



Configuring SNMP

This chapter describes how to configure the Simple Network Management Protocol (SNMP) on the Catalyst enterprise LAN switches.

SNMP is an application-layer protocol that facilitates the exchange of management information between network devices. SNMP allows network administrators to manage network performance, find and solve network problems, and plan for network growth.

There are three versions of SNMP:

- Version 1 (SNMPv1)—This is the initial implementation of SNMP. Refer to Request for Comments (RFC) 1157 for a full description of functionality.
- Version 2 (SNMPv2c)—The second release of SNMP is described in RFC 1902, and has additions and enhancements to data types, counter size, and protocol operations.
- Version 3 (SNMPv3)—This is the most recent version of SNMP and is described in RFC 2571, RFC 2572, RFC 2573, RFC 2574, and RFC 2575. SNMPv3 has significant enhancements to administration and security features.

The SNMP functionality on the Catalyst enterprise LAN switches for SNMP v1 and v2c has not changed, however, the functionality has greatly expanded for SNMPv3. See the [“Understanding SNMPv3” section on page 25-7](#) for more information on SNMPv3.



Note

For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 5000 Family Command Reference*.

This chapter consists of these sections:

- [SNMP Terminology, page 25-2](#)
- [Understanding How SNMPv1 and SNMPv2c Work, page 25-4](#)
- [SNMPv1 and SNMPv2c Default Configuration, page 25-5](#)
- [Configuring SNMPv1 and SNMPv2c from an NMS, page 25-5](#)
- [Configuring SNMPv1 and SNMPv2c from the CLI, page 25-6](#)
- [Understanding SNMPv3, page 25-7](#)
- [Configuring SNMPv3 from an NMS, page 25-10](#)
- [Configuring SNMPv3 from the CLI, page 25-10](#)
- [Using CiscoWorks2000, page 25-13](#)

SNMP Terminology

Table 25-1 defines the terms used in SNMP:

Table 25-1 SNMP Terminology

Term	Definition
authentication	The process of ensuring message integrity and protection against message replays, including both data integrity and data origin authentication.
authoritative SNMP engine	One of the SNMP copies involved in network communication is designated the allowed SNMP engine to protect against message replay, delay, and redirection. The security keys used for authenticating and encrypting SNMPv3 packets are generated as a function of the authoritative SNMP engine's ID and user passwords. When an SNMP message expects a response (for example, get exact, get next, set request), the <i>receiver</i> of these messages is authoritative. When an SNMP message does not expect a response, the <i>sender</i> is authoritative.
community string	A text string used to authenticate messages between a management station and an SNMPv1 or SNMPv2c engine.
data integrity	A condition or state of data in which a message packet has not been altered or destroyed in an unauthorized manner.
data origin authentication	The ability to verify the identity of a user that the message is supposedly sent to. This ability protects users against both message capture and replay by a different SNMP engine, and against packets received or sent to a particular user that uses an incorrect password or security level.
encryption	A method of hiding data from an unauthorized user by scrambling the contents of an SNMP packet.
group	A set of users belonging to a particular security model. A group defines the access rights for all the users belonging to it. Access rights define the SNMP objects that can be read, written to, or created. In addition, the group defines the notifications that a user is allowed to receive.
notification host	An SNMP entity to which notifications (traps) are to be sent.
notify view	A view name (not to exceed 64 characters) for each group; the view name defines the list of notifications that can be sent to each user in the group.
privacy	An encrypted state of the contents of an SNMP packet; in this state the contents are prevented from being disclosed on a network. Encryption is performed with an algorithm called CBC-DES (DES-56).
read view	A view name (not to exceed 64 characters) for each group; the view name defines the list of object identifiers (OIDs) that can be read by users belonging to the group.

Table 25-1 *SNMP Terminology (continued)*

Term	Definition
security level	A type of security algorithm performed on each SNMP packet. There are three levels: noauth, auth, and priv. The noauth level authenticates a packet by a string match of the username. The auth level authenticates a packet by using either the HMAC MD5 or SHA algorithms. The priv level authenticates a packet by using either the HMAC MD5 or SHA algorithms and encrypts the packet using the CBC-DES (DES-56) algorithm.
security model	The security strategy used by the SNMP agent. Currently, Cisco IOS supports three security models: SNMPv1, SNMPv2c, and SNMPv3.
Simple Network Management Protocol (SNMP)	A network management protocol that provides a method to monitor and control network devices, and to manage configurations, statistics collection, performance, and security.
Simple Network Management Protocol Version 2c (SNMPv2c)	Second version of SNMP. This protocol supports centralized and distributed network management strategies and includes improvements in the structure of management information (SMI), protocol operations, management architecture, and security.
SNMP engine	A copy of SNMP that can reside on the local or remote device.
SNMP group	A collection of SNMP users that belong to a common SNMP list that defines an access policy, in which object identification numbers (OIDs) are both read-accessible and write-accessible. Users belonging to a particular SNMP group inherit all of these attributes defined by the group.
SNMP user	A person for which an SNMP management operation is performed. For informs, the user is the person on a remote SNMP engine who receives the informs.
SNMP view	A mapping between SNMP objects and the access rights available for those objects. An object can have different access rights in each view. Access rights indicate whether the object is accessible by either a community string or a user.
trap	A message sent by an SNMP agent to a console or terminal which indicates a significant event occurred.
write view	A view name (not to exceed 64 characters) for each group; the view name defines the list of object identifiers (OIDs) that can be created or modified by users of the group.

Understanding How SNMPv1 and SNMPv2c Work

The components of SNMPv1 and SNMPv2c network management fall into three categories:

- Managed devices (such as a switch)
- SNMP agents and management information bases (MIBs), including Remote Monitoring (RMON) MIBs, which run on managed devices
- SNMP management applications, such as CiscoWorks2000, which communicate with agents to get statistics and alerts from the managed devices



Note An SNMP management application, together with the computer it runs on, is called a network management system (NMS).

SNMP network management uses these SNMP agent functions:

- Accessing a MIB variable—This function is initiated by the SNMP agent in response to a request from the NMS. The agent retrieves the value of the requested MIB variable and responds to the NMS with that value.
- Setting a MIB variable—This function is also initiated by the SNMP agent in response to a message from the NMS. The SNMP agent changes the value of the MIB variable to the value requested by the NMS.
- SNMP trap—This function is used to notify an NMS that a significant event has occurred at an agent. When a trap condition occurs, the SNMP agent sends an SNMP trap message to any NMSs specified as the trap receivers, under the following conditions:
 - When a port or module goes up or down
 - When temperature limitations are exceeded
 - When there are spanning tree topology changes
 - When there are authentication failures
 - When power supply errors occur
- SNMP community strings—SNMP community strings authenticate access to MIB objects and function as embedded passwords:
 - Read-only—Gives read access to all objects in the MIB except the community strings, but does not allow write access
 - Read-write—Gives read and write access to all objects in the MIB, but does not allow access to the community strings
 - Read-write-all—Gives read and write access to all objects in the MIB, including the community strings



Note The community string definitions on your NMS must match at least one of the three community string definitions on the switch.

The Catalyst enterprise LAN switches are managed devices that support SNMP network management with the following features:

- SNMP traps (see the [“Configuring SNMPv1 and SNMPv2c from the CLI”](#) section on page 25-6)
- RMON in the supervisor engine module software (see [Chapter 26, “Configuring RMON”](#))

- RMON and RMON2 on a Network Analysis Module (see [Chapter 28, “Configuring the Network Analysis Module”](#))
- RMON and RMON2 on an external SwitchProbe device

**Note**

For more information about MIBs, refer to:
<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtm>.

SNMP ifindex Persistence Feature

The SNMP ifIndex persistence feature is always enabled. With the ifIndex persistence feature, the ifIndex value of the port and VLAN is always retained and used after the following occurrences:

- Switch reboot
- High-availability switchover
- Software upgrade
- Module reset
- Module removal and insertion of the same type of module

For Fast EtherChannel and Gigabit EtherChannel interfaces, the ifIndex value is only retained and used after a high-availability switchover.

SNMPv1 and SNMPv2c Default Configuration

[Table 25-2](#) describes the SNMPv1 and SNMPv2c default configuration.

Table 25-2 *SNMP Default Configuration*

Feature	Default Setting
SNMP community strings	<ul style="list-style-type: none"> • Read-Only: Public • Read-Write: Private • Read-Write-all: Secret
SNMP trap receiver	None configured
SNMP traps	None enabled

Configuring SNMPv1 and SNMPv2c from an NMS

To configure SNMPv1 and SNMPv2c from an network management system (NMS), refer to the NMS documentation (see the [“Using CiscoWorks2000”](#) section on page 25-13).

The switch supports up to 20 trap receivers through the RMON2 trap destination table. Configure the RMON2 trap destination table from the NMS.

Configuring SNMPv1 and SNMPv2c from the CLI



Note

This section provides very basic SNMPv1 and SNMPv2c configuration information. For detailed information on the SNMP commands supported by the Catalyst enterprise LAN switches, refer to the *Catalyst 5000 Family Command Reference*.

To configure SNMP from the command-line interface (CLI), perform this task in privileged mode:

	Task	Command
Step 1	Define the SNMP community strings for each access type.	set snmp community read-only <i>community_string</i> set snmp community read-write <i>community_string</i> set snmp community read-write-all <i>community_string</i>
Step 2	Assign a trap receiver and community. You can specify up to ten trap receivers.	set snmp trap <i>rcvr_address rcvr_community</i>
Step 3	Specify the SNMP traps to send to the trap receiver.	set snmp trap enable [all module chassis bridge repeater auth vtp ippermit vmpls config entity stpx]
Step 4	Verify the SNMP configuration.	show snmp

This example shows how to define community strings, assign a trap receiver, and specify which traps to send to the trap receiver:

```

Console> (enable) set snmp community read-only Everyone
SNMP read-only community string set to 'Everyone'.
Console> (enable) set snmp community read-write Administrators
SNMP read-write community string set to 'Administrators'.
Console> (enable) set snmp community read-write-all Root
SNMP read-write-all community string set to 'Root'.
Console> (enable) set snmp trap 172.16.10.10 read-write
SNMP trap receiver added.
Console> (enable) set snmp trap 172.16.10.20 read-write-all
SNMP trap receiver added.
Console> (enable) set snmp trap enable all
All SNMP traps enabled.
Console> (enable) show snmp
RMON:                               Disabled
Extended RMON:                       Extended RMON module is not present
Traps Enabled:
Port,Module,Chassis,Bridge,Repeater,Vtp,Auth,ippermit,Vmps,config,entity,stpx
Port Traps Enabled: 1/1-2,4/1-48,5/1
Community-Access      Community-String
-----
read-only              Everyone
read-write             Administrators
read-write-all        Root
Trap-Rec-Address      Trap-Rec-Community
-----
172.16.10.10          read-write
172.16.10.20          read-write-all
Console> (enable)

```

**Note**

To disable access for an SNMP community, set the community string for that community to the null string (do not enter a value for the community string).

Understanding SNMPv3

Simple Network Management Protocol Version 3 (SNMPv3) is an interoperable standards-based protocol. SNMPv3 provides secure access to devices by authenticating and encrypting packets over the network.

The following security features are provided in SNMPv3:

- Message integrity—Ensures that a packet has not been interfered with during transmission.
- Authentication—Determines that the message is from a valid source.
- Encryption—Scrambles the contents of a packet to prevent it from being seen by an unauthorized source.

SNMPv3 provides for both security models and security levels. A security model is an authentication process that is set up for a user and the group in which the user resides. A security level is the permitted level of security within a security model. A combination of a security model and a security level determines which security process is used when handling an SNMP packet. Three security models are available: SNMPv1, SNMPv2c, and SNMPv3. [Table 25-3](#) describes the combinations of security models and levels.

Table 25-3 *SNMP Security Models and Levels*

Model	Level	Authentication	Encryption	Process
v1	noAuthNoPriv	Community String	No	Uses a community string match for authentication.
v2c	noAuthNoPriv	Community String	No	Uses a community string match for authentication.
v3	noAuthNoPriv	Username	No	Uses a username match for authentication.
v3	authNoPriv	MD5 or SHA	No	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms.
v3	authPriv	MD5 or SHA	DES	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Provides DES 56-bit encryption in addition to authentication based on the CBC-DES (DES-56) standard.

The following applies to SNMPv3 objects:

- Each user belongs to a group.
- A group defines the access policy for a set of users.
- SNMP objects access an access policy for reading, writing, and creating.

- A group determines the list of notifications its users can receive.
- A group also defines the security model and security level for its users.

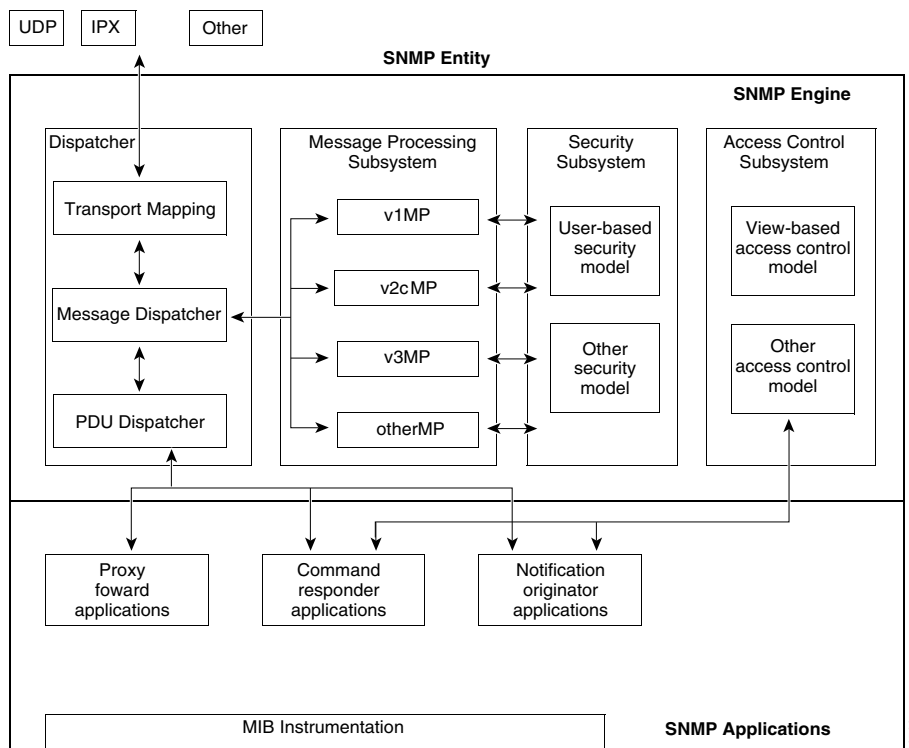
SNMP Entity

The concepts of *SNMP Agents* and *SNMP Managers* no longer apply in SNMPv3. These concepts have been combined into an *SNMP entity*. An SNMP entity consists of an SNMP engine and SNMP applications. An SNMP engine consists of four components:

- Dispatcher
- Message Processing Subsystem
- Security Subsystem
- Access Control Subsystem

Figure 25-1 outlines an SNMP engine.

Figure 25-1 SNMP Entity for Traditional SNMP Agents



Dispatcher

The dispatcher is a traffic manager that sends and receives messages. After receiving a message, the dispatcher tries to determine the version number of the message and then passes the message to the appropriate message processing model. The dispatcher is also responsible for dispatching PDUs to applications and for selecting the appropriate transports for sending messages.

Message Processing Subsystem

The message processing subsystem accepts outgoing PDUs from the dispatcher and prepares them for transmission by wrapping them in a message header and returning them to the dispatcher. The message processing subsystem also accepts incoming messages from the dispatcher, processes each message header, and returns the enclosed PDU to the dispatcher. An implementation of the message processing subsystem may support a single message format corresponding to a single version of SNMP (SNMPv1, SNMPv2c, SNMPv3), or it may contain a number of modules, each supporting a different version of SNMP.

Security Subsystem

The security subsystem authenticates and encrypts messages. Each outgoing message is passed to the security subsystem from the message processing subsystem. Depending on the services required, the security subsystem may encrypt the enclosed PDU and some fields in the message header. The security subsystem may generate an authentication code and insert it into the message header. After encryption, the message is returned to the message processing subsystem.

Each incoming message is passed to the security subsystem from the message processing subsystem. If required, the security subsystem checks the authentication code and performs decryption. The processed message is returned to the message processing subsystem. An implementation of the security subsystem may support one or more distinct security models. The only currently defined security model is the user-based security model (USM) for SNMPv3, specified in RFC 2274.

The USM protects SNMPv3 messages from the following potential security threats:

- An authorized user sending a message that gets modified in transit by an unauthorized SNMP entity.
- An unauthorized user trying to masquerade as an authorized user.
- A user modifying the message stream.
- An unauthorized user listening to the message.

The USM currently defines the use of HMAC-MD5-96 and HMAC-SHA-96 as the possible authentication protocols and CBC-DES as the privacy protocol.

SNMPv1 and SNMPv2c security models provide only weak authentication (community names) and no privacy.

Access Control Subsystem

The responsibility of the access control subsystem is to determine whether access to a managed object should be allowed. One access control model, the view-based access control model (VACM), currently has been defined. With VACM you can control which users and which operations can have access to which managed objects.

Applications

SNMPv3 applications refer to internal applications within an SNMP entity. These internal applications can do the following operations:

- Generate SNMP messages
- Respond to received SNMP messages
- Generate notifications
- Receive notifications
- Forward messages between SNMP entities

There are currently five types of applications:

- Command generators—Generate SNMP commands to collect or set management data.
- Command responders—Provide access to management data. For example, **processing get, get-next, get-bulk and set pdus** commands are used in a command responder application.
- Notification originators —Initiate Trap or Inform messages.
- Notification receivers—Receive and process Trap or Inform messages.
- Proxy forwarders—Forward messages between SNMP entities.

Configuring SNMPv3 from an NMS

To configure SNMP from an Network Management System (NMS), refer to the NMS documentation (see the [“Using CiscoWorks2000” section on page 25-13](#)).

The switch supports up to 20 trap receivers through the RMON2 trap destination table. Configure the RMON2 trap destination table from the NMS.

Configuring SNMPv3 from the CLI



Note

This section provides very basic SNMP v3 configuration information. For detailed information on the SNMP commands supported by the Catalyst enterprise LAN switches, refer to the *Catalyst 5000 Family Command Reference*.

To configure SNMPv3 from the command-line interface (CLI), perform this task in privileged mode:

	Task	Command
Step 1	Set the SNMP-Server EngineID name for the local SNMP engine.	set snmp engineid <i>engineid</i>
Step 2	Configure the MIB views.	set snmp view [-hex] {viewname} {subtree} [mask] [included excluded] [volatile nonvolatile]

Task	Command
Step 3 Set the access rights for a group with a certain security model in different security levels.	set snmp access [-hex] {groupname} {security-model v3} {noauthentication authentication privacy} [read [-hex] {readview}] [write [-hex] {writeview}] [notify [-hex] {notifyview}] [context [-hex] {contextname}] [exact prefix] [volatile nonvolatile]
Step 4 Specify the target addresses for notifications.	set snmp notify [-hex] {notifyname} tag [-hex] {notifytag} [trap inform] [volatile nonvolatile]
Step 5 Set the snmpTargetAddrEntry in the target address table.	set snmp targetaddr [-hex] {addrname} param [-hex] {paramsname} {ipaddr} [udpport {port}] [timeout {value}] [retries {value}] [volatile nonvolatile] [taglist [{-hex} tag] [{-hex} tag]]
Step 6 Set the SNMP parameters used to generate a message to a target.	set snmp targetparams [-hex] {paramsname} user [-hex] {username} {security-model v3} {message-processing v3} {noauthentication authentication privacy} [volatile nonvolatile]
Step 7 Configure a new user.	set snmp user [-hex] {username} [remote {engineid}] [{authentication {md5 sha} {authpassword}}] [privacy {privpassword}] [volatile nonvolatile]
Step 8 Relate a user to a group using a specified security model.	set snmp group [-hex] {groupname} user [-hex] {username} {security-model v1 v2 v3} [volatile nonvolatile]
Step 9 Configure the community table for the system default part, which maps community strings of previous versions of SNMP to SNMPv3.	set snmp community {access_type} [community_string] (access_type = read-only read-write read-write-all)
Step 10 Configure the community table for mappings between different community strings and security models with full permissions.	set snmp community index {index_name} name [community_string] security {security_name} context {context_name} transporttag {tag_value} [volatile nonvolatile]
Step 11 Verify the SNMP configuration.	show snmp

The following example shows how to set a MIB view to interfacesMibView:

```
Console> (enable) set snmp view interfacesMibView 1.3.6.1.2.1.2 included
Snmp view name was set to interfacesMibView with subtree 1.3.6.1.2.1.2 included,
nonvolatile.
```

The following example shows how to set the access rights for a group called guestgroup to SNMPv3 authentication read mode:

```
Console> (enable) set snmp access guestgroup security-model v3 authentication read
interfacesMibView
Snmp access group was set to guestgroup version v3 level authentication,
readview interfacesMibView, context match:exact, nonvolatile.
```

The following example shows how to specify the target addresses:

```
Console> (enable) set snmp notify notifytable1 tag routers trap
Snmp notify name was set to notifytable1 with tag routers notifyType trap, and storageType
nonvolatile.
```

The following examples show how to set the `snmpTargetAddrEntry` in the target address table:

```
Console> (enable) set snmp targetaddr router_1 param p1 172.20.21.1
Snmp targetaddr name was set to router_1 with param p1
ipAddr 172.20.21.1, udpport 162, timeout 1500, retries 3, storageType nonvolatile.
```

```
Console> (enable) set snmp targetaddr router_2 param p2 172.20.30.1
Snmp targetaddr name was set to router_2 with param p2
ipAddr 172.20.30.1, udpport 162, timeout 1500, retries 3, storageType nonvolatile.
```

The following examples show how to set SNMP target parameters:

```
Console> (enable) set snmp targetparams p1 user guestuser1 security-model v3
message-processing v3 authentication
Snmp target params was set to p1 v3 authentication, message-processing v3,
user guestuser1 nonvolatile.
```

```
Console> (enable) set snmp targetparams p2 user guestuser2 security-model v3
message-processing v3 privacy
Snmp target params was set to p2 v3 privacy, message-processing v3,
user guestuser2 nonvolatile.
```

The following examples show how to configure `guestuser1` and `guestuser2` as users:

```
Console> (enable) set snmp user guestuser1 authentication md5 guestuser1password privacy
privacypasswd1
Snmp user was set to guestuser1 authProt md5 authPasswd guestuser1password privProt des
privPasswd
privacypasswd1 with engineid 00:00:00:09:00:10:7b:f2:82:00:00:00 nonvolatile.
```

```
Console> (enable) set snmp user guestuser2 authentication sha guestuser2password
Snmp user was set to guestuser2 authProt sha authPasswd guestuser2password privProt
no-priv with engineid
00:00:00:09:00:10:7b:f2:82:00:00:00 nonvolatile.
```

The following examples show how to set `guestuser1` and `guestuser2` as members of the groups `guestgroup` and `mygroup`:

```
Console> (enable) set snmp group guestgroup user guestuser1 security-model v3
Snmp group was set to guestgroup user guestuser1 and version v3, nonvolatile.
```

```
Console> (enable) set snmp group mygroup user guestuser1 security-model v3
Snmp group was set to mygroup user guestuser1 and version v3, nonvolatile.
```

```
Console> (enable) set snmp group mygroup user guestuser2 security-model v3
Snmp group was set to mygroup user guestuser2 and version v3, nonvolatile.
```

The following example shows how to verify the SNMPv3 setup for `guestuser1` from a workstation:

```
workstation% getnext -v3 10.6.4.201 guestuser1 ifDescr.0
Enter Authentication password :guestuser1password
Enter Privacy password      :privacypasswd1
ifDescr.1 = sc0
```

The following example shows how to verify the SNMPv3 setup for `guestgroup` in the `snmpEngineID` MIB from a workstation:

```
workstation% getnext -v3 10.6.4.201 guestuser1 snmpEngineID
Enter Authentication password :guestuser1password
Enter Privacy password      :privacypasswd1
snmpEngineID = END_OF_MIB_VIEW_EXCEPTION
```

The following example shows how to verify the SNMPv2c setup for public access from a workstation:

```
workstation% getnext -v2c 10.6.4.201 public snmpEngineID
snmpEngineID.0 =
00 00 00 09 00 10 7b f2 82 00 00 00
```

The following examples show how to increase guestgroup's access right to read privileges for snmpEngineMibView:

```
Console> (enable) set snmp view snmpEngineMibView 1.3.6.1.6.3.10.2.1 included
Snmp view name was set to snmpEngineMibView with subtree 1.3.6.1.6.3.10.2.1 included,
nonvolatile
```

```
Console> (enable) set snmp access guestgroup security-model v3 authentication read
snmpEngineMibView
Snmp access group was set to guestgroup version v3 level authentication,
readview snmpEngineMibView, nonvolatile.
```

The following example shows how to verify the SNMPv3 access for guestuser1 from a workstation:

```
% getnext -v3 10.6.4.201 guestuser1 snmpEngineID
Enter Authentication password :guestuser1password
Enter Privacy password      :privacypasswd1
snmpEngineID.0 =
00 00 00 09 00 10 7b f2 82 00 00 00
```

The following example shows how to remove access for guestgroup:

```
Console> (enable) clear snmp acc guestgroup security-model v3 authentication
Cleared snmp access guestgroup version v3 level authentication.
```

The following example shows how to verify that the access for guestuser1 has been removed from a workstation:

```
% getnext -v3 10.6.4.201 guestuser1 ifDescr.1
Enter Authentication password :guestuser1password
Enter Privacy password      :privacypasswd1
Error code set in packet - AUTHORIZATION_ERROR:1.
```

The following example shows how to verify the access for guestuser2 from a workstation:

```
% getnext -v3 10.6.4.201 guestuser2 ifDescr.1
Enter Authentication password :guestuser2password
Enter Privacy password      :privacypasswd2
REPORT received, cannot recover:
usmStatsUnsupportedSecLevels.0 = 1
```

Using CiscoWorks2000

CiscoWorks2000 is a family of Web-based and management platform-independent products for managing Cisco enterprise networks and devices. CiscoWorks2000 includes Resource Manager Essentials and CWSI Campus, which allow you to deploy, configure, monitor, manage, and troubleshoot a switched internetwork. For more information, see the following publications:

- *Getting Started with Resource Manager Essentials*
- *Getting Started with CWSI Campus*

