test snmp trap storm-control event-rev1	Tests SNMP storm-control traps.

snmp-server inform

To specify inform request options, use the **snmp-server inform**command in global configuration mode. To return settings to their default values, use the **no** form of this command.

snmp-server inform [**pending** *pending*] [**retries** *retries*] [**timeout** *seconds*]

no snmp-server inform [**pending** *pending*] [**retries** *retries*] [**timeout** *seconds*]

Syntax Description

pending	(Optional) Specifies a maximum number of informs waiting for acknowledgment at any one time. When the maximum is reached, older pending informs are discarded.
pending	(Optional) Number of unacknowledged informs to hold. The range is from 1 to 4294967295. The default is 25.
retries	(Optional) Specifies a maximum number of times to resend an inform request.
retries	(Optional) Number of retries. The range is from 1 to 100. The default value is 3.
timeout	(Optional) Specifies a number of seconds to wait for an acknowledgment before resending.
seconds	(Optional) Time in seconds. The range is from 0 to 42949671. The default is 30.

Command Default

Inform requests are resent three times. Informs are resent after 30 seconds if no response is received. The maximum number of informs waiting for acknowledgment at any one time is 25.

Command Modes

Global configuration (config)

Command History

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

Examples

The following example shows how to increase the pending queue size when several informs drop:

```
Router(config)# snmp-server inform pending 50
```

The following example shows how to increase the default timeout when you send informs over slow network links. Because informs will remain in the queue longer than other types of messages, you also may need to increase the pending queue size.

```
snmp-server inform timeout 60 pending 40
```

The following example shows how to decrease the default timeout when you send informs over very fast links:

```
Router(config)# snmp-server inform timeout 5
```

The following example shows how to increase the retry count when you send informs over unreliable links. Because informs will remain in the queue longer than other types of messages, you may need to increase the pending queue size.

```
Router(config)# snmp-server inform retries 10 pending 45
```

Related Commands

Command	Description
snmp-server enable traps	Enables a router to send SNMP traps and informs.

snmp-server ip dscp

To set the IP Differentiated Services Code Point (DSCP) value for Simple Network Management Protocol (SNMP) traffic, use the **snmp-server ip dscp** command in global configuration mode. To disable the configured value, use the **no** form of this command.

snmp-server ip dscp *value*

no snmp-server ip dscp *value*

Syntax Description

value	The IP DSCP value to apply to SNMP traffic. Valid values for IP DSCP are 0 through 63. The default is 0.

Command Default

The IP DSCP default value for SNMP traffic is 0.

Command Modes

Global config

Release	Modification
12.0(26)S	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use this command to specify an IP DSCP value to give SNMP traffic higher or lower priority in your network.

The following example shows how to set the IP DSCP value to 45:

```
Router(config)# snmp-server ip dscp 45
```

Related Commands

Command	Description
snmp-server ip precedence	Configures the IP Precedence value.

snmp-server ip precedence

snmp-server ip precedence *value*

no snmp-server ip precedence *value*

Syntax Description

value	The IP Precedence value to apply to SNMP traffic. Valid values for IP Precedence are 0 through 7. The default is 0.

Command Default

The IP Precedence default value for SNMP traffic is 0.

Command Modes

Global config.

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use this command to specify an IP Precedence value to give SNMP traffic higher or lower priority in your network.

Examples

The following example shows how to set the IP Precedence value to 7:

```
Router(config)# snmp-server ip precedence
 7
```

Related Commands

Command	Description
snmp-server ip dscp	Configures the IP DSCP value.

snmp-server location

To set the system location string, 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 *text*

no snmp-server location

Syntax Description

text	String that describes the system location information.

Command Default

No system location string is set.

Command Modes

Global configuration

Command History

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

Examples

The following example shows how to set a system location string:

```
Router(config)# snmp-server location Building 3/Room 214
```

Related Commands

Command	Description
show snmp location	Displays the SNMP system location string.
snmp-server contact	Sets the system contact (sysContact) string.

snmp-server manager

To start the Simple Network Management Protocol (SNMP) manager process, use the **snmp-server manager**command in global configuration mode. To stop the SNMP manager process, use the **no** form of this command.

snmp-server manager

no snmp-server manager

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

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

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

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

Examples

The following example shows how to enable the SNMP manager process:

```
Router(config)# snmp-server manager
```

Related Commands

Command	Description
show snmp	Checks the status of SNMP communications.
show snmp pending	Displays the current set of pending SNMP requests.
show snmp sessions	Displays the current SNMP sessions.
snmp-server manager session-timeout	Sets the amount of time before a nonactive session is destroyed.

snmp-server manager session-timeout

To set the amount of time before a nonactive session is destroyed, use the **snmp-server manager session-timeout** command in global configuration mode. To return the value to its default, use the **no** form of this command.

snmp-server manager session-timeout *seconds*

no snmp-server manager session-timeout

Syntax Description

seconds	Number of seconds before an idle session is timed out. The default is 600.

Command Default

Idle sessions time out after 600 seconds (10 minutes).

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

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

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

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

Examples

The following example shows how to set the session timeout to a larger value than the default:

```
Router(config)# snmp-server manager
Router(config)# snmp-server manager session-timeout 1000
```

Related Commands

Command	Description
show snmp pending	Displays the current set of pending SNMP requests.
show snmp sessions	Displays the current SNMP sessions.
snmp-server manager	Starts the SNMP manager process.

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 *byte-count*

no snmp-server packetsize

Syntax Description

byte-count	Integer from 484 to 8192. The default is 1500.

Command Default

Packet size is not configured.

Command Modes

Global configuration

Command History

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

Examples

The following example establishes a packet filtering of a maximum size of 1024 bytes:

```
Router(config)# snmp-server packetsize 1024
```

Related Commands

Command	Description
snmp-server queue-length	Establishes the message queue length for each trap host.

snmp-server queue-length

To establish the message queue length for each trap host, use the **snmp-server queue-length** command in global configuration mode.

snmp-server queue-length *length*

Syntax Description

length	Integer that specifies the number of trap events that can be held before the queue must be emptied. The default is 10.

Command Default

The queue length is set to 10.

Command Modes

Global configuration

Command History

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

Usage Guidelines

This command defines the length of the message queue for each trap host. When a trap message is successfully transmitted, Cisco IOS software will continue to empty the queue but never faster than at a rate of four trap messages per second.

During device bootup, some traps could be dropped because of trap queue overflow on the device. If you think that traps are being dropped, you can increase the size of the trap queue (for example, to 100) to determine if traps can then be sent during bootup.

Examples

The following example shows how to set the Simple Network Management Protocol (SNMP) notification queue to 50 events:

```
Router(config)# snmp-server queue-length 50
```

Related Commands

Command	Description
snmp-server packetsize	Establishes control over the largest SNMP packet size permitted when the SNMP server is receiving a request or generating a reply.

snmp-server queue-limit

To establish the message queue size for various queues, use the **snmp-server queue-limit** command in global configuration mode. To disable the configured settings, use the **no** form of this command.

snmp-server queue-limit {**dispatcher**| **engine**| **notification-host**} *queue-length*

no snmp-server queue-limit {**dispatcher**| **engine**| **notification-host**}

Syntax Description

dispatcher	Specifies the SNMP PDU dispatcher queue length.
engine	Specifies the SNMP engine queue length.
notification-host	Specifies the message queue length for each notification host.
queue-length	Length of the queue. The range for **dispatcher** and **engine** is 1 to 1000. The range for **notification-host** is 1 to 5000. The default *queue-length* value for notification-host is 10.

Command Default

By default, message queue size is not set.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(33)S	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
12.4(22)T	This command was modified. The range of queue length for notification host was changed to 1 to 5000.

Usage Guidelines

Use the **snmp-server queue-limit** command to set the message queue size for different queues. Using this command you can resize the queue for dispatcher, engine, and host traps.

Examples

The following example shows how to set the message queue length of each notification host to 50:

```
Router(config)# snmp-server queue-limit notification-host 50
```

Related Commands

Command	Description
snmp-server queue-length	Establishes the message queue length for each trap host.

snmp-server source-interface

To specify the interface from which a Simple Network Management Protocol (SNMP) trap originates the informs or traps, use the **snmp-server source-interface** command in global configuration mode. To remove the source designation, use the **no** form of this command.

snmp-server source-interface {**traps**| **informs**} *interface*

no snmp-server source-interface {**traps**| **informs**} [*interface*]

Syntax Description

traps	Specifies SNMP traps.
informs	Specifies SNMP informs.
interface	The interface type and the module and port number of the source interface.

Command Default

No interface is designated.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(18)SXB2	This command was introduced.
12.2(18)SXF6	The **informs** keyword was added. This command replaced the **snmp-server trap-source**command.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command replaced the **snmp-server trap-source**command.

Note The **snmp-server trap-source**command is available in other versions of Cisco IOS software for backward compatibility.

The source interface must have an IP address. Enter the *interface* argument in the following format: *interface-type module* / *port*.

An SNMP trap or inform sent from a Cisco SNMP server has a notification IP address of the interface it went out of at that time. Use this command to monitor notifications from a particular interface.

Examples

The following example shows how to specify that Gigabit Ethernet interface 5/2 is the source for all informs:

```
snmp-server source-interface informs gigabitethernet5/2
```

The following example shows how to specify that the Gigabit Ethernet interface 5/3 is the source for all traps:

```
snmp-server source-interface traps gigabitethernet5/3
```

The following example shows how to remove the source designation for all traps for a specific interface:

```
no snmp-server source-interface traps gigabitethernet5/3
```

Related Commands

Command	Description
snmp-server enable traps	Enables a router to send SNMP traps and informs.
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server trap-source	Specifies the interface from which a SNMP trap should originate.

snmp-server system-shutdown

To use the Simple Network Management Protocol (SNMP) message reload feature, the router configuration must include the **snmp-server system-shutdown** command in global configuration mode. To prevent an SNMP system-shutdown request (from an SNMP manager) from resetting the Cisco agent, use the **no**form of this command.

snmp-server system-shutdown

no snmp-server system-shutdown

Syntax Description

This command has no arguments or keywords.

Command Default

This command is not included in the configuration file.

Command Modes

Global configuration

Command History

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

Examples

The following example enables the SNMP message reload feature:

```
Router(config)# snmp-server system-shutdown
```

snmp-server tftp-server-list

Note This command was replaced with the **snmp-server file-transfer access-group**command in Cisco IOS Release 12.4(12). Use the **snmp-server file-transfer access-group** command in Cisco IOS Release 12.4(12) and in later releases.

To limit the TFTP servers used via Simple Network Management Protocol (SNMP) controlled TFTP operations (saving and loading configuration files) to the servers specified in an access list, use the **snmp-server tftp-server-list** command in global configuration mode. To disable this function, use the **no** form of this command.

snmp-server tftp-server-list {*acl-number*| *acl-name*}

no snmp-server tftp-server-list {*acl-number*| *acl-name*}

Syntax Description

acl-number	Integer from 1 to 99 that specifies a standard access control list (standard ACL).
acl-name	String (not to exceed 64 characters) that specifies a standard ACL.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
10.2	This command was introduced.
12.3(2)T	Support for standard named access lists was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example shows how to limit the TFTP servers that can be used for saving and loading configuration files via SNMP to the servers specified in the standard named access list lmnop:

Router(config)# **snmp-server tftp-server-list lmnop**

The following example shows how to limit the TFTP servers that can be used for copying configuration files via SNMP to the servers in access list 44:

```
Router(config)# snmp-server tftp-server-list 44
```

snmp-server trap authentication unknown-context

To enable the Simple Network Management Protocol (SNMP) authorization failure (authFail) traps during an unknown context error, use the **snmp-server trap authentication unknown-context** command in global configuration mode. To disable the authFail traps, use the **no** form of this command.

snmp-server trap authentication unknown-context

no snmp-server trap authentication unknown-context

Syntax Description

This command has no arguments or keywords.

Command Default

No authFail traps are generated.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(18)SXF5	This command was introduced on the Supervisor Engine 720 and the Supervisor Engine 32.
12.4(22)T	This command was integrated into a release earlier than Cisco IOS Release 12.4(22)T.
12.2(33)SXI	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.

Examples

The following example shows how to enable the authorization failure traps during an unknown context error:

```
Router(config)# snmp-server trap authentication unknown-context
```

The following example shows how to disable the authorization failure traps during an unknown context error:

```
Router(config)# no snmp-server trap authentication unknown-context
```

snmp-server trap authentication vrf

To enable virtual private network (VPN) routing and forwarding (VRF) instance context authentication notifications, use the **snmp-server trap authentication vrf**command in global configuration mode. To suppress authentication notifications for Simple Network Management Protocol (SNMP) packets dropped due specifically to VRF context mismatches while keeping all other SNMP authentication notifications enabled, use the **no** form of this command.

snmp-server trap authentication vrf

no snmp-server trap authentication vrf

Syntax Description

This command has no arguments or keywords.

Command Default

No VRF-specific authentication notifications are enabled when SNMP authentication notifications are not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.3(2)T	This command was integrated into Release 12.3(2)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

The **snmp-server enable traps snmp authentication**command controls SNMP authentication traps and the **no** form of this command disables all SNMP authentication failure notifications. The **snmp-server trap authentication vrf** command provides more granular control of these notifications.

With context-based MIB access, SNMP requests on each VRF are tied to a specific context. This context is used for access control. If SNMP contexts are configured for VPNs, any SNMP request not matching the configured context will generate an SNMP authentication failure notification.The **no snmp-server trap**

authentication vrf command allows you to suppress the authentication failure notifications that are specific to these VRF contexts, while keeping all other SNMP authentication failure notifications enabled.

The **no snmp-server trap authentication vrf** command has no effect if the **snmp-server enable traps snmp authentication**command has not been configured..

Examples

The following example shows how to enable a router to send SNMP authentication traps to host myhost.cisco.com using the community string public while disabling all VRF authentication traps:

```
Router(config)# snmp-server enable traps snmp authentication

Router(config)# no snmp-server trap authentication vrf
Router(config)# snmp-server host myhost.cisco.com public
```

Related Commands

Command	Description
snmp-server enable traps snmp	Enables the sending of RFC 1157 SNMP notifications.
snmp-server host	Specifies the recipient of an SNMP notification operation.

snmp-server trap link

To enable linkUp/linkDown Simple Network Management Protocol (SNMP) traps that are compliant with RFC2233, use the **snmp-server trap link** command in global configuration mode. To disable IETF- compliant functionality and revert to the default Cisco implementation of linkUp/linkDown traps, use the **no** form of this command.

snmp-server trap link ietf

no snmp-server trap link ietf

Syntax Description

ietf	Notifies the command parser to link functionality of SNMP linkUp/linkDown traps to the Internet Engineering Task Force (IETF) standard (instead of the previous Cisco implementation).

Command Default

This command is disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.1(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **snmp-server trap link ietf** command is used to configure your router to use the RFC2233 IETF standards-based implementation of linkUp/linkDown traps. This command is disabled by default to allow you to continue using the earlier Cisco implementation of linkUp/linkDown traps if you so choose.

However, please note that when using the default Cisco object definitions, linkUp/linkDown traps are not generated correctly for sub-interfaces. In the default implementation an arbitrary value is used for the *locIfReason* object in linkUp/linkDown traps for sub-interfaces, which may give you unintended results. This is because the *locIfReason* object is not defined for sub-interfaces in the current Cisco implementation, which uses OLD-CISCO-INTERFACES-MIB.my.

If you do not enable this functionality, the link trap varbind list will consist of {ifIndex, ifDescr, ifType, locIfReason}. After you enable this functionality with the **snmp-server trap link ietf** command, the varbind list will consist of {inIndex, ifAdminStatus,ifOperStatus, if Descr, ifType}. The *locIfReason* object will also

be conditionally included in this list depending on whether meaningful information can be retrieved for that object. A configured sub-interface will generate retrievable information. On non-HWIDB interfaces, there will be no defined value for *locIfReason* , so it will be omitted from the trap message.

Examples

The following example shows the enabling of the RFC 2233 linkUp/linkDown traps, starting in privileged EXEC mode:

```
Router#
configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
snmp-server trap link ietf

Router(config)#
end
Router#
 more system:running configuration
.
.
.
!
snmp-server engineID local 00000009000000A1616C2056
snmp-server community public RO
snmp-server community private RW
snmp-server trap link ietf
!
.
.
.
```

Related Commands

Command	Description
debug snmp packets	Displays information about every SNMP packet sent or received by the router for the purposes of troubleshooting.

snmp-server trap link switchover

To enable sending a linkdown trap followed by a linkup trap for every interface in the switch during a switch failover, use the **snmp-server trap link switchover** command in global configuration mode. To disable linkdown during a switch failover, use the **no** form of this command.

snmp-server trap link switchover

no snmp-server trap link switchover

Syntax Description

This command has no arguments or keywords.

Command Default

This command is enabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXF2	This command was introduced on the Supervisor Engine 720 and the Supervisor Engine 32.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

By default, no link traps are generated during a switchover.

Examples

This example shows how to enable sending a linkdown trap followed by a linkup trap for every interface in the switch during a switch failover:

```
snmp-server trap link switchover
```

This example shows how to disable linkdown followed by a linkup trap for every interface in the switch during a switch failover:

```
no snmp-server trap link switchover
```

snmp-server trap retry

To define the number of times the Simple Network Management Protocol (SNMP) agent on a device tries to find a route before it sends traps, use the **snmp-server trap retry** command in global configuration mode.

snmp-server trap retry *number*

Syntax Description

number	Integer from 0 to 10 that sets the number of times the message will be retransmitted. The default is 3.

Command Default

Messages are not retransmitted.

Command Modes

Global configuration

Command History

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

Usage Guidelines

The SNMP agent looks for a configured route in the system before sending a trap out to a destination. If a route is not present, traps are queued in the trap queue and discarded when the queue becomes full. When the **snmp-server trap retry** command is configured, the route search retry number tells the agent how many times to look for the route before sending the trap out.

Configuring the **snmp-server trap retry** command also ensures that policy-based routing traps are sent and not discarded. Policy-based traps must be sent immediately and routes are not needed. The number of retries must be set to 0 so that policy-based traps are sent immediately.

Examples

The following example shows how to set the number of times a SNMP agent on a device tries to find a route to 10:

```
Router(config)# snmp-server trap retry 10
```

Related Commands

Command	Description
snmp-server trap timeout	Defines an interval of time between retransmissions of traps on a retransmission queue.

snmp-server trap timeout

To define an interval of time between retransmissions of trap messages on a retransmission queue, use the **snmp-server trap timeout** command in global configuration mode.

snmp-server trap timeout *seconds*

Syntax Description

seconds	Integer from 1 to 1000 that sets the interval, in seconds, for resending messages. The default is 30.

Command Default

This command is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(33)SRA	This command was introduced. This command replaces the **snmp-server trap-timeout** command in Cisco IOS Release 12.2SR only.

Usage Guidelines

Before a trap is sent, the SNMP agent looks for a route to the destination address. If there is no known route, the trap is saved in a retransmission queue. Issue the **snmp-server trap timeout** command to configure the number of seconds between retransmission attempts.

Examples

The following example shows how to set an interval of 20 seconds between retransmissions of traps:

```
Router(config)# snmp-server trap timeout 20
```

Related Commands

Command	Description
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server queue-length	Establishes the message queue length for each trap host.

snmp-server trap-authentication

The **snmp-server trap-authentication** command has been replaced by the **snmp-server enable traps snmp authentication** command. See the description of the **snmp-server enable traps snmp** command in this chapter for more information.

snmp-server trap-source

Note Effective with Cisco IOS Release 12.2(18)SXB6, the **snmp-server trap-sourc**e command is replaced by the **snmp-server source-interface**command. See the **snmp-server source-interface**command for more information.

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 the command.

snmp-server trap-source *interface*

no snmp-server trap-source

Syntax Description

interface	Interface from which the SNMP trap originates. Includes the interface type and number in platform-specific syntax (for example, *typeslot* /*port*).

Command Default

No interface is specified.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated in to Cisco IOS Release 12.2(33)SRA.
12.2(18)SXB6	This command was replaced by the **snmp-server source-interface**commandin Cisco IOS Release 12.2(18)SXB6.

Usage Guidelines

An SNMP trap or inform sent from a Cisco SNMP server has a notification address of the interface it went out of at that time. Use this command to monitor notifications from a particular interface.

Examples

The following example shows how to set the IP address for Ethernet interface 0 as the source for all SNMP notifications:

```
Router(config)# snmp-server trap-source ethernet 0
```

The following example shows how to set the IP address for the Ethernet interface in slot 2, port 1 as the source for all SNMP notifications:

```
Router(config)# snmp-server trap-source ethernet 2/1
```

Related Commands

Command	Description
snmp-server enable traps	Enables a router to send SNMP traps and informs.
snmp-server host	Specifies the recipient of a SNMP notification operation.

snmp-server trap-timeout

Note This command is not supported in Cisco IOS Release 12.2SR. For Cisco IOS Release12.2SR, use the **snmp-server trap timeout** command.

To define an interval of time before resending trap messages on the retransmission queue, use the **snmp-server trap-timeout** command in global configuration mode.

snmp-server trap-timeout *seconds*

Syntax Description

seconds	Integer from 1 to 1000 that sets the interval, in seconds, for resending messages. The default is 30.

Command Default

30 seconds

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was replaced by the **snmp-server trap timeout** command in Cisco IOS Release 12.2SR.

Usage Guidelines

The **snmp-server trap-timeout** command remains in Cisco IOS software for compatibility but is written in the configuration as **snmp-server trap timeout**.

Before the Cisco IOS 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. The **snmp-server trap-timeout** command determines the number of seconds between retransmission attempts.

Examples

The following example shows how to set an interval of 20 seconds between resending trap messages on the retransmission queue:

```
Router(config)# snmp-server trap-timeout 20
```

Related Commands

Command	Description
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server queue-length	Establishes the message queue length for each trap host.

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 group-name* [**remote** *host* [**udp-port** *port*] [**vrf** *vrf-name*]] {**v1**| **v2c**| **v3** **[encrypted]** [**auth** {**md5**| **sha**} *auth-password*]} [**access** [**ipv6** *nacl*] [**priv** {**des**| **3des**| **aes** {**128**| **192**| **256**}} *privpassword*] {*acl-number*| *acl-name*}]

no snmp-server user *username group-name* [**remote** *host* [**udp-port** *port*] [**vrf** *vrf-name*]] {**v1**| **v2c**| **v3** **[encrypted]** [**auth** {**md5**| **sha**} *auth-password*]} [**access** [**ipv6** *nacl*] [**priv** {**des**| **3des**| **aes** {**128**| **192**| **256**}} *privpassword*] {*acl-number*| *acl-name*}]

Syntax Description

username	Name of the user on the host that connects to the agent.
group-name	Name of the group to which the user belongs.
remote	(Optional) Specifies a remote SNMP entity to which the user belongs, and the hostname or IPv6 address or IPv4 IP address of that entity. If both an IPv6 address and IPv4 IP address are being specified, the IPv6 host must be listed first.
host	(Optional) Name or IP address of the remote SNMP host.
udp-port	(Optional) Specifies the User Datagram Protocol (UDP) port number of the remote host.
port	(Optional) Integer value that identifies the UDP port. The default is 162.
vrf	(Optional) Specifies an instance of a routing table.
vrf-name	(Optional) Name of the Virtual Private Network (VPN) routing and forwarding (VRF) table to use for storing data.
v1	Specifies that SNMPv1 should be used.
v2c	Specifies that SNMPv2c should be used.
v3	Specifies that the SNMPv3 security model should be used. Allows the use of the **encrypted** keyword or **auth** keyword or both.

encrypted	(Optional) Specifies whether the password appears in encrypted format.
auth	(Optional) Specifies which authentication level should be used.
md5	(Optional) Specifies the HMAC-MD5-96 authentication level.
sha	(Optional) Specifies the HMAC-SHA-96 authentication level.
auth-password	(Optional) String (not to exceed 64 characters) that enables the agent to receive packets from the host.
access	(Optional) Specifies an Access Control List (ACL) to be associated with this SNMP user.
ipv6	(Optional) Specifies an IPv6 named access list to be associated with this SNMP user.
nacl	(Optional) Name of the ACL. IPv4, IPv6, or both IPv4 and IPv6 access lists may be specified. If both are specified, the IPv6 named access list must appear first in the statement.
priv	(Optional) Specifies the use of the User-based Security Model (USM) for SNMP version 3 for SNMP message level security.
des	(Optional) Specifies the use of the 56-bit Digital Encryption Standard (DES) algorithm for encryption.
3des	(Optional) Specifies the use of the 168-bit 3DES algorithm for encryption.
aes	(Optional) Specifies the use of the Advanced Encryption Standard (AES) algorithm for encryption.
128	(Optional) Specifies the use of a 128-bit AES algorithm for encryption.
192	(Optional) Specifies the use of a 192-bit AES algorithm for encryption.
256	(Optional) Specifies the use of a 256-bit AES algorithm for encryption.
privpassword	(Optional) String (not to exceed 64 characters) that specifies the privacy user password.

acl-number	(Optional) Integer in the range from 1 to 99 that specifies a standard access list of IP addresses.
acl-name	(Optional) String (not to exceed 64 characters) that is the name of a standard access list of IP addresses.

Command Default

See the table in the "Usage Guidelines" section for default behaviors for encryption, passwords, and access lists.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.3(2)T	Support for named standard access lists was added.
12.0(27)S	The **ipv6** keyword and *nacl*argument were added to allow for configuration of IPv6 named access lists and IPv6 remote hosts.
12.3(14)T	The **ipv6** keyword and *nacl*argument were integrated into Cisco IOS Release 12.3(14)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(11)T	The **priv** keyword and associated arguments were added to enable the use of the USM for SNMP version 3 for SNMP message level security.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Aggregation Services Routers.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

To configure a remote user, specify the IP address or port number for the remote SNMP agent of the device where the user resides. Also, before you configure remote users for a particular agent, configure the SNMP engine ID, using the **snmp-server engineID** command with the **remote** keyword. The remote agent's SNMP engine ID is needed when computing the authentication and privacy digests from the password. If the remote engine ID is not configured first, the configuration command will fail.

For the *privpassword* and *auth-password*arguments, the minimum length is one character; the recommended length is at least eight characters, and should include both letters and numbers.

The table below describes the default user characteristics for encryption, passwords, and access lists.

Table 16: snmp-server user Default Descriptions

Characteristic	Default
Access lists	Access from all IP access lists is permitted.
Encryption	Not present by default. The **encrypted** keyword is used to specify that the passwords are message digest algorithm 5 (MD5)digests and not text passwords.
Passwords	Assumed to be text strings.
Remote users	All users are assumed to be local to this SNMP engine unless you specify they are remote with the **remote** keyword.

SNMP passwords are localized using the SNMP engine ID of the authoritative SNMP engine. For informs, the authoritative SNMP agent is the remote agent. You need to configure the remote agent's SNMP engine ID in the SNMP database before you can send proxy requests or informs to it.

Note Changing the engine ID after configuring the SNMP user, does not allow to remove the user. To remove the user, you need to first reconfigure the SNMP user.

Working with Passwords and Digests

No default values exist for authentication or privacy algorithms when you configure the command. Also, no default passwords exist. The minimum length for a password is one character, although Cisco recommends using at least eight characters for security. If you forget a password, you cannot recover it and will need to reconfigure the user. You can specify either a plain-text password or a localized MD5 digest.

If you have the localized MD5 or Secure Hash Algorithm (SHA) digest, you can specify that string instead of the plain-text password. The digest should be formatted as aa:bb:cc:dd where aa, bb, and cc are hexadecimal values. Also, the digest should be exactly 16 octets long.

Examples

The following example shows how to add the user abcd to the SNMP server group named public. In this example, no access list is specified for the user, so the standard named access list applied to the group applies to the user.

```
Router(config)# snmp-server user abcd public v2c
```

The following example shows how to add the user abcd to the SNMP server group named public. In this example, access rules from the standard named access list qrst apply to the user.

```
Router(config)# snmp-server user abcd public v2c access qrst
```

In the following example, the plain-text password cisco123 is configured for the user abcd in the SNMP server group named public:

```
Router(config)# snmp-server user abcd public v3 auth md5 cisco123
```

When you enter a **show running-config** command, a line for this user will be displayed. To learn if this user has been added to the configuration, use the show snmp user command.



Note The **show running-config** command does not display any of the active SNMP users created in authPriv or authNoPriv mode, though it does display the users created in noAuthNoPriv mode. To display any active SNMPv3 users created in authPriv, authNoPrv, or noAuthNoPriv mode, use the **show snmp user** command.

If you have the localized MD5 or SHA digest, you can specify that string instead of the plain-text password. The digest should be formatted as aa:bb:cc:dd where aa, bb, and cc are hexadecimal values. Also, the digest should be exactly 16 octets long.

In the following example, the MD5 digest string is used instead of the plain-text password:

```
Router(config)# snmp-server user abcd public v3 encrypted auth md5
00:11:22:33:44:55:66:77:88:99:AA:BB:CC:DD:EE:FF
```

In the following example, the user abcd is removed from the SNMP server group named public:

```
Router(config)# no snmp-server user abcd public v2c
```

In the following example, the user abcd from the SNMP server group named public specifies the use of the 168-bit 3DES algorithm for privacy encryption with secure3des as the password.

```
Router(config)# snmp-server user abcd public priv v2c 3des secure3des
```

Related Commands

Command	Description
show running-config	Displays the contents of the currently running configuration file or the configuration for a specific interface, or map class information.
show snmp user	Displays information on each SNMP username in the group username table.
snmp-server engineID	Displays the identification of the local SNMP engine and all remote engines that have been configured on the router.

snmp-server usm cisco

To enable Cisco-specific error messages for Simple Network Management Protocol Version 3 (SNMPv3), which is a User-based Security Model (USM), use the **snmp-server usm cisco** command in global configuration mode. To disable the Cisco-specific error messages for SNMPv3 USM, use the **no** form of this command.

snmp-server usm cisco

no snmp-server usm cisco

Syntax Description

This command has no arguments or keywords.

Command Default

Cisco-specific error messages for SNMPv3 USM are disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(1)T	This command was introduced.

Usage Guidelines

The RFC 3414-compliant error messages are descriptive and can lead to misuse of information by malicious users. Use the **snmp-server usm cisco** command to enable Cisco-specific messages that help to hide the exact error condition. Enabling Cisco-specific messages for SNMPv3 is a deviation from RFC 3414.

Examples

The following example shows how to enable the Cisco-specific error messages for SNMPv3 USM:

```
Router> enable
Router# configure terminal
Router(config)# snmp-server usm cisco
Router(config)# exit
```

Related Commands

Command	Description
show running-config	Displays the contents of the current running configuration file or the configuration for a specific module, Layer 2 VLAN, class map, interface, map class, policy map, or virtual circuit (VC) class.

snmp-server view

To create or update a view entry, use the **snmp-server view** command in global configuration mode. To remove the specified Simple Network Management Protocol (SNMP) server view entry, use the **no**form of this command.

snmp-server view *view-name oid-tree* {**included**| **excluded**}

no snmp-server view *view-name*

Syntax Description

view-name	Label for the view record that you are updating or creating. The name is used to reference the record.
oid-tree	Object identifier 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.
included	Configures the OID (and subtree OIDs) specified in *oid-tree* argument to be included in the SNMP view.
excluded	Configures the OID (and subtree OIDs) specified in *oid-tree* argument to be explicitly excluded from the SNMP view.

Command Default

No view entry exists.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.3(4)T	This command was modified to exclude USM, VACM, and Community MIBs from any parent OIDs in a configured view by default.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Other SNMP commands require an SMP view as an argument. You use this command to create a view to be used as arguments for other commands.

Two standard predefined views can be used when a view is required, instead of defining a view. One is *everything*, which indicates that the user can see all objects. The other is *restricted,*which indicates that the user can see three groups: system, snmpStats, and snmpParties. The predefined views are described in RFC 1447.

Note Beginning in Release 12.0(26)S and 12.2(2)T, the USM, VACM, and Community MIBs are excluded from any parent OIDs in a configured view by default. If you wish to include these MIBs in a view, you must now explicitly include them.

The first **snmp-server** command that you enter enables SNMP on your routing device.

Examples

The following example creates a view that includes all objects in the MIB-II subtree:

```
snmp-server view mib2 mib-2 included
```

The following example creates a view that includes all objects in the MIB-II system group and all objects in the Cisco enterprise MIB:

```
snmp-server view root_view system included
snmp-server view root_view cisco included
```

The following example creates 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:

```
snmp-server view agon system included
snmp-server view agon system.7 excluded
snmp-server view agon ifEntry.*.1 included
```

In the following example, the USM, VACM, and Community MIBs are explicitly included in the view “test” with all other MIBs under the root parent “internet”:

```
! -- include all MIBs under the parent tree “internet”
snmp-server view test internet included
! -- include snmpUsmMIB
snmp-server view test 1.3.6.1.6.3.15 included
! -- include snmpVacmMIB
snmp-server view test 1.3.6.1.6.3.16 included
! -- exclude snmpCommunityMIB
snmp-server view test 1.3.6.1.6.3.18 excluded
```

Related Commands

Command	Description
snmp-server community	Sets up the community access string to permit access to the SNMP protocol.

snmp trap if-monitor

To enable if-monitor traps for a particular interface, use the **snmp trap if-monitor**command in interface configuration mode. To disable traps on an interface, use the **no** form of this command.

snmp trap if-monitor

no snmp trap if-monitor

Syntax Description

This command has no arguments or keywords.

Command Default

Traps are not generated.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

Traps are sent for the interface only if they have been enabled globally by issuing the **snmp-server enable traps if-monitor** command and then explicitly on that interface by issuing the **snmp trap if-monitor**command.

Examples

The following example shows how to enable if-monitor traps on a specific interface:

```
Router(config)# snmp-server enable traps if-monitor
Router(config)# interface ethernet 1/1
Router(config-if)# snmp trap if-monitor
```

Related Commands

Command	Description
snmp-server enable traps if-monitor	Globally enables if-monitor traps.

snmp trap link-status

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

snmp trap link-status [**permit duplicates**]

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

Syntax Description

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

Command Default

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

Command Modes

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

Command History

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

Usage Guidelines

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

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

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

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

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

Cisco 10000 Series Router

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

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

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

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

Examples

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

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

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

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

Related Commands

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



startup (test boolean) through write mib-data

- startup (test boolean), page 409
- startup (test existence), page 410
- startup (test threshold), page 411
- test (event trigger), page 413
- test snmp trap auth-framwork sec-violation, page 415
- test snmp trap bridge, page 416
- test snmp trap c6kxbar, page 417
- test snmp trap call-home, page 420
- test snmp trap config-copy, page 421
- test snmp trap dhcp bindings, page 423
- test snmp trap dhcp-snooping bindings, page 424
- test snmp trap dot1x, page 425
- test snmp trap entity-diag, page 426
- test snmp trap errdisable ifevent, page 428
- test snmp trap flex-links status, page 429
- test snmp trap fru-ctrl, page 430
- test snmp trap l2-control vlan, page 431
- test snmp trap l2tc, page 432
- test snmp trap mac-notification, page 433
- test snmp trap module-auto-shutdown, page 434
- test snmp trap port-security, page 435
- test snmp trap power-ethernet port-on-off, page 436
- test snmp trap snmp, page 437
- test snmp trap stack, page 439

- test snmp trap storm-control, page 440
- test snmp trap stpx, page 441
- test snmp trap syslog, page 442
- test snmp trap trustsec, page 444
- test snmp trap trustsec-interface, page 446
- test snmp trap trustsec-policy, page 447
- test snmp trap trustsec-server, page 448
- test snmp trap trustsec-sxp, page 449
- test snmp trap udld, page 451
- test snmp trap vswitch dual-active, page 452
- test snmp trap vswitch vsl, page 454
- test snmp trap vtp, page 455
- test snmp trap vtp pruning-change, page 457
- type (test existence), page 458
- url (bulk statistics), page 460
- value (test boolean), page 462
- value type, page 463
- wildcard (expression), page 466
- write mib-data, page 467

startup (test boolean)

To specify whether an event can be triggered for the Boolean trigger test, use the **startup** command in event trigger boolean configuration mode. To disable the configured settings, use the **no** form of this command.

startup

no startup

Syntax Description

This command has no arguments or keywords.

Command Default

The startup event is enabled when the Boolean trigger test is enabled.

Command Modes

Event trigger boolean configuration (config-event-trigger-boolean)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.

Usage Guidelines

The **startup** command triggers an event when the conditions specified for the Boolean trigger test are met.

Examples

The following example shows how to specify startup for the Boolean trigger test:

```
Router(config)# snmp mib event trigger owner owner1 name EventA
Router(config-event-trigger)# test boolean
Router(config-event-trigger-boolean)# startup
Router(config-event-trigger-boolean)# end
```

Related Commands

Command	Description
test	Enables a trigger test.

startup (test existence)

To specify whether an event can be triggered for the existence trigger test, use the **startup** command in event trigger existence configuration mode. To disable the configured settings, use the **no** form of this command.

startup {**present**| **absent**}

no startup {**present**| **absent**}

Syntax Description

present	Triggers the present startup test when the existence trigger conditions are met.
absent	Triggers the absent startup test when the existence trigger conditions are met.

Command Default

By default, both present and absent startup tests are triggered.

Command Modes

Event trigger existence configuration (config-event-trigger-existence)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.

Usage Guidelines

The **startup** command triggers an event when the conditions specified for the existence trigger test are met.

Examples

The following example shows how to specify startup for the existence trigger test:

```
Router(config)# snmp mib event trigger owner owner1 name EventA
Router(config-event-trigger)# test existence
Router(config-event-trigger-existence)# startup
Router(config-event-trigger-existence)# end
```

Related Commands

Command	Description
test	Enables a trigger test.

startup (test threshold)

To specify whether an event can be triggered for the threshold trigger test, use the **startup** command in event trigger threshold configuration mode. To disable the configured settings, use the **no** form of this command.

startup {**rising**| **falling**| **rise-or-falling**}

no startup

Syntax Description

rising	Specifies the rising threshold value to check against the set value during startup when the trigger type is threshold.
falling	Specifies the falling threshold value to check against the set value during startup when the trigger type is threshold.
rise-or-falling	Specifies the rising or falling threshold value to check against the set value during startup when the trigger type is threshold. This is the default value.

Command Default

The rising or falling threshold value is checked against the set value during startup when the trigger type is threshold.

Command Modes

Event trigger threshold configuration (config-event-trigger-threshold)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.

Usage Guidelines

The **startup** command starts an event when conditions for the threshold trigger test are met.

Examples

The following example shows how to specify startup for the threshold trigger test:

```
Router(config)# snmp mib event trigger owner owner1 name EventA
Router(config-event-trigger)# test threshold
Router(config-event-trigger-threshold)# startup rising
Router(config-event-trigger-threshold)# end
```

Related Commands

Command	Description
test	Enables a trigger test.

test (event trigger)

To specify the type of test to perform during an event trigger, use the **test** command in event trigger configuration mode. To disable the trigger test configuration settings, use the **no** form of this command.

test {**existence**| **boolean**| **threshold**}

no test {**existence**| **boolean**| **threshold**}

Syntax Description

existence	Enables the existence trigger test.
boolean	Enables the Boolean trigger test. Boolean test is the default trigger test performed during event triggers.
threshold	Enables the threshold trigger test.

Command Default

The Boolean trigger test is enabled by default.

Command Modes

Event trigger configuration (config-event-trigger)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.

Usage Guidelines

The trigger table in the Event MIB has supplementary tables for additional objects that are configured based on the type of test performed for the trigger. For each trigger entry type such as existence, threshold, or Boolean, the corresponding tables (existence, threshold, and Boolean tables) are populated with the information required to perform the test. You can set event triggers based on existence, threshold, and Boolean trigger types.

The existence trigger tests are performed based on the following parameters:

- Absent
- Present
- Changed

The Boolean tests are comparison tests that are performed based on one of the following parameters:

- Unequal
- Equal
- Less
- Less Or Equal
- Greater
- Greater Or Equal

The threshold tests are performed based on the following parameters:

- Rising
- Falling
- Rising or Falling

Examples

The following example shows how to enable the existence trigger test:

```
Router(config)# snmp mib event trigger owner owner1 name triggerA
Router(config-event-trigger)# test existence
Router(config-event-trigger-existence)#
```

The following example shows how to enable the Boolean trigger test:

```
Router(config)# snmp mib event trigger owner owner1 name EventA
Router(config-event-trigger)# test boolean
Router(config-event-trigger-boolean)#
```

The following example shows how to enable the threshold trigger test:

```
Router(config)# snmp mib event trigger owner owner1 name triggerA
Router(config-event-trigger)# test threshold
Router(config-event-trigger-threshold)#
```

Related Commands

Command	Description
comparison	Specifies the type of Boolean comparison to be performed.
event owner	Specifies the event owner for an event trigger according to the trigger type and status of the trigger.
object list	Configures a list of objects during an event.
startup	Specifies whether an event can be triggered for the Boolean, existence, or threshold trigger test.
value	Sets a value for the Boolean trigger test.

test snmp trap auth-framwork sec-violation

To test CISCO-AUTH-FRAMEWORK-MIB Simple Network Management Protocol (SNMP) notifications (traps and informs), use the **test snmp trap auth-framwork sec-violation**command in priveleged EXEC mode.

test snmp trap auth-framwork sec-violation

Syntax Description

This command has no keywords or arguments.

Command Default

This command has no default setting.

Command Modes

Privileged EXEC mode

Command History

Release	Modification
12.2(33)SXI	This command was introduced on the Supervisor Engine 720.

Examples

This example shows the output of the SNMP camSecurityViolationNotif trap when it is not configured:

```
Router# test
 snmp trap auth-framework sec-violation
cafSecurityViolationNotif was disabled.
Router#
```

This example shows the output of the SNMP camSecurityViolationNotif trap when it is configured:

```
Router# test
 snmp trap auth-framework sec-violation
cafSecurityViolationNotif was sent.
Router#
```

test snmp trap bridge

To test BRIDGE-MIB Simple Network Management Protocol (SNMP) notifications (traps and informs), use the **test snmp trap bridge**command in priveleged EXEC mode.

test snmp trap bridge {**newroot**| **topologychange**}

Syntax Description

newroot	Tests SNMP newRoot notifications.
topologychange	Tests SNMP topologyChange notifications.

Command Default

This command has no default setting.

Command Modes

Priveleged EXEC mode

Command History

Release	Modification
12.2(33)SXI	This command was introduced on the Supervisor Engine 720 and Supervisor Engine 32.

Examples

This example shows the output of **test snmp trap bridge newroot** when snmp-server enable traps bridge newroot is not configured:

```
Router# test
 snmp trap bridge newroot
newRoot notification is disabled.
Router#
```

This example shows the output of **test snmp trap bridge newroot** when snmp-server enable traps bridge newroot is configured:

```
Router# test
 snmp trap bridge newroot
newRoot notification was sent.
Router#
```

Related Commands

Command	Description
snmp-server enable traps bridge	Enables the SNMP BRIDGE-MIB notifications.

test snmp trap c6kxbar

To test CISCO-CAT6K-CROSSBAR-MIB Simple Network Management Protocol (SNMP) notifications (traps and informs), use the **test snmp trap c6kxbar**command in priveleged EXEC mode.

test snmp trap c6kxbar {**flowctrl-bus**| **intbus-crccvrd**| **intbus-crcexcd**| **swbus**| **tm-channel-above**| **tm-channel-below**| **tm-swbus-above**| **tm-swbus-below**}

Syntax Description

flowctrl-bus	Tests SNMP cc6kxbarFlowCtrlBusThrExcdNotif notifications.
intbus-crcvrd	Tests SNMP cc6kxbarIntBusCRCErrRcvrdNotif notifications.
intbus-crcexcd	Tests SNMP cc6kxbarIntBusCRCErrExcdNotif notifications.
swbus	Tests SNMP cc6kxbarSwBusStatusChangeNotif notifications.
tm-channel-above	Tests cc6kxbarTMChUtilAboveNotif notifications.
tm-channel-below	Tests cc6kxbarTMChUtilBelowNotif notifications.
tm-swbus-above	Tests cc6kxbarTMSwBusUtilAboveNotif notifications.
tm-swbus-below	Tests cc6kxbarTMSwBusUtilBelowNotif notifications.

Command Default

This command has no default setting.

Command Modes

Priveleged EXEC mode

Command History

Release	Modification
12.2(33)SXI	This command was introduced on the Supervisor Engine 720.
12.2(33)SXI5	Added **tm-channel-above**, **tm-channel-below**and **tm-swbus-above**, **tm-channel-below**keywords.

Usage Guidelines

The **flowctrl-bus** keyword is supported on the Supervisor Engine 32 only.

The **tm-channel-above** and **tm-channel-below** keywords are not supported on Supervisor Engine 32.

Examples

This example shows the output of the SNMP cc6kxbarFlowCtrlBusThrExcdNotif notification when it is not configured:

```
Router# test
 snmp trap c6kxbar flowctrl-bus
cc6kxbarFlowCtrlBusThrExcdNotif notification is disabled.
Router#
```

This example shows the output of the SNMP cc6kxbarFlowCtrlBusThrExcdNotif notification when it is configured:

```
Router# test
 snmp trap c6kxbar flowctrl-bus
cc6kxbarFlowCtrlBusThrExcdNotif notification was sent.
Router#
```

This example shows the output of the SNMP cc6kxbarIntBusCRCErrExcdNotif notification when it is not configured:

```
Router# test
 snmp trap c6kxbar intbus-crcexcd
cc6kxbarIntBusCRCErrExcdNotif notification is disabled.
Router#
```

This example shows the output of the SNMP cc6kxbarIntBusCRCErrExcdNotif notification when it is configured:

```
Router# test
 snmp trap c6kxbar intbus-crcexcd
cc6kxbarIntBusCRCErrExcdNotif notification was sent.
Router#
```

This example shows the output of the SNMP cc6kxbarIntBusCRCErrRcvrdNotif notification when it is not configured:

```
Router# test snmp trap c6kxbar intbus-crcvrd
cc6kxbarIntBusCRCErrExcdNotif notification is disabled.
Router#
```

This example shows the output of the SNMP cc6kxbarIntBusCRCErrRcvrdNotif notification when it is configured:

```
Router# test snmp trap c6kxbar intbus-crcvrd
cc6kxbarIntBusCRCErrExcdNotif notification was sent.
Router#
```

This example shows the output of the SNMP cc6kxbarSwBusStatusChangeNotif notification when it is not configured:

```
Router# test snmp trap c6kxbar swbus
cc6kxbarSwBusStatusChangeNotif notification is disabled.
Router#
```

This example shows the output of the SNMP cc6kxbarSwBusStatusChangeNotif notification when it is configured:

```
Router# test snmp trap c6kxbar swbus
cc6kxbarSwBusStatusChangeNotif notification was sent.
Router#
```

This example shows the output of the SNMP cc6kxbarTMChUtilAboveNotif notification when it is not configured:

```
Router# test snmp trap c6kxbar tm-channel-above
cc6kxbarTMChUtilAboveNotif notification is disabled.
Router#
```

This example shows the output of the SNMP cc6kxbarTMChUtilAboveNotif notification when it is configured:

```
Router# test snmp trap c6kxbar tm-channel-above
cc6kxbarTMChUtilAboveNotif notification was sent.
Router#
```

This example shows the output of the SNMP cc6kxbarTMChUtilBelowNotif notification when it is not configured:

```
Router# test snmp trap c6kxbar tm-channel-below
cc6kxbarTMChUtilBelowNotif notification is disabled.
Router#
```

This example shows the output of the SNMP cc6kxbarTMChUtilBelowNotif notification when it is configured:

```
Router# test snmp trap c6kxbar tm-channel-below
cc6kxbarTMChUtilBelowNotif notification was sent.
Router#
```

This example shows the output of the SNMP cc6kxbarTMSwBusUtilAboveNotif notification when it is not configured:

```
Router# test snmp trap c6kxbar tm-swbus-above
cc6kxbarTMSwBusUtilAboveNotif notification is disabled.
Router#
```

This example shows the output of the SNMP cc6kxbarTMSwBusUtilAboveNotif notification when it is configured:

```
Router# test snmp trap c6kxbar tm-swbus-above
cc6kxbarTMSwBusUtilAboveNotif notification was sent.
Router#
```

This example shows the output of the SNMP cc6kxbarTMSwBusUtilBelowNotif notification when it is not configured:

```
Router# test snmp trap c6kxbar tm-swbus-below
cc6kxbarTMSwBusUtilBelowNotif notification is disabled.
Router#
```

This example shows the output of the SNMP cc6kxbarTMSwBusUtilBelowNotif notification when it is configured:

```
Router# test snmp trap c6kxbar tm-swbus-below
cc6kxbarTMSwBusUtilBelowNotif notification was sent.
Router#
```

Related Commands

Command	Description
snmp-server enable traps c6kxbar	Enables the SNMP c6kxbar notification traps.

test snmp trap call-home

To test CISCO-CALLHOME-MIB Simple Network Management Protocol (SNMP) notifications (traps and informs), use the **test snmp trap call-home**command in priveleged EXEC mode.

test snmp trap call-home {**message-send-fail**| **server-fail**}

Syntax Description

message-send-fail	Tests SNMP ccmSmtpMsgSendFailNotif notifications.
server-fail	Tests SNMP ccmSmtpServerFailNotif notifications.

Command Default

This command has no default setting.

Command Modes

Privileged EXEC mode

Command History

Release	Modification
12.2(33)SXI	This command was introduced on the Supervisor Engine 720.

Examples

This example shows the output of the SNMP ccmSmtpMsgSendFailNotif notification when it is not configured:

```
Router# test
 snmp trap call-home message-send-fail
ccmSmtpMsgSendFailNotif notification is disabled.
Router#
```

This example shows the output of the SNMP ccmSmtpMsgSendFailNotif notification when it is configured:

```
Router# test
 snmp trap call-home message-send-fail
ccmSmtpMsgSendFailNotif notification was sent.
Router#
```

This example shows the output of the SNMP ccmSmtpServerFailNotif notification when it is not configured:

```
Router# test
 snmp trap call-home server-fail
ccmSmtpServerFailNotif notification is disabled.
Router#
```

This example shows the output of the SNMP ccmSmtpServerFailNotif notification when it is configured:

```
Router# test
 snmp trap call-home server-fail
ccmSmtpServerFailNotif notification was sent.
Router#
```

test snmp trap config-copy

To verify the reception of config-copy notifications by the Network Management System (NMS) or the Simple Network Management Protocol (SNMP) manager in a simulated scenario, use the **test snmp trap config-copy** command in privileged EXEC mode.

test snmp trap config-copy

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SXI	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.

Usage Guidelines

The Config-Copy MIB facilitates the copying of SNMP agent configuration files to the startup configuration or the local Cisco IOS file system, and vice versa. The config-copy notifications are sent to the NMS or the SNMP manager to indicate the successful completion of config-copy operation to or from the SNMP agent.

Examples

The following example shows how to simulate the verification of config-copy traps:

```
Router#
 test snmp trap config-copy
Generating CONFIG-COPY-MIB trap
00:20:44: SNMP: Queuing packet to 10.2.14.2
00:20:44: SNMP: V2 Trap, reqid 2, errstat 0, erridx 0
 sysUpTime.0 = 124470
 snmpTrapOID.0 = ccCopyMIBTraps.1
 ccCopyTable.1.5.2 = 10.10.10.10
 ccCopyTable.1.6.2 =
 ccCopyTable.1.10.2 = 3
 ccCopyTable.1.11.2 = 124470
 ccCopyTable.1.12.2 = 124470
Router#
```

Related Commands

Command	Description
debug snmp packet	Displays information about every SNMP packet sent or received by the router.
snmp-server enable traps	Enables all SNMP notification types that are available on your system.

Command	Description
snmp-server host	Specifies the recipient of an SNMP notification operation.

test snmp trap dhcp bindings

To test the cdsBindingsNotification trap, use the **test snmp trap dhcp bindings**EXEC command.

test snmp trap dhcp bindings

Syntax Description

This command has no keywords or arguments.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC mode

Command History

Release	Modification
12.2(33)SXI	Support for this command was introduced on the Catalyst 6500 series switch.

Examples

This example shows how to test the cdsBindingsNotification traps:

```
Router# test snmp trap dhcp bindings
cdsBindingsNotification notification is disabled.
```

test snmp trap dhcp-snooping bindings

To test the cdsBindingsNotification trap, use the **test snmp trap dhcp-snooping bindings**privileged EXEC command.

test snmp trap dhcp-snooping bindings

Syntax Description

This command has no keywords or arguments.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC mode

Command History

Release	Modification
12.2(33)SXI4	Support for this command was introduced on the Catalyst 6500 series.

Examples

This example shows how to test the cdsBindingsNotification trap:

```
Router# test snmp trap dhcp-snooping bindings
cdsBindingsNotification notification is disabled.
```

test snmp trap dot1x

To test CISCO-PAE-MIB Simple Network Management Protocol (SNMP) notifications (traps and informs), use the **test snmp trap dot1x**command in priveleged EXEC mode.

test snmp trap dot1x {**auth-fail-vlan**| **guest-vlan**| **no-auth-fail-vlan**| **no-guest-vlan**}

Syntax Description

auth-fail-vlan	Tests SNMP cpaeAuthFailVlanNotif notifications.
guest-vlan	Tests SNMP cpaeGuestVlanNotif notifications.
no-auth-fail-vlan	Tests SNMP cpaeNoAuthFailedVlanNotif notifications.
no-guest-vlan	Tests SNMP cpaeNoGuestVlanNotif notifications.

Command Default

This command has no default setting.

Command Modes

Privileged EXEC mode

Command History

Release	Modification
12.2(33)SXI	This command was introduced on the Supervisor Engine 720.

Examples

This example shows the output of the SNMP cpaeAuthFailVlanNotif notification when it is not configured:

```
Router# test
 snmp trap dot1x auth-fail-vlan
cpaeAuthFailVlanNotif notification was disabled.
Router#
```

This example shows the output of the SNMP cpaeAuthFailVlanNotif notification when it is configured:

```
Router# test
 snmp trap dot1x auth-fail-vlan
cpaeAuthFailVlanNotif notification was sent.
Router#
```

test snmp trap entity-diag

To test CISCO-ENTITY-DIAG-MIB Simple Network Management Protocol (SNMP) notifications (traps and informs), use the **test snmp trap c6kxbar**command in privileged EXEC mode.

test snmp trap entity-diag {**boot-up-fail| hm-test-recover| hm-thresh-reached| scheduled-test-fail**}

Syntax Description

boot-up-fail	Tests SNMP ceDiagBootUpFailedNotif notifications.
hm-test-recover	Tests SNMP ceDiagHMTestRecoverNotif notifications.
hm-thresh-reached	Tests SNMP ceDiagHMThresholdReachedNotif notifications.
scheduled-test-fail	Tests SNMP ceDiagScheduledTestFailedNotif notifications.

Command Default

This command has no default setting.

Command Modes

Privileged EXEC mode

Command History

Release	Modification
12.2(33)SXI	This command was introduced on the Supervisor Engine 720.

Examples

This example shows the output of the SNMP ceDiagBootupFailedNotif notification when it is not configured:

```
Router# test
 snmp trap entity-diag boot-up-fail
ceDiagBootupFailedNotif notification is disabled.
Router#
```

This example shows the output of the SNMP ceDiagBootupFailedNotif notification when it is configured:

```
Router# test
 snmp trap entity-diag boot-up-fail
ceDiagBootupFailedNotif notification was sent.
Router#
```

This example shows the output of the SNMP ceDiagHMTestRecoverNotif notification when it is not configured:

```
Router# test
 snmp trap dot1x hm-test-recover
ceDiagHMTestRecoverNotif notification is disabled.
Router#
```

This example shows the output of the SNMP ceDiagHMTestRecoverNotif notification when it is configured:

```
Router# test
 snmp trap dot1x hm-test-recover
ceDiagHMTestRecoverNotif notification was sent.
Router#
```

This example shows the output of the SNMP ceDiagHMThresholdReachedNotif notification when it is not configured:

```
Router# test snmp trap entity-diag hm-thresh-reached
ceDiagHMThresholdReachedNotif notification is disabled.
Router#
```

This example shows the output of the SNMP ceDiagHMThresholdReachedNotif notification when it is configured:

```
Router# test snmp trap entity-diag hm-thresh-reached
ceDiagHMThresholdReachedNotif notification was sent.
Router#
```

This example shows the output of the SNMP ceDiagScheduledTestFailedNotif notification when it is not configured:

```
Router# test snmp trap entity-diag scheduled-test-fail
ceDiagHMThresholdReachedNotif notification is disabled.
Router#
```

This example shows the output of the SNMP ceDiagScheduledTestFailedNotif notification when it is configured:

```
Router# test snmp trap entity-diag scheduled-test-fail
ceDiagHMThresholdReachedNotif notification was sent.
Router#
```

test snmp trap errdisable ifevent

To test CISCO-ERR-DISABLE-MIB cErrDisableInterfaceEventRev1 Simple Network Management Protocol (SNMP) traps and informs, use the **test snmp trap errdisable ifevent**command in priveleged EXEC mode.

test snmp trap errdisable ifevent

Syntax Description

This command has no keywords or arguments.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC mode

Command History

Release	Modification
12.2(33)SXI4	This command was introduced on the Supervisor Engine 720 and Supervisor Engine 32.

Examples

This example shows the output of **test snmp trap errdisable ifevent** when snmp-server enable traps errdisable is not configured:

```
Router# test
 snmp trap errdisable ifevent
cErrDisableInterfaceEventRev1 notification is disabled.
Router#
```

This example shows the output of **test snmp trap errdisable ifevent** when snmp-server enable traps errdisable is configured:

```
Router# test
 snmp trap errdisable ifevent
cErrDisableInterfaceEventRev1 notification was sent.
Router#
```

Related Commands

Command	Description
snmp-server enable traps errdisable	Enables SNMP errdisable notifications.

test snmp trap flex-links status

To test CISCO-FLEX-LINKS-MIB cflIfStatusChangeNotif traps Simple Network Management Protocol (SNMP) traps and informs, use the **test snmp trap flex-links status**command in priveleged EXEC mode.

test snmp trap flex-links status

Syntax Description

This command has no keywords or arguments.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC mode

Command History

Release	Modification
12.2(33)SXI	This command was introduced on the Supervisor Engine 720 and Supervisor Engine 32.

Examples

This example shows the output of the SNMP cflIfStatusChangeNotif trap when it is not configured:

```
Router# test
 snmp trap flex-links status
cflIfStatusChangeNotifnotification is disabled.
Router#
```

This example shows the output of the SNMP cflIfStatusChangeNotif trap when it is configured:

```
Router# test
 snmp trap flex-links status
cflIfStatusChangeNotif notification was sent.
Router#
```

test snmp trap fru-ctrl

To test CISCO-ENTITY-FRU-CONTROL-MIB traps Simple Network Management Protocol (SNMP) traps and informs, use the **test snmp trap fru-ctrl**command in privileged EXEC mode.

test snmp trap fru-ctrl {**insert**| **module-status**| **power-status**| **ps-out-change**| **remove**}

Syntax Description

insert	Tests SNMP cefcFRUInserted notifications.
module-status	Tests SNMP cefcModuleStatusChange notifications.
power-status	Tests SNMP cefcPowerStatusChange notifications.
ps-out-change	Tests SNMP cefcPowerSupplyOutputChange notifications.
remove	Tests SNMP cefcFRURemoved notifications.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC mode

Command History

Release	Modification
12.2(33)SXI	This command was introduced on the Supervisor Engine 720 and Supervisor Engine 32.

Examples

This example shows the output of the test SNMP cefcFRUInserted trap when it is not configured:

```
Router# test
 snmp trap fru-ctrl insert
cefcFRUInserted notification is disabled.
Router#
```

This example shows the output of the SNMP cefcFRUInserted trap when it is configured:

```
Router# test
 snmp trap fru-ctrl insert
cefcFRUInserted notification was sent.
Router#
```

test snmp trap l2-control vlan

To test CISCO-ENTITY-FRU-CONTROL-MIB clcVLANMacLimitNotif traps Simple Network Management Protocol (SNMP) traps and informs, use the **test snmp trap l2-control vlan**command in privileged EXEC mode.

test snmp trap l2-control vlan

Syntax Description

This command has no keywords or arguments.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC mode

Command History

Release	Modification
12.2(33)SXI	This command was introduced on the Supervisor Engine 720 and Supervisor Engine 32.

Examples

This example shows the output of the clcVLANMacLimitNotif trap when it is not configured:

```
Router# test
 snmp trap l2-control vlan
clcVLANMacLimitNotif notification is disabled.
Router#
```

This example shows the output of the SNMP clcVLANMacLimitNotif trap when it is configured:

```
Router# test
 snmp trap l2-control vlan
clcVLANMacLimitNotif notification was sent.
Router#
```

test snmp trap l2tc

To test CISCO-L2-TUNNEL-CONFIG-MIB traps Simple Network Management Protocol (SNMP) traps and informs, use the **test snmp trap l2tc**command in privileged EXEC mode.

test snmp trap l2tc {**drop**| **shutdown**| **sys-threshold**}

Syntax Description

drop	Tests SNMP cltcTunnelDropThresholdExceeded notifications.
shutdown	Tests SNMP cltcTunnelShutdwonThresholdExceeded notifications.
sys-threshold	Tests SNMP cltcTunnelSysDropThresholdExceeded notifications.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC mode

Command History

Release	Modification
12.2(33)SXI	This command was introduced on the Supervisor Engine 720 and Supervisor Engine 32.

Examples

This example shows the output of the cltcTunnelDropThresholdExceeded trap when it is not configured:

```
Router# test
 snmp trap l2tc drop
cltcTunnelDropThresholdExceeded notification is disabled.
Router#
```

This example shows the output of the SNMP cltcTunnelDropThresholdExceeded trap when it is configured:

```
Router# test
 snmp trap l2tc drop
cltcTunnelDropThresholdExceeded notification was sent.
Router#
```

test snmp trap mac-notification

To test CISCO-MAC-NOTIFICATION-MIB traps Simple Network Management Protocol (SNMP) traps and informs, use the **test snmp trap mac-notification**command in privileged EXEC mode.

test snmp trap mac-notification {**change**| **move**| **threshold**}

Syntax Description

change	Tests SNMP cmnMacChangeNotification notifications.
move	Tests SNMP cmnMacMoveNotification notifications.
threshold	Tests SNMP cmnMacThresholdExceedNotif notifications.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC mode

Command History

Release	Modification
12.2(33)SXI	This command was introduced on the Supervisor Engine 720 and Supervisor Engine 32.

Examples

This example shows the output of the SNMP cmnMacChangeNotification trap when it is not configured:

```
Router# test
 snmp trap mac-notification change
cmnMacChangeNotification notification is disabled.
Router#
```

This example shows the output of the SNMP cmnMacChangeNotification trap when it is configured:

```
Router# test
 snmp trap mac-notification change
cmnMacChangeNotification notification was sent.
Router#
```

test snmp trap module-auto-shutdown

To test CISCO-MODULE-AUTO-SHUTDOWN-MIB traps Simple Network Management Protocol (SNMP) traps and informs, use the **test snmp trap module-auto-shutdown**command in privileged EXEC mode.

test snmp trap module-auto-shutdown {**auto-shutdown**| **sys-action**}

Syntax Description

auto-shutdown	Tests SNMP cmasModuleAutoShutdown notifications.
sys-action	Tests SNMP cmasModuleSysActionNotif notifications.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC mode

Command History

Release	Modification
12.2(33)SXI	This command was introduced on the Supervisor Engine 720 and Supervisor Engine 32.

Examples

This example shows the output of the SNMP cmasModuleAutoShutdown trap when it is not configured:

```
Router# test
 snmp trap module-auto-shutdown auto-shutdown
cmasModuleAutoShutdown notification is disabled.
Router#
```

This example shows the output of the SNMP cmasModuleAutoShutdown trap when it is configured:

```
Router# test
 snmp trap module-auto-shutdown auto-shutdown
cmasModuleAutoShutdown notification is sent.
Router#
```

test snmp trap port-security

To test CISCO-PORT-SECURITY-MIB traps Simple Network Management Protocol (SNMP) traps and informs, use the **test snmp trap port-security**command in privileged EXEC mode.

test snmp trap port-security {**ifvlan-mac**| **mac**}

Syntax Description

ifvlan-mac	Tests SNMP cpsIfVlanSecureMacAddrViolation notifications.
mac	Tests SNMP cpsSecureMacAddrViolation notifications.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC mode

Command History

Release	Modification
12.2(33)SXI	This command was introduced on the Supervisor Engine 720 and Supervisor Engine 32.

Examples

This example shows the output of the SNMP cpsIfVlanSecureMacAddrViolation trap when it is not configured:

```
Router# test
 snmp trap port-security ifvlan-mac
cpsIfVlanSecureMacAddrViolation notification is disabled.
Router#
```

This example shows the output of the SNMP cpsIfVlanSecureMacAddrViolation trap when it is configured:

```
Router# test
 snmp trap port-security ifvlan-mac
cpsIfVlanSecureMacAddrViolation notification was sent.
Router#
```

test snmp trap power-ethernet port-on-off

To test POWER-ETHERNET-MIB traps Simple Network Management Protocol (SNMP) traps and informs, use the **test snmp trap power-ethernet**command in privieleged EXEC mode.

test snmp trap power-ethernet port-on-off

Syntax Description

This command has no keywords or arguments.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC mode

Command History

Release	Modification
12.2(33)SXI	This command was introduced on the Supervisor Engine 720 and Supervisor Engine 32.

Examples

This example shows the output of the SNMP pethPsePortOnOffNotification trap when it is not configured:

```
Router# test
 snmp trap power-ethernet port-on-off
pethPsePortOnOffNotification notification is disabled.
Router#
```

This example shows the output of the SNMP pethPsePortOnOffNotification trap when it is configured:

```
Router# test
 snmp trap power-ethernet port-on-off
pethPsePortOnOffNotification notification was sent.
Router#
```

test snmp trap snmp

To verify the reception of Simple Network Management Protocol (SNMP) notifications by the Network Management System (NMS) or the SNMP manager in a simulated scenario, use the **test snmp trap snmp** command in privileged EXEC mode.

test snmp trap snmp {**authentication**| **coldstart**| **linkup**| **linkdown**| **warmstart**}

Syntax Description

authentication	Verifies the generation and reception of the SNMP authentication failure notification by the SNMP manager. The authentication failure trap indicates that the SNMP agent has received a protocol message from the SNMP manager that is not properly authenticated.
coldstart	Verifies the generation and reception of the SNMP coldStart notifications by the SNMP manager. A coldStart trap indicates that the SNMP agent is reinitializing and its configuration may have changed.
linkup	Verifies the generation and reception of the SNMP linkUp notifications by the SNMP manager. A linkUp trap indicates if a communication link represented in the agent's configuration is activated.
linkdown	Verifies the generation and reception of the SNMP linkDown notifications by the SNMP manager. A linkDown trap indicates if a communication link represented in the agent's configuration fails.
warmstart	Verifies the generation and reception of the SNMP warmStart notifications by the SNMP manager. A warmStart trap indicates that the SNMP agent is reinitializing and its configuration is not modified.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SXI	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.

Usage Guidelines

SNMP traps or notifications provide information about improper user authentication, restarts, closing of a connection, loss of connection to a neighbor router, or other significant events to the NMS.

Before testing the SNMP traps, configure the SNMP manager for the device and enable SNMP traps.

Examples

The following example shows how to simulate the verification of the authentication failure trap:

```
Router#
 test snmp trap snmp authentication
Generating Authentication failure trap
Sep 12 08:37:49.935: SNMP: Queuing packet to 10.4.9.2
Sep 12 08:37:49.935: SNMP: V1 Trap, ent snmpTraps, addr 192.168.0.1, gentrap 4
lsystem.5.0 = 10.10.10.10
 ciscoMgmt.412.1.1.1.0 = 1
 ciscoMgmt.412.1.1.2.0 = 10.10.10.10
Sep 12 08:38:55.995: SNMP: Packet sent via UDP to 10.4.9.2
Sep 12 08:38:56.263: SNMP: Packet sent via UDP to 10.4.9.2
```

Related Commands

Command	Description
debug snmp packet	Displays information about every SNMP packet sent or received by the router.
snmp-server enable traps	Enables all SNMP notification types that are available on your system.
snmp-server host	Specifies the recipient of an SNMP notification operation.

test snmp trap stack

To test CISCO-STACK-MIB traps Simple Network Management Protocol (SNMP) traps and informs, use the **test snmp trap stack**command in privileged EXEC mode.

test snmp trap stack {**chassis-off**| **chassis-on**| **module-down**| **module-up**}

Syntax Description

chassis-off	Test SNMP chassisAlarmOff notifications.
chassis-on	Tests SNMP chassisAlarmOn notifications.
module-down	Tests SNMP moduleDown notifications.
module-up	Tests SNMP moduleUp notifications.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC mode

Command History

Release	Modification
12.2(33)SXI	This command was introduced on the Supervisor Engine 720 and Supervisor Engine 32.

Examples

This example shows the output of the SNMP chassisAlarmOff trap when it is not configured:

```
Router# test
 snmp trap stack chassis-off
chassisAlarmOff notification is disabled.
Router#
```

This example shows the output of the SNMP chassisAlarmOff trap when it is configured:

```
Router# test
 snmp trap stack chassis-off
chassisAlarmOff notification was sent.
Router#
```

test snmp trap storm-control

To test the Simple Network Management Protocol (SNMP) CISCO-PORT-STORM-CONTROL-MIB traps, use the **test snmp trap storm-control**command in privileged EXEC mode.

test snmp trap strom-control event-rev1

Syntax Description

event-rev1	Tests the cpscEventRev1 trap.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

SNMP traps or notifications provide information about storm-control events.

Examples

The following example shows how to test the SNMP CISCO-PORT-STORM-CONTROL-MIB trap:

```
Router#
 test snmp trap storm-control event-rev1
cpscEventRev1 notification was sent.
Router#
```

Related Commands

Command	Description
snmp-server enable traps storm-control	Enables SNMP storm-control trap notifications.
snmp-server host	Specifies the recipient of an SNMP notification operation.

test snmp trap stpx

To test CISCO-STP-EXTENSIONS-MIB traps Simple Network Management Protocol (SNMP) traps and informs, use the **test snmp trap stpx**command in privileged EXEC mode.

test snmp trap stpx {**inconsistency**| **loop-inconsistency**| **root-inconsistency**}

Syntax Description

inconsistency	Tests SNMP stpxInconsistencyUpdate notifications.
loop-inconsistency	Tests SNMP stpxLoopInconsistencyUpdate notifications.
root-inconsistency	Tests SNMP stpxRootInconsistencyUpdate notifications.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC mode

Command History

Release	Modification
12.2(33)SXI	This command was introduced on the Supervisor Engine 720 and Supervisor Engine 32.

Examples

This example shows the output of the SNMP stpxInconsistencyUpdate trap when it is not configured:

```
Router# test
 snmp trap stpx inconsistency
stpxInconsistencyUpdate notification is disabled.
Router#
```

This example shows the output of the SNMP stpxInconsistencyUpdate trap when it is configured:

```
Router# test
 snmp trap stpx inconsistency
stpxInconsistencyUpdate notification was sent.
Router#
```

test snmp trap syslog

To verify the reception of the system logging message Simple Network Management Protocol (SNMP) notifications by the SNMP manager in a simulated scenario, use the **test snmp trap syslog**command in privileged EXEC mode.

test snmp trap syslog

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SXI	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.

Usage Guidelines

System logging messages are status notification messages that are generated by the routing device during operation. These messages are typically logged to a destination such as the terminal screen, or to a remote syslog host.

Examples

The following example shows how to replicate a syslog trap and its reception by the NMS:

```
Router# test snmp trap syslog
Generating SYSLOG-MIB Trap
00:07:25: SNMP: Queuing packet to 10.4.9.2
00:07:25: SNMP: V1 Trap, ent ciscoSyslogMIB.2, addr 192.16.12.8, gentrap 6, spectra
 clogHistoryEntry.2.1 = TEST
 clogHistoryEntry.3.1 = 5
 clogHistoryEntry.4.1 = 1.3.6.1.4.1.9.9.10.1
 clogHistoryEntry.5.1 =  Syslog test trap
 clogHistoryEntry.6.1 = 44596
00:07:25: SNMP: Queuing packet to 10.4.9.2
00:07:25: SNMP: V2 Trap, reqid 4, errstat 0, erridx 0
 sysUpTime.0 = 44596
 snmpTrapOID.0 = ciscoSyslogMIB.2.0.1
 clogHistoryEntry.2.1 = TEST
 clogHistoryEntry.3.1 = 5
 clogHistoryEntry.4.1 = 1.3.6.1.4.1.9.9.10.1
 clogHistoryEntry.5.1 =  Syslog test trap
 clogHistoryEntry.6.1 = 44596
```

Related Commands

Command	Description
debug snmp packet	Displays information about every SNMP packet sent or received by the router.

Command	Description
snmp-server enable traps	Enables all SNMP notification types that are available on your system.
snmp-server host	Specifies the recipient of an SNMP notification operation.

test snmp trap trustsec

To test CISCO-TRUSTSEC-MIB Simple Network Management Protocol (SNMP) notification (traps and informs), use the **test snmp trap trustsec** command in privileged EXEC mode.

test snmp trap trustsec {**authz-file-error**| **cache-file-error**| **keystore-file-error**| **keystore-sync-fail**| **random-number-fail**| **src-entropy-fail**}

Syntax Description

authz-file-error	Tests SNMP ctsAuthzCacheFileErrNotif notifications.
cache-file-error	Tests SNMP ctsCacheFileAccessErrNotif notifications.
keystore-file-error	Tests SNMP ctsSwKeystoreFileErrNotif notifications.
keystore-sync-fail	Tests SNMP ctsSwKeystoreSyncFailNotif notifications.
random-number-fail	Tests SNMP ctsSapRandomNumberFailNotif notifications.
src-entropy-fail	Tests SNMP ctsSrcEntropyFailNotif notifications.

Command Modes

Privileged EXEC (#).

Command History

Release	Modification
15.1(1)SY	This command was introduced.

Examples

This example shows the output of the test SNMP ctsAuthzCacheFileErrNotif trap when it is not configured:

```
Device# test snmp trap trustsec authz-file-error
ctsAuthzCacheFileErrNotif notification is disabled.
```

This example shows the output of the test SNMP ctsAuthzCacheFileErrNotif trap when it is configured:

```
Device# test snmp trap trustsec authz-file-error
ctsAuthzCacheFileErrNotif notification was sent.
```

Related Commands

Command	Description
snmp-server enable traps trustsec	Enables SNMP trustsec notification traps and informs.

test snmp trap trustsec-interface

To test CISCO-TRUSTSEC-INTERFACE-MIB Simple Network Management Protocol (SNMP) notifications (traps and informs), use the **test snmp trap trustsec-interface** command in privileged EXEC mode.

test snmp trap trustsec-interface {**authc-fail**| **authz-fail**| **sap-fail**| **supplicant-fail**| **unauthorized**}

Syntax Description

authc-fail	Tests SNMP ctsiIfAuthenticationFailNotif notifications.
authz-fail	Tests SNMP ctsiAuthorizationFailNotif notifications.
sap-fail	Tests SNMP ctsiIfSapNegotiationFailNotif notifications.
supplicant-fail	Tests SNMP ctsiIfAddSupplicantFailNotif notifications.
unauthorized	Tests SNMP ctsiIfUnauthorizedNotif notifications.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(1)SY	This command was introduced.

Examples

This example shows the output of the test SNMP ctsiIfAuthenticationFailNotif trap when it is not configured:

```
Device# test snmp trap trustsec-interface authc-fail
ctsiIfAuthenticationFailNotif notification is disabled.
```

This example shows the output of the test SNMP ctsiIfAuthenticationFailNotif trap when it is configured:

```
Device# test snmp trap trustsec-interface authc-fail
ctsiIfAuthenticationFailNotif notification was sent.
```

Related Commands

Command	Description
snmp-server enable traps trustsec-interface	Enables SNMP trustsec-interface notification traps and informs.

test snmp trap trustsec-policy

To test CISCO-TRUSTSEC-POLICY-MIB Simple Network Management Protocol (SNMP) notifications (traps and informs), use the **test snmp trap trustsec-policy** command in privileged EXEC mode.

test snmp trap trustsec-policy {**authz-sgacl-fail**| **peer-policy-updated**}

Syntax Description

authz-sgacl-fail	Tests SNMP ctspAuthorizationSgaclFailNotif notifications.
peer-policy-updated	Tests SNMP ctspPeerPolicyUpdatedNotif notifications.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(1)SY	This command was introduced.

Examples

This example shows the output of the test SNMP ctspAuthorizationSgaclFailNotif trap when it is not configured:

```
Device# test snmp trap trustsec-policy authz-sgacl-fail
ctspAuthorizationSgaclFailNotif notification is disabled.
```

This example shows the output of the test SNMP ctspAuthorizationSgaclFailNotif trap when it is configured:

```
Device# test snmp trap trustsec-policy authz-sgacl-fail
ctspAuthorizationSgaclFailNotif notification was sent.
```

Related Commands

Command	Description
snmp-server enable traps trustsec-policy	Enables SNMP trustsec-policy notification traps and informs.

test snmp trap trustsec-server

To test CISCO-TRUSTSEC-SERVER-MIB Simple Network Management Protocol (SNMP) notifications (traps and informs), use the **test snmp trap trustsec-server** command in privileged EXEC mode.

test snmp trap trustsec-server {**provision-secret**| **radius-server**}

Syntax Description

provision-secret	Tests SNMP ctsvNoProvisionSecretNotif notifications.
radius-server	Tests SNMP ctsvNoRadiusServerNotif notifications.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(1)SY	This command was introduced.

Examples

This example shows the output of the test SNMP ctsvNoProvisionSecretNotif trap when it is not configured:

```
Device# test snmp trap trustsec-server provision-secret
ctsvNoProvisionSecretNotif notification is disabled.
```

This example shows the output of the test SNMP ctsvNoProvisionSecretNotif trap when it is configured:

```
Device# test snmp trap trustsec-sxp-server provision-secret
ctsvNoProvisionSecretNotif notification was sent.
```

Related Commands

Command	Description
snmp-server enable traps trustsec-server	Enables SNMP trustsec-server notification traps and informs.

test snmp trap trustsec-sxp

To test CISCO-TRUSTSEC-SXP-MIB Simple Network Management Protocol (SNMP) notification (traps and informs), use the **test snmp trap trustsec-sxp** command in privileged EXEC mode.

test snmp trap trustsec-sxp {**binding-conflict**| **binding-err**| **binding-expn-fail**| **conn-config-err**| **conn-down**| **conn-srcaddr-err**| **conn-up**| **msg-parse-err**| **oper-nodeid-change**}

Syntax Description

binding-conflict	Tests SNMP ctsxSxpBindingConflictNotif notifications.
binding-err	Tests SNMP ctsxSxpBindingErrNotif notifications.
binding-expn-fail	Tests SNMP ctsxSxpBindingExpnFailNotif notifications.
conn-config-err	Tests SNMP ctsxSxpConnConfigErrNotif notifications.
conn-down	Tests SNMP ctsxSxpConnDownNotif notifications.
conn-srcaddr-err	Tests SNMP ctsxSxpConnSourceAddrErrNotif notifications.
conn-up	Tests SNMP ctsxSxpConnUpNotif notifications.
msg-parse-err	Tests SNMP ctsxSxpMsgParseErrNotif notifications.
oper-nodeid-change	Tests SNMP ctsxSxpOperNodeIdChangeNotif notifications.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(1)SY	This command was introduced.

Examples

This example shows the output of the test SNMP ctsxSxpBindingConflictNotif trap when it is not configured:

```
Device# test snmp trap trustsec-sxp binding-conflict
ctsxSxpBindingConflictNotif notification is disabled.
```

This example shows the output of the test SNMP ctsxSxpBindingConflictNotif trap when it is configured:

```
Device# test snmp trap trustsec-sxp binding-conflict
ctsxSxpBindingConflictNotif notification was sent.
```

Related Commands

Command	Description
snmp-server enable traps trustsec-sxp	Enables SNMP trustsec-sxp notification traps and informs.

test snmp trap udld

To test CISCO-UDLDP-MIB Simple Network Management Protocol (SNMP) notifications (traps and informs), use the **test snmp trap udld**command in privileged EXEC mode.

test snmp trap udld {**link-fail-rpt**| **status-change**}

Syntax Description

link-fail-rpt	Tests SNMP cudldpFastHelloLinkFailRptNotification notifications.
status-change	Tests SNMP cudldFastHelloStatusChangeNotification notifications.

Command Default

This command has no default setting.

Command Modes

Privileged EXEC mode

Command History

Release	Modification
12.2(33)SXI4	This command was introduced on the Supervisor Engine 720 and Supervisor Engine 32.

Examples

This example shows the output of the SNMP cudldpFastHelloLinkFailRptNotification notification when it is not configured:

```
Router# test
 snmp trap udld link-fail-rpt
cudldpFastHelloLinkFailRptNotification notification is disabled.
Router#
```

This example shows the output of the SNMP cudldpFastHelloLinkFailRptNotification notification when it is configured:

```
Router# test
 snmp trap udld link-fail-rpt
cudldpFastHelloLinkFailRptNotification notification was sent.
Router#
```

test snmp trap vswitch dual-active

To test whether the CISCO-VIRTUAL-SWITCH-MIB Simple Network Management Protocol (SNMP) notification (trap) can be generated in the dual-active state, use the **test snmp trap vswitch dual-active** command in privileged EXEC mode.

test snmp trap vswitch dual-active

Syntax Description

This command has no keywords or arguments.

Command Default

The CISCO-VIRTUAL-SWITCH-MIB SNMP notification is not sent.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(1)SY	This command was introduced.

Usage Guidelines

The **snmp-server enable traps vswitch dual-active** command enables the dual-active state change notification. When the VSS changes state to dual-active, the SNMP agent sends the cvsDualActiveDetectionNotif notification.

Enable the **snmp-server enable traps vswitch dual-active** command before running the **test snmp trap vswitch dual-active** command.

Examples

The following is sample output from the **test snmp trap vswitch dual-active** command when the SNMP cvsDualActiveDetectionNotif notification is enabled:

```
Device(config)# snmp-server enable traps vswitch dual-active
Device(config)# exit
Device# test snmp trap vswitch dual-active

cvsDualActiveDetectionNotif notification was sent.
```

The following is sample output from the **test snmp trap vswitch dual-active** command when the SNMP cvsDualActiveDetectionNotif notification is disabled:

```
Device(config)# no snmp-server enable traps vswitch dual-active
Device(config)# exit
Device# test snmp trap vswitch dual-active

cvsDualActiveDetectionNotif notification is disabled.
```

Related Commands

Command	Description
snmp-server enable traps vswitch dual-active	Enables the CISCO-VIRTUAL-SWITCH-MIB SNMP cvsDualActiveDetectionNotif notification.
test snmp trap vswitch vsl	Tests the CISCO-VIRTUAL-SWITCH-MIB SNMP notification (trap and inform).

test snmp trap vswitch vsl

To test CISCO-VIRTUAL-SWITCH-MIB Simple Network Management Protocol (SNMP) notifications (traps and informs), use the **test snmp trap vswitch vsl**command in privileged EXEC mode.

test snmp trap vswitch vsl

Syntax Description

This command has no keywords or arguments.

Command Default

This command has no default setting.

Command Modes

Privileged EXEC mode

Command History

Release	Modification
12.2(33)SXI	This command was introduced on the Supervisor Engine 720.

Examples

This example shows the output of the SNMP cvsVSLConnectionChangeNotif notification when it is not enabled:

```
Router# test
 snmp trap vswitch vsl
cvsVSLConnectionChangeNotif notification is disabled.
Router#
```

This example shows the output of the SNMP cvsVSLConnectionChangeNotif notification when it is enabled:

```
Router# test
 snmp trap vswitch vsl
cvsVSLConnectionChangeNotif notification was sent.
Router#
```

test snmp trap vtp

To test CISCO-VTP-MIB traps Simple Network Management Protocol (SNMP) traps and informs, use the **test snmp trap vtp**command in privileged EXEC mode.

test snmp trap vtp {**digest-error**| **mode-change**| **port-status**| **pruning-change**| **rev-error**| **server-disable**| **v1-detected**| **version-change**| **vlan-create**| **vlan-delete**}

Syntax Description

digest-error	Tests SNMP vtpConfigDigestError notifications.
mode-change	Tests SNMP vtpLocalModeChange notifications.
port-status	Tests SNMP vlanTrunkPortDynamicStatusChange notifications.
pruning-change	Tests SNMP vtpPruningStateOperChange notifications.
rev-error	Tests SNMP vtpConfigRevNumberError notifications.
server-disable	Tests SNMP vtpServerDisabled notifications.
v1-detected	Tests SNMP vtpVersionOneDeviceDetected notifications.
version-change	Tests SNMP vtpVersionInUseChanged notifications.
vlan-create	Tests SNMP vtpVlanCreated notifications.
vlan-delete	Tests SNMP vtpVlanDeleted notifications.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC mode

Command History

Release	Modification
12.2(33)SXI	This command was introduced on the Supervisor Engine 720 and Supervisor Engine 32.

Examples

This example shows the output of the SNMP vtpConfigDigestError trap when it is not configured:

```
Router# test
 snmp trap vtp digest-error
vtpConfigDigestError notification is disabled.
Router#
```

This example shows the output of the SNMP vtpConfigDigestError trap when it is configured:

```
Router# test
 snmp trap vtp digest-error
vtpConfigDigestError notification was sent.
Router#
```

test snmp trap vtp pruning-change

To test the vtpPruningStateOperChange trap, use the **test snmp trap vtp pruning-change**EXEC command.

test snmp trap vtp pruning-change

Syntax Description

This command has no keywords or arguments.

Command Default

This command has no default settings.

Command Modes

EXEC mode

Command History

Release	Modification
12.2(33)SXI4	Support for this command was introduced on the Catalyst 6500 series.

Examples

This example shows that testing the vtpPruningStateOperChange cannot occur without first enabling SNMP VTP traps:

```
Router# test snmp trap vtp pruning-change
vtpPruningStateOperChange notification is disabled.
```

This example shows how to test the vtpPruningStateOperChange:

```
Router# test snmp trap vtp pruning-change
vtpPruningStateOperChange notification is sent.
```

Related Commands

Command	Description
snmp-server enable traps vtp	Enables SNMP VTP traps.

type (test existence)

To specify the type of existence trigger test to perform, use the **type** command in event trigger existence configuration mode. To disable the specified trigger test type, use the **no** form of this command.

type {**present**| **absent**| **changed**}

no type {**present**| **absent**| **changed**}

Syntax Description

present	Specifies whether the trigger conditions for the existence test are present.
absent	Specifies whether the trigger conditions for the existence test are absent.
changed	Specifies whether the trigger conditions for the existence test are changed.

Command Default

By default, both present and absent tests are performed.

Command Modes

Event trigger existence configuration (config-event-trigger-existence)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.

Usage Guidelines

The existence trigger tests are performed based on the following parameters:

- Absent
- Present
- Changed

When the test type is not specified, both present and absent tests are performed.

Examples

The following example shows how to specify the existence trigger test as present:

```
Router(config)#snmp mib event trigger owner owner1 name triggerA
Router(config-event-trigger)# test existence
Router(config-event-trigger-existence)# type present
Router(config-event-trigger-existence)# end
```

Related Commands

Command	Description
test	Enables a trigger test.

url (bulk statistics)

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**}

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, RCP, or TFTP. The Cisco IOS File System (IFS) syntax for these URLs is as follows: • **ftp:** [[[//*username* [:*password*]@]*location*]/*directory*]/*filename* • **rcp:** [[[//*username*@]*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 (config-bulk-tr)

Command History

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

Release	Modification
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS Release XE 2.1.

Usage Guidelines

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.

Examples

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.

```
Router(config)# snmp mib bulkstat transfer ifMibTesting
Router(config-bulk-tr)# schema carMibTesting1
Router(config-bulk-tr)# schema carMibTesting2
Router(config-bulk-tr)# format bulkBinary
Router(config-bulk-tr)# transfer-interval 60
Router(config-bulk-tr)# buffer-size 10000
Router(config-bulk-tr)# url primary ftp://user2:pswd@192.168.10.5/functionality/
Router(config-bulk-tr)# url secondary tftp://user2@192.168.10.8/tftpboot/
Router(config-bulk-tr)# buffer-size 2500000
Router(config-bulk-tr)# enable
Router(config-bulk-tr)# exit
```

Related Commands

Command	Description
retry (bulk statistics)	Configures the number of retries that should be attempted for sending bulk statistics files.
snmp mib bulkstat transfer	Names a bulk statistics transfer configuration and enters Bulk Statistics Transfer configuration mode.

value (test boolean)

To set a value for the Boolean trigger test, use the **value** command in event trigger boolean configuration mode. To disable the configured settings, use the **no** form of this command.

value *integer-value*

no value

Syntax Description

integer-value	Numerical value to set for the Boolean test. The default is 0.

Command Default

The Boolean trigger test value is set to 0.

Command Modes

Event trigger boolean configuration (config-event-trigger-boolean)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.

Usage Guidelines

The **value** command specifies the value to be set for the Boolean trigger test.

Examples

The following example shows how to set a value for the Boolean trigger test:

```
Router(config)# snmp mib event trigger owner owner1 name triggerA
Router(config-event-trigger)# test boolean
Router(config-event-trigger-boolean)# value 10
Router(config-event-trigger-boolean)# end
```

Related Commands

Command	Description
test	Enables a trigger test.

value type

To specify the type of bulkstat expression to use during object sampling, use the **value type** command in Bulkstat expression configuration mode. To disable the specified value type, use the **no** form of this command.

value type [**counter32**| **unsigned32**| **timeticks**| **integer32**| **ipaddress**| **octetstring**| **objectid**| **counter64**]

no value type

Syntax Description

counter32	(Optional) Specifies a counter32 value. Counter32 specifies a value that represents a count. The value ranges from 0 to 4,29,49,67,295.
unsigned32	(Optional) Specifies an unsigned integer value. Unsigned32 specifies a value that includes only non-negative integers. The value ranges from 0 to 4294967295.
timeticks	(Optional) Specifies a value based on timeticks. Timeticks represents a non-negative integer value that specifies the elapsed time between two events, in units of hundredth of a second. When objects in the MIB are defined using the subset of Abstract Syntax Notation One (ASN.1), the description of the object type identifies this reference period.
integer32	(Optional) Specifies an integer32 value. The Integer32 represents 32-bit signed integer values for the Simple Network Management Protocol (SNMP). The value range includes both negative and positive numbers.
ipaddress	(Optional) Specifies a value based on the IP address. The IP address is a string of four octets. The IP address value type is generally an IPv4 address. This value is encoded as four bytes in the network byte order.
octetstring	(Optional) Specifies a value based on octetstring. The octetstring specifies octets of binary or textual information. The octet string length ranges from 0 to 65535 octets.
objectid	(Optional) Specifies a value based on the object identifier of an object. Each object type in a MIB is identified by an object identifier value assigned by the administrator. The object identifier identifies the value type that has an assigned object identifier value.

counter64	(Optional) Specifies a counter64 value that represents a count. However, the counter64 value ranges from 0 to 18446744073709551615. This value type is used when a 32-bit counter rollover occurs in less than an hour.

Command Default

By default, the value type is not configured.

Command Modes

expression configuration (config-expression)#

Bulkstat data set expression configuration (config-bs-ds-expr)#

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.
15.3(1)S	This command was integrated into Cisco IOS Release 15.3(1)S.
Cisco IOS Release XE 3.8S	This command was integrated into Cisco IOS Release XE 3.8S.

Usage Guidelines

The **value type** command specifies a value for expression evaluation.

Examples

The following example shows how to specify the counter32 value type:

```
Device> enable
Device# configure terminal
Device(config)# snmp mib expression owner owner1 name ExpressionA
Device(config-expression)# value type counter32
```

The following example shows how to specify the counter32 value type for Bulkstat expression data set:

```
Device> enable
Device# configure terminal
Device(config)# bulkstat data interface-util type expression
Device(config-bs-ds-expr)# expression 100*$1+$2
Device(config-bs-ds-expr)# value type counter32
```

Related Commands

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

Command	Description
bulkstat data	Configures Bulkstat data set for expression type.

wildcard (expression)

To specify whether an object used for evaluating an expression is to be wildcarded during an event configuration, use the **wildcard** command in expression configuration mode. To remove the wildcard object identifier, use the **no** form of this command.

wildcard

no wildcard

Syntax Description

This command has no arguments or keywords.

Command Default

This command is enabled by default.

Command Modes

Expression configuration (config-expression)

Command History

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

Usage Guidelines

The **wildcard** command allows you to apply a single expression to multiple instances of the same MIB object. When you specify this choice and provide a partial object identifier, the application obtains the object values and discovers the instances of the object. By default, the objects are identified based on instances and are not wildcarded.

Examples

The following example shows how to specify the wildcard object identifier by using the **wildcard** command:

```
Router(config)# snmp mib expression owner owner1 name expression1
Router(config-expression)#object 2
Router(config-expression-object)# wildcard
Router(config-expression-object)# end
```

Related Commands

Command	Description
object id	Specifies the object identifier of an object associated with an event.
snmp mib expression owner	Specifies the owner of an expression.

write mib-data

To save MIB data to system memory (NVRAM) for MIB Data Persistence, use the **write mib-data**command in EXEC mode.

write mib-data

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.
12.2(33)SRC	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRC.
12.2(33)SXI	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.1	This command was implemented on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

The MIB Data Persistence feature allows the SNMP data of a MIB to be persistent across reloads; that is, the values of certain MIB objects are retained even if your networking device reboots.

To determine which MIBs support “MIB Persistence” in your release, use the **snmp mib persist** command in global configuration mode.

Any modified MIB data must be written to NVRAM memory using the **write mib-data** command. If the **write mib-data** command is not used, modified MIB data is not saved automatically, even if MIB Persistence is enabled. Executing the **write mib-data** command saves only the current MIB data; if the MIB object values are changed, you should reenter the **write mib-data** command to ensure that those values are persistent across reboots.

Examples

The following example shows the enabling of event MIB persistence, circuit MIB persistence, and saving the changes to set object values for these MIBs to NVRAM:

```
Router# configure terminal
Router(config)# snmp mib persist circuit
Router(config)# snmp mib persist event
Router(config)# end
Router# write mib-data
```

Related Commands

Command	Description
snmp mib persist	Enables MIB data persistence.