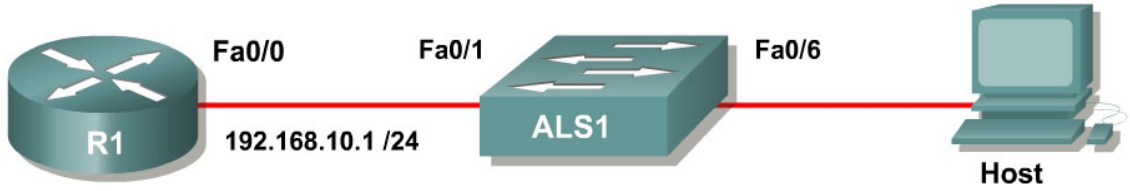
Lab 3.3 Configuring Wireshark and SPAN

Learning Objectives

- Install Wireshark on a host PC
- Configure a switch to use the SPAN monitoring tool.

Topology Diagram



Scenario

In this lab, you will configure a switch to mirror traffic from a certain port out to a destination port for analyzing. In addition, you will configure Wireshark on a host PC to monitor the mirrored traffic flow.

Wireshark is a packet sniffing application that can read and analyze the incoming packets. Because it is useful for troubleshooting and verification, Wireshark is used in many of the labs in this course.

Step 1: Configure the Router

Configure the R1 FastEthernet0/0 interface with the IP address shown in the diagram. On the switch ALS1, place all the ports in VLAN 1. Configure EIGRP AS 1 with the 192.168.10.0 network in order to generate traffic on the wire.

```
R1(config)# interface fastethernet0/0
R1(config-if)# ip address 192.168.10.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# router eigrp 1
R1(config-router)# network 192.168.10.0
```

What kind of packets would you expect R1 to send toward ALS1's Fast Ethernet interface?

R1 will send EIGRP Hello packets toward ALS1 via Fast Ethernet.

Step 2: Install Wireshark and WinPcap

Run the Wireshark installer executable file. If you do not have the installer, download it from http://www.wireshark.org. Once the installation wizard opens, click **Next**.

Figure 2-1: Wireshark Installation Wizard

Click **I Agree** to agree to the Wireshark license agreement.

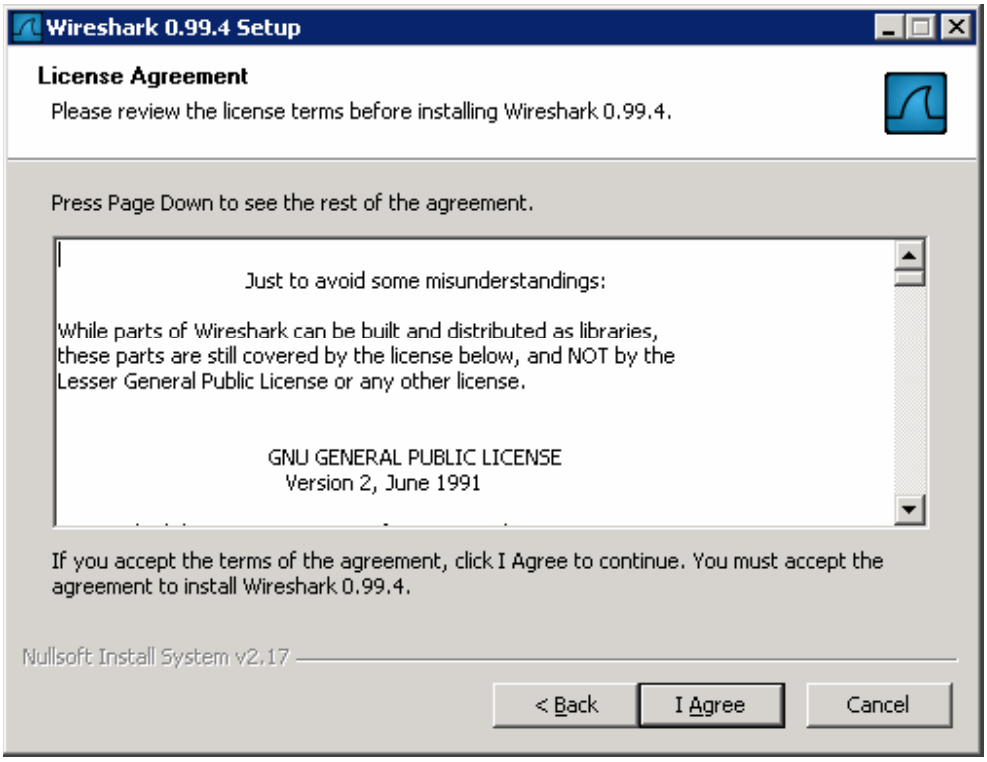


Figure 2-2: Wireshark License Agreement

Use the default settings and click **Next**.

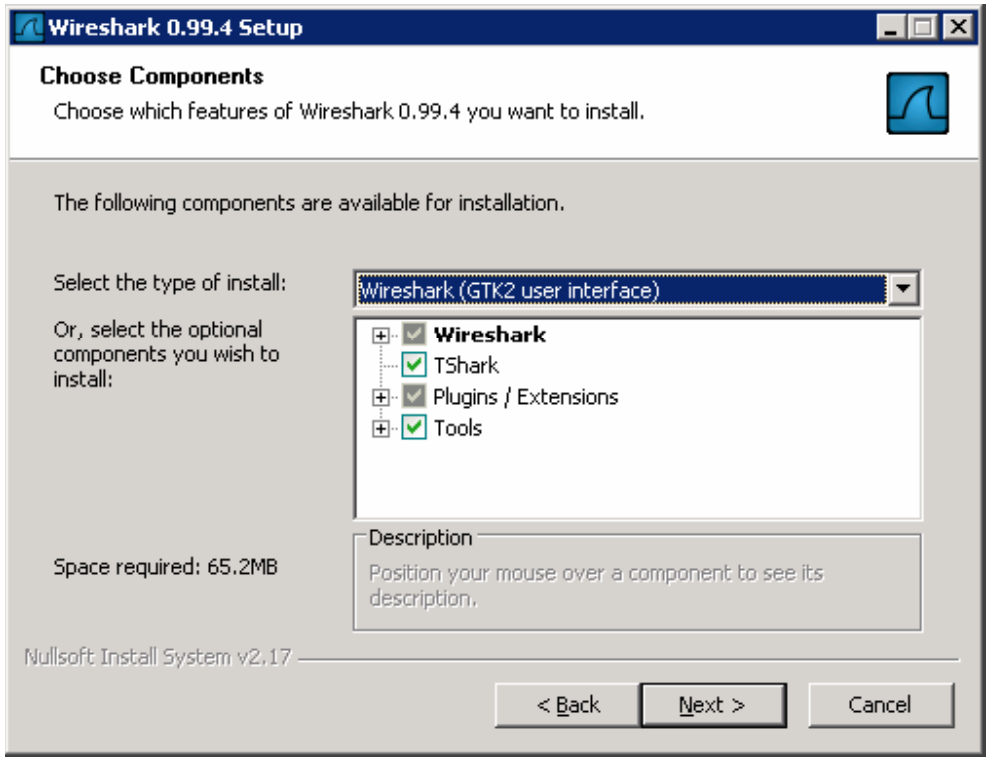


Figure 2-3: Selecting Wireshark Components

Use your own personal preference to determine where you want the shortcuts to be placed, and check those boxes accordingly. Then click **Next**.

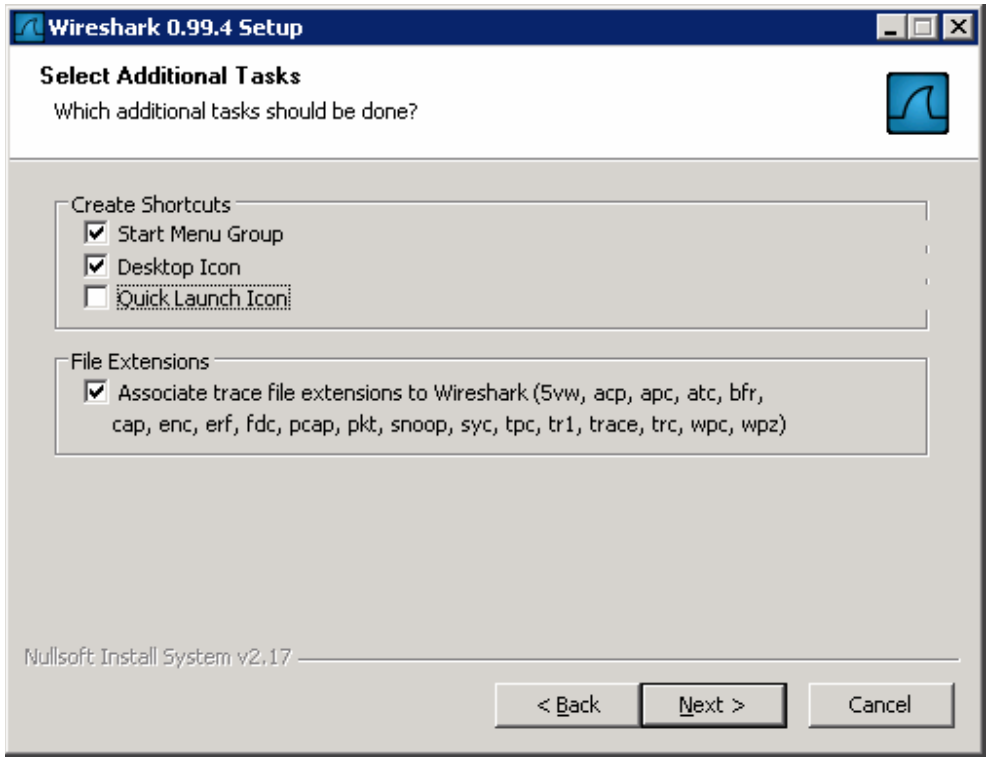


Figure 2-4: Additional Tasks Selection

Use the default installation directory, and then click **Next**.

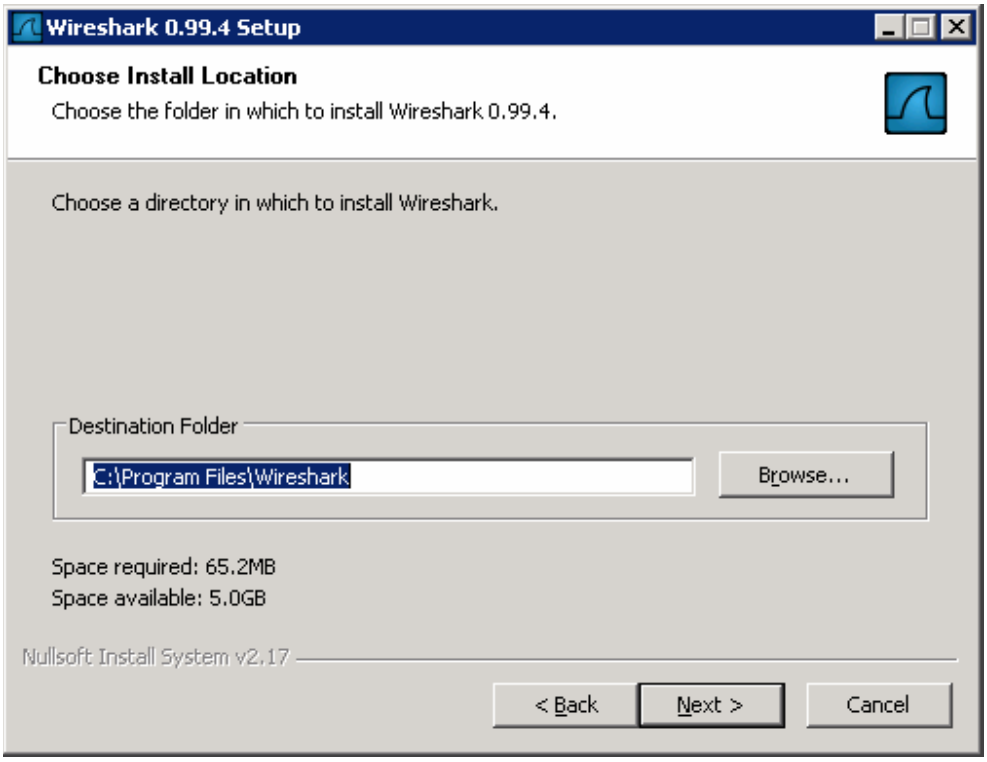


Figure 2-5: Installation Location Dialog

Check the option to install WinPcap, because you will need it for Wireshark to work. If you plan to have non-administrators use Wireshark, choose the Services option also.

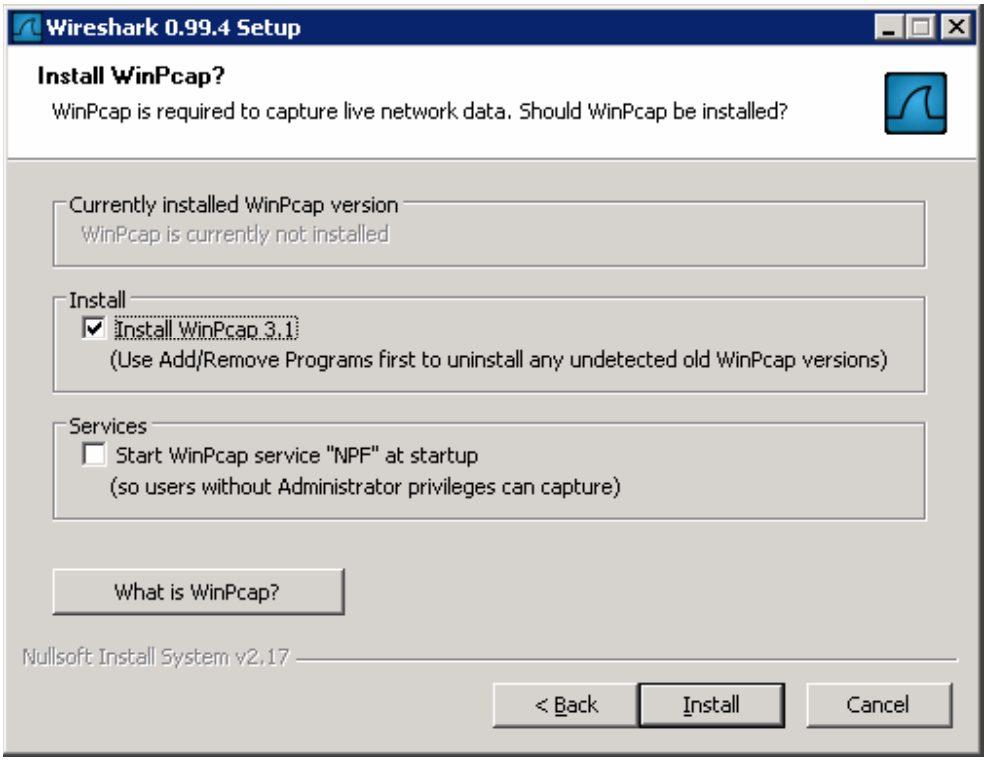


Figure 2-6: WinPcap Installation Options

The WinPcap installation wizard will now run.

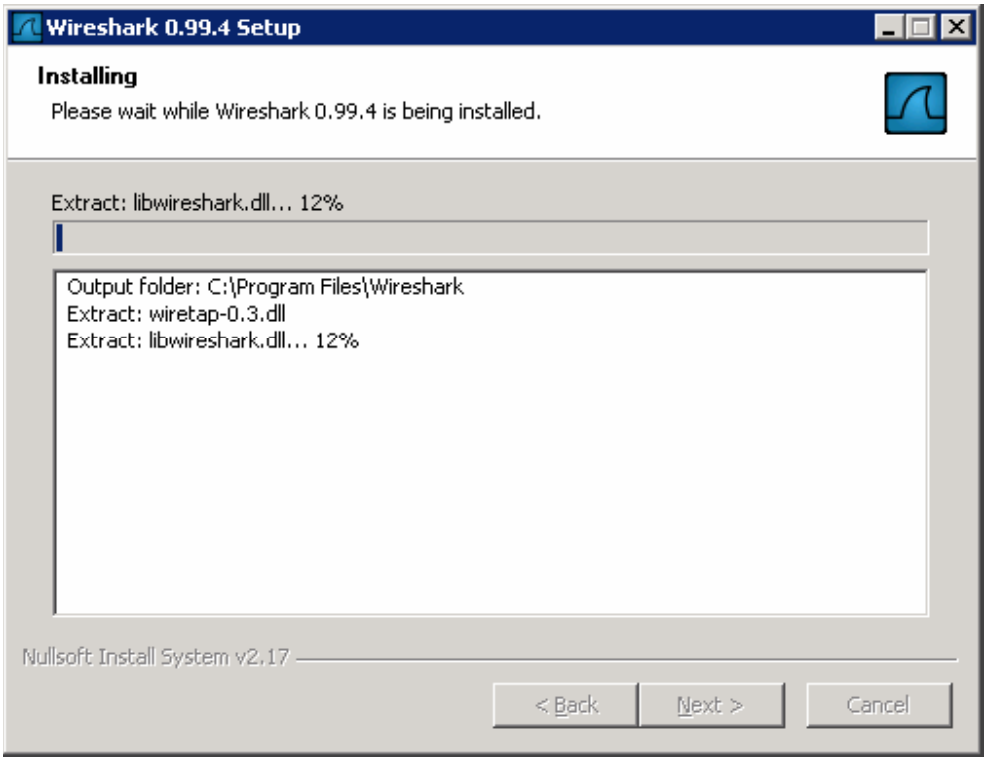


Figure 2-7: Wireshark Installation Progress Indicator

During the install, the WinPcap installer starts up if you selected the launch option earlier (see Figure 2-4). Agree to the license agreement by clicking the **I Agree** button.

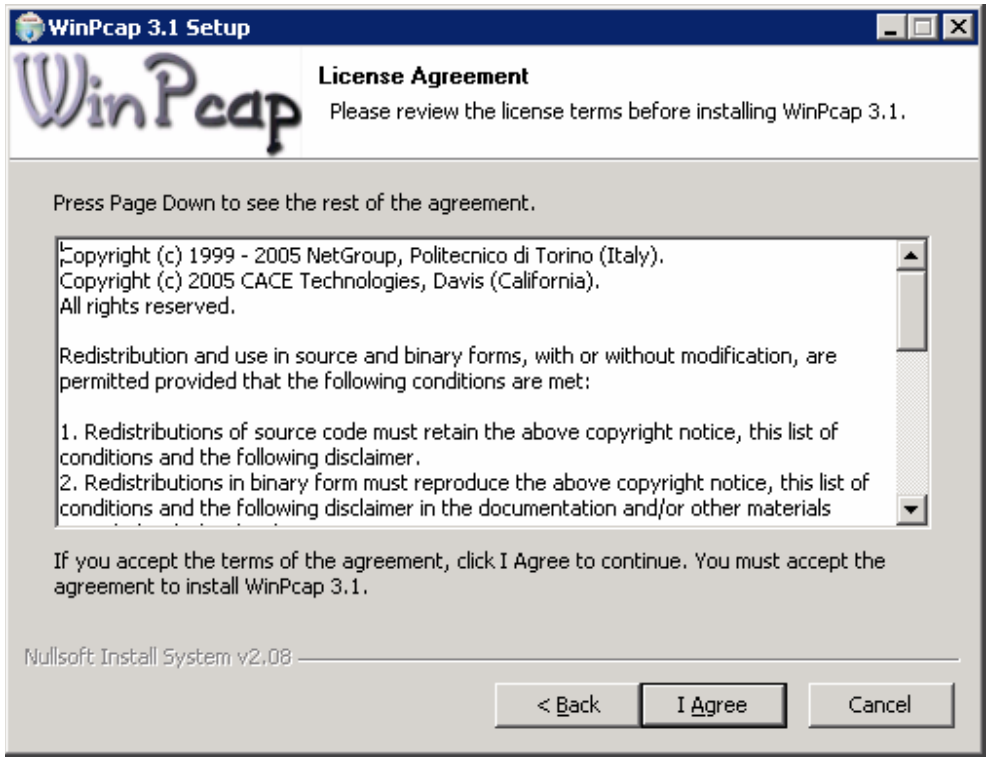


Figure 2-8: WinPcap License Agreement

After clicking **I Agree**, WinPcap installs.

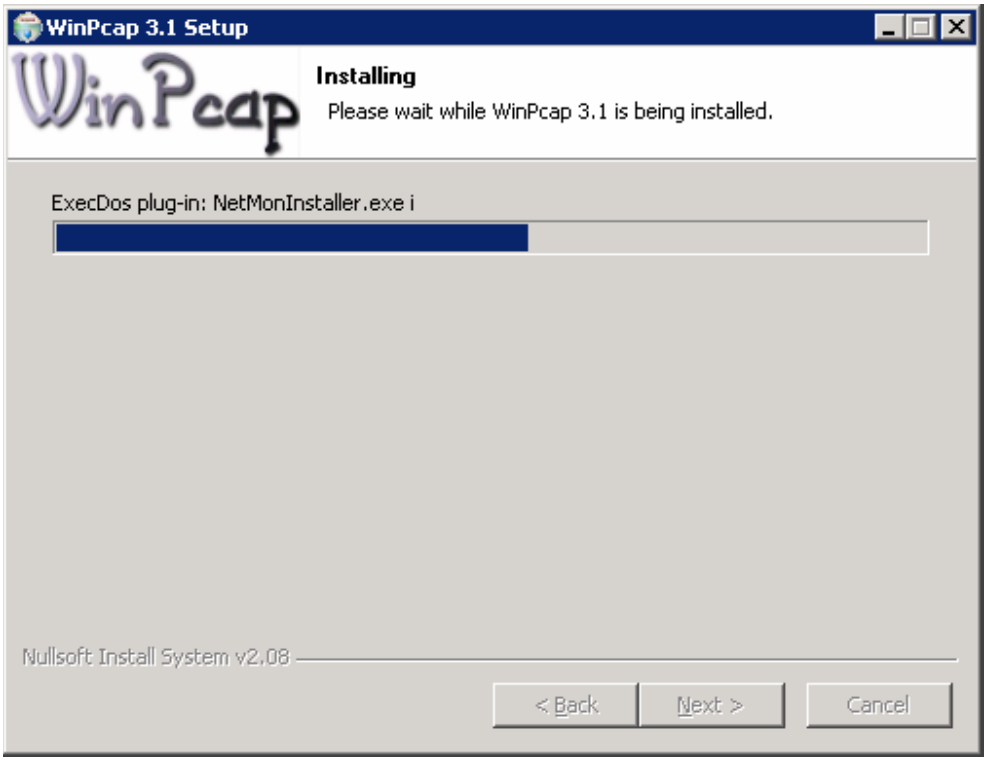


Figure 2-9: WinPcap Installation Progress Indicator

Click **Finish** to complete the WinPcap installation, and the Wireshark installer will continue.

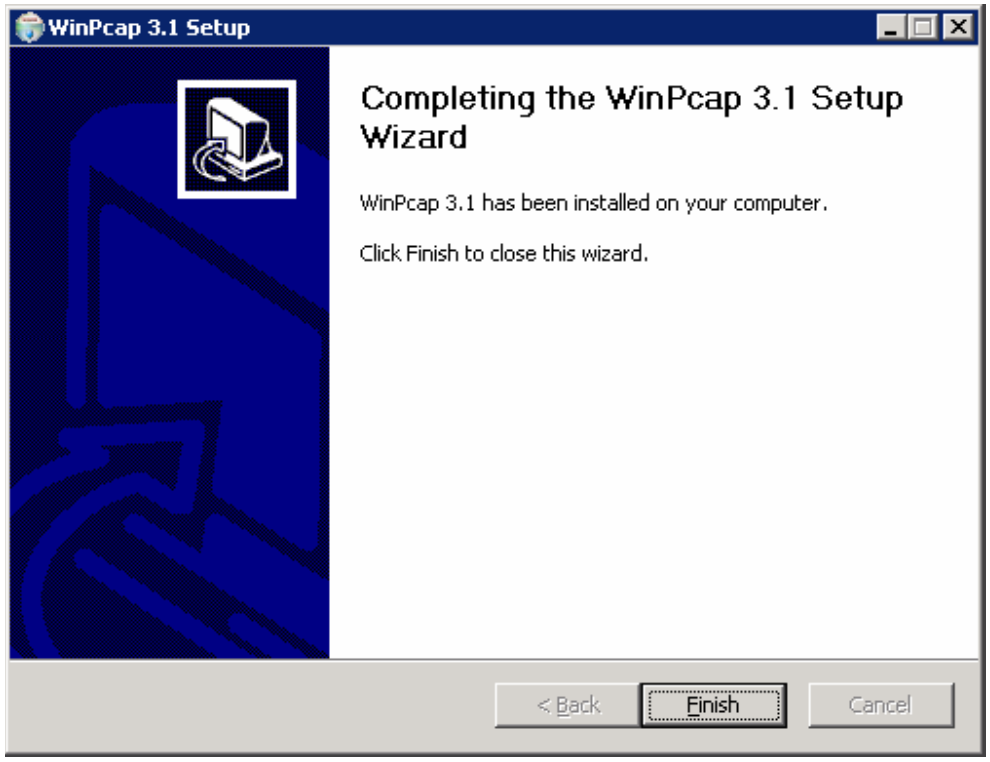


Figure 2-10: Final WinPcap Installation Window

After the Wireshark installer has finished, click **Next** to go to the final screen.

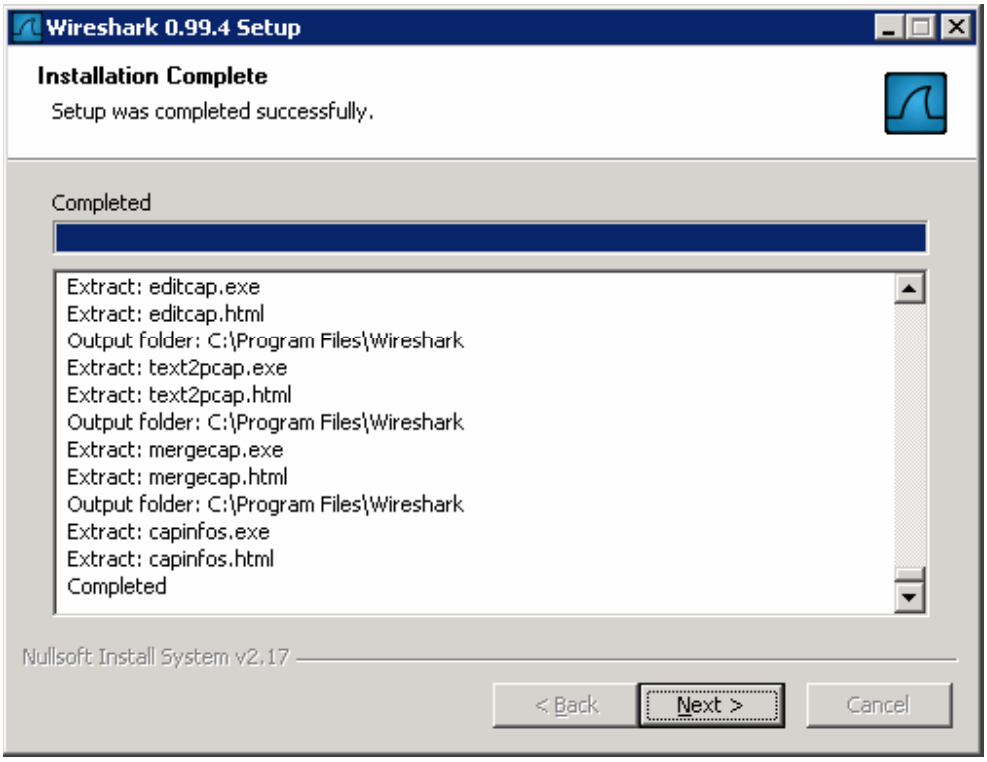


Figure 2-11: Wireshark Installation Progress Indicator

Check **Run Wireshark** if you want to run the program now, and then click **Finish**.

Step 3: Configure SPAN on a Switch

On the Catalyst switch, you need to configure Switched Port Analyzer (SPAN) to mirror traffic going in and out of the router port to the host port. To do this, use the **monitor session** *number* **source interface** *interface-type interface-number* command. This specifies the source interface that is the interface to be monitored. The destination interface is specified in a similar way using the **monitor session** *number* **destination interface** *interface-type interface-number* command. You must use the same session number in both lines, indicating that they are the same monitoring session.

```
ALS1(config)# monitor session 1 source interface fastethernet0/1
ALS1(config)# monitor session 1 destination interface fastethernet0/6
```

It is important to note that when an interface is a SPAN destination interface, the switch will not forward any frames at OSI Layer 2 or Layer 3 aside from those captured from the SPAN session. Thus, the destination port does not participate in Dynamic Trunk Protocol (DTP), VLAN Trunking Protocol (VTP), Cisco Discovery Protocol (CDP), Spanning-tree Protocol (STP), or

EtherChannel negotiation protocols such as PAgP or LACP. The only traffic sent out of the destination interface is the traffic from the SPAN session.

Verify the configuration using the **show monitor** command.

```
ALS1# show monitor
Session 1
---------
Type              : Local Session
Source Ports      :
    Both          : Fa0/1
Destination Ports : Fa0/6
    Encapsulation : Native
          Ingress : Disabled
```

If you had not implemented the following command, would the host still receive the EIGRP hello packets? Explain.

```
ALS1(config)# monitor session 1 destination interface fastethernet0/6
```

Yes, the host would have received the EIGRP packets via VLAN 1. When you configured the destination interface, all normal traffic out FastEthernet0/6 ended and only the SPAN data was sent. To verify that you are receiving data via the SPAN session, observe the output of the **show monitor** command shown above.

Step 4: Sniff Packets using Wireshark

Now that the switch is sending SPAN packets to the host, you can show packets generated from R1 in Wireshark. To do this, open Wireshark. It opens with an empty Wireshark window.

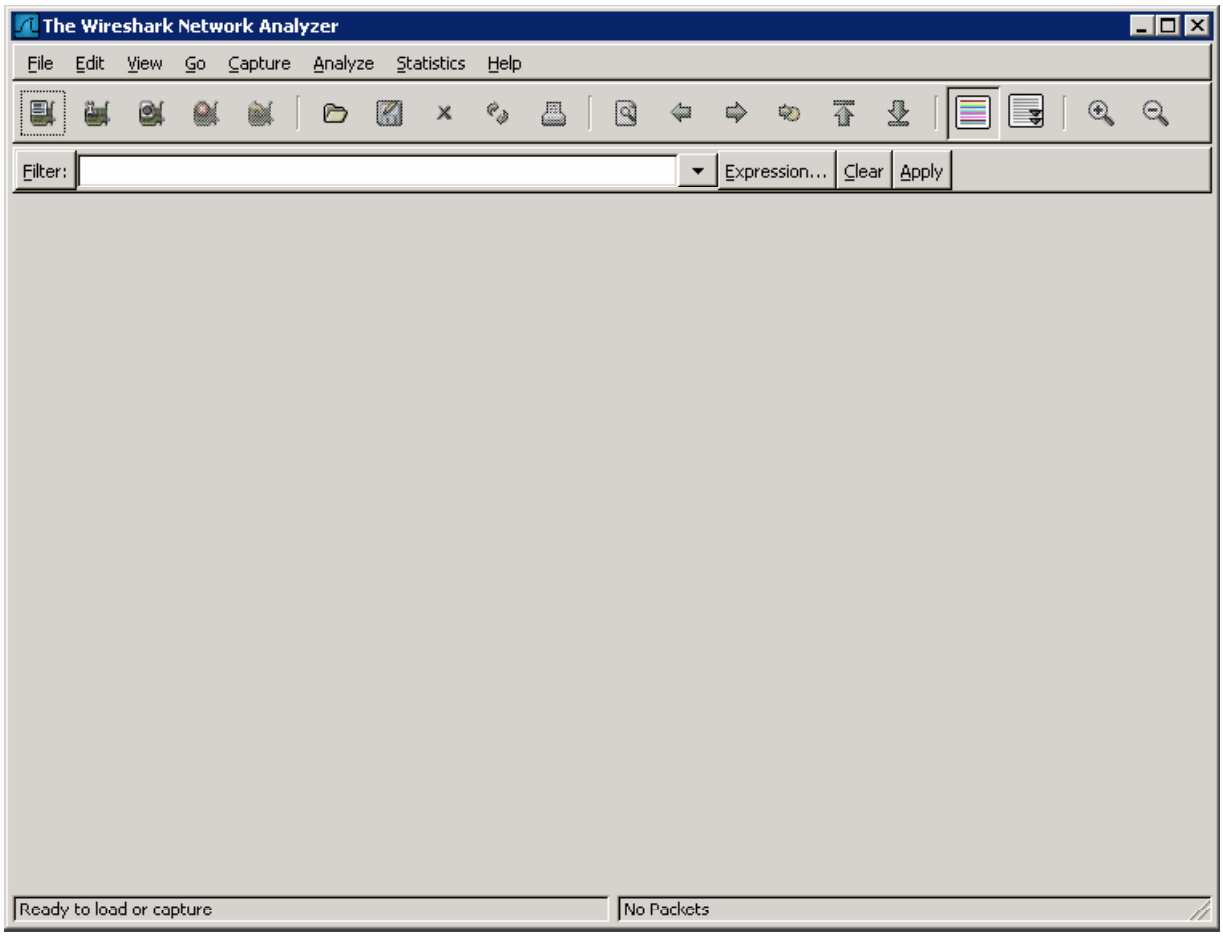


Figure 4-1: Wireshark Application Window

Click **Capture** on the toolbar, and then click **Interfaces...**.

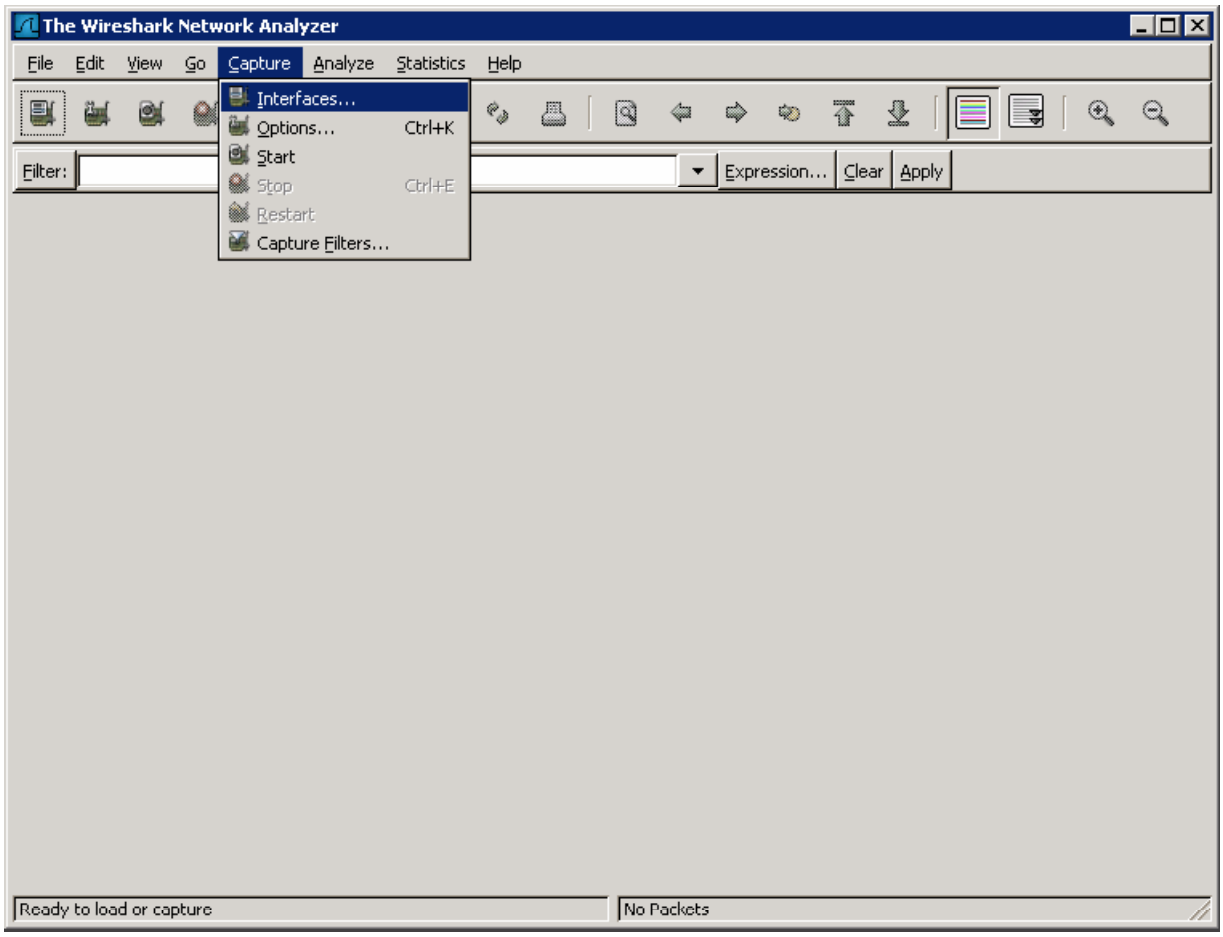


Figure 4-2: Capture Menu

Choose the interface on the PC that is connected to the SPAN destination port and click **Start** for that interface. The IP on the host does not necessarily need to be in the same subnet as the traffic you are sniffing.

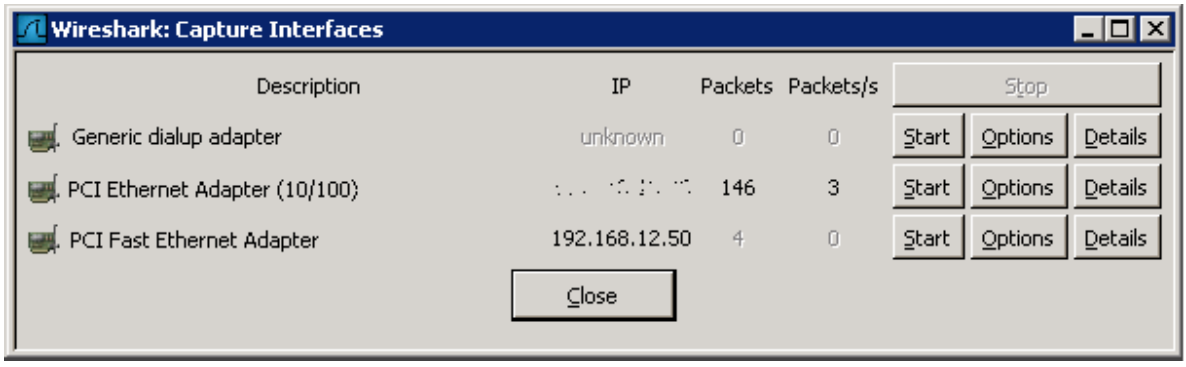


Figure 4-3: Interface List

Once you have sniffed a decent amount of traffic (~30 seconds), click **Stop**. EIGRP packets are classified as **Other** in this list.

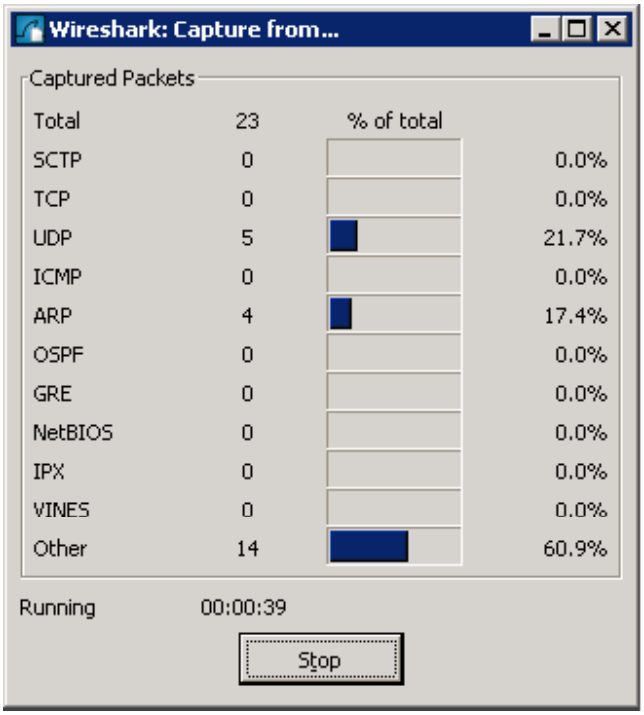


Figure 4-4: Capture Summary Window

Why are EIGRP packets not classified in any of these protocols?

EIGRP does not use TCP or UDP to transport its IP packets. Instead, it uses IP protocol number 88 as the identifier for both unicast and multicast EIGRP packets.

Wireshark lists all captured packets. In addition, deeper packet information and a raw readout of the packet are available for the selected packet (see Figure 4-5.) Explore the detailed information available for each packet. Note the EIGRP hello multicasts are sent to the host via the SPAN session.

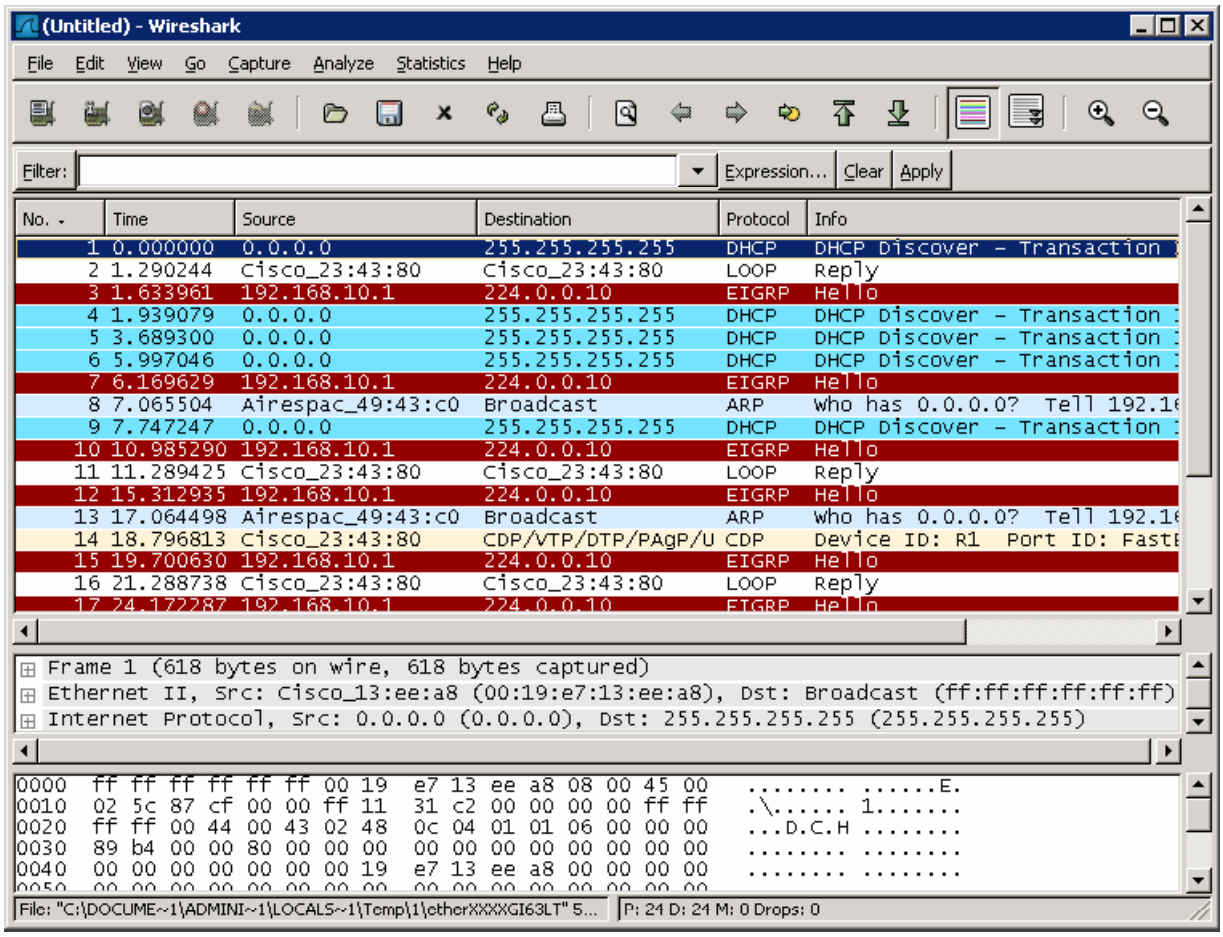


Figure 4-5: Wireshark Packet Detail Window

Final Configurations

```
R1# show run
!
hostname R1
!
interface fastethernet0/0
 ip address 192.168.10.1 255.255.255.0
!
router eigrp 1
 network 192.168.10.0
!
end

ALS1# show run
!
hostname ALS1
!
monitor session 1 source interface fastethernet0/1
monitor session 1 destination interface fastethernet0/6
!
end
```

