CCNPv7 SWITCH

Lab 7-2 Configure Campus Network Devices to support Simple Network Management Protocol (SNMPv3) **Instructor Version**

Topology

Objective

* Configure an SNMP View
* Configure SNMP version 2c
* Configure SNMP version 3
* Verify SNMP operation

Background

The Simple Network Management Protocol (SNMP) is an application layer protocol that facilitates the exchange of management information between an agent and a management server. SNMP enables network administrators to monitor and manage network performance, find and solve network problems, and plan for network growth. SNMP management workstations can ask (*get*) for the value of a specific *object identifier* (*OID*) from the *management information base* (*MIB*) maintained by SNMP agents. The Manager can also configure (*set*) specific variable values in an OID. Additionally, the agent can send notifications (*traps or informs*) when an event occurs or threshold is reached (simply put, an *inform* is a trap that must be acknowledged by the manager). Like any powerful tool, SNMP can be dangerous if not used properly, and securing the protocol and its uses are critical.

There are three SNMP versions. SNMPv3 is considered the most secure because it offers authentication and encryption, where SNMP versions 1 and 2 offer neither. SNMP access can also be limited using an access control list.

In this lab you will configure SNMP v3 on the distribution layer switches and SNMP v2c on the access layer switches. The network should still be configured and operating based on the configurations that you applied in Lab 7-1 Synchronizing NTP in the campus network. All SNMP communications will be carried on the Management VLAN (VLAN 99), and agent access will be restricted to the IP address of the Network management Server.

**Note:** This lab uses Cisco Catalyst 3560 and 2960 switches running Cisco IOS 15.0(2) IP Services and LAN Base images, respectively. The 3560 and 2960 switches are configured with the SDM templates “dual-ipv4-and-ipv6 routing” and “lanbase-routing”, respectively. Depending on the switch model and Cisco IOS Software version, the commands available and output produced might vary from what is shown in this lab. Catalyst 3650 switches (running any Cisco IOS XE release) and Catalyst 2960-Plus switches (running any supported Cisco IOS image) can be used in place of the Catalyst 3560 switches and the Catalyst 2960 switches.

Required Resources

* 2 switches (Cisco 2960 with the Cisco IOS Release 15.0(2)SE6 C2960-LANBASEK9-M image or comparable)
* 2 switches (Cisco 3560 with the Cisco IOS Release 15.0(2)SE6 C3560-ipservicesK9-M image or comparable)
* Ethernet and console cables
* 1 PC (Windows Host with a Static IP) with Network Monitoring software (the free version of ManageEngine MIB Browser is used in this lab

1. Prepare for the Lab

This lab uses the existing configurations from **Lab 7-1 Synchronizing NTP in the Campus Network**. The NTP functionality and security is not critical to perform this lab. However, you will need L2 trunking configured.

* 1. Configure general SNMP information

Configure general values to identify the device, it's location, and a point of contact. **Configure this with appropriate values on all four switches**:

DLS1(config)# **snmp-server location Rack 1**

DLS1(config)# **snmp-server contact Student**

DLS1(config)# **snmp-server chassis-id Cisco 3560 SN FTX2222222**

* 1. Configure access-lists for SNMP.

Configure an access list on each switch. This ACL will be used to specify exactly where SNMP get and set messages should be coming from. In this lab, the 172.16.99.0/24 network is the management network. **Configure this ACL on all four switches**:

DLS1(config)# **ip access-list standard NMS-SERVERS**

DLS1(config-std-nacl)# **permit 172.16.99.0 0.0.0.255**

DLS1(config-std-nacl)# **exit**

* 1. Configure SNMP view.

Access to the MIB is open access by default, and any authorized user can read or change the value of any OID in the MIB. Besides the ACL, you should also configure SNMP VIEWs. A view specifically allows or disallows access to certain parts of the MIB, which can provide both security and help control CPU utilization by limiting large SNMP polls.

The MIB is large and there are many different branches and variables, so how the views are configured really depends on how the NMS is implemented versus other SNMP access to the system. Views should be created and configured to contain those variables required by the different entities that might use SNMP to access your devices.

The output below is a basic view configuration that follows Cisco's guidance for OID access located at  <http://www.cisco.com/en/US/docs/ios-xml/ios/snmp/configuration/12-4t/nm-snmp-cfg-snmp-support.html>. The commands specify the "root" of the MIB tree and then further specifies sub-branches that are excluded. **Configure this view on all four switches.**

DLS1(config)#**snmp-server view NMS-LIMIT iso included**

DLS1(config)#**snmp-server view NMS-LIMIT 1.3.6.1.2.1.4.21 excluded**

DLS1(config)#**snmp-server view NMS-LIMIT 1.3.6.1.2.1.4.22 excluded**

DLS1(config)#**snmp-server view NMS-LIMIT 1.3.6.1.2.1.4.35 excluded**

DLS1(config)#**snmp-server view NMS-LIMIT 1.3.6.1.2.1.3 excluded**

DLS1(config)#**snmp-server view NMS-LIMIT 1.3.6.1.6.3.15 excluded**

DLS1(config)#**snmp-server view NMS-LIMIT 1.3.6.1.6.3.16 excluded**

DLS1(config)#**snmp-server view NMS-LIMIT 1.3.6.1.6.3.18 excluded**

The OID values in the above configuration correspond to the following:

**Note: *iso* in the text *below* refers to the root of the MIB tree**

1.3.6.1.2.1.4.21 is (iso-1).(org-3).(dod-6).(internet-1).(mgmt-2).(mib2-1).(ip-4).(ipRouteTable-21).

1.3.6.1.2.1.4.21 is (iso-1).(org-3).(dod-6).(internet-1).(mgmt-2).(mib2-1).(ip-4).(ipNetToMediaTable-22).

1.3.6.1.2.1.4.21 is (iso-1).(org-3).(dod-6).(internet-1).(mgmt-2).(mib2-1).(ip-4).(ipNetToPhysicalTable-35).

1.3.6.1.2.1.3 is (iso-1).(org-3).(dod-6).(internet-1).(mgmt-2).(mib2-1).(atTable-3)

1.3.6.1.6.3.15 is (iso-1).(org-3).(dod-6).(internet-1).(snmpv2-6).(snmpModules-3).(snmpUsmMIB-15)

1.3.6.1.6.3.16 is (iso-1).(org-3).(dod-6).(internet-1).(snmpv2-6).(snmpModules-3).(snmpVacMMIB-16)

1.3.6.1.6.3.18 is (iso-1).(org-3).(dod-6).(internet-1).(snmpv2-6).(snmpModules-3).(snmpCommunityMIB-18)

The NMS-LIMIT view above will protect some of the SNMP credentials from accidental exposure (nsmpUsmMIB, snmpVacmMIB, snmpCommunityMIB) and deny access to the Routing Table (ipRouteTable), the ARP table (atTable), and the deprecated ipNetToMediaTable and ipNetToPhysicalTable OIDs.

* 1. Configure SNMP groups.

SNMP groups are a construct that allows for users and views to be associated with one another.

Included as a part of the group configuration for SNMPv3 is the security model (no auth, auth, or priv), optional associated read, write, and inform views, and optional access-list controlling source addresses in the group.

In the output below, a group called **ccnp-switch3** is created to use SNMPv3, the security features implemented by the group, the read view of NMS-LIMIT and is restricted by the ACL NMS-SERVERS. **Do this on DLS1 and DLS2.**

DLS1(config)# **snmp-server group ccnp-switch3 v3 priv read NMS-LIMIT access NMS-SERVERS**

In the output below, a group called ccnp-switch2 is created to use SNMPv2c, the NMS-LIMIT view and the NMS-SERVERS ACL. **Do this on ALS1 and ALS2**.

ALS1(config)# **snmp-server group ccnp-switch2 v2c read NMS-LIMIT access NMS-SERVERS**

* 1. Configure SNMP users.

Configure users on all four switches.

* DLS1 and DLS2 will use an **SNMPv3 user** who is a part of the group **ccnp-switch3**. They will authenticate using **SHA** with **password cisco123**, and will encrypt using **AES 128** with a **password** of **cisco123.**
* ALS1 and ALS2 will use SNMP v2c user. The user is a part of the group **ccnp-switch2**.

DLS1(config)# **snmp-server user student ccnp-switch3 v3 auth sha cisco123 priv aes 128 cisco123**

ALS1(config)# **snmp-server user student ccnp-switch2 v2c**

**Note**: This command will **not** show in the running configuration after it is entered.

* 1. Configure SNMP trap receiver

Configure the NMS server traps will be sent to. As a part of this command, specific traps or sets of traps to send can be specified. If no traps are specified, this receiver will be forwarded all traps that are enabled. This particular configuration needs to be coordinated with the network management system and network monitoring requirements for the organization.

Configure 172.16.99.100 as a trap receiver on all four switches. DLS1 and DLS2 will use SNMPv3, while ALS1 and ALS2 will use SNMPv2c. For simplicity, do not configure any trap limits.

DLS1(config)# **snmp-server host 172.16.99.100 traps version 3 priv student**

ALS1(config)# **snmp-server host 172.16.99.100 ver 2 ccnp-switch2**

* 1. Configure Interface Index Persistence.

Network monitoring systems record throughput and other interface statistics using SNMP polling. Each interface is referenced by its unique index number, which is dynamically assigned by the IOS upon boot. The index of each interface can be determined with the command **show snmp mib ifmib ifindex**. The dynamic assignment aspect of this can be problematic for documentation. Therefore, it is a good idea to instruct the system to keep a persistent list of interfaces, rather than a dynamic one. The use of this command creates a file stored in NVRAM. **Do this on all four switches**:

DLS1(config)# **snmp-server ifindex persist**

* 1. Enable SNMP Trap Sending

This final command actually enables the forwarding of traps to the configured trap receivers. As a part of this command, traps can be limited (as they can be in the snmp-server host command). Once again this will need to be coordinated with the network management system and network monitoring requirements for the organization.

DLS1(config)# **snmp-server traps enable**

* 1. Verify SNMP configuration.

Use the **show snmp** command to view configuration information for SNMP:

DLS1# **show snmp**

Chassis: FDT11111111

2932 SNMP packets input

0 Bad SNMP version errors

0 Unknown community name

0 Illegal operation for community name supplied

20 Encoding errors

1421 Number of requested variables

0 Number of altered variables

1421 Get-request PDUs

0 Get-next PDUs

0 Set-request PDUs

0 Input queue packet drops (Maximum queue size 1000)

2912 SNMP packets output

0 Too big errors (Maximum packet size 1500)

0 No such name errors

0 Bad values errors

0 General errors

0 Response PDUs

0 Trap PDUs

SNMP global trap: enabled

SNMP logging: enabled

Logging to 172.16.99.100.162, 0/10, 0 sent, 0 dropped.

SNMP agent enabled

Use the **show snmp view** command:

DLS1# **show snmp view**

cac\_view pimMIB - included read-only active

cac\_view msdpMIB - included read-only active

cac\_view ip - included read-only active

cac\_view ospf - included read-only active

cac\_view bgp - included read-only active

cac\_view dot1dBridge - included read-only active

cac\_view ipMRouteStdMIB - included read-only active

cac\_view igmpStdMIB - included read-only active

cac\_view ipForward - included read-only active

cac\_view ipTrafficStats - included read-only active

cac\_view ospfTrap - included read-only active

cac\_view sysUpTime.0 - included read-only active

cac\_view ciscoPingMIB - included read-only active

cac\_view ciscoStpExtensionsMIB - included read-only active

cac\_view ciscoIpSecFlowMonitorMIB - included read-only active

cac\_view ciscoPimMIB - included read-only active

cac\_view ciscoMgmt.187 - included read-only active

cac\_view ciscoEigrpMIB - included read-only active

cac\_view ciscoCefMIB - included read-only active

cac\_view ciscoIpMRouteMIB - included read-only active

cac\_view ciscoIPsecMIB - included read-only active

cac\_view cospf - included read-only active

cac\_view ciscoExperiment.101 - included read-only active

cac\_view ciscoIetfIsisMIB - included read-only active

cac\_view ifIndex - included read-only active

cac\_view ifDescr - included read-only active

cac\_view ifType - included read-only active

cac\_view ifAdminStatus - included read-only active

cac\_view ifOperStatus - included read-only active

cac\_view snmpTraps.3 - included read-only active

cac\_view snmpTraps.4 - included read-only active

cac\_view snmpTrapOID.0 - included read-only active

cac\_view snmpMIB.1.4.3.0 - included read-only active

cac\_view lifEntry.20 - included read-only active

cac\_view cciDescriptionEntry.1 - included read-only active

NMS-LIMIT iso - included nonvolatile active

NMS-LIMIT at - excluded nonvolatile active

NMS-LIMIT snmpUsmMIB - excluded nonvolatile active

NMS-LIMIT snmpVacmMIB - excluded nonvolatile active

NMS-LIMIT snmpCommunityMIB - excluded nonvolatile active

NMS-LIMIT ip.21 - excluded nonvolatile active

NMS-LIMIT ip.22 - excluded nonvolatile active

NMS-LIMIT ip.35 - excluded nonvolatile active

v1default iso - included permanent active

v1default internet - included permanent active

v1default snmpUsmMIB - excluded permanent active

v1default snmpVacmMIB - excluded permanent active

v1default snmpCommunityMIB - excluded permanent active

v1default ciscoMgmt.252 - excluded permanent active

\*tv.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFF0F iso - included volatile active

\*tv.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFF0F iso.2.840.10036 - included volatile active

Verify SNMP groups.

DLS1# **show snmp group**

groupname: ccnp-switch3 security model:v3 priv

contextname: <no context specified> storage-type: nonvolatile

readview : NMS-LIMIT writeview: <no writeview specified>

notifyview: \*tv.FFFFFFFF.FFFFFFFF.FFFFFFFF.F

row status: active access-list: NMS-SERVERS

ALS1# **show snmp group**

groupname: ccnp-switch2 security model:v1

contextname: <no context specified> storage-type: volatile

readview : <no readview specified> writeview: <no writeview specified>

notifyview: \*tv.FFFFFFFF.FFFFFFFF.FFFFFFFF.F

row status: active

groupname: ccnp-switch2 security model:v2c

contextname: <no context specified> storage-type: nonvolatile

readview : NMS-LIMIT writeview: <no writeview specified>

notifyview: <no notifyview specified>

row status: active access-list: NMS-SERVERS

Verify SNMPv3 users:

DLS1#**show snmp user**

User name: student

Engine ID: 800000090300E840406F8B83

storage-type: nonvolatile active

Authentication Protocol: SHA

Privacy Protocol: AES128

Group-name: ccnp-switch3

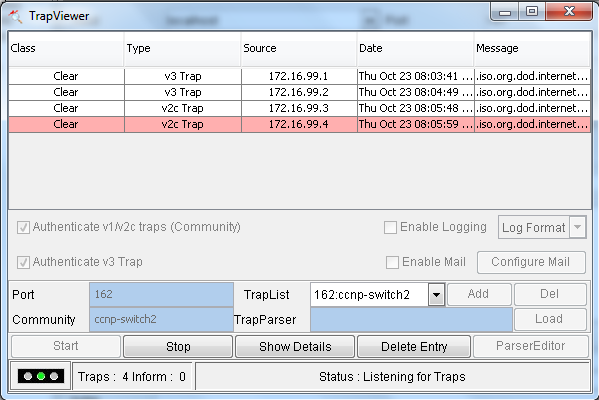
* 1. Verify SNMP TRAP Operation

STIAHNI z: http://www.kis.fri.uniza.sk/~palo/soft/

This lab uses the free tool "MIBBrowser" from ManageEngine for verification. Other tools that will listen for traps at are acceptable substitutes as well.

Run MibBrowser. Select View and then Trap Viewer from the File Menu. The TrapViewer window will open. Click into the Community field and change 'public' to 'ccnp-switch2' and click the add button,. Finally, click Start. TrapViewer is now listening for traps in those two communities.

Go to the command prompt at each switch and enter configuration mode. You should see at least two SNMPv3 traps and at least two SNMPv2c traps collected in the TrapViewer. This validates that traps are being sent to the designated host.

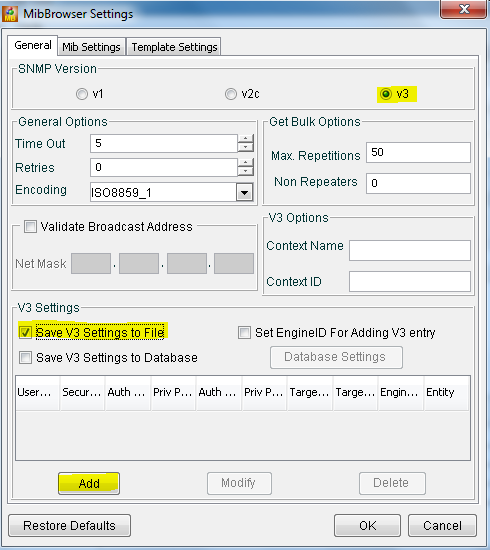


* 1. Verify SNMP GET Operation

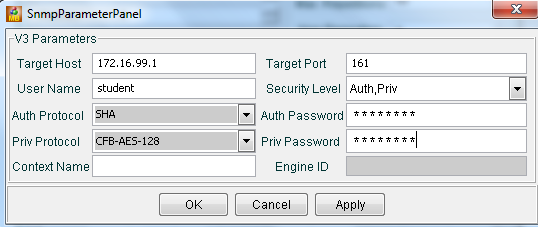
This lab uses the free tool "MIBBrowser" from ManageEngine for verification. Other tools that will do an SNMP walk and support SNMP version 3 are acceptable substitutes as well.

On the MIBBrowser file menu, select Edit and Settings.

In the MIBBrowser Settings window, select the SNMP version 3 radio button, select “Save V3 Settings to file and then click ADD.

. 

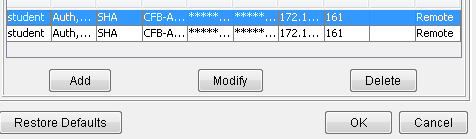
On the SnmpParameterPanel, fill in the values for the SNMPv3 user:



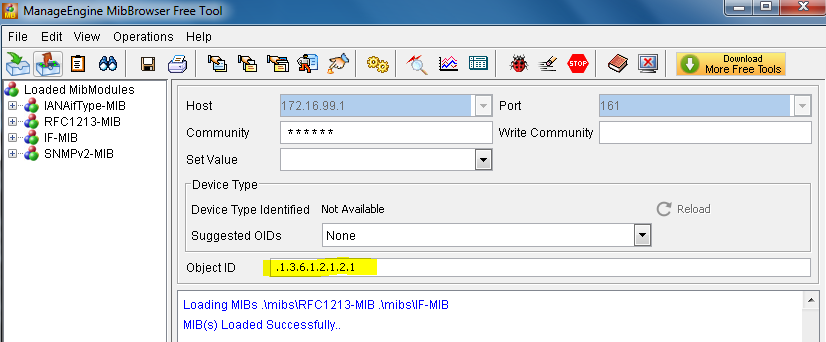
* Target Host: **IP Address of DLS1 (172.16.99.1)**
* User Name: **student**
* Security Level: **Auth,Priv**
* Auth Protocol: **SHA**
* Auth Password: **cisco123**
* Priv Protocol: **CFB-AES-128**
* Priv Password: **cisco123**

Once the values are entered, then, click ok. Then, click Add again and add DLS2 (172.16.99.2) with the same values.

Once values are added for both devices, select DLS1’s entry and click OK.

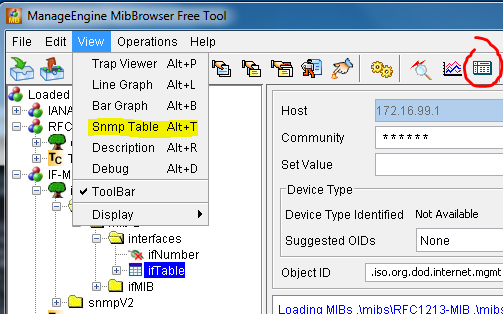


This takes you back to the main window. In the **Object ID** field in the middle of the screen, type .1.3.6.1.2.1.2.1.

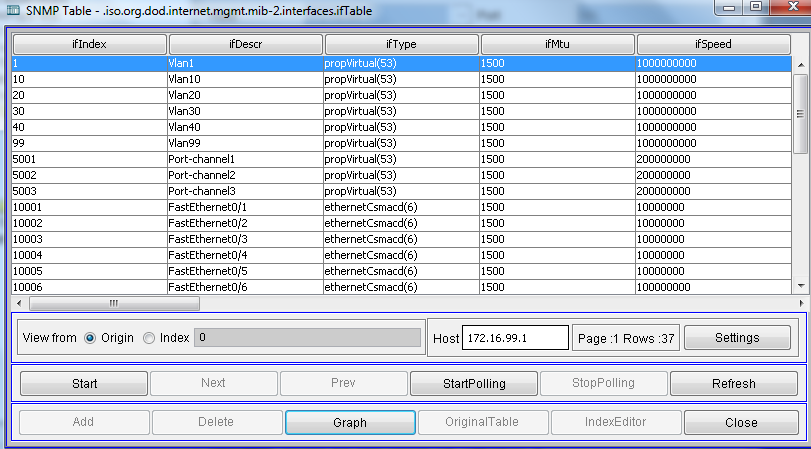


Next, from the file menu select **Operations** and **Get**. You should see information being retrieved from DLS1. This indicates that the NMS is able to gather information from DLS1 using SNMPv3.

In the left pane, select the **ifTable** entry and then on the file menu select **View** and **Snmp Table** (Alt+T), and a table will be built showing interface data from DLS1 (or select the table icon).

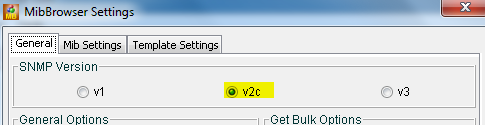


In the SNMP Table window, press **Start** and you should see interface information populated from DLS1.



Repeat the above steps for DLS2 to verify SNMPv3 is working.

Next to verify SNMP v2 is working, go back to the Settings screen and change the radio button selection from **v3** to **v2.**



Once you click OK you will be returned to the main screen. Here the host settings fields will be available for editing . In the Host field, type **172.16.99.3** (ALS1), and in the Community field, type **ccnp-switch2**. Then, in the Object ID field, type **.1.3.6.1.2.1.2.1** and then select **Edit** and **Get**. Go through the same process used above to view the interface table information. This verifies that the NMS is able to gather information from ALS1 using SNMPv2c. Repeat this process for ALS2 (172.16.99.4) to verify SNMPvc is configured correctly on this device.

* 1. End of Lab

Using the same procedures as in Lab 1, reset all four of your switches

* **delete vlan.dat**
* **erase startup-config**
* **reload**

1. Device Configuration Scripts - INSTRUCTOR VERSION

**Note: DLS1 and DLS2 have the same basic configurations.**

!Step 1:

conf t

snmp-server location Rack 1

snmp-server contact Student

snmp-server chassis-id Cisco 3560 SN FTX2222222

!Step 2:

ip access-list standard NMS-SERVERS

permit 172.16.99.0 0.0.0.255

exit

!Step 3:

snmp-server view NMS-LIMIT iso included

snmp-server view NMS-LIMIT 1.3.6.1.2.1.4.21 excluded

snmp-server view NMS-LIMIT 1.3.6.1.2.1.4.22 excluded

snmp-server view NMS-LIMIT 1.3.6.1.2.1.4.35 excluded

snmp-server view NMS-LIMIT 1.3.6.1.2.1.3 excluded

snmp-server view NMS-LIMIT 1.3.6.1.6.3.15 excluded

snmp-server view NMS-LIMIT 1.3.6.1.6.3.16 excluded

snmp-server view NMS-LIMIT 1.3.6.1.6.3.18 excluded

!Step 4:

snmp-server group ccnp-switch3 v3 priv read NMS-LIMIT access NMS-SERVERS

!Step 5:

snmp-server user student ccnp-switch3 v3 auth sha cisco123 priv aes 128 cisco123

!Step 6:

snmp-server host 172.16.99.100 version 3 priv student

!Step 7:

snmp-server ifindex persist

!Step 8:

snmp-server enable traps

ALS1 and ALS2 have the same basic configurations:

!Step 1:

conf t

snmp-server location Rack 1

snmp-server contact Student

snmp-server chassis-id Cisco 3560 SN FTX2222222

!Step 2:

ip access-list standard NMS-SERVERS

permit 172.16.99.0 0.0.0.255

exit

!Step 3:

snmp-server view NMS-LIMIT iso included

snmp-server view NMS-LIMIT 1.3.6.1.2.1.4.21 excluded

snmp-server view NMS-LIMIT 1.3.6.1.2.1.4.22 excluded

snmp-server view NMS-LIMIT 1.3.6.1.2.1.4.35 excluded

snmp-server view NMS-LIMIT 1.3.6.1.2.1.3 excluded

snmp-server view NMS-LIMIT 1.3.6.1.6.3.15 excluded

snmp-server view NMS-LIMIT 1.3.6.1.6.3.16 excluded

snmp-server view NMS-LIMIT 1.3.6.1.6.3.18 excluded

!Step 4:

snmp-server group ccnp-switch2 v2c read NMS-LIMIT access NMS-SERVERS

!Step 5:

snmp-server user student ccnp-switch2 v2c

!Step 6:

snmp-server host 172.16.99.100 version 2 ccnp-switch2

!Step 7:

snmp-server ifindex persist

!Step 8:

snmp-server enable traps