Lab 7.4.5 Configure SNMP Messages on a Cisco Router

Objective

In this lab, the students will complete the following tasks:

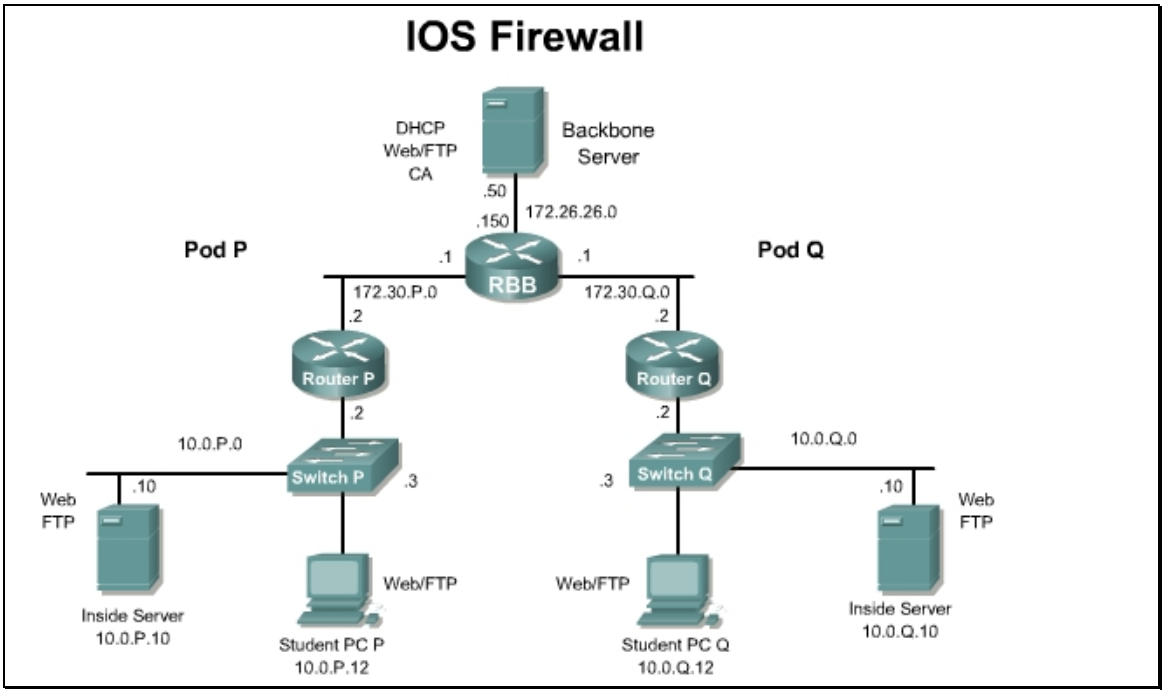
- Enable SNMP community string
- Establishing the Contact and location of the SNMP Agent
- Testing the configuration
- Limit SNMP to inside server
- Disable SNMP traps, SNMP service and associated access list

Scenario

A small company has recently expanded. The IT department is having problems maintaining logs, configuration changes, and so on. The security policy has been updated allowing SNMP management of key devices. SNMP access must be limited to key management stations.

Topology

This figure illustrates the lab network environment.



Preparation

Begin with the standard lab topology and verify the starting configuration on the pod router. Test the connectivity between the pod routers. Access the perimeter router console port using the terminal emulator on the Student PC. If desired, save the router configuration to a text file for later analysis. Refer back to the *Student Lab Orientation* if more help is needed.

Tools and resources or equipment

In order to complete the lab, the following is required:

- Standard IOS Firewall lab topology
- Console cable
- HyperTerminal
- Kiwi Syslog Server

Additional materials

Further information about the objectives covered in this lab can be found at the following websites:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a008030c762.html

http://www.kiwisyslog.com

Command list

In this lab exercise, the following commands will be used. Refer to this list if assistance or help is needed during the lab exercise.

Command	Description
`no snmp-server`	Disable SNMP.
`show snmp`	Monitors SNMP status.
`snmp-server community`	Defines the community access string.
`snmp-server contact`	Sets the system contact string.
`snmp-server enable traps snmp`	Enables the sending of traps and specifies the type of notification to be sent.
`snmp-server host`	Configures the recipient of an SNMP trap operation.
`snmp-server location`	Sets the system location string.

Step 1 Open Kiwi Syslog

Kiwi Syslog server can be used to receive syslog and SNMP messages from network equipment, including routers, switches, and workstations. Traps are sent when errors or specific events occur on the network.

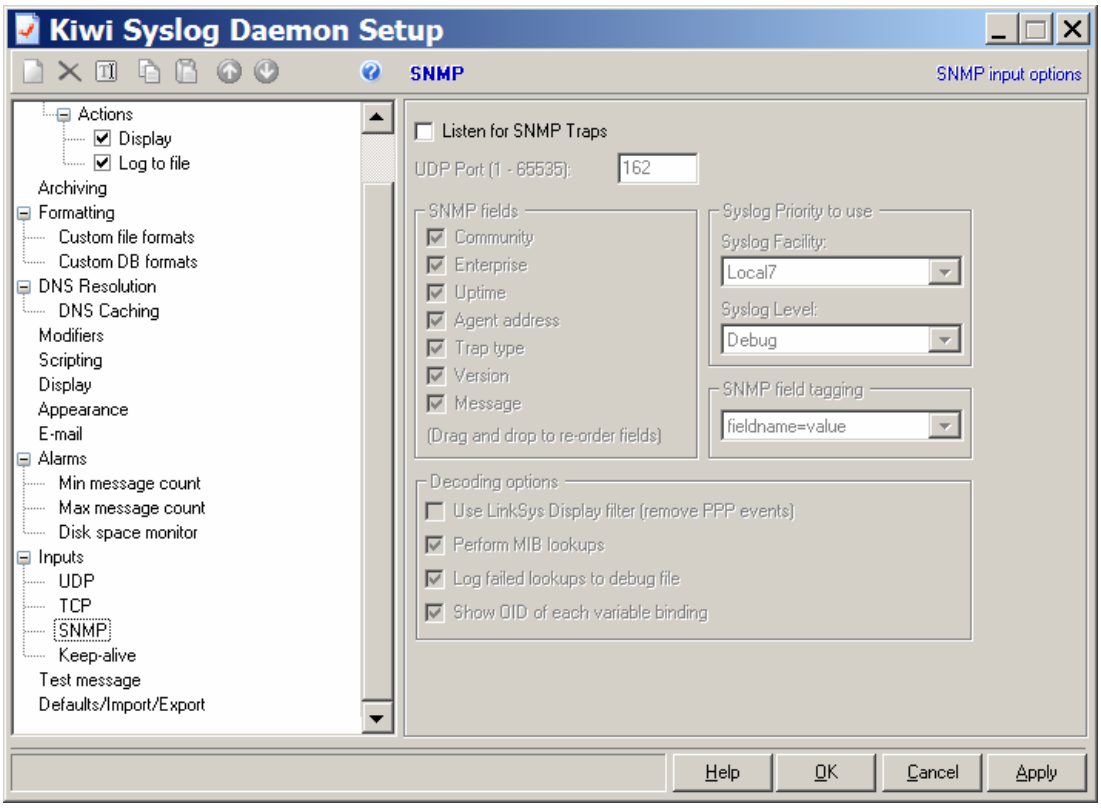
a. Go to the following website to download the free copy of Kiwi if needed,

   http://www.kiwisyslog.com

b. After opening the Kiwi application navigate to File>Setup or click on the Setup Icon  in the menu bar.

c. Go to **Inputs>SNMP**.

d. Check the **Listen for SNMP Traps**.



e. Notice that the Syslog server can be configured to send alerts automatically via email. Also, note the port number that SNMP uses for listening for traps, this will be used later.

f. Click the **OK** button.

Step 2 Enable SNMP Community String

a. Use an SNMP community string to define the relationship between the SNMP manager and the agent. The community string acts like a password to permit access to the agent on the router. The default values for these strings are “public” for read-only and “private” for read-write. These should always be changed to some other string values. Configure the community string by using the **`snmp-server community`** command. Let writemib be the read-write permission and readmib be the read-only permission.

```
RouterP(config)#snmp-server community writemib rw
RouterP(config)#snmp-server community readmib ro
```

Step 3 Establishing the Contact and Location of the SNMP Agent

a. Set the system contact and location of the SNMP agent. To do so, use the following commands in global configuration mode.

```
RouterP(config)#snmp-server contact Dial System Operator at beeper # 27345
RouterP(config)#snmp-server location Floor 4 Room 20
```

1. What command displays this information on a router?

_____

Step 4 Configure the Router to Send Traps to a Host

a. To enable all the SNMP trap types at once, use the **`snmp-server enable traps snmp`** command.

```
RouterP(config)#snmp-server enable traps snmp
```

b. Specify to the router what host the trap notifications will be sent to by using the **`snmp-server host`** ***`host community_string`*** **`udp-port`** ***`port_number`*** command.

```
RouterP(config)#snmp-server host 10.0.P.12 writemib udp-port 162
```

c. Look at the applications main window to see the UDP-port that it is listening on.

1. If the default for an SNMP response is on port 162, what port is the request sent on?

   _____

2. Why is it important to know the SNMP port?

   _____

Step 5 Testing the Configuration

a. Exit out of the router and log back in using the wrong password. After the failed attempts, log back into the router and issue the following commands:

```
RouterP(config)#interface fastEthernet 0/1
RouterP(config-if)#shutdown
RouterP(config-if)#no shutdown
```

b. Now check the Kiwi Syslog software

There will now be entries of traps sent from the router to the manager.

1. Where would information be found on the contact, location, and SNMP logging information for SNMP on the router besides startup-config and running-config?

   _____

   _____

Step 6 Limit SNMP to Inside Server

a. Limit the SNMP access to the inside server located at 10.0.P.12 by creating a restrictive access list along with a read-only community string.

```
RouterP(config)#no snmp-server community writemib rw
RouterP(config)#no snmp-server community readmib ro
RouterP(config)#access-list 70 permit 10.0.P.12
RouterP(config)#access-list 70 deny any
RouterP(config)#snmp-server community readmib ro 70
```

1. What command would be used to secure the SNMP **rw** access?

   _____

b. Issue the following commands to generate SNMP traps:

```
RouterP(config)#int fa 0/1
RouterP(config-if)#shutdown
RouterP(config-if)#no shutdown
```

c. View the SNMP trap application.

1. Were the new traps displayed?

   _____

d. If desired, compare the running configuration with the ending configuration provided for this lab.

Step 7 Disable SNMP Traps

a. Disable the SNMP traps on the router by using the following commands:

```
RouterP(config)#no snmp-server enable traps
RouterP(config)#no snmp-server system-shutdown
RouterP(config)#no snmp-server trap-auth
```

By disabling SNMP trap notifications, network performance will increase by freeing up bandwidth and eliminate unnecessary SNMP processing tasks.

Step 8 Disable SNMP and Associated Access List

a. Disable the SNMP and the associated access list by using the following commands:

```
RouterP(config)#no snmp-server
RouterP(config)#no access-list 70
```

1. When should the SNMP be disabled?

   _____

   _____

