

Chapter 9

Summary of SNMP Configuration Statements

The following sections explain each of the SNMP configuration statements. The statements are organized alphabetically.

access

Syntax

```
access {
  context context-name {
    description description;
    group group-name {
      model usm;
      security-level (none | authentication | privacy);
      read-view view-name;
      write-view view-name;
    }
  }
  group group-name {
    user [ user-names ];
    model usm;
  }
  user [user-name] {
    authentication-type (none | md5 | sha);
    authentication-password authentication-password;
    privacy-password privacy-password;
    privacy-type (none | des);
    clients {
      address restrict;
    }
  }
}
```

Hierarchy Level [edit snmp]

Description Specifies the SNMPv3 access level by context, group, and user.

Options The remaining statements are explained separately.

Usage Guidelines See “Configure SNMPv3 Access” on page 30.

Required Privilege Level snmp—To view this statement in the configuration.
snmp-control—To add this statement to the configuration.

agent-address

Syntax agent-address outgoing-interface;

Hierarchy Level [edit snmp trap-options]

Description Set the agent address of all SNMPv1 traps generated by this router. Currently, the only option is outgoing-interface, which sets the agent address of each SNMPv1 trap to the address of the outgoing interface of that trap.

Options outgoing-interface—Value of agent address of all SNMPv1 traps generated by this router. The outgoing-interface option sets the agent address of each SNMPv1 trap to the address of the outgoing interface of that trap.

Default: disabled (agent address is not specified in SNMPv1 traps)

Usage Guidelines See “Configure the Agent Address for SNMP Traps” on page 25.

Required Privilege Level snmp—To view this statement in the configuration.
snmp-control—To add this statement to the configuration.

authentication-password

Syntax authentication-type *authentication-password*;

Hierarchy Level [edit snmp access user *user-name*]

Description Password used for authentication.

Options *authentication-password*—Contents of password used for authentication.

Usage Guidelines See “Configure SNMPv3 Access” on page 30.

Required Privilege Level snmp—To view this statement in the configuration.
snmp-control—To add this statement to the configuration.

authentication-type

Syntax	authentication-type (none md5 sha);
Hierarchy Level	[edit snmp access user <i>user-name</i>]
Description	The type of authentication algorithm.
Options	Includes the following authentication types: <ul style="list-style-type: none"> none—No security. SNMPv3 provides no authentication and no encryption on any SNMP information. md5—Message Digest Algorithm (see RFC 1321) sha—Secure Hash Algorithm (see NIST FIPS 180-1)
Usage Guidelines	See “Configure SNMPv3 Access” on page 30.
Required Privilege Level	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.

authorization

Syntax	authorization <i>authorization</i> ;
Hierarchy Level	[edit snmp community <i>community-name</i>]
Description	Set the access authorization for SNMP Get, GetBulk, GetNext, and Set requests.
Options	<i>authorization</i> —Access authorization level: <ul style="list-style-type: none"> read-only—Enable Get, GetNext, and GetBulk requests. read-write—Enable all requests, including Set requests. You must configure a view to enable Set requests. Default: read-only
Usage Guidelines	See “Configure the SNMP Community String” on page 21.
Required Privilege Level	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.

categories

Syntax	categories [<i>categories</i>];
Hierarchy Level	[edit snmp trap-group <i>group-name</i>]
Description	Define the types of traps that will be sent to the targets of the named trap group.
Default	If you omit the categories statement, all trap types are included in trap notifications.
Options	<i>categories</i> —One or more trap types. Values: authentication, chassis, configuration, link, remote-operations, rmon-alarm, routing, sonet-alarms, startup, vrrp-events
Usage Guidelines	See “Configure SNMP Trap Groups” on page 25.
Required Privilege Level	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.

clients

clients (for associating clients with communities)

Syntax	clients { <i>address</i> restrict; }
Hierarchy Level	[edit snmp community <i>community-name</i>]
Description	Specify the IPv4 or IPv6 addresses of the SNMP client hosts that are authorized to use this community.
Default	If you omit the clients statement, all SNMP clients using this community string are authorized to access the router.
Options	<i>address</i> —Address of an SNMP client that is authorized to access this router. You must specify an address, not a hostname. To specify more than one client, include multiple <i>address</i> options. restrict—(Optional) Do not allow the specified SNMP client to access the router. Default: If you omit the restrict option after the address, access is permitted for this particular client.
Usage Guidelines	See “Configure the SNMP Community String” on page 21.
Required Privilege Level	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.

clients (for associating clients with an SNMPv3 user)

Syntax	clients { <i>address</i> restrict; }
Hierarchy Level	[edit snmp user <i>user-name</i>]
Description	List of source address prefix ranges to accept.
Options	<i>address</i> —IPv4 or IPv6 address of an SNMP client that is authorized to access this router. You must specify an address, not a hostname. To specify more than one client, include multiple <i>address</i> options. restrict—(Optional) Do not allow the specified SNMP client to access the router. Default: If you omit the restrict option after the address, access is permitted for this particular client.
Usage Guidelines	See “Configure the SNMP Community String” on page 21.
Required Privilege Level	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.

community

Syntax	community <i>community-name</i> { authorization <i>authorization</i> ; clients { <i>address</i> restrict; } view <i>view-name</i> ; }
Hierarchy Level	[edit snmp]
Description	Define an SNMP community. An SNMP community authorizes SNMP clients based on source IP address of incoming SNMP request packets. A community also defines which MIB objects are available and the operations (read-only or read-write) allowed on those objects. The SNMP client application specifies an SNMP community name in Get, GetBulk, GetNext, and Set SNMP requests.
Default	If you omit the community statement, all SNMP requests are denied.
Options	<i>community-name</i> —Community string. If the name includes spaces, enclose it in quotation marks (" "). The remaining statements are explained separately.
Usage Guidelines	See “Configure the SNMP Community String” on page 21.
Required Privilege Level	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.

contact

- Syntax** `contact contact;`
- Hierarchy Level** [edit snmp]
- Description** Define the value of the MIB II sysContact object, which is the contact person for the managed system.
- Options** *contact*—Name of contact person. If the name includes spaces, enclose it in quotation marks (" ").
- Usage Guidelines** See “Configure the System Contact” on page 19.
- Required Privilege Level** snmp—To view this statement in the configuration.
snmp-control—To add this statement to the configuration.

context

- Syntax**

```
context context-name {
    description description;
    group group-name {
        model usm;
        security-level [none | authentication | privacy];
        read-view view-name;
        write-view view-name;
    }
}
```
- Hierarchy Level** [edit snmp access]
- Description** A collection of management information accessible by an SNMP entity. An item of management information can exist in more than one context. An SNMP entity can have access to many contexts.
- Options** *context-name*—Sets a collection of management information accessible by an SNMP entity.

The remaining statements are explained separately.
- Usage Guidelines** See “Configure SNMPv3 Access” on page 30.
- Required Privilege Level** snmp—To view this statement in the configuration.
snmp-control—To add this statement to the configuration.

description

description (for describing the MIB II sysDescription object)

Syntax	description <i>description</i> ;
Hierarchy Level	[edit snmp]
Description	Define the value of the MIB II sysDescription object, which is the description of the system being managed.
Options	<i>description</i> —System description. If the name includes spaces, enclose it in quotation marks (" ").
Usage Guidelines	See “Configure the System Description” on page 20.
Required Privilege Level	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.

description (for describing the SNMPv3 context)

Syntax	description <i>description</i> ;
Hierarchy Level	[edit snmp access context <i>context-name</i>]
Description	Define the value of the context name accessible by the SNMP entity.
Options	<i>description</i> —Describes the value of the context name. If the name includes spaces, enclose it in quotation marks (" ").
Usage Guidelines	See “Configure SNMPv3 Access” on page 30.
Required Privilege Level	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.

destination-port

Syntax	destination-port < <i>port-number</i> >;
Hierarchy Level	[edit snmp trap-group]
Description	Assign a trap port number other than the default.
Options	<i>port-number</i> —(Optional) SNMP trap port number.
	Default: port number 162.
Usage Guidelines	See “Configure SNMP Trap Groups” on page 25.
Required Privilege Level	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.

engine-id

Syntax engine-id {
 local *engine-id*;
}

Hierarchy Level [edit snmp]

Description Set the SNMPv3 engine ID.

Options *engine-id*—An SNMPv3 engine’s administratively unique identifier. It is used for identification, not for addressing. You must configure the local engine ID explicitly. The engine ID is in text format with its fifth octet equal to 4. If the engine ID is not configured, the system default IP address of the router is used as the default engine ID. The fifth octet of the default engine ID is 1.

Default: IPv4 address format with the fifth octet equal to 1.

Usage Guidelines See “Configure the Local Engine ID” on page 29.

Required Privilege Level snmp—To view this statement in the configuration.
snmp-control—To add this statement to the configuration.

group

group (for associating a group with an SNMPv3 context)

Syntax group *group-name*;

Hierarchy Level [edit snmp access context *context-name*]

Description Associates a group with an SNMPv3 context.

Options *group-name*—SNMPv3 USM group name associated with an SNMPv3 context.

Usage Guidelines See “Configure SNMPv3 Access” on page 30.

Required Privilege Level snmp—To view this statement in the configuration.
snmp-control—To add this statement to the configuration.

group (for creating an SNMPv3 group)

Syntax	group <i>group-name</i> { user [<i>user-names</i>]; model usm; }
Hierarchy Level	[edit snmp access]
Description	Creates an SNMPv3 group.
Options	<i>group-name</i> —SNMPv3 group name created for an SNMPv3 group. The remaining statements are described separately.
Usage Guidelines	See “Configure SNMPv3 Access” on page 30.
Required Privilege Level	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.

interface

Syntax	interface [<i>interface-names</i>];
Hierarchy Level	[edit snmp]
Description	Configure the interfaces on which SNMP requests can be accepted.
Default	If you omit this statement, SNMP requests entering the router through any interface will be accepted.
Options	<i>interface-names</i> —Names of one or more logical interfaces.
Usage Guidelines	See “Configure the Interfaces on Which SNMP Requests Can Be Accepted” on page 28.
Required Privilege Level	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.

location

Syntax	location <i>location</i> ;
Hierarchy Level	[edit snmp]
Description	Define the value of the MIB II sysLocation object, which is the physical location of the managed system.
Options	<i>location</i> —Location of local system. You must enclose the name within quotation marks (" ").
Usage Guidelines	See “Configure the System Location” on page 19.
Required Privilege Level	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.

model

Syntax	model usm;
Hierarchy Level	[edit snmp access context <i>context-name</i>]; [edit snmp access group <i>group-name</i>]
Description	Describes the security model used for SNMPv3 access.
Options	usm—User-based Security Model (USM), which provides data integrity, data origin authentication, message replay protection, and protection against disclosure of the message payload.
Usage Guidelines	See “Configure SNMPv3 Access” on page 30.
Required Privilege Level	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.

name

Syntax	name <i>name</i> ;
Hierarchy Level	[edit snmp]
Description	Set the system name from the command-line interface.
Options	<i>name</i> —System name override.
Usage Guidelines	See “Configure the System Name” on page 20.
Required Privilege Level	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.

oid

Syntax	oid <i>object-identifier</i> (include exclude);
Hierarchy Level	[edit snmp view <i>view-name</i>]
Description	Specify an object identifier (OID) used to represent a subtree of MIB objects.
Options	<i>object-identifier</i> —OID used to represent a subtree of MIB objects. All MIB objects represented by this statement have the specified OID as a prefix. It can be specified either by a sequence of dotted integers or by a subtree name. include—Include the subtree of MIB objects represented by the specified OID. exclude—Exclude the subtree of MIB objects represented by the specified OID.
Usage Guidelines	See “Configure MIB Views” on page 28.
Required Privilege Level	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.

privacy-password

Syntax	<code>privacy-password <i>privacy-password</i>;</code>
Hierarchy Level	<code>[edit snmp access user <i>user-name</i>]</code>
Description	Password used for encryption.
Options	<i>privacy-password</i> —Contents of password used for encryption.
Usage Guidelines	See “Configure SNMPv3 Access” on page 30.
Required Privilege Level	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.

privacy-type

Syntax	<code>privacy-type (none des);</code>
Hierarchy Level	<code>[edit snmp access user <i>user-name</i>]</code>
Description	Level of privacy a user has with SNMPv3.
Options	Includes the following privacy types: <ul style="list-style-type: none"> none—No security. SNMPv3 provides no authentication and no encryption on any SNMP information. des—Data Encryption Algorithm (see FIPS Publication 46-1).
Usage Guidelines	See “Configure SNMPv3 Access” on page 30.
Required Privilege Level	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.

read-view

Syntax	<code>read-view <i>view-name</i>;</code>
Hierarchy Level	<code>[edit snmp access context <i>context-name</i> group <i>group-name</i>]</code>
Description	Specify read access for an SNMP user group.
Options	<i>view-name</i> —The name of the view to which the SNMP user group has access.
Usage Guidelines	See “Configure SNMPv3 Access” on page 30.
Required Privilege Level	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.

security-level

Syntax	security-level (none authentication privacy);
Hierarchy Level	[edit snmp access context <i>context-name</i> group <i>group-name</i>]
Description	Level of security assigned to an SNMPv3 context.
Options	includes three security levels: <ul style="list-style-type: none"> none—No security. SNMPv3 provides no authentication and no encryption on any SNMP information. authentication only—Provides authentication capability but no encryption on any SNMP information. privacy—Provides authentication and encryption on all SNMP information.
Usage Guidelines	See “Configure SNMPv3 Access” on page 30.
Required Privilege Level	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.

snmp

Syntax	snmp { ... }
Hierarchy Level	[edit]
Description	Configure SNMP.
Usage Guidelines	See “Configure SNMP” on page 17.
Required Privilege Level	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.

source-address

Syntax	source-address <i>address</i> ;
Hierarchy Level	[edit snmp trap-options]
Description	Set the source address of every SNMP trap packet sent by this router to a single address regardless of the outgoing interface. If the source address is not specified, the default is to use the address of the outgoing interface as the source address. Currently, the only value that can be specified for source address is lo0. The value lo0 indicates the source address of all SNMP trap packets will be set to the lowest loopback address configured at the interface lo0.
Options	<i>address</i> —Source address of SNMP traps. Currently, the only value that can be specified is lo0. Default: disabled (The source address is the address of outgoing interface)
Usage Guidelines	See “Configure the Source Address for SNMP Traps” on page 24.
Required Privilege Level	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.

targets

Syntax	targets { <i>address</i> ; }
Hierarchy Level	[edit snmp trap-group <i>group-name</i>]
Description	Configure one or more systems to receive SNMP traps.
Options	<i>address</i> —IPv4 or IPv6 address of the system to receive traps. You must specify an address, not a hostname.
Usage Guidelines	See “Configure SNMP Trap Groups” on page 25.
Required Privilege Level	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.

traceoptions

Syntax traceoptions {
 file size *size* files *number*;
 flag *flag*;
 }

Hierarchy Level [edit snmp]

Description The output of the tracing operations is placed into log files in the /var/log directory. Each of these log files is named after the SNMP agent that generates it. Currently, the following logs are created in the /var/log directory when the traceoptions statement is used:

chassisd

craftd

ilmid

mib2d

rmopd

serviced

snmpd

Options file *number*—(Optional) Maximum number of trace files per SNMP subagent. When a trace file (for example, snmpd) reaches its maximum size, it is archived by being renamed to snmpd.0. The previous snmpd.1 is renamed to snmpd.2, and so on. The oldest archived file is deleted.

Range: 2 through 1000 files

Default: 10 files

flag—Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements:

all—Trace all SNMP events

general—Trace general events

interface-stats—Trace physical and logical interface statistics

pdu—Trace SNMP request and response packets

protocol-timeouts—Trace SNMP response timeouts

routing-socket—Trace routing socket calls

subagent—Trace subagent restarts

timer—Trace internal timer events

varbind-error—Trace variable binding errors

size *size*—(Optional) Maximum size in kilobytes (KB) of each trace file before it is closed and archived.

Range: 1 KB through the maximum file size supported on your system

Default: 1000 KB

Usage Guidelines See “Trace SNMP Activity” on page 32.

Required Privilege Level snmp—To view this statement in the configuration.
snmp-control—To add this statement to the configuration.

trap-group

Syntax trap-group *group-name* {
categories [*categories*];
destination-port <*port-number*>;
targets {
 address;
}
version (all | v1 | v2);
}

Hierarchy Level [edit snmp]

Description Create a named group of hosts to receive the specified trap notifications. The name of the trap group is embedded in SNMP trap notification packets as one variable binding (varbind) known as the community name. At least one trap group must be configured for SNMP traps to be sent.

Options *group-name*—Name of the trap group. If the name includes spaces, enclose it in quotation marks (" ").

The remaining statements are explained separately.

Usage Guidelines See “Configure SNMP Trap Groups” on page 25.

Required Privilege Level snmp—To view this statement in the configuration.
snmp-control—To add this statement to the configuration.

trap-options

Syntax trap-options {
 agent-address outgoing-interface;
 source-address *address*;
 }

Hierarchy Level [edit snmp]

Description Using SNMP trap options, you can set the source address of every SNMP trap packet sent by the router to a single address, regardless of the outgoing interface. In addition, you can set the agent address of each SNMPv1 trap. For more information on the contents of SNMPv1 traps, see RFC 1157.

Options The remaining statements are explained separately.

Default: disabled

Usage Guidelines See “Configure SNMP Trap Options” on page 23.

Required Privilege Level snmp—To view this statement in the configuration.
 snmp-control—To add this statement to the configuration.

user

user (for associating a list of users with an SNMPv3 group)

Syntax user [*user-name*];

Hierarchy Level [edit snmp access group *group-name*]

Description Specify a list of users associated with an SNMPv3 group.

Options *user-name*—SNMPv3 USM user name.

Usage Guidelines See “Configure SNMPv3 Access” on page 30.

Required Privilege Level snmp—To view this statement in the configuration.
 snmp-control—To add this statement to the configuration.

user (for creating an SNMPv3 user)

Syntax user *user-name*;

Hierarchy Level [edit snmp access]

Description Specify a user for whom management operations are performed and authorized.

Options *user-name*—SNMPv3 USM user name.

Usage Guidelines See “Configure SNMPv3 Access” on page 30.

Required Privilege Level snmp—To view this statement in the configuration.
 snmp-control—To add this statement to the configuration

version

Syntax	version (all v1 v2);
Hierarchy Level	[edit snmp trap-group <i>group-name</i>]
Description	Specify the version number of SNMP traps.
Options	all—Send an SNMPv1 and SNMPv2 trap for every trap condition. v1—Send SNMPv1 traps only. v2—Send SNMPv2 traps only. Default: all
Usage Guidelines	See “Configure SNMP Trap Groups” on page 25.
Required Privilege Level	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.

view

view (for configuring MIB views)

Syntax	view <i>view-name</i> { oid <i>object-identifier</i> (include exclude); }
Hierarchy Level	[edit snmp]
Description	Define a MIB view. A MIB view identifies a group of MIB objects. Each MIB object in a view has a common OID prefix. Each object identifier represents a subtree of the MIB object hierarchy. The view statement uses a view to specify a group of MIB objects on which to define access. To enable a view, you must associate the view with a community by including the view statement at the [edit snmp community <i>community-name</i>] hierarchy level.

**Note**

To remove an OID completely, use the delete view all oid oid-number command but omit the include parameter.

Options	<i>view-name</i> —Name of the view The remaining statements are explained separately.
Usage Guidelines	See “Configure MIB Views” on page 28.
Required Privilege Level	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.
See Also	community on page 101

view (for associating MIB views with a community)

Syntax view *view-name*;

Hierarchy Level [edit snmp community *community-name*]

Description Associate a view with a community. A view represents a group of MIB objects.

Options *view-name*—Name of the view. You must use a view name already configured in the view statement at the [edit snmp] hierarchy level.

Usage Guidelines See “Configure MIB Views” on page 28.

Required Privilege Level snmp—To view this statement in the configuration.
snmp-control—To add this statement to the configuration.

write-view

Syntax write-view *view-name*;

Hierarchy Level [edit snmp access context *context-name* group *group-name*]

Description Specifies write-view access for an SNMP user group.

Options *view-name*—The name of the view to which the SNMP user group has access.

Usage Guidelines See “Configure SNMPv3 Access” on page 30.

Required Privilege Level snmp—To view this statement in the configuration.
snmp-control—To add this statement to the configuration.