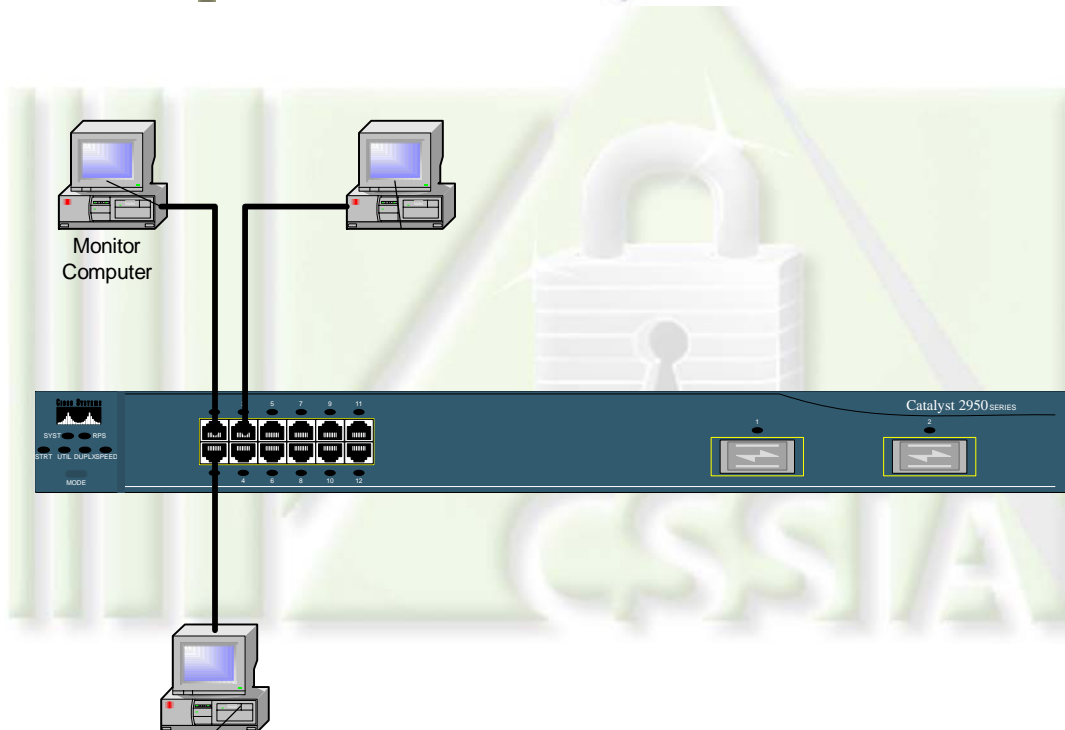


4.5.1

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:



Capture.txt - Ethereal					
File Edit View Go Capture Analyze Statistics Help					
No.	Time	Source	Destination	Protocol	Info
18	13.526099	10.20.40.2	10.20.40.1	ICMP	Echo (ping) reply
21	14.527339	10.20.40.1	10.20.40.2	ICMP	Echo (ping) request
22	14.527512	10.20.40.2	10.20.40.1	ICMP	Echo (ping) reply
26	16.395773	10.20.40.1	10.20.40.3	ICMP	Echo (ping) request
27	16.395951	10.20.40.3	10.20.40.1	ICMP	Echo (ping) reply
28	17.401449	10.20.40.1	10.20.40.3	ICMP	Echo (ping) request
29	17.401629	10.20.40.3	10.20.40.1	ICMP	Echo (ping) reply
31	18.402882	10.20.40.1	10.20.40.3	ICMP	Echo (ping) request
32	18.403061	10.20.40.3	10.20.40.1	ICMP	Echo (ping) reply
33	19.404324	10.20.40.1	10.20.40.3	ICMP	Echo (ping) request
34	19.404504	10.20.40.3	10.20.40.1	ICMP	Echo (ping) reply
42	28.156162	10.20.40.2	10.20.40.1	ICMP	Echo (ping) request
43	28.156267	10.20.40.1	10.20.40.2	ICMP	Echo (ping) reply
44	29.152930	10.20.40.2	10.20.40.1	ICMP	Echo (ping) request
45	29.153037	10.20.40.1	10.20.40.2	ICMP	Echo (ping) reply
47	30.154315	10.20.40.2	10.20.40.1	ICMP	Echo (ping) request

Frame 22 (74 bytes on wire, 74 bytes captured)

Ethernet II, Src: 00:10:5a:9f:a8:20, Dst: 00:10:5a:9f:a7:0c

Internet Protocol, Src Addr: 10.20.40.2 (10.20.40.2), Dst Addr: 10.20.40.1 (10.20.40.1)

Internet Control Message Protocol

0000	00 10 5a 9f a7 0c 00 10 5a 9f a8 20 08 00 45 00	..Z..... Z.. ..E.
0010	00 3c 01 9e 00 00 80 01 d4 f8 0a 14 28 02 0a 14	..<..... ..(...
0020	28 01 00 00 47 5c 02 00 0c 00 61 62 63 64 65 66	(...G)... ..abcdef
0030	67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76	ghijklmn opqrstuv
0040	77 61 62 63 64 65 66 67 68 69	wabcdefg hi

Filter:
Add Expression...
Clear
Apply
File: Capture.txt 8458 bytes 00:01:20 P: 97 L

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:

No.	Time	Source	Destination	Protocol	Info
27	10.724593	Cisco_1b:eb:82	10.20.40.3	LLC	U, func=UI; SNAP, OUI 0xc
24	9.682261	10.20.40.2	10.20.40.3	ICMP	Echo (ping) reply
23	9.682197	10.20.40.3	10.20.40.2	ICMP	Echo (ping) request
22	8.680784	10.20.40.2	10.20.40.3	ICMP	Echo (ping) reply
21	8.680706	10.20.40.3	10.20.40.2	ICMP	Echo (ping) request
19	7.681842	10.20.40.2	10.20.40.3	ICMP	Echo (ping) reply
18	7.681769	10.20.40.3	10.20.40.2	ICMP	Echo (ping) request
17	6.678455	10.20.40.2	10.20.40.3	ICMP	Echo (ping) reply
16	6.678277	10.20.40.3	10.20.40.2	ICMP	Echo (ping) request
14	6.046882	10.20.40.3	10.20.40.2	ICMP	Echo (ping) reply
13	6.046819	10.20.40.2	10.20.40.3	ICMP	Echo (ping) request
12	5.045462	10.20.40.3	10.20.40.2	ICMP	Echo (ping) reply
11	5.045403	10.20.40.2	10.20.40.3	ICMP	Echo (ping) request
9	4.044006	10.20.40.3	10.20.40.2	ICMP	Echo (ping) reply
8	4.043944	10.20.40.2	10.20.40.3	ICMP	Echo (ping) request
7	3.040647	10.20.40.3	10.20.40.2	ICMP	Echo (ping) reply

Frame 23 (74 bytes on wire, 74 bytes captured)

- Ethernet II, Src: 00:10:5a:9e:4d:93, Dst: 00:10:5a:9f:a8:20
- Internet Protocol, Src Addr: 10.20.40.3 (10.20.40.3), Dst Addr: 10.20.40.2 (10.20.40.2)
- Internet Control Message Protocol

```

0000  00 10 5a 9f a8 20 00 10 5a 9e 4d 93 08 00 45 00  ..Z... Z.M...E.
0010  00 3c 00 60 00 00 80 01 d6 34 0a 14 28 03 0a 14  .<.... .4...
0020  28 02 08 00 28 5c 02 00 23 00 61 62 63 64 65 66  (...)\... #.abcdef
0030  67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76  ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67 68 69                    wabcdefg hi

```

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. To 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

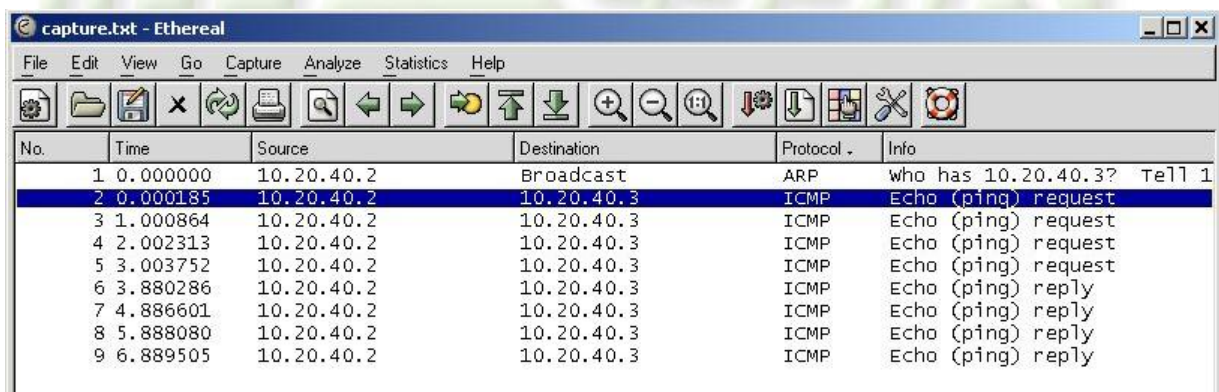
```

```

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,



No.	Time	Source	Destination	Protocol	Info
1	0.000000	10.20.40.2	Broadcast	ARP	who has 10.20.40.3? Tell 1
2	0.000185	10.20.40.2	10.20.40.3	ICMP	Echo (ping) request
3	1.000864	10.20.40.2	10.20.40.3	ICMP	Echo (ping) request
4	2.002313	10.20.40.2	10.20.40.3	ICMP	Echo (ping) request
5	3.003752	10.20.40.2	10.20.40.3	ICMP	Echo (ping) request
6	3.880286	10.20.40.2	10.20.40.3	ICMP	Echo (ping) reply
7	4.886601	10.20.40.2	10.20.40.3	ICMP	Echo (ping) reply
8	5.888080	10.20.40.2	10.20.40.3	ICMP	Echo (ping) reply
9	6.889505	10.20.40.2	10.20.40.3	ICMP	Echo (ping) reply

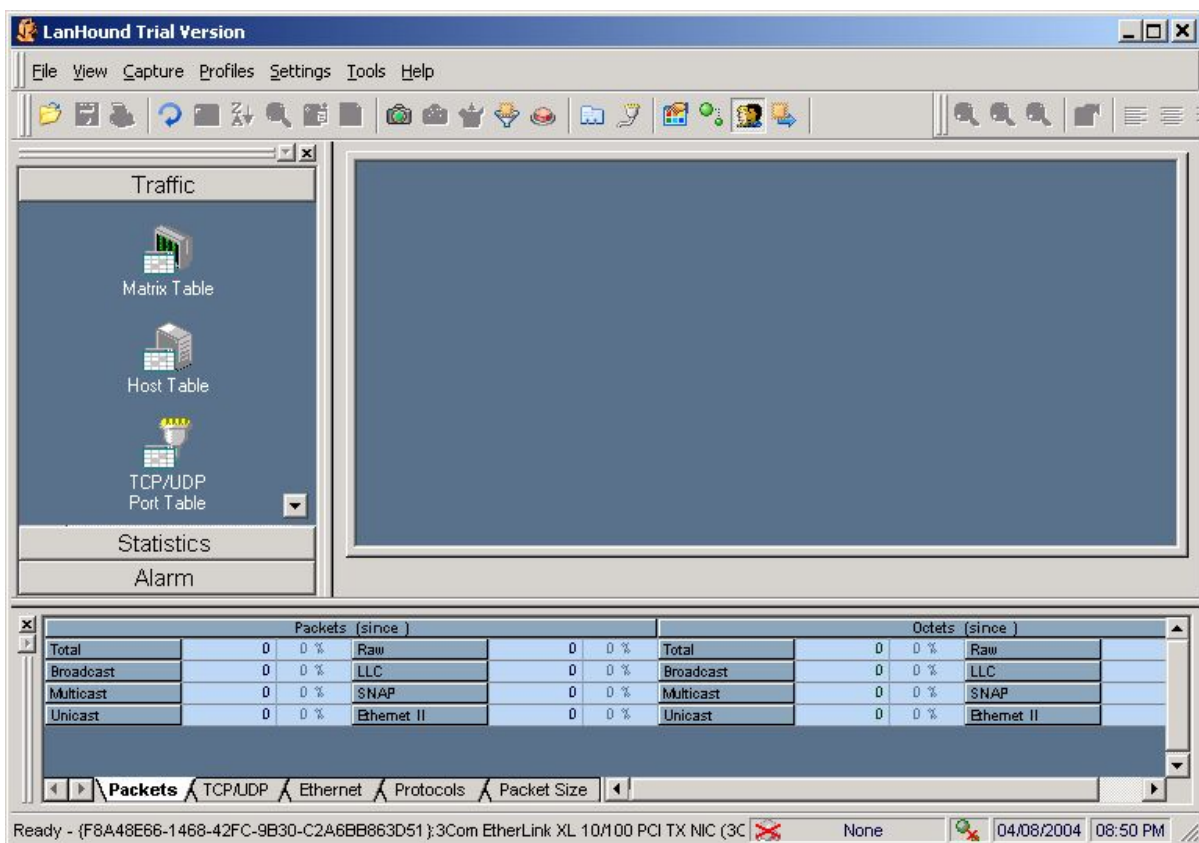
It can be readily seen that only traffic sourced from 10.20.40.2 is monitored.



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.



Packet Capture 1					
▼	Destination	Source	Protocol	Summary	Size

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,

Packet Capture 1							
▼	Destination	Source	Protocol	Summary	Size	Tick (msec.)	
1	10.20.40.3	10.20.40.2	ICMP	Echo ID=0002 Seq=0038	74	0.000	
2	10.20.40.3	10.20.40.2	ICMP	Echo ID=0002 Seq=0039	74	1001.440	
3	10.20.40.3	10.20.40.2	ICMP	Echo ID=0002 Seq=003A	74	1001.440	
4	10.20.40.3	10.20.40.2	ICMP	Echo ID=0002 Seq=003B	74	1001.440	
5	10.20.40.3	10.20.40.2	ICMP	Echo Reply ID=0002 Seq=002C	74	580.835	
6	10.20.40.3	10.20.40.2	ICMP	Echo Reply ID=0002 Seq=002D	74	1011.454	
7	10.20.40.3	10.20.40.2	ICMP	Echo Reply ID=0002 Seq=002E	74	1001.440	
8	10.20.40.3	10.20.40.2	ICMP	Echo Reply ID=0002 Seq=002F	74	1001.440	

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.

⏪	⏩	⏴	⏵	Packets	TCP/UDP	Ethernet	Protocols	Packet Size	⏴
Ready - {F8A48E66-1468-42FC-9B30-C2A6BB863D51} 3Com EtherLink XL 10/100 PCI TX NIC (3C905B-TX)									

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?

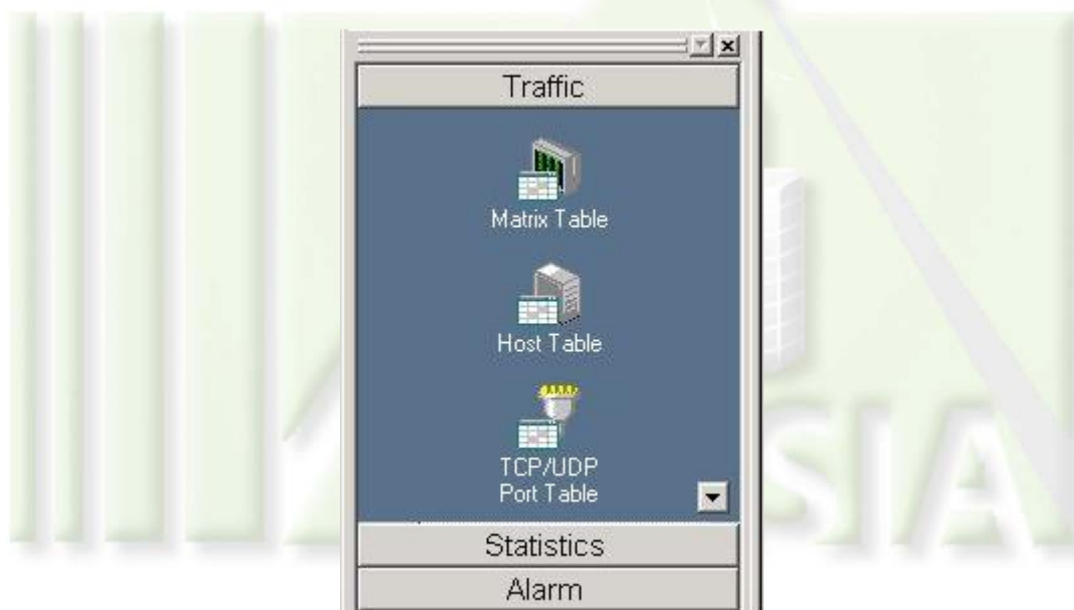


Summary Discussion

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.

