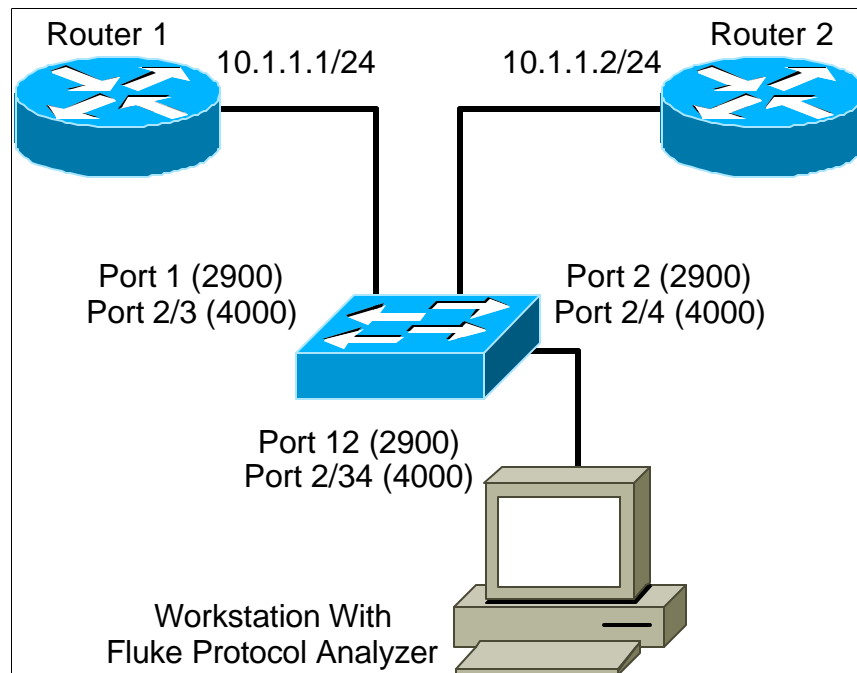


Lab 5.4.4: Port Mirroring



Objective:

Configure a port on your switch to monitor another port on the switch. This will be used to capture data from one port to a protocol analyzer.

Scenario:

After converting your network from hubs to switches you may find it difficult to use your protocol analyzer to observe traffic between devices. Since switches filter traffic based on the MAC address, you can no longer see traffic destined for a device on a particular port on any of the other ports. You need to setup a port on your Ethernet switch as a "Monitor" or "Span" port. Once you have designated a port on your switch as a monitor port, you can copy input and output traffic from another port to your monitor port.

This lab contains commands for both the 2900 series and 4000 series Catalyst switches. You are encouraged to complete this lab twice, once on each platform.

Lab Tasks:

1. First, we need to configure two routers. These two routers will be used to create traffic from one to another. It is this traffic that we will capture with our Fluke Protocol analyzer.

The routers will not be configured with any routing protocol, just IP addresses on their Ethernet interfaces.

Router1:

```
Router(config)#host Router1
```

```
Router1(config)#int fa0/0
Router1(config-if)#ip address 10.1.1.1 255.255.255.0
```

Router2:

```
Router(config)#host Router2
Router2(config)#int fa0/0
Router2(config-if)#ip address 10.1.1.2 255.255.255.0
Router2(config-if)#line vty 0 4
Router2(config-line)#login
Router2(config-line)#password cisco
```

If using a Catalyst 4000 switch:

Plug Router1 into port 2/3
Plug Router 2 into port 2/4

If using a Catalyst 2900 switch:

Plug Router1 into port 1
Plug Router 2 into port 2

2. Test your router configuration by pinging Router2 from Router1. If you are not successful, verify your router configuration.
3. Take a workstation that has the Fluke Protocol Analyzer software installed. Connect it to the following port:

If using a Catalyst 4000 switch:

Plug the protocol analyzer PC into port 2/34

If using a Catalyst 2900 switch:

Plug the protocol analyzer PC into port 12

It is not necessary to configure an IP address on your protocol analyzer PC. This is because this PC will just be used to capture data with the analyzer. It will not be sending/receiving any data of its own.

4. Configure the Ethernet switch to mirror traffic to the monitor/span port. We are only interested in capturing data from Router1's Ethernet port.

The following commands configure a port as a monitor/span port. We will specify the port that we want to "copy" frames from and send them to the monitor/span port. Both frames transmitted and received will be copied to the monitor/span port.

If using a Catalyst 4000 switch:

```
DLSwitch1> (enable) set span 2/3 2/34
```

The first port specified is the port that the frames will be copied from. The second port specified would be the port the frames are copied to. You have the option of copying

many ports to the monitor/span port.

If using a Catalyst 2900 switch:

```
ALSwitch(config)#int fa0/12
ALSwitch(config-if)#port monitor fa0/1
```

On the 2900, we enter interface configuration mode on the port that we will use as our monitor port. Then we use the **show port monitor** command to specify which ports frames are copied to this port.

5. Verify your monitor/span port configuration:

If using a Catalyst 4000 Switch:

Use the **show span** command to display which port is the destination (the port connected to the protocol analyzer) and which port is the source (the port we are monitoring).

```
DLSwitch1> (enable) show span

Destination      : Port 2/34
Admin Source     : Port 2/3
Oper Source      : Port 2/3
Direction        : transmit/receive
Incoming Packets : disabled
Learning         : enabled
```

If using a Catalyst 2900 switch:

Use the **show port monitor** command to display which port is the monitor port (the port connected to the protocol analyzer) and which port is being monitored.

```
ALSwitch#show port monitor
Monitor Port      Port Being Monitored
-----
FastEthernet0/12  FastEthernet0/1
```

6. Start capturing data with your Fluke Protocol Analyzer software.

Telnet from Router1 to Router2. Log in and issue several show commands to create traffic.

Check your protocol analyzer, you should see traffic that was captured.

Do you have the ability to capture more than one port to a monitor/span port?

Would it be smart to also capture the Router2 port to your monitor/span port? Why?

Can you think of any other precautions to take when using the monitor/span port?
