

Configure SNMP Community Strings

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Conventions](#)

[Background Information](#)

[Configurate SNMP on Router and Catalyst Switch](#)

[Enable SNMP Community Strings](#)

[Verify SNMP Community Strings](#)

[Modify SNMP Community Strings](#)

[Disable/Remove SNMP Community Strings](#)

[Configure SNMP on a Multilayer Switch Feature Card \(MSFC\)](#)

[Enable SNMP Community Strings](#)

[Verify SNMP Community Strings](#)

[Modify, Remove, or Disable SNMP Community Strings](#)

[Related Information](#)

Introduction

This document describes how to configure Simple Network Management Protocol strings on Cisco routers, Route Switch Modules, and Catalyst switches.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

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.

This document is not restricted to specific software and hardware versions.

Conventions

Refer to the [Cisco Technical Tips Conventions](#) for more information on document conventions.

Background Information

This document describes how to configure Simple Network Management Protocol (SNMP) community strings on Cisco routers, Route Switch Modules (RSMs), and Catalyst switches. In the context of this

document, configure is defined as verify, enable, modify, and disable SNMP community strings.

Configure SNMP on Router and Catalyst Switch

Enable SNMP Community Strings

This procedure is the same for both routers and Cisco IOS® software-based XL Catalyst Switches.

1. Telnet to the router:

```
<#root>  
prompt#  
telnet 172.16.99.20
```

2. Enter the enable password at the prompt in order to enter the enable mode:

```
<#root>  
Router>  
enable  
  
Password:  
Router#
```

3. Display the running configuration and look for the SNMP information:

```
<#root>  
Router#  
show running-config  
  
Building configuration...  
....  
....
```

Note: If no SNMP information is present, continue with these steps. If any SNMP commands are listed, you can modify or disable them.

4. Go into the configuration mode:

```
<#root>  
Router#
```

```
configure terminal
```

```
Enter configuration commands, one per line. End  
with CNTL/Z.  
Router(config)#
```

5. Use this command in order to enable the read-only (RO) community string:

```
<#root>  
  
Router(config)#  
  
snmp-server community public RO
```

where "public" is the read-only community string.

6. Use this command in order to enable the read-write (RW) community string:

```
<#root>  
  
Router(config)#  
  
snmp-server community private RW
```

where "private" is the read-write community string.

7. Exit out of the configuration mode and return to the main prompt:

```
<#root>  
  
Router(config)#  
  
exit  
  
Router#
```

8. Write the modified configuration to nonvolatile RAM (NVRAM) to save the settings:

```
<#root>  
  
Router#  
  
write memory  
  
Building configuration...  
[OK]  
Router#
```

Verify SNMP Community Strings

Complete these steps to verify SNMP community strings:

1. Verify that there is TCP/IP connectivity between the Network Management Server (NMS) server and the router

```
<#root>
```

```
C:\>
```

```
ping 172.16.99.20
```

```
Pinging 172.16.99.20 with 32 bytes of data:
```

```
Reply from 172.16.99.20: bytes=32 time<10ms TTL=247
```

```
Reply from 172.16.99.20: bytes=32 time=10ms TTL=247
```

```
Reply from 172.16.99.20: bytes=32 time<10ms TTL=247
```

```
Reply from 172.16.99.20: bytes=32 time<10ms TTL=247
```

```
Ping statistics for 172.16.99.20:
```

```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
    Minimum = 0ms, Maximum = 10ms, Average = 2ms
```

2. Telnet to the router:

```
<#root>
```

```
prompt#
```

```
telnet 172.16.99.20
```

3. Enter the enable password at the prompt in order to enter the enable mode:

```
<#root>
```

```
Router>
```

```
enable
```

```
Password:
```

```
Router#
```

4. Display the running configuration and look for the SNMP information:

```
<#root>
```

```
Router#  
  
show running-config  
  
....  
....  
snmp-server community public RO  
snmp-server community private RW  
....  
....
```

In this sample output, "public" is the read-only community string and "private" is the read-write community string.

If no SNMP information is present, continue with these steps. If any SNMP commands are listed, you can modify or disable them.

Note: If you do not see any "snmp-server" statements, SNMP is not enabled on the router. Alternatively, execute the **show snmp** command in the enable mode. If you see this message, it also indicates that SNMP is not enabled on the router. For example:

```
<#root>  
  
Router#  
  
show snmp  
%SNMP agent not enabled  
  
Router#
```

5. Exit the enable mode and return to the main prompt:

```
<#root>  
  
Router#  
  
disable  
  
Router>
```

Modify SNMP Community Strings

Complete these steps in order to modify SNMP community strings.

1. Telnet to the router:

```
<#root>
```

```
prompt#  
telnet 172.16.99.20
```

2. Enter the enable password at the prompt in order to enter the enable mode:

```
<#root>
```

```
Router>
```

```
enable
```

```
Password:
```

```
Router#
```

3. Display the running configuration and look for the SNMP information:

```
<#root>
```

```
Router#
```

```
show running-config
```

```
Building configuration...
```

```
...  
...
```

```
snmp-server community public RO
```

```
snmp-server community private RW
```

```
....  
....
```

4. Go into the configuration mode:

```
<#root>
```

```
Router#
```

```
configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
Router(config)#
```

Complete these steps to modify the current read-only (RO) community string:

a. Delete the current read-only (RO) community string with this command:

```
<#root>  
Router(config)#  
no snmp-server community public RO
```

where "public" is the read-only community string.

b. Enter the new read-only (RO) community string with this command:

```
<#root>  
Router(config)#  
snmp-server community XXXX RO
```

where "XXXX" is the read-only community string.

Complete these steps to modify the current read-write (RW) community string:

a. Delete the current read-write (RW) community string with this command:

```
<#root>  
Router(config)#  
no snmp-server community private RW
```

where "private" is the read-write (RW) community string.

b. Enter the new read-write (RW) community string with this command:

```
<#root>  
Router(config)#  
snmp-server community YYYY RW
```

where "YYYY" is the read-write community string.

5. Exit the configuration mode and return to the main prompt:

```
<#root>
```

```
Router(config)#
```

```
exit
```

```
Router#
```

6. Write the modified configuration to nonvolatile RAM (NVRAM) to save the settings:

```
<#root>
```

```
Router#
```

```
write memory
```

```
Building configuration...
```

```
[OK]
```

```
Router#
```

Disable/Remove SNMP Community Strings

Complete these steps to disable or remove SMMP community strings.

1. Telnet to the router:

```
<#root>
```

```
prompt#
```

```
telnet 172.16.99.20
```

2. Enter the enable password at the prompt in order to enter the enable mode:

```
<#root>
```

```
Router>
```

```
enable
```

```
Password:
```

```
Router#
```

3. Display the running configuration and look for the SNMP information:

```
<#root>
```



```
Router#
```

```
show running-config
```

```
Building configuration...
```

```
...  
...
```

```
snmp-server community public RO  
snmp-server community private RW
```

```
....  
....
```

4. Go into the configuration mode:

```
<#root>
```

```
Router#
```

```
configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
Router(config)#
```

5. In order to disable/remove the current read-only (RO) community string, use this command:

```
<#root>
```

```
Router(config)#
```

```
no snmp-server community public RO
```

where "public" is the read-only community string.

6. In order to disable/remove the current read-write (RW) community string, use this command:

```
<#root>
```

```
Router(config)#
```

```
no snmp-server community private RW
```

where "private" is the read-write community string.

7. Exit out of the configuration mode and return to the main prompt:

```
<#root>  
Router(config)#  
exit  
  
Router#
```

8. Write the modified configuration to nonvolatile RAM (NVRAM) to save the settings:

```
<#root>  
  
Router#  
write memory  
  
Building configuration...  
[OK]  
Router#
```

Configure SNMP on a Multilayer Switch Feature Card (MSFC)

Enable SNMP Community Strings

A multilayer switch feature card (MSFC) runs the same Cisco IOS software code as the routers do.

Verify SNMP Community Strings

Complete these steps to verify SNMP community strings on a multilayer switch feature card (MSFC).

1. Telnet to the Catalyst Switch (the Catalyst 6509 is used in this example):

```
<#root>  
  
prompt#  
telnet 172.16.99.66
```

2. Enter the enable password at the prompt in order to enter the enable mode:

```
<#root>  
  
Cat6509>
```

```
enable
```

```
Password:
```

```
Cat6509> (enable)
```

3. Execute the **show module** command in order to display the system modules and locate the MSFC module. Here is an example:

```
<#root>
```

```
Cat6509 (enable)
```

```
show module
```

```
Mod Slot Ports Module-Type Model Sub Status
-----
1 1 2 1000BaseX Supervisor WS-X6K-SUP1A-2GE yes ok
15 1 1 Multilayer Switch Feature WS-F6K-MSFC no ok
3 3 8 1000BaseX Ethernet WS-X6408A-GBIC no ok
4 4 48 10/100BaseTX Ethernet WS-X6348-RJ-45 yes ok
5 5 48 10/100BaseTX Ethernet WS-X6348-RJ-45 no ok
6 6 8 T1 WS-X6608-T1 no ok
7 7 24 FXS WS-X6624-FXS no ok
8 8 0 FlexWAN Module WS-X6182-2PA no ok

....
....
--<snip>--
```

4 After you identify the Mod number, start a "session" to the MSFC module. For example:

```
<#root>
```

```
Cat6509> (enable)
```

```
session 15
```

```
Trying Router-15...
```

```
Connected to Router-15.
```

```
Escape character is '^]'.  
MSFC>
```

5. Enter the enable password at the prompt in order to enter the enable mode:

```
<#root>
```

```
MSFC>
```

```
enable
```

```
Password:  
MSFC#
```

6. Display the running configuration and look for the SNMP information:

```
<#root>  
  
MSFC#  
  
show running-config  
  
Building configuration...  
....  
....  
snmp-server community public RO  
snmp-server community private RW  
....  
....
```

In this output, "public" is the read-only community string and "private" is the read-write community string.

Note: If you do not see any "snmp-server" statements, SNMP is not enabled on the router. Alternatively, you can execute the **show snmp** command in the enable mode. If you see this message, it also indicates that SNMP is not enabled on the router. For example:

```
<#root>  
  
MSFC#  
  
show snmp  
  
%SNMP agent not enabled  
  
MSFC#
```

7. Exit out of the enable mode and return to the main prompt:

```
<#root>  
  
MSFC#  
  
exit
```

Cat65509> (enable)

Modify, Remove, or Disable SNMP Community Strings

The MSFC runs the same Cisco IOS software code as the routers do. You can complete the same procedure in order to modify, remove, or disable SNMP as described in the [router example](#).

Related Information

- [Cisco Security Advisory: Cisco IOS Software SNMP read-Write ILMI Community String Vulnerability](#)
- [Cisco Security Advisory: Cisco IOS Software Multiple SNMP Community String](#)
- [Cisco Technical Support & Downloads](#)