

Network Management

1 Topology

Setup the Switch, Router1, Router2, and Vista host as shown in Figure 1.

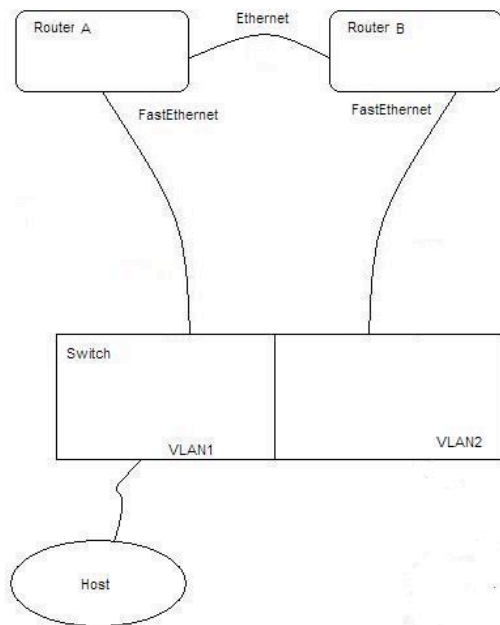


Figure 1

1.1 Addressing

Setup the addresses for the Vista Host and Router1 on your specified 10.10X.0/24 subnet, using VLAN1. Use addresses for the Linux host and Router2 interface from the VLAN2 subnet 10.10X.2/24. Likewise, use the defined subnet addresses 10.10X.3/24 for the Ethernet interfaces between routers. Make sure the Management interface of the switch is configured on the 10.10X.0/24 subnet.

1.2 Routing

Configure the RIP routing protocol on the routers. Verify that the Host is running RIP, or that a default gateway is configured. Verify that PING's between the Vista Host and Router2 succeed (The Vista host needs IP connectivity between every device it manages, so you may want to verify you can reach every device with PING).

2 SNMP

2.1 Vista Host

Verify that the SNMP services are enabled on your Vista Host using the following procedure:

1. Click Start -> Control Panel
2. Open "Programs and Features" in Classic view
3. Open "Turn Windows Features on or off" in the Tasks sidebar
4. Verify that the checkbox next to SNMP feature is selected
5. Expand SNMP feature and verify that the checkbox next to WMI SNMP Provider
6. Click Start -> Run
7. Open Services.msc
8. Verify that SNMP Service is started and SNMP Trip is stopped

2.2 Switch

SNMP Example

This example shows how to enable all versions of SNMP. The configuration permits any SNMP manager to access all objects with read-only permissions using the community string public. This configuration does not cause the switch to send any traps.

```
Switch(config)# snmp-server community public
```

This example shows how to permit any SNMP manager to access all objects with read-only permission using the community string public. The switch also sends VTP traps to the hosts 192.180.1.111 and 192.180.1.33 using SNMPv1 and to the host 192.180.1.27 using SNMPv2C. The community string public is sent with the traps.

```
Switch(config)# snmp-server community public
Switch(config)# snmp-server enable traps vtp
Switch(config)# snmp-server host 192.180.1.27 version 2c public
Switch(config)# snmp-server host 192.180.1.111 version 1 public
Switch(config)# snmp-server host 192.180.1.33 public
```

This example shows how to allow read-only access for all objects to members of access list 4 that use the comaccess community string. No other SNMP managers have access to any objects. SNMP Authentication Failure traps are sent by SNMPv2C to the host cisco.com using the community string public.

```
Switch(config)# snmp-server community comaccess ro 4
Switch(config)# snmp-server enable traps snmp authentication
Switch(config)# snmp-server host cisco.com version 2c public
```

2.3 Routers

SNMP communities and traps are configured on the Routers in the same manner as the switch.

Also, verify that HTTP server is enabled on both routers by running the command `ip http server` when in configuration mode.

3 Network Management System

3.1 Cisco Network Assistant

Network Assistant simplifies the management of communities or clusters by offering a GUI, alternative modes for configuring network devices, two levels of access, and comprehensive online help

Open Cisco Network Assistant, located on the Desktop of the Vista Host

1. Select “Create Community” and click Connect.
2. In the Create Community dialog box, use name is representative of your environment (e.g. Station1)
3. Using the discovery method of your choice, add the switch and both routers to your community. When prompted for credentials, remember to leave login blank and use “123” as the password.
4. Click OK

Access the switch and both routers through the Topology View. Experiment with the tools available in the context menu and explain how they can be used. Experiment with the tools available in the Feature Bar (left-hand pane) inside of the Configure, Monitor, Troubleshoot and Maintenance tabs.

3.2 SNMP

SNMP is used in network management systems to monitor network-attached devices for conditions that warrant administrative attention. SNMP exposes management data in the form of variables on the managed systems, which describe the system configuration. These variables can then be queried (and sometimes set) by managing applications.

In order to tap into the Vista Host’s SNMP functionality, we will use Axence Free Net tools—used to view SNMP tree variables—and Kiwi Syslog Daemon—used to collect and receive SNMP traps. Keep in mind; these programs are by no means the only programs that perform these tasks and you are encouraged to find different programs should the need present itself.

3.2.1 Axence Free Net Tools

Open Axence Free Net Tools located on the Desktop of the Vista Host

1. Click SNMP
2. Type the address of the device for which you would like to view SNMP tree data

Expand the tree and comment on some of the variables and their significance. For example, expand Internet.mgmt.mib-2.system.interfaces.ifTable to see bandwidth usage (the most common use of SNMP).

3.2.2 Kiwi Syslog Daemon

Open Kiwi Syslog Daemon located on the Desktop of the Vista Host

1. Click File->Setup
2. Expand Inputs and select SNMP
3. Check "Listen for SNMP Traps"
4. Verify that the UDP port is set to 162
5. Bind to the address of the Vista host (10.10X.0.3)

If the Switch/Router is configured correctly, the traps will be displayed as they occur. Trigger the traps set on the switch and/or router and verify that they are displayed in Kiwi.

Note: SNMP traps can be configured from Cisco Network Assistant by selecting a device in the Topology View and opening Configure->Device Properties->SNMP from the Feature bar.

4 Advanced

4.1 PIX Firewall

Connect the PIX Firewall to the Switch via the 10/100 Ethernet 1 Ethernet port (clearly labeled on the back panel of the Firewall).

Connect to the Firewall over the Console connection and begin to configure the firewall in much the same way as the router and switch were configured.

Make sure your Firewall begins with a clear/fresh configuration by issuing the command write erase. Add the Firewall to your community in Cisco Network Assistant. Connect to the device manager using the context menu of the firewall. When prompted, accept security warnings and enter credentials. If there are any errors, attempt to use a different browser to navigate to the same URL.

Explore the device manager and comment on some of the features. Use the device manager to setup a SNMP community and traps on the Firewall and verify that they are working properly using the tools described earlier in this lab.