

How to Configure SNMP Community Strings

Document ID: 7282

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

How To Configure SNMP Community Strings on a Router and a Cisco IOS

Software-based XL Catalyst Switch

- Enable SNMP Community Strings
- Verify SNMP Community Strings
- Modify SNMP Community Strings
- Disable/Remove SNMP Community Strings

How To Configure SNMP Community Strings on an RSM

- Enable SNMP Community Strings
- Verify SNMP Community Strings
- Modify SNMP Community Strings
- Disable/Remove SNMP Community Strings

How To Configure SNMP Community Strings on a Multilayer Switch Feature Card (MSFC)

- Enable SNMP Community Strings
- Verify SNMP Community Strings
- Modify SNMP Community Strings
- Disable/Remove SNMP Community Strings

How To Configure SNMP Community Strings on a Catalyst Switch

- Enable SNMP Community Strings
- Verify SNMP Community Strings
- Modify SNMP Community Strings
- Disable/Remove SNMP Community Strings

Related Information

Introduction

This document explains 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.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

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

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, make sure

that you understand the potential impact of any command.

Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

How To Configure SNMP Community Strings on a Router and a Cisco IOS Software–based XL 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:

```
prompt#telnet 172.16.99.20
```

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

```
Router>enable  
Password:  
Router#
```

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

```
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:

```
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:

```
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:

```
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:

```
Router(config)#exit  
Router#
```

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

```
Router#write memory  
Building configuration...  
[OK]  
Router#
```

Verify SNMP Community Strings

Here is how to verify SNMP community strings.

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

```
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:

```
prompt# telnet 172.16.99.20
```

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

```
Router>enable
Password:
Router#
```

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

```
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.

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:

```
Router#show snmp
%SNMP agent not enabled
Router#
```

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

```
Router#disable
Router>
```

Modify SNMP Community Strings

Complete these steps in order to modify SNMP community strings.

1. Telnet to the router:

```
prompt# telnet 172.16.99.20
```

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

```
Router>enable  
Password:  
Router#
```

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

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

4. Go into the configuration mode:

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

◆ In order to modify the current Read-only (RO) community string:

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

· 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:

· Router(config)#**snmp-server community XXXX RO** (where "XXXX" is the Read-only community string)

◆ In order to modify the current Read-write (RW) community string:

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

· Router(config)#**no snmp-server community private RW** (where "private" is the Read-write community string)

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

· Router(config)#**snmp-server community YYYY RW** (where "YYYY" is the Read-write community string)

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

```
Router(config)#exit  
Router#
```

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

```
Router#write memory  
Building configuration...  
[OK]  
Router#
```

Disable/Remove SNMP Community Strings

Complete these steps in order to disable or remove SMMP community strings.

1. Telnet to the router:

```
prompt# telnet 172.16.99.20
```

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

```
Router>enable  
Password:  
Router#
```

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

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

4. Go into the configuration mode:

```
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:

```
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:

```
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:

```
Router(config)#exit  
Router#
```

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

```
Router#write memory  
Building configuration...  
[OK]  
Router#
```

How To Configure SNMP Community Strings on an RSM

Enable SNMP Community Strings

RSMs run the same Cisco IOS software code as the routers do. Consequently, you can complete the same procedure in order to enable SNMP on an RSM as described for the routers.

Verify SNMP Community Strings

Complete this procedure to verify SNMP community strings on an RSM.

1. Telnet to the Catalyst Switch (in our example, we use the Catalyst 5500):

```
prompt# telnet 172.16.99.55
```

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

```
Cat5500>enable
Password:
Cat5500> (enable)
```

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

```
Cat5500> (enable) show module

Mod Slot Ports Module-Type Model Sub Status
-----
1 1 0 Supervisor III WS-X5530 yes ok
2 2 Gigabit Ethernet Ext WS-X5410
3 3 9 Gigabit Ethernet WS-X5410 no ok
4 4 24 10BaseT Ethernet WS-X5010 no ok
5 5 1 Route Switch WS-X5302 no ok
6 6 1 Network Analysis/RMON WS-X5380 no ok
7 7 12 10/100BaseTX Ethernet WS-X5213A no ok
9 9 16 Token Ring WS-X5030 no ok
10 10 12 10BaseFL Ethernet WS-X5011 no ok
11 11 24 10/100BaseTX Ethernet WS-X5225R no ok
13 13 ASP/SRP no

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

4. After you identify the Mod number, start a "session" to the RSM module. Here is an example:

```
Cat5500> (enable) session 5
Trying Router-5...
Connected to Router-5.
Escape character is '^]'.

RSM>
```

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

```
RSM>enable
Password:
RSM#
```

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

```
RSM#show running-config

Building configuration...
....
....
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.

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.

```
RSM#show snmp

%SNMP agent not enabled
```

RSM#

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

```
RSM#exit
Cat5500> (enable)
```

Modify SNMP Community Strings

RSM runs the same Cisco IOS software code as the routers do. You can complete the same procedure to modify SNMP as described in the router example.

Disable/Remove SNMP Community Strings

RSM runs the same Cisco IOS software code as the routers do. You can complete the same procedure to disable SNMP as described in the router example.

How To Configure SNMP Community Strings 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. You can complete the same procedure to enable SNMP as described in the .

Verify SNMP Community Strings

Here is how 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):

```
prompt# telnet 172.16.99.66
```

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

```
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:

```
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. Here is an example:

```
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:

```
MSFC>enable
Password:
MSFC#
```

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

```
MSFC#show running-config

Building configuration...
....
....
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.

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:

```
MSFC#show snmp

%SNMP agent not enabled

MSFC#
```

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

```
MSFC#exit
Cat65509> (enable)
```

Modify 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 SNMP as described in the router example.

Disable/Remove 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 disable SNMP as described in the router example.

How To Configure SNMP Community Strings on a Catalyst Switch

On Catalyst switches such as the 4000, 5000, and 6000 series that run a regular catalyst Operating System (OS), SNMP is enabled by default with the community strings set to:

- Read-Only: Public
- Read-Write: Private
- Read-Write-all: Secret

With these community strings and the IP address of your switch's management interface, anyone is able to reconfigure the device. You must change the community strings on the Catalyst switch immediately after you set the device on the network. This is very important.

Enable SNMP Community Strings

Complete these steps in order to enable SNMP community strings on a catalyst switch.

1. Telnet to the Catalyst Switch (the Catalyst 5500 is used in this example):

```
prompt# telnet 172.16.99.55
```

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

```
Cat5500>enable
Password:
Cat5500> (enable)
```

3. In order to enable Read-only (RO) community string, use this command:

```
Cat5500> (enable) set snmp community read-only XXXX
```

(where "XXXX" is the Read-only community string)

4. In order to enable Read-write (RW) community string, use this command:

```
Cat5500> (enable) set snmp community read-write YYYY
```

where "YYYY" is the Read-write community string

Note: The Catalyst 4000, 5000, and 6000 series switches do not have Start-up configurations. That is why there is no **write memory** command in these switches compared to the routers.

5. Verify that the new community strings are added:

```
Cat5500> (enable) show snmp

RMON:                               Enabled
Extended RMON:                       Enabled
Extended RMON Netflow:                Enabled
Extended RMON Vlanmode:               Disabled
Extended RMON Vlanagent:              Disabled
SPAN Configuration:
Traps Enabled:
Port ,Module,Chassis,Bridge,Repeater,Vtp,Auth,ippermit,Vmps,config,
entity,stpx,syslog
Port Traps Enabled: 3/1-9,4/1-24,7/1-12,9/1-16,10/1-12,11/1-24
Community-Access      Community-String
-----
read-only              XXXX (XXXX is the new Read-only community string)
read-write             YYYY (YYYY is the new Read-write community string)
read-write-all        secret
....
....
--<snip>--
```

Verify SNMP Community Strings

Complete these steps in order to configure SNMP community strings on a catalyst switch.

1. Telnet to the Catalyst Switch (the Catalyst 5500 is used in this example):

```
prompt# telnet 172.16.99.55
```

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

```
Cat5500>enable
Password:
Cat5500>(enable)
```

3. Execute the **show snmp** command in order to display the current SNMP information and look for the community-access information. Here is an example:

```
Cat5500> (enable) show snmp

RMON:                               Enabled
Extended RMON:                       Enabled
Extended RMON Netflow:                Enabled
Extended RMON Vlanmode:               Disabled
Extended RMON Vlanagent:              Disabled
SPAN Configuration:
Traps Enabled:
Port,Module,Chassis,Bridge,Repeater,Vtp,Auth,ippermit,Vmps,config,
  entity,stpx,syslog
Port Traps Enabled: 3/1-9,4/1-24,7/1-12,9/1-16,10/1-12,11/1-24
Community-Access      Community-String
-----
read-only            XXXX          ("XXXX" is the Read-only community string)
read-write             YYYY          ("YYYY" is the Read-write community string)
read-write-all        secret
....
....
--<snip>--
```

Modify SNMP Community Strings

Complete these steps in order to modify SNMP community strings on a catalyst switch.

1. Telnet to the Catalyst Switch (the Catalyst 5500 is used in this example):

```
prompt# telnet 172.16.99.55
```

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

```
Cat5500>enable
Password:
Cat5500> (enable)
```

3. In order to modify the Read-only (RO) community string, use this command:

```
Cat5500> (enable) set snmp community read-only public
```

where "public" is the Read-only community string. The command overwrites the existing community string if the switch has one.

4. In order to enable the Read-write (RW) community string, use this command:

```
Cat5500> (enable) set snmp community read-write private
```

where "private" is the Read-write community string. The command overwrites the existing community string if the switch has one.

Note: Cat OS supports only one community string for each read-only, read-write and read-write-all communities. You can not configure multiple community strings, unlike Cisco IOS.

5. Execute the **show snmp** command in order to display the current SNMP information and look for the community-access information. Here is an example:

```
Cat5500> (enable) show snmp

RMON:                               Enabled
Extended RMON:                       Enabled
Extended RMON Netflow:                 Enabled
Extended RMON Vlanmode:                 Disabled
Extended RMON Vlanagent:                 Disabled
SPAN Configuration:
Traps Enabled:
Port,Module,Chassis,Bridge,Repeater,Vtp,Auth,ippermit,Vmps,config,
  entity,stpx,syslog
Port Traps Enabled: 3/1-9,4/1-24,7/1-12,9/1-16,10/1-12,11/1-24
Community-Access      Community-String
-----
read-only              public

!--- public is the modified Read-only community string

read-write             private

!--- private is the modified Read-write community string

read-write-all        secret
....
....
--<snip>--
```

Disable/Remove SNMP Community Strings

Complete these steps in order to disable or remove SNMP community strings on a catalyst switch.

1. Telnet to the Catalyst Switch (the Catalyst 5500 is used in this example):

```
prompt# telnet 172.16.99.55
```

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

```
Cat5500>enable
Password:
Cat5500>(enable)
```

3. In order to delete/remove the Read-only (RO) community string, use this command:

```
Cat5500> (enable) set snmp community read-only
SNMP read-only community string cleared
```

4. In order to delete/remove the Read-write (RW) community string, use this command:

```
Cat5500>(enable) set snmp community read-write
SNMP read-write community string cleared
```

5. Verify that the community strings are deleted/removed. Here is an example:

```
Cat5500> (enable) show snmp

RMON:                               Enabled
Extended RMON:                       Enabled
```

```
Extended RMON Netflow:    Enabled
Extended RMON Vlanmode:  Disabled
Extended RMON Vlanagent: Disabled
SPAN Configuration:
Traps Enabled:
Port,Module,Chassis,Bridge,Repeater,Vtp,Auth,ippermit,Vmps,config,
    entity,stpx,syslog
Port Traps Enabled: 3/1-9,4/1-24,7/1-12,9/1-16,10/1-12,11/1-24
Community-Access    Community-String
-----
read-only
read-write
....
....
--<snip>--
```

As you can see, the column for "Community-String" is blank. This indicates that both the read-only and read-write community strings are deleted or removed.

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**
- **Technical Support – Cisco Systems**

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Oct 26, 2005

Document ID: 7282
