Configure SNMPv2c/v3 on Catalyst 9000 Series Switches

Contents

Introduction

This document describes the basic configuration of SNMPv2c and SNMPv3 on Catalyst 9000 Switches.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- SNMP protocol(Simple Network Management Protocol).
- Familiarity with Catalyst 9000 Series Switches.
- Familiarity with SNMP Object Identifier (OID).

Components Used

The information in this document is based on these software and hardware versions:

- C9200
- C9300
- C9400
- C9500

- C9600
- Cisco IOS® XE &17.X software

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Prerequisites for SNMP

Both SNMPv1 and SNMPv2C use a community-based form of security. The community of managers able to access the agent's MIB is defined by an IP address access control list and password.

SNMPv2C includes a bulk retrieval function and more detailed error message reporting to management stations. The bulk retrieval function retrieves tables and large quantities of information, minimizing the number of round-trips required. The SNMPv2C improved error-handling includes expanded error codes that distinguish different kinds of error conditions; these conditions are reported through a single error code in SNMPv1. Error return codes in SNMPv2C report the error type.

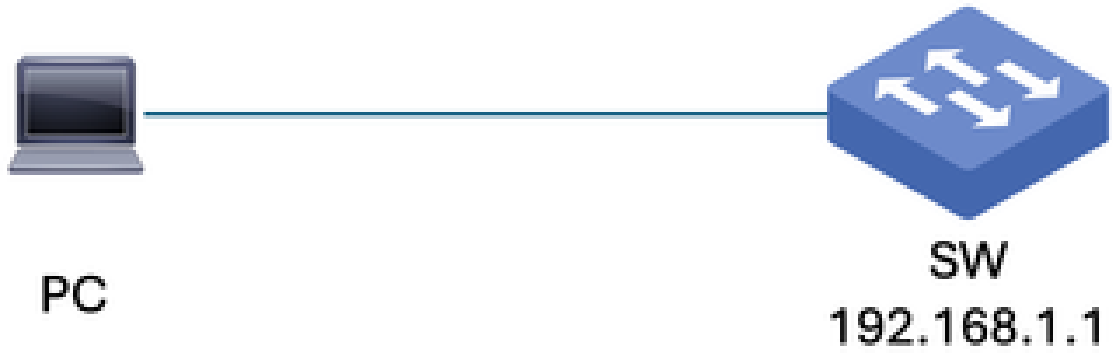
SNMPv3 provides for both security models and security levels. A security model is an authentication strategy set up for a user and the group within which the user resides. A security level is the permitted level of security within a security model. A combination of the security level and the security model determine which security method is used when handling an SNMP packet. Available security models are SNMPv1, SNMPv2C, and SNMPv3.

This table identifies characteristics and compares different combinations of security models and levels:

Model	Level	Authentication	Encryption	Result
SNMPv1	noAuthNoPriv	Community string	No	Uses a community string match for authentication.
SNMPv2C	noAuthNoPriv	Community string	No	Uses a community string match for authentication.
SNMPv3	noAuthNoPriv	Username	No	Uses a username match for authentication.
SNMPv3	authNoPriv	Message Digest 5 (MD5) or Secure Hash Algorithm (SHA)	No	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms.
SNMPv3	authPriv	MD5 or SHA	Data Encryption Standard (DES) or Advanced Encryption Standard (AES)	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Allows specifying the User-based Security Model (USM) with these encryption algorithms: • DES 56-bit encryption in addition to authentication based on the CBC-DES (DES-56) standard. • 3DES 168-bit

Model	Level	Authentication	Encryption	Result
				encryption • AES 128-bit, 192-bit, or 256-bit encryption

Network Diagram



SNMPv2c

Config

```
Switch(config)#snmp-server community cisco RW        >Read-only access with this community string
Switch(config)#snmp-server community cisco RO        >Read-write access with this community string
```

Verify

```
Switch#show snmp community
Community name: cisco
Community Index: cisco
Community SecurityName: cisco
storage-type: nonvolatile active
```

```
~ % snmpwalk -v2c -c cisco 192.168.1.1 1.3.6.1.2.1.1.3
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (111410969) 12 days, 21:28:29.69
```

SNMPv3

noAuthNoPriv

Config

```
Switch(config)#snmp-server group noAuthNoPrivGroup v3 noauth
Switch(config)#snmp-server user testuser1 noAuthNoPrivGroup v3
```

Verify

```
Switch#show snmp user
User name: testuser1
Engine ID: 800000090300EC1D8B0A7B80
storage-type: nonvolatile active
Authentication Protocol: None
Privacy Protocol: None
Group-name: noAuthNoPrivGroup
```

```
~ % snmpwalk -v3 -u testuser1 -l noAuthNoPriv 192.168.1.1 1.3.6.1.2.1.1.3
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (111425887) 12 days, 21:30:58.87
```

authNoPriv

auth-SHA

Config

```
Switch(config)#snmp-server group AuthNoPrivGroup v3 auth
Switch(config)#snmp-server user testuser2 AuthNoPrivGroup v3 auth sha Password123
```

Verify

```
Switch#show snmp user
User name: testuser2
Engine ID: 800000090300EC1D8B0A7B80
storage-type: nonvolatile active
Authentication Protocol: SHA
Privacy Protocol: None
Group-name: AuthNoPrivGroup
```

```
~ % snmpwalk -v3 -u testuser3 -l authNoPriv -a MD5 -A Password123 192.168.1.1 1.3.6.1.2.1.1.3
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (111447478) 12 days, 21:34:34.78
```

auth-MD5

Config

```
Switch(config)#snmp-server group AuthNoPrivGroup v3 auth
Switch(config)#snmp-server user testuser3 AuthNoPrivGroup v3 auth md5 Password123
```

Verify

```
Switch#show snmp user
User name: testuser3
Engine ID: 800000090300EC1D8B0A7B80
storage-type: nonvolatile active
Authentication Protocol: MD5
Privacy Protocol: None
Group-name: AuthNoPrivGroup
```

```
~ % snmpwalk -v3 -u testuser3 -l authNoPriv -a MD5 -A Password123 192.168.1.1 1.3.6.1.2.1.1.3
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (111455526) 12 days, 21:35:55.26
```

authPriv

auth-SHA + priv-DES

Config

```
Switch(config)#snmp-server group AuthPrivGroup v3 priv
Switch(config)#snmp-server user testuser4 AuthPrivGroup v3 auth sha Password123 priv des Password123
```

Verify

```
Switch#show snmp user
User name: testuser4
Engine ID: 800000090300EC1D8B0A7B80
storage-type: nonvolatile active
Authentication Protocol: SHA
Privacy Protocol: DES
Group-name: AuthPrivGroup
```

```
~ % snmpwalk -v3 -u testuser4 -l authPriv -a SHA -A Password123 -x DES -X Password123 192.168.1.1 1.3.6
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (111472744) 12 days, 21:38:47.44
```

auth-SHA + priv-AES

Config

```
Switch(config)#snmp-server group AuthPrivGroup v3 priv
Switch(config)#snmp-server user testuser5 AuthPrivGroup v3 auth sha Password123 priv aes 128 Password12
```

Verify

```
Switch#show snmp user
User name: testuser5
Engine ID: 800000090300EC1D8B0A7B80
storage-type: nonvolatile active
Authentication Protocol: SHA
Privacy Protocol: AES128
Group-name: AuthPrivGroup
```

```
~ % snmpwalk -v3 -u testuser5 -l authPriv -a SHA -A Password123 -x AES -X Password123 192.168.1.1 1.3.6
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (111476608) 12 days, 21:39:26.08
```

auth-MD5 + priv-DES

Config

```
Switch(config)#snmp-server group AuthPrivGroup v3 priv
Switch(config)#snmp-server user testuser6 AuthPrivGroup v3 auth md5 Password123 priv des Password123
```

Verify

```
Switch#show snmp user
User name: testuser6
Engine ID: 800000090300EC1D8B0A7B80
storage-type: nonvolatile active
Authentication Protocol: MD5
Privacy Protocol: DES
Group-name: AuthPrivGroup
```

```
~ % snmpwalk -v3 -u testuser6 -l authPriv -a MD5 -A Password123 -x DES -X Password123 192.168.1.1 1.3.6
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (76726018) 8 days, 21:07:40.18
```

auth-MD5 + priv-AES

Config

```
Switch(config)#snmp-server group AuthPrivGroup v3 priv
Switch(config)#snmp-server user testuser7 AuthPrivGroup v3 auth md5 Password123 priv aes 128 Password12
```

Verify

```
Switch#show snmp user
User name: testuser7
Engine ID: 800000090300EC1D8B0A7B80
storage-type: nonvolatile active
Authentication Protocol: MD5
Privacy Protocol: AES128
Group-name: AuthPrivGroup
```

```
~ % snmpwalk -v3 -u testuser7 -l authPriv -a MD5 -A Password123 -x AES -X Password123 192.168.1.1 1.3.6
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (76738170) 8 days, 21:09:41.70
```

Related Information

- Network Management Configuration Guide, Cisco IOS XE 17.15.x (Catalyst 9300 Switches)
- SNMP Object Navigator