

Versions

SNMPv1—Simple Network Management Protocol: a full Internet standard, defined in RFC 1157. (RFC 1157 replaces the earlier versions that were published as RFC 1067 and RFC 1098.) Security is based on community strings.

SNMPv2c—The community string-based Administrative Framework for SNMPv2. SNMPv2c (the "c" is for "community") is an experimental Internet protocol defined in RFC 1901, RFC 1905, and RFC 1906. SNMPv2c is an update of the protocol operations and data types of SNMPv2p (SNMPv2 Classic) and uses the community-based security model of SNMPv1.

SNMPv3—Version 3 of SNMP. SNMPv3 is an interoperable standards-based protocol defined in RFCs 3413 to 3415. SNMPv3 provides secure access to devices by authenticating and encrypting packets over the network.

The security features provided in SNMPv3 are as follows:

- Message integrity—Ensuring that a packet has not been tampered with in transit.
- Authentication—Determining that the message is from a valid source.
- Encryption—Scrambling the contents of a packet to prevent it from being learned by an unauthorized source.

Terminology

Community String

Passwords for SNMP access to network devices

MIB

Management Information Base, collection of variables which is shared between NMS and network device.

SNMP Trap

Message sent by device and sent to NMS

SNMP GET

Message sent by NMS to retrieve MIB data from network device

SNMP SET

Message sent by NMS when it wants to *change* or *configure* network device

Troubleshooting

```
show snmp community
```

```
show snmp host
```

```
show snmp group
```

```
show snmp user
```

```
show snmp view
```

```
debug snmp packet
```

Configuration Block

! There is no specific command that you use to enable SNMP. The first snmp-server command that you enter enables the supported versions of SNMP. All other configurations are optional.

```
snmp-server community <text string> [ro | rw]
snmp-server host <host-id> version <{1 | 2c | 3 [auth | noauth | priv]}> <community string>
```

!When you configure SNMP version 3 and you want to use the SNMPv3 security mechanism for handling SNMP packets, you must establish SNMP groups and users with passwords. You can assign views to community strings to limit which MIB objects an SNMP manager can access.

```
snmp-server view <view-name> <oid-tree> {included | excluded}
snmp-server group <[groupname {v1 | v2c | v3 [auth | noauth | priv]}] [read readview] [write writeview] [notify notifyview] [access access-list]>
snmp-server user <username groupname [remote ip-address {v1 | v2c | v3 [auth | noauth | priv]}] [read readview] [write writeview] [notify notifyview] [access access-list]>
```

Versions SNMP Security Models and Levels

Model	Level	Authentication	Encryption	What Happens
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.