Lab 5: SNMP in Cisco Routers

NET311 - Computer Network Management

Instructor: Dr. Mostafa Dahshan

Objectives

1. Configuring SNMP agent on Cisco Routers.
2. Understanding SNMP v2 traps.

References

1. Cisco Networking Academy, Lab 8.2.2.4 Configuring SNMP.
2. GNS3 Documentation.

Instructions

1. Read the lab instructions.
2. Provide question answers and screenshots in the supplied answer sheet.
3. After finishing the lab, upload your saved answer sheet to LMS.
Part 1: Lab Setup

The following programs need to be installed on your PC before starting this lab.

1. Winpcap 4.1.3
2. Wireshark 2.0.2
3. GNS3 1.4.4
4. SnmpB

Refer to the supplemental video for setting up the environment of this lab.

1. Verify that the programs are installed.

Lab sheet 1.1: provide a screenshot of the Programs and Features screen.
Install the Microsoft KM-TEST Loopback Adapter using the Hardware Wizard

2. Right click on the Windows icon and click **Run**.

3. Type the command **hdwwiz**

4. Follow the instructions
Add Hardware

From the list below, select the type of hardware you are installing.

If you do not see the hardware category you want, click Show All Devices.

Common hardware types:
- IEEE 1394 host controllers
- Imaging devices
- Infrared devices
- Media Center Extender
- Memory technology devices
- Modems
- Multi-post serial adapters
- Network adapters
- PCMCIA adapters

Add Hardware

Select Network Adapter
Which network adapter do you want to install?

Click the Network Adapter that matches your hardware, then click OK. If you have an installation disk for this feature, click Have Disk.

Manufacturer: Intel
Intel Corporation
Mellanox Technologies Ltd.
Microsoft
QLogic Corp

Network Adapter:
- Microsoft ISATAP Adapter
- Microsoft Kernel Debug Network Adapter
- Microsoft KM-TEST Loopback Adapter
- Microsoft Network Adapter Multiplexer Default Miniport
- Microsoft Teredo Tunneling Adapter

This driver is digitally signed.
Tell me why driver signing is important

Have Disk...
5. Run **PowerShell** as **Administrator**.

6. Type the following commands to configure the Microsoft KM-TEST Loopback Adapter:

```powershell
$adapter=Get-NetAdapter -InterfaceDescription "Microsoft KM-TEST Loopback Adapter"
Rename-NetAdapter -InterfaceDescription "Microsoft KM-TEST Loopback Adapter" -NewName "Loop1"
New-NetIPAddress -InterfaceIndex $adapter.ifIndex -AddressFamily "IPv4" -IPAddress "172.16.0.2" -PrefixLength 24
Route add 172.16.0.0 mask 255.240.0.0 172.16.0.1 metric 1
```
Lab sheet 1.2: provide a screenshot of the PowerShell screen.

To allow SnmpB to receive traps, create a rule in Windows Firewall with Advanced Features to allow the program SnmpB through the firewall.

7. Type the following command to add a rule to allow SNMP PDUs through the firewall:

```
New-NetFirewallRule -DisplayName "SNMP" -Direction Inbound -Action Allow -Protocol UDP -LocalPort 161-162
```

Lab sheet 1.3: provide a screenshot of the PowerShell screen.
Part 2: Configure SNMP Manager

1. Run the SnmpB program.

2. Go to Manage Agent Profiles and add a profile called R1, using the following parameters:

   - **Name:** R1
   - **Agent address:** 172.16.0.1
   - **Supported SNMP Version:** SNMPv1, SNMPv2
   - **Read community:** public

Lab sheet 2.1: provide a screenshot of the SnmpB Agent Profiles screen.
3. Go to the Traps tab and leave the SnmpB window running to watch for traps.
Part 3: Configure SNMP Agent on Cisco Router

1. Run **GNS3** as an administrator.

2. Open the GNS3 project **NET311-Lab-05.gns3**

3. Right-click on the link from **Loop1 to R1** and click **Start capture**.
4. Add the filter `snmp` then click `Enter`.

5. Run the network by clicking on the green icon.

6. After the network is started, **right-click** on the R1 router to access its console.
7. Type the following commands to configure the SNMP agent on R1 router. Use your name as a contact:

```
config t
snmp-server community public ro SNMP_ACL
snmp-server location Lab4
snmp-server contact Mostafa Dahshan
snmp-server host 172.16.0.2 version 2c public
snmp-server enable traps
ip access-list standard SNMP_ACL
  permit 172.16.0.2
exit
```

8. Type the following commands to configure the network interface e0/0.

```
int e0/0
  ip address 172.16.0.1 255.255.255.0
  no shutdown
```

9. Go to SnmpB and check for traps sent from R1.

![SnmpB Traps Screen](image)

Lab sheet 3.1: provide a screenshot of the SnmpB Traps screen showing initial traps.

10. Go to SnmpB Tree window and perform a Walk on system using SnmpB profile.

![SnmpB Tree Window](image)
Lab sheet 3.2: provide a screenshot of the SnmpB Tree windows showing the result of Walk.

11. Go to Wireshark and check the captured SNMP packets.

![Wireshark Screenshot]

Lab sheet 3.3: provide a screenshot of the Wireshark window showing captured SNMP packets.

To experiment with traps, change the status of the network interface e1/0 and watch for the trap in SnmpB and Wireshark.

12. Go to R1 console in GNS3 and run the following commands:

```
int e1/0
no shutdown
```

13. Go to SnmpB Traps window and look for the LinkUp trap received from R1.

![SnmpB Traps Screenshot]
Lab sheet 3.4: provide a screenshot of the SnmpB Traps screen showing the Bindings in the LinkUp trap.

14. Go to R1 console in GNS3 and run the following commands:

```
int e1/0
shutdown
```

15. Go to SnmpB Traps window and look for the **LinkDown** trap received from R1.

Lab sheet 3.5: provide a screenshot of the SnmpB Traps screen showing the Bindings in the LinkDown trap.

16. Go to Wireshark window and double click on the last captured SNMP trap.