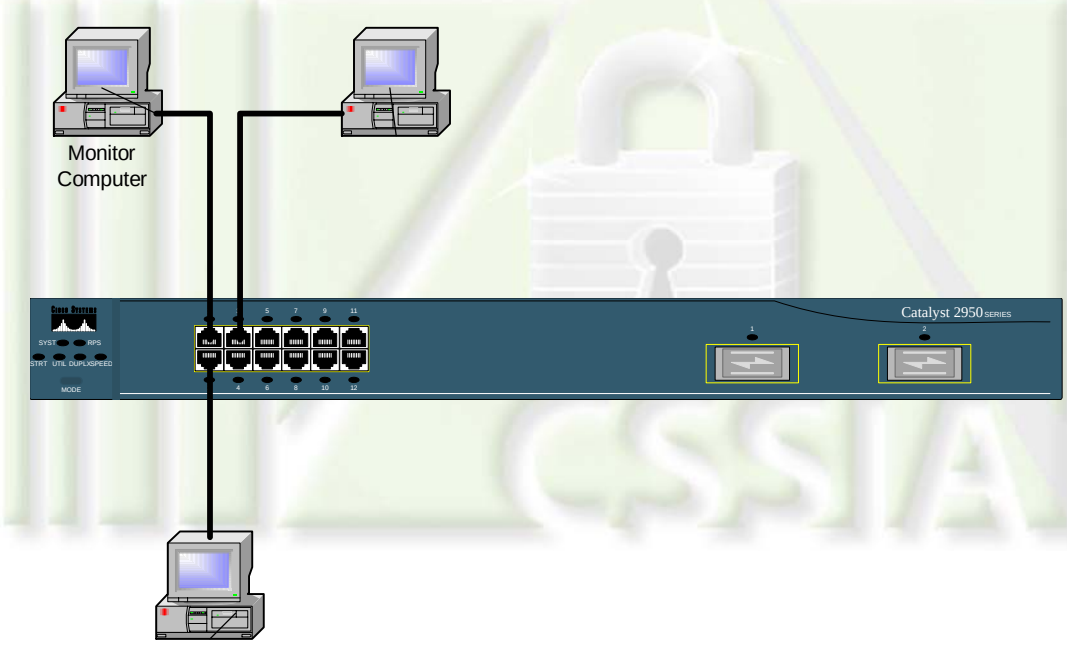
4.5.1

Monitoring a Cisco Switch with a SPAN [Switch Port Analyzer]

(Ethereal and LANHound)



Laboratory Overview

Objective

In this lab students will configure a dedicated switch port to monitor traffic on a common network segment in conjunction with a network monitor program. Use of both Ethereal and LanHound network analyzers will be examined.

Information for Laboratory

A. Students will use Ethereal to monitor network traffic on a single switch port.
B. Students will configure a switch to monitor a single, different, switch port in conjunction with network monitoring software.
C. Student will explore the monitoring of multiple switch ports, as well as the ability to specify directionality (receive/ transmit) of monitored ports.
D. Students will use LanHound as an alternative to Ethereal network monitoring software.

Student Preparation

The student will have completed requisite reading, and should be familiar with Ethereal network monitor. The student will require paper for notes and should be prepared to discuss the exercises upon completion.

Estimated Completion Time

60 Minutes

Switch Port Analyzers

Network monitors are excellent educational tools, even when monitoring a dedicated workstation. Students may examine the details of operation for many protocols and network services.

To be of practical use for network administrators, monitoring must be performed on a wider basis in order to assess network performance and possible security breaches.

The next level of monitoring would be the local network segment. Years ago, local segments were typically interconnected via hubs, which are low level devices that function to completely interconnect all connected devices. If one were to connect a computer with a network monitor into a hub, the network monitor would be able to capture all traffic on the local network segment. This would also be true in the case of multiple hubs on the same segment.

Contemporary LAN networks are much more likely to use switches rather than hubs. Switches are intelligent devices that are not designed to flood traffic out all ports like hubs. Although switches may initially behave like hubs by flooding all ports, they quickly acquire information about the hosts connected to them via physical addresses (MAC). They always have the ability to buffer transmissions (unless the buffers overflow!).

The result is that directed transmissions are forwarded only out the proper physical port. If a network administrator places a computer with a network monitor on a single switch port, the result will be the monitoring only of traffic sent and received by that single workstation.

If only one other workstation is to be monitored, then an easy solution is to attach a hub to the relevant switch port, and then attach the target workstation and monitor workstation to the same hub. This arrangement should be viewed as too crude for practical consideration.

All this underscores the idea of a Switch Port ANalyzer (SPAN), or sometimes, SPAN port, or yet again, port monitor. A SPAN

is a switch port that monitors or mirrors other ports. Thus if a workstation armed with a network monitor is attached to the SPAN, it is able to capture all traffic according to the configuration of the SPAN.

Configuring a SPAN on a Cisco 2950 Switch

It is assumed that the 2950 switch has been returned to a state of factory default without a startup-configuration. It is also assumed that students know how to connect to a switch via the console port and communicate via Hyperterminal. For information on performing these steps see the lab entitled – Network Configuration (Network Switch).

Step 1:

Connect workstations according to the network diagram shown on the cover of this lab. Computers connected to ports 1,2,3 will be identified as hosts 1,2,3 respectively.

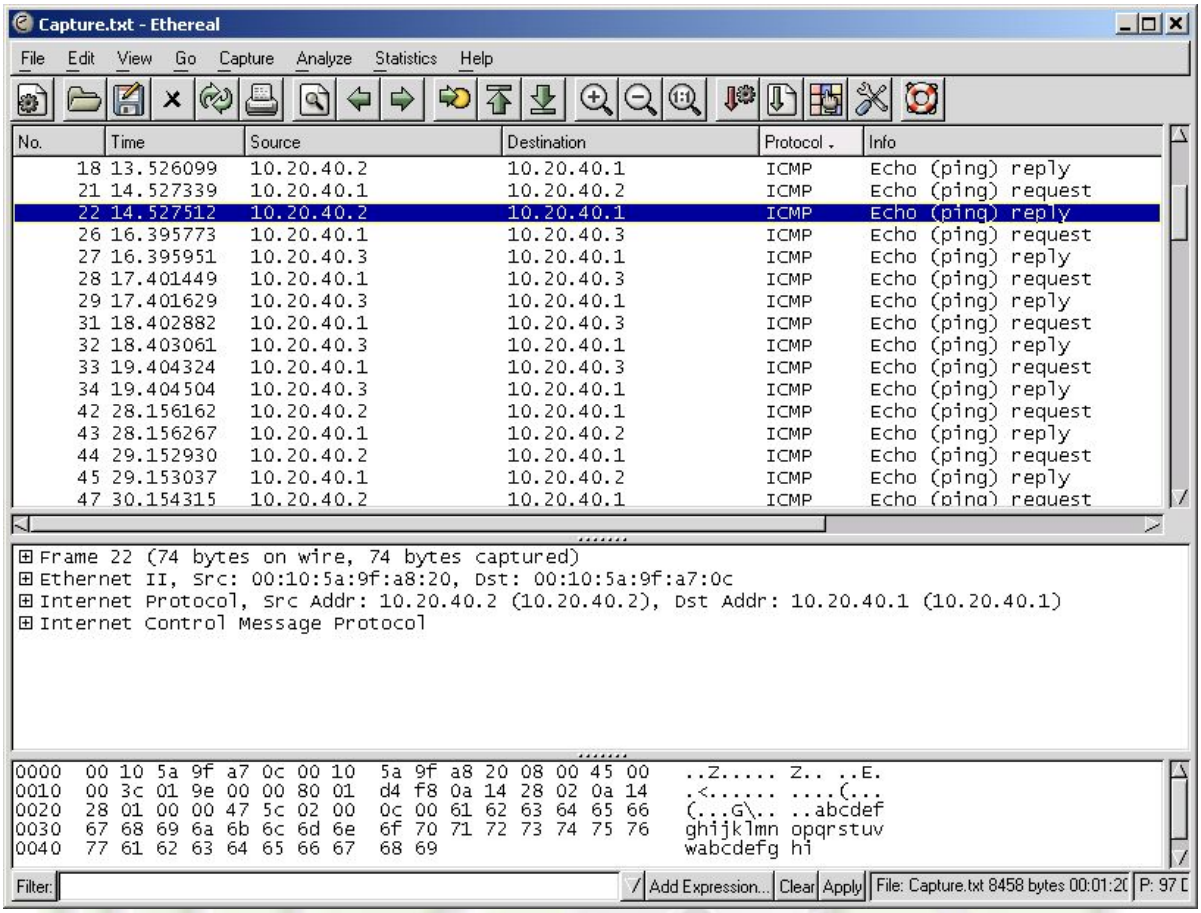
Use the following static IP address scheme:

Host	IP Address	SNM
1	10.20.40.1	255.255.255.0
2	10.20.40.2	255.255.255.0
3	10.20.40.3	255.255.255.0

Step 2:

Initiate an Ethereal capture session on host 1, making it the computer monitor. At each workstation ping the other two hosts on the local network segment, and then stop the Ethereal capture.

The capture should appear similar to the following graphic:



Note that captured transmissions only include those where host 1, IP 10.20.40.1, is either the source or destination. No transmissions between hosts 2 and 3 are present.

Step 2:

Configure a SPAN port on port 1 to monitor all traffic from port 2. To do so one needs to establish a monitor session on the 2950 switch from global configuration mode as follows:

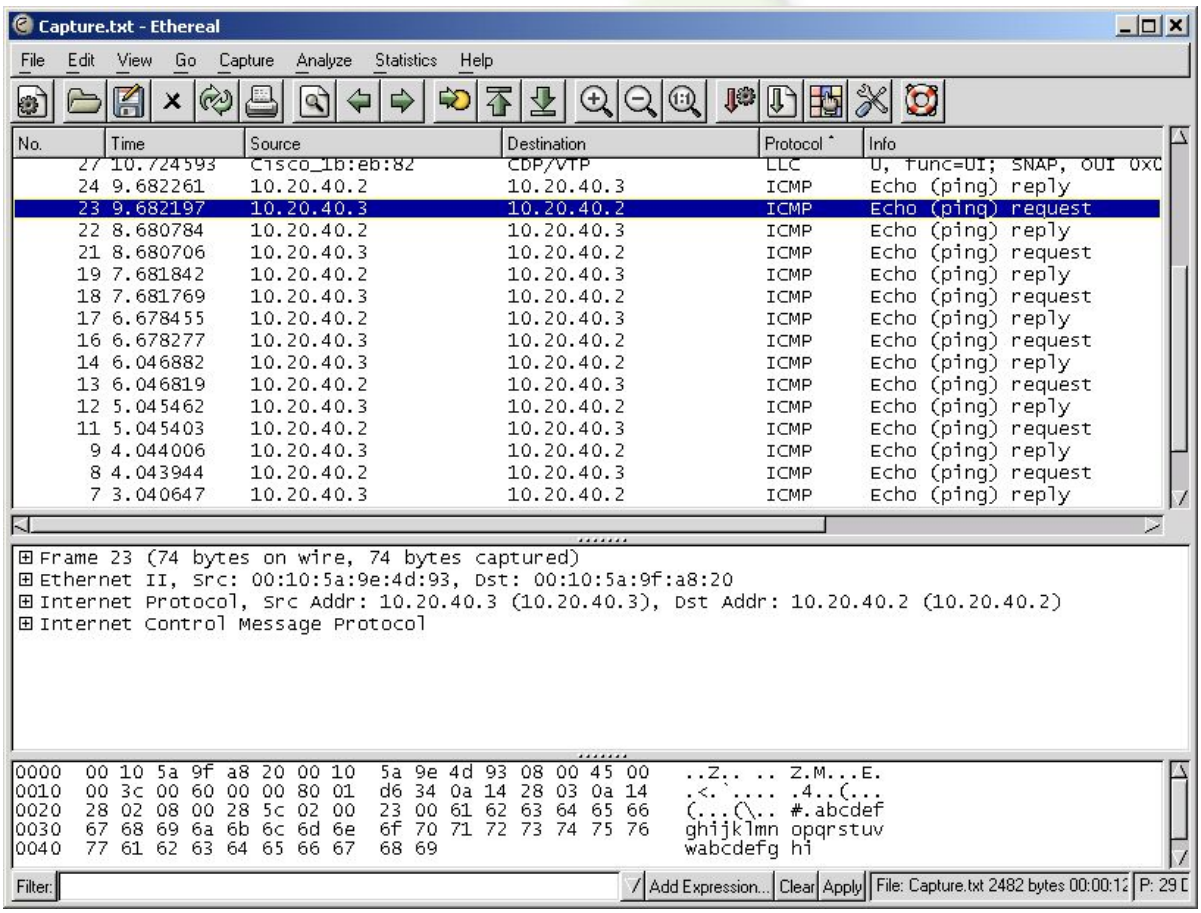
```
Switch#configure terminal
Enter configuration commands, one per line.  End
with CNTL/Z.
Switch(config)#monitor session 1 source interface
f0/2
Switch(config)#monitor session 1 destination
interface f0/1
```

```
Switch(config)#
2d03h: %LINEPROTO-5-UPDOWN: Line protocol on
Interface FastEthernet0/1, changed
state to down
```

Note that the monitor session commands are to be input all on one line. Any monitor session needs to have at least two commands, one specifying source and other destination.

Initiate another Ethereal capture, and once again at each workstation ping the other two hosts on the local network segment, and then stop the Ethereal capture.

The data from Ethereal should appear like the following:



Since the port connected to the computer monitor is a SPAN port, it is unable to communicate, so the pings fail.

All traffic in or out of port 2 is now being monitored. You can see this at the switch by using the following show command:

```
Switch#show monitor session 1
Session 1
---------
Type               : Local Session
Source Ports       :
    Both           : Fa0/2
Destination Ports  : Fa0/1
    Encapsulation: Native
          Ingress: Disabled
```

Step 3:

Other ports can easily be added to the monitor session. To add port 3,

```
Switch#configure terminal
Enter configuration commands, one per line.  End
with CNTL/Z.
Switch(config)#monitor session 1 source interface
f0/3
```

The configuration can be verified using the show monitor session command, and also seen via another Ethereal capture. Extending this scheme, every port other than the SPAN can be monitored.

Step 4:

A SPAN can also be established to monitor traffic only in one direction. The configure this, first remove the current SPAN.

```
Switch#config t
Switch(config)#no monitor session 1
Switch(config)#^Z
Switch#
2d03h: %LINEPROTO-5-UPDOWN: Line protocol on
```

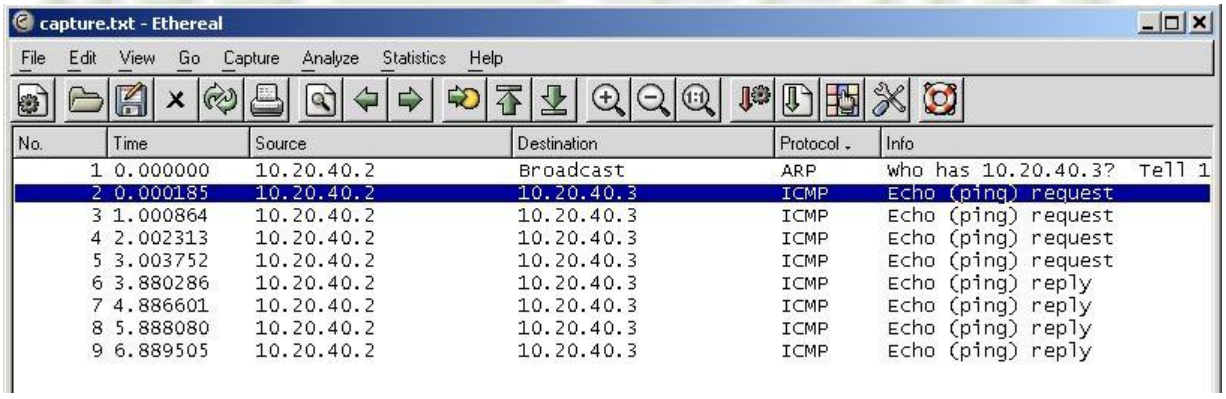
```
Interface FastEthernet0/1, changed state to up
2d03h: %SYS-5-CONFIG_I: Configured from console by
console
Switch#show monitor session 1
 No SPAN configuration is present in the system for
session [1].
```

Next, configure a new monitor session only for traffic incoming on port 2.

```
Switch(config)#monitor session 1 source interface
f0/2 rx
Switch(config)#monitor session 1 destination
interface f0/1

Switch#show monitor session 1
Session 1
---------
Type                : Local Session
Source Ports        :
    RX Only         : Fa0/2
Destination Ports   : Fa0/1
    Encapsulation: Native
          Ingress: Disabled
```

To test the SPAN, initiate another Ethereal capture, and have hosts 2 and 3 ping each other. After stopping the capture,

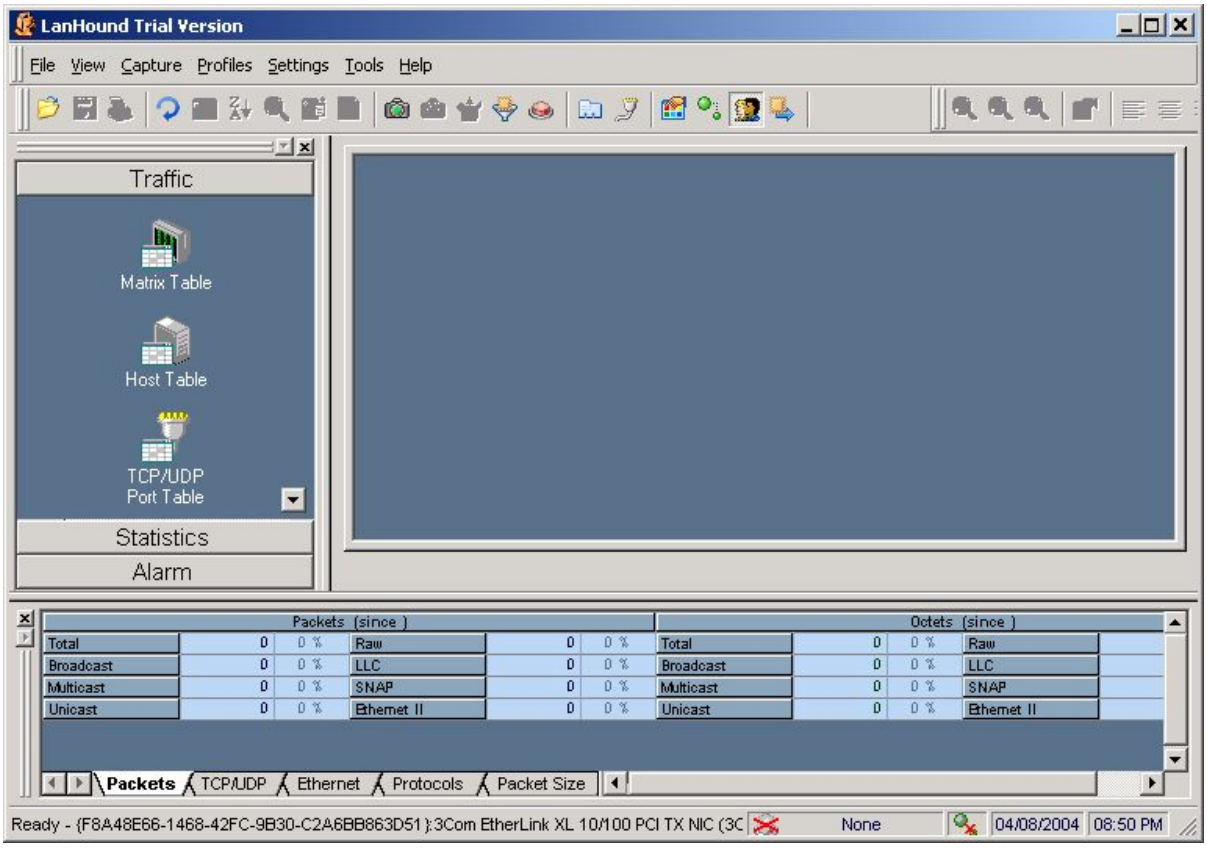


It can be readily seen that only traffic sourced from 10.20.40.2 is monitored.

Step 5:

With the SPAN still configured to receive traffic only from port 2, exit Ethereal, and start LanHound. Unlike Ethereal, LanHound is a commercial network monitor with built-in capture capability. Here the evaluation package will be used. Note that LanHound may have difficulty initiating a capture with certain wireless adaptors.

The initial LanHound screen looks like the following:

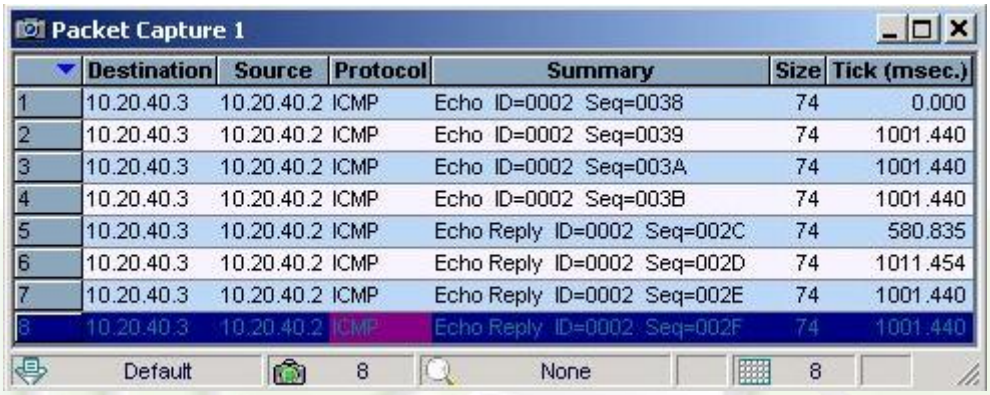


Initiating a LanHound capture is similar to that of Ethereal. Simply drop down the **Capture** menu and start. Generate some traffic out of host 2 by pinging host 3. Note that LanHound defaults to live capture seen in the main middle right window.

The destination/ source data may not look familiar. Right click on the title bar of the packet capture window.

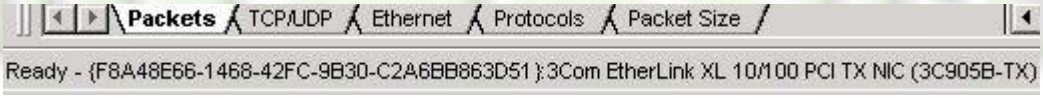
Then deselect host name and vendor code.

The Packet Capture window can be maximized within the main display area. After stopping the capture (**Capture** menu and stop), the Packet Capture window of LanHound will appear similar to,



Once again note that the monitor is reading traffic only into port 2.

Review the information shown for each tab at the bottom portion of LanHound.



Analysis

1) What advantages does a SPAN have over the use of hubs to affect monitoring?
2) Why might a network administrator configure a SPAN to monitor only receiving traffic from one port? What if that port is connected to gateway router?
3) Could monitoring of every port on a large switch adversely affect performance? What strategy should a network administrator develop in such a case?

Summary Discussion

A classroom discussion should follow the lab. Review the lab questions and your analyses as a group. Share your experiences and knowledge with the class.

If You Want To Learn More

Some of the more interesting features of LanHound include other presentations of network data accessed by the controls on the left.

Unfortunately there is little data from the SPAN port to analyze. To acquire a better idea of these capabilities, remove the SPAN port, and reconnect to the Internet by configuring dynamic IP addresses. Start another LanHound capture, and search the Internet for more information concerning LanHound.

After a brief search, stop the capture and examine the aforementioned added features of LanHound.

Appendix:

This lab was developed using Ethereal v0.10.8, and LanHound v1.1 (evaluation), Ethereal can be obtained from:

www.ethereal.com

-or-

http://winpcap.polito.it/

-and-

http://www.download.com

This lab was developed using LanHound v1.1(evaluation),which can be obtained from:

http://www.extralan.co.uk/index.htm

The OS environment for this lab was Windows XP Professional, Version 2002, Service Pack 2 (8/04). Note that Ethereal, in particular WinPcap, may have difficulty starting a capture from a wireless network adaptor.