# Lab – Configuring Wireshark and SPAN

## Topology


## Addressing Table

| Device | Interface | IP Address | Subnet Mask |
|---|---|---|---|
| R1 | G0/1 | 192.168.10.1 | 255.255.255.0 |
| PC-A | NIC | 192.168.10.3 | 255.255.255.0 |

## Objectives

**Part 1: Installing Wireshark**

**Part 2: Configuring the Switch for SPAN Monitoring Tool**

## Background / 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 install and 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.

## Required Resources

- 1 Router (Cisco 1941 with Cisco IOS Release 15.4(3) universal image or comparable)
- 1 Switch (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 1 PC (Windows with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet and serial cables as shown in the topology

# Part 1: Installing Wireshark

## Step 1: Download Wireshark.

a. Wireshark can be downloaded from www.wireshark.org.

b. Click the **Download** icon.


c. Choose the software version you need based on your PC architecture and operating system. For instance, if you have a 64-bit PC running Windows, choose **Windows Installer (64-bit)**.

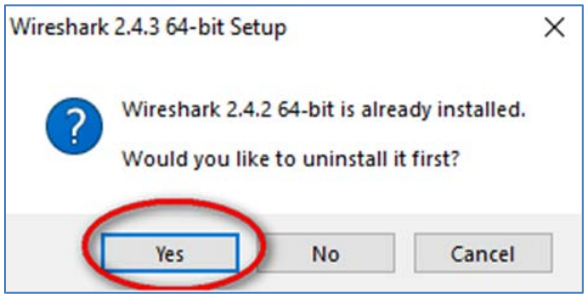

d. After making a selection, the download should start. The location of the downloaded file depends on the browser and operating system that you use. For Windows users, the default location is the **Downloads** folder.

## Step 2: Install Wireshark.

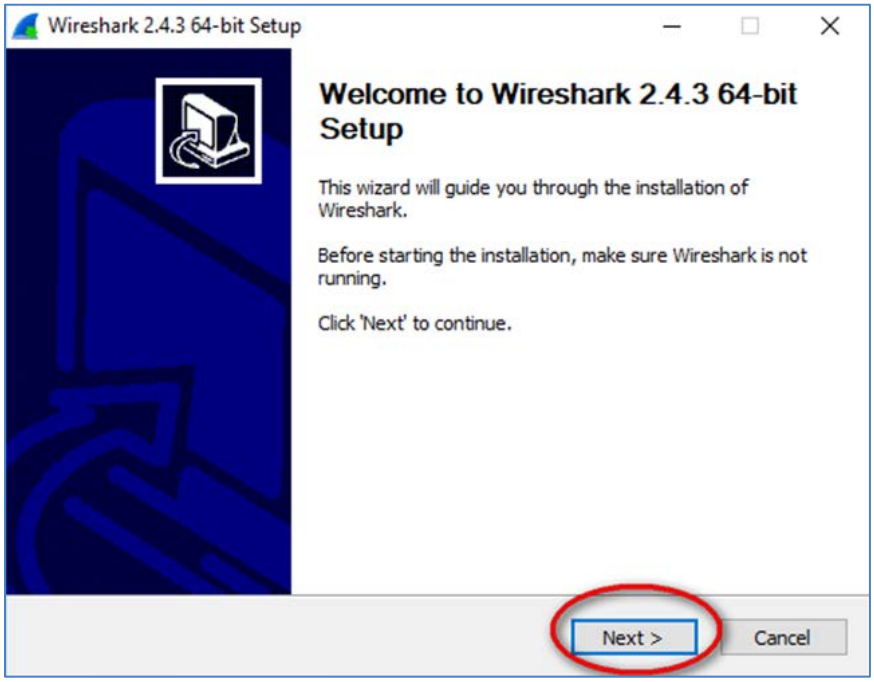
a. The downloaded file is named **Wireshark-win64-x.x.x.exe**, where **x** represents the version number. Double-click the file to start the installation process.

b. Respond to any security messages that may display on your screen. If you already have a copy of Wireshark on your PC, you will be prompted to uninstall the old version before installing the new version.

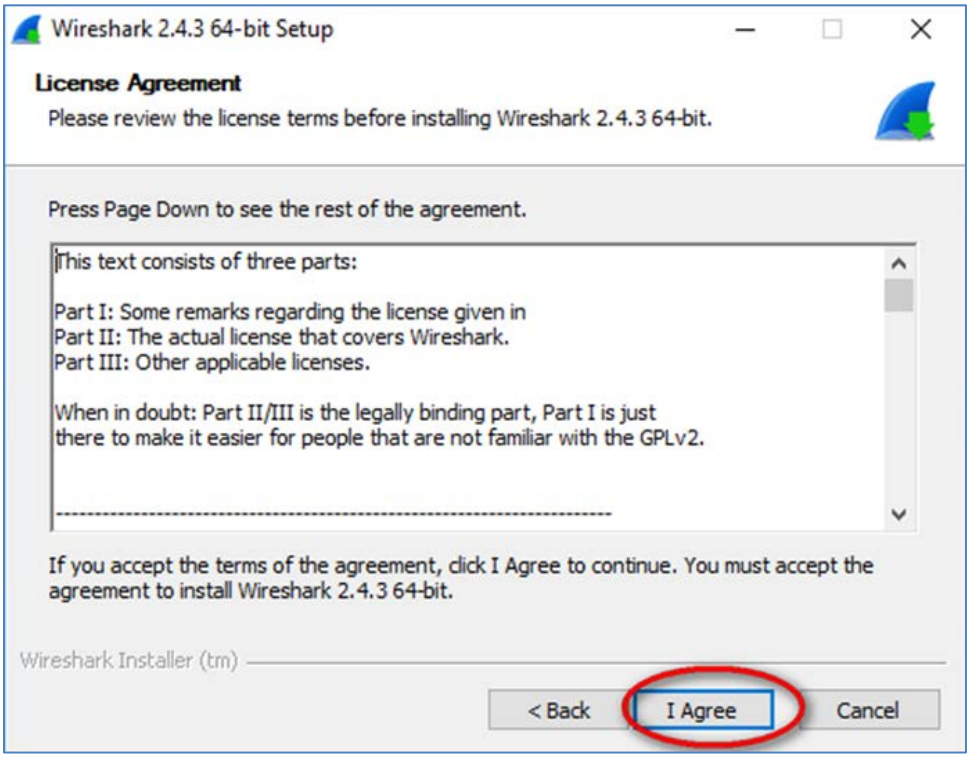
It is recommended that you remove the old version of Wireshark prior to installing another version. Click **Yes** to uninstall the previous version of Wireshark.



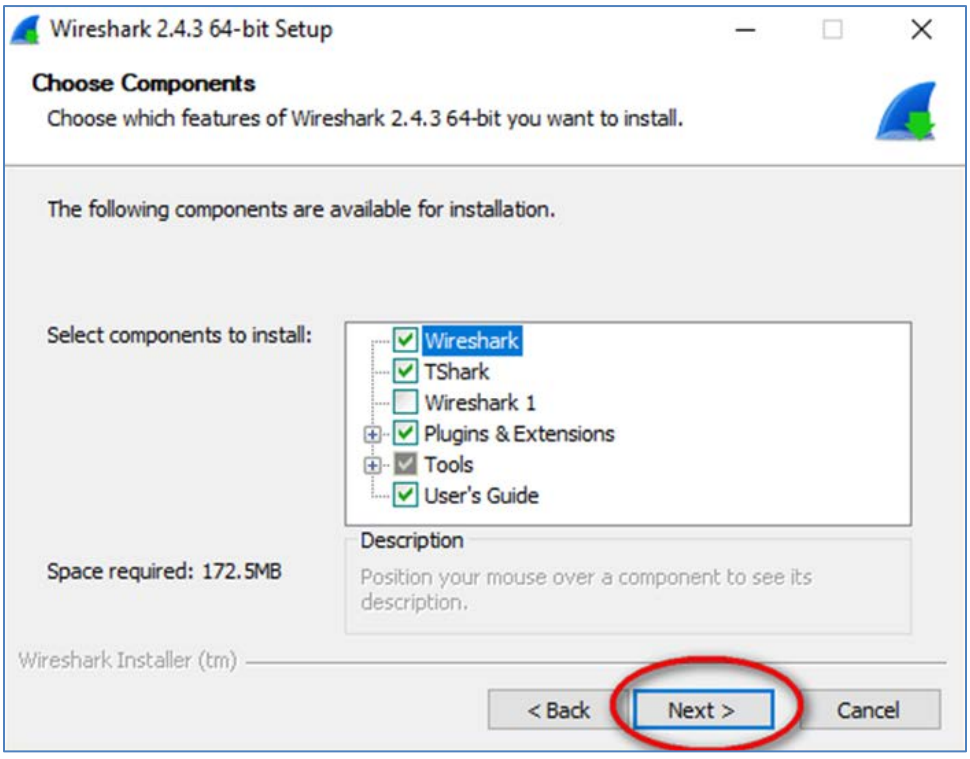

c. If this is the first time you have installed Wireshark, or this is after you have completed the uninstall process, you will navigate to the Wireshark Setup wizard. Click **Next**.



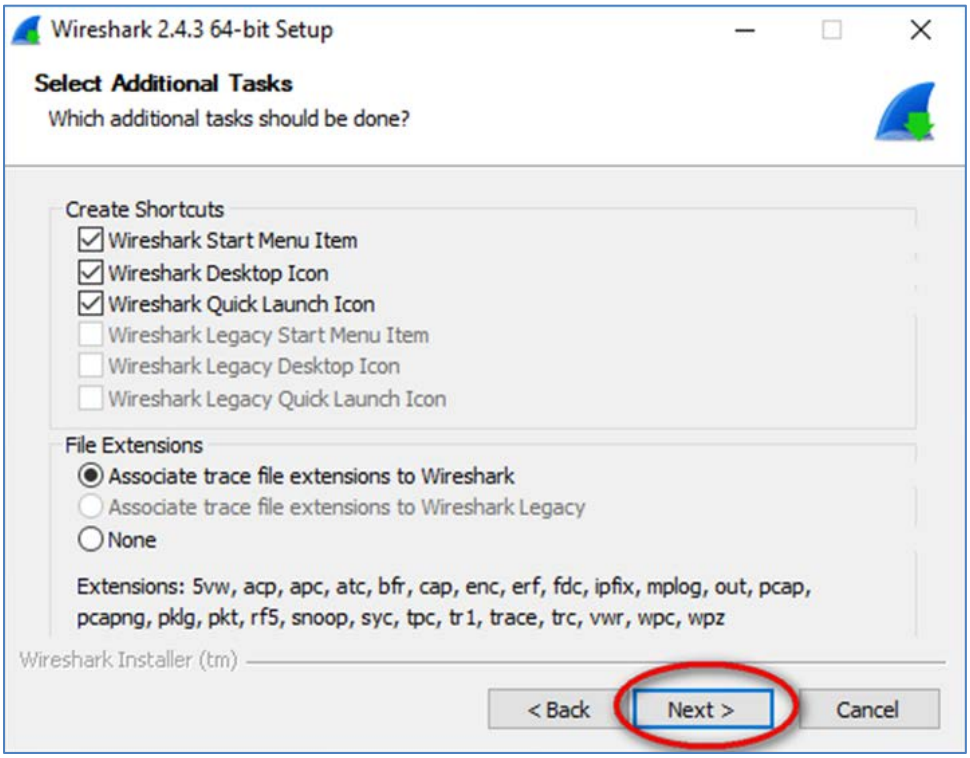
d. Continue advancing through the installation process. Click **I Agree** when the License Agreement window displays.



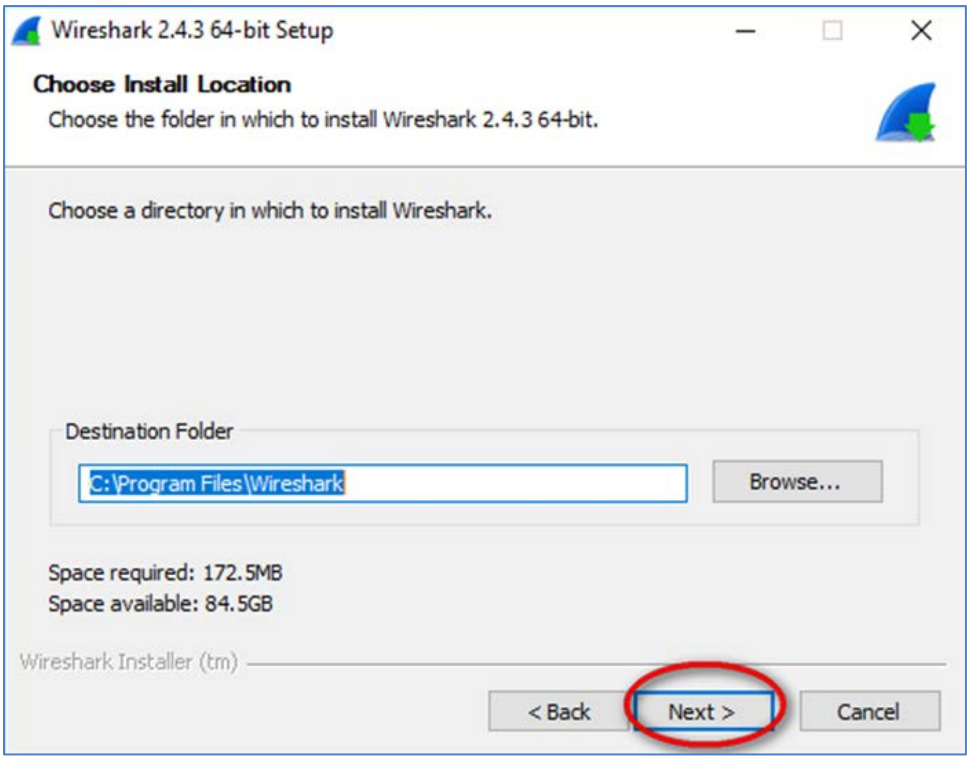

e. Keep the default settings on the **Choose Components** window and click **Next**.



f. Choose your desired shortcut options and click **Next**.

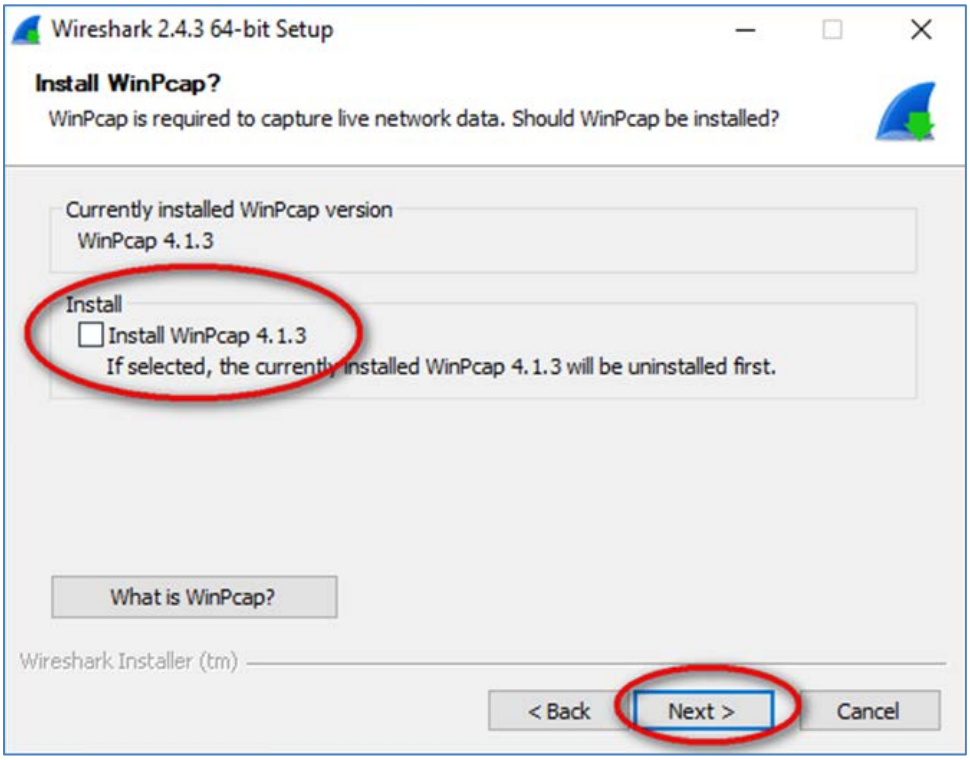



g. You can change the installation location of Wireshark, but unless you have limited disk space, it is recommended that you keep the default location.



h. To capture live network data, WinPcap must be installed on your PC. If WinPcap is already installed on your PC, the **Install** check box will be unchecked. If your installed version of WinPcap is older than the version that comes with Wireshark, it is recommended that you allow the newer version to be installed by clicking the **Install WinPcap x.x.x** (version number) check box.

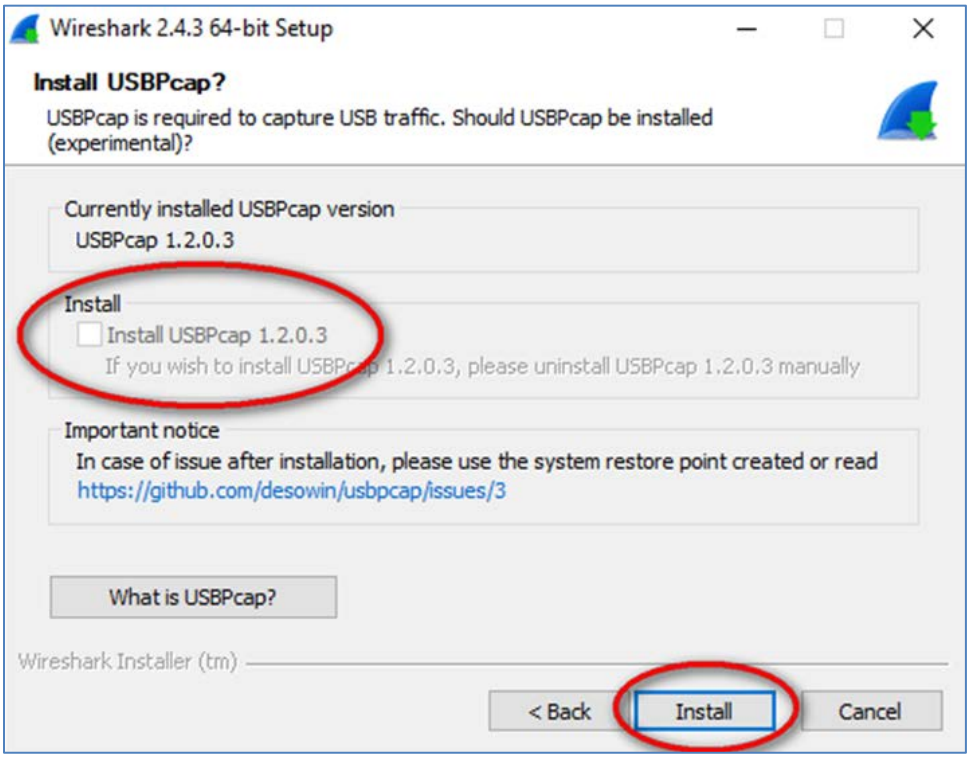
i. Finish the WinPcap Setup Wizard if installing WinPcap.



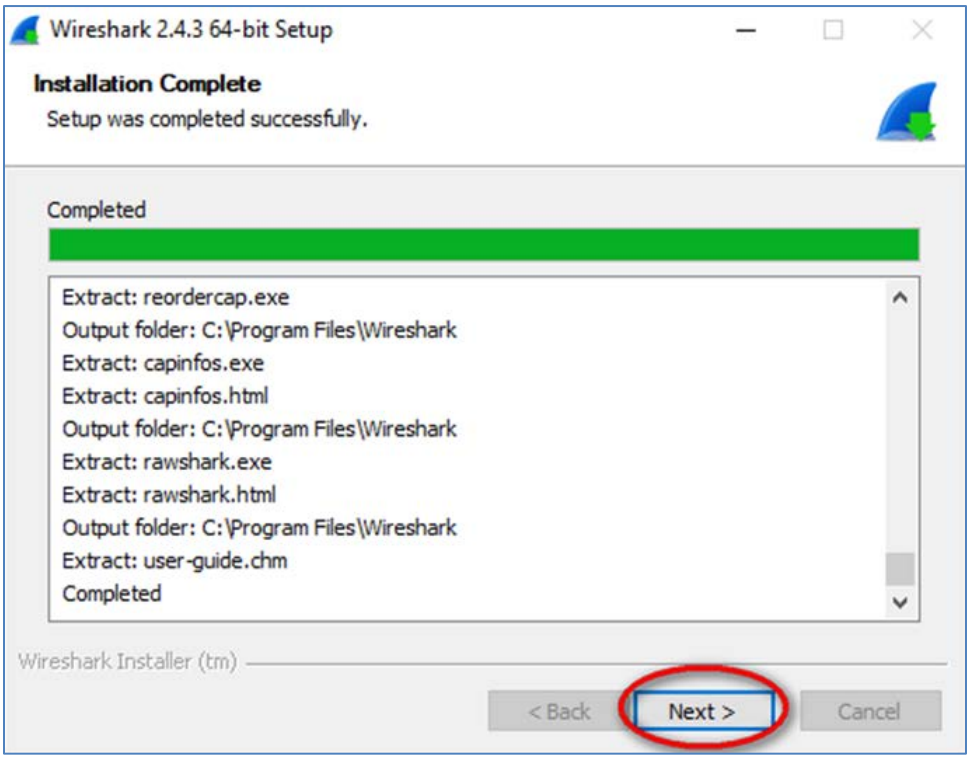

j. In addition, USBPcap can be installed on your PC. If USBPcap is already installed on your PC, the **Install** check box will be unchecked. If your installed version of USBPcap is older than the version that comes with Wireshark, it is recommended that you allow the newer version to be installed by clicking the **Install USBPcap x.x.x** (version number) check box.

**Note**: Because USBcap is still experimental, it is recommended that you **DO NOT** install USBcap unless you need to capture USB traffic.

k. Finish the USBPcap Setup wizard if installing USBPcap.




l. Wireshark starts installing its files and a separate window displays with the status of the installation. Click **Next** when the installation is complete.



m. Click **Finish** to complete the Wireshark install process.

# Part 2: Configuring the Router and Switch for SPAN

## Step 1: Configure the router.

a. Configure the hostname R1 for the router.

```
Router(config)# hostname R1
```

b. Configure the R1 GigabitEthernet0/1 interface with the IP address shown in the diagram.

```
R1(config)# interface g0/1
R1(config-if)# ip address 192.168.10.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# exit
```

c. Configure EIGRP AS 1 with the 192.168.10.0 network in order to generate traffic on the wire.

```
R1(config)# router eigrp 1
R1(config-router)# network 192.168.10.0
```

What kind of packets would you expect R1 to send toward the Fast Ethernet interface on switch S1?

## Step 2: Configuring the Switch for SPAN Monitoring Tool

a. Configure the host name R1 for the switch.

b. On the switch S1, place all the ports in VLAN 1.

c. 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.

```
S1(config)# monitor session 1 source interface fastethernet0/5
S1(config)# monitor session 1 destination interface fastethernet0/6
```

d. 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.

```
S1# show monitor
Session 1
---------
Type              : Local Session
Source Ports      :
    Both          : Fa0/5
```

```
Destination Ports : Fa0/6
    Encapsulation : Native
          Ingress : Disabled
```

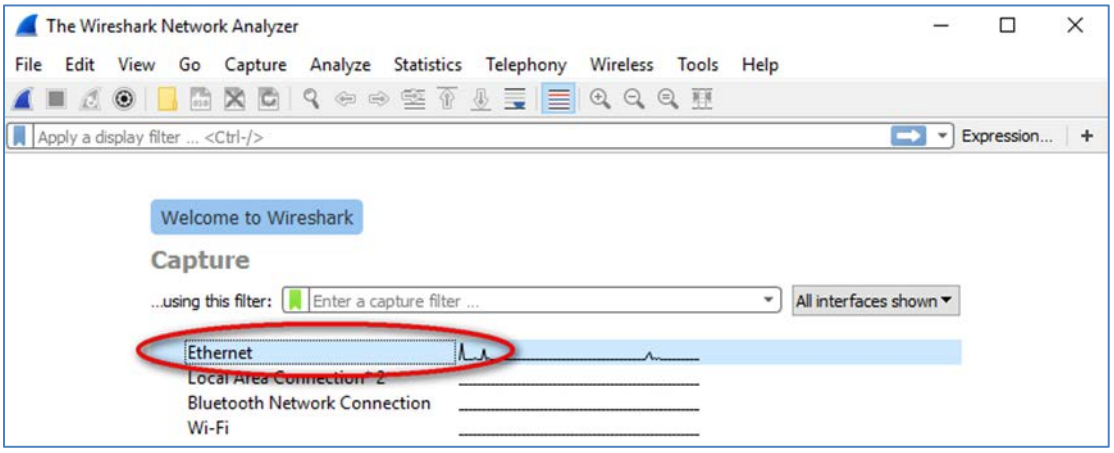
If you had not implemented the following command, would the host still receive the EIGRP hello packets? Explain.

```
S1(config)# monitor session 1 destination interface fastethernet0/6
```

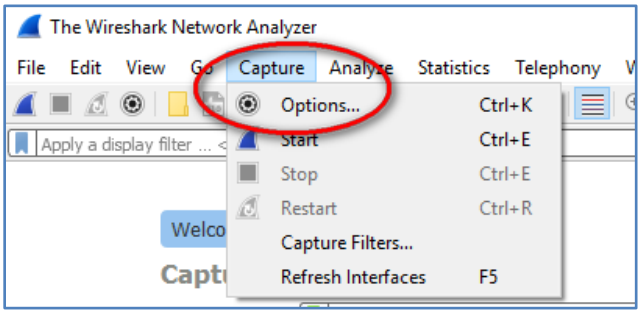
## Step 3: Sniff Packets using Wireshark

a. Change the IP address on PC-A so it is in the same network as the router R1 as necessary.

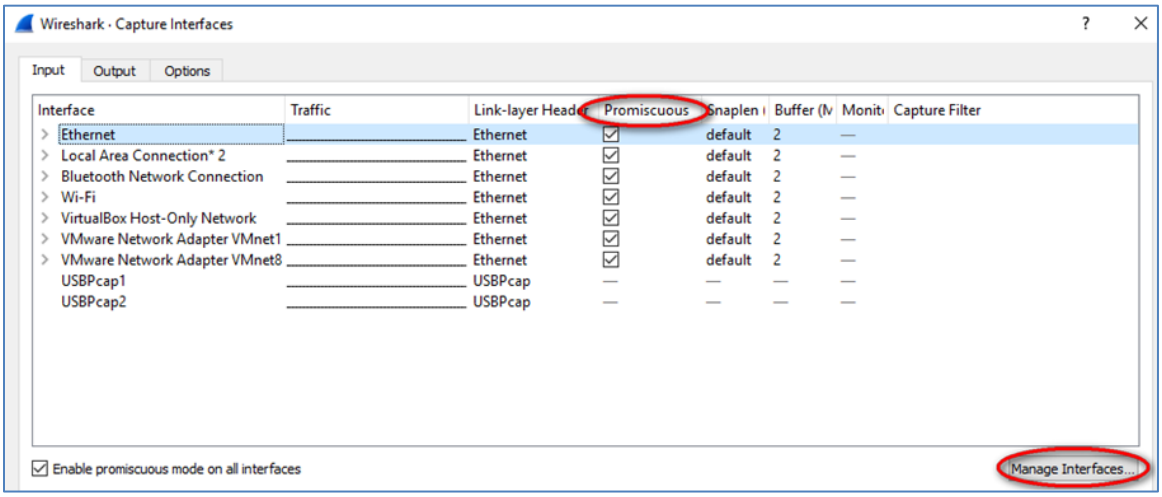
b. Now that the switch is sending SPAN packets to the host, you can show packets generated from R1 in Wireshark. To do this, open Wireshark. It opens with a list of network interfaces on the PC.



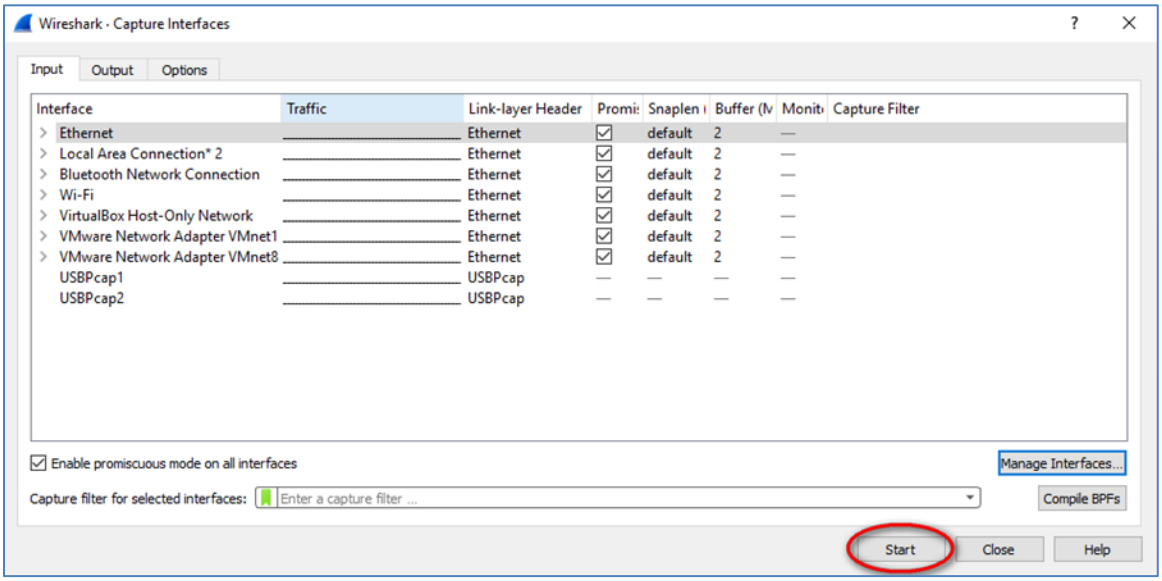

c. You can manage the capture interface by clicking **Capture** and **Options**:



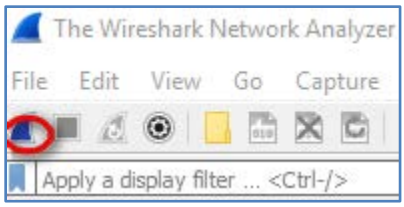
d. A list of interfaces will display. Make sure the capture interface is checked under **Promiscuous**.



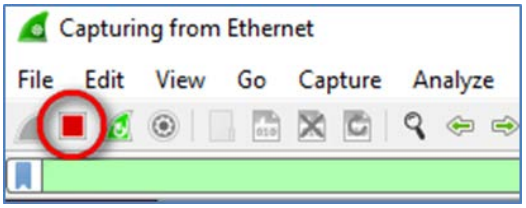

e. Highlight the capture interface and click **Start** to start the data capture.



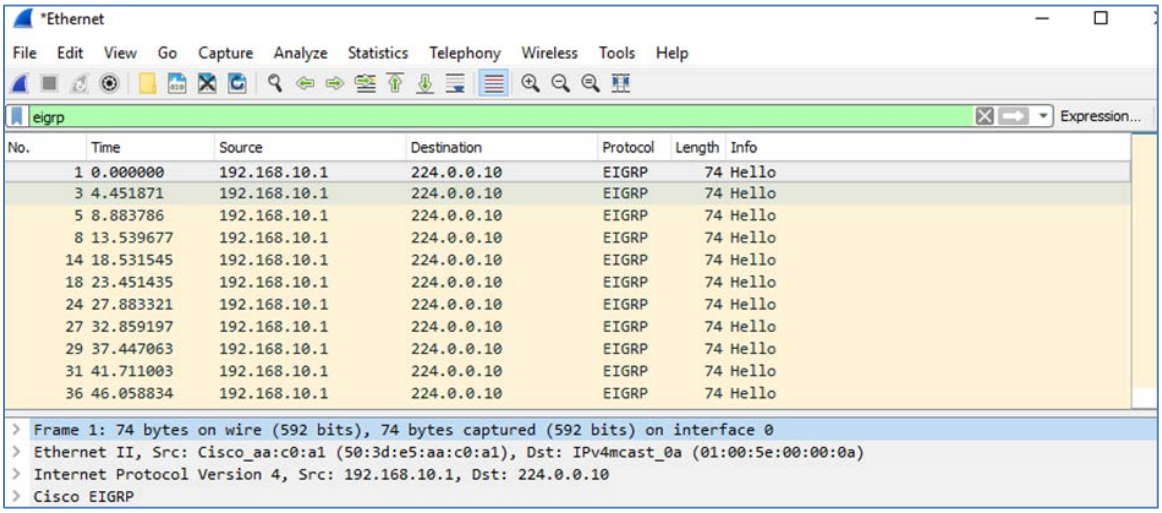

**Note**: You can also start the data capture by clicking the **Wireshark** icon in the main interface.



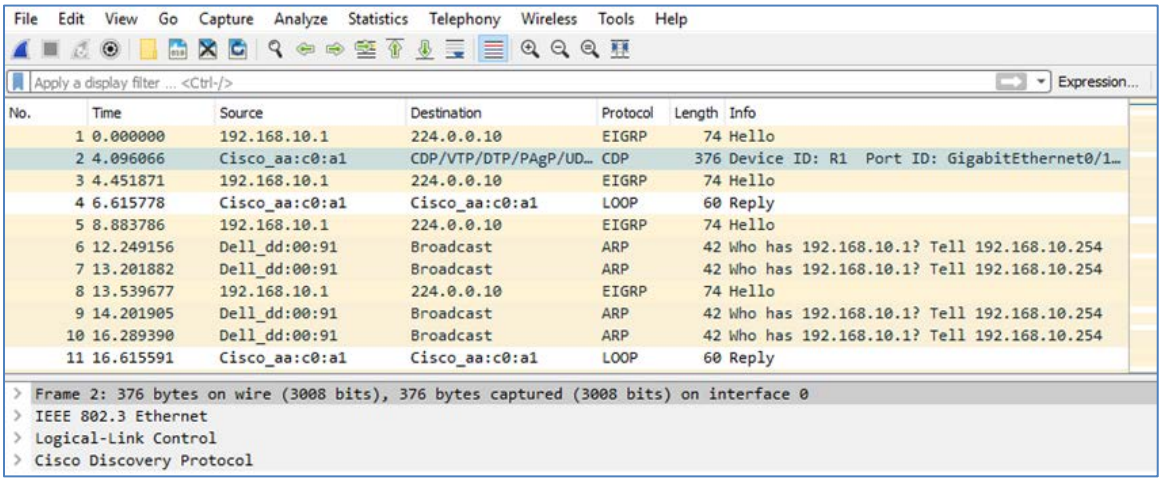
f. When you have sniffed a decent amount of traffic (~30 seconds), click the **Stop Capture** icon.




g. Enter **eigrp** to filter captured packets.


h. Wireshark lists all captured packets. In addition, deeper packet information and a raw readout of the packet are available for the selected packet. Explore the detailed information available for each packet. Note that the EIGRP hello multicasts are sent to the host via the SPAN session.



## Router Interface Summary Table

| Router Interface Summary | | | | |
|---|---|---|---|---|
| **Router Model** | **Ethernet Interface #1** | **Ethernet Interface #2** | **Serial Interface #1** | **Serial Interface #2** |
| 1800 | Fast Ethernet 0/0 (F0/0) | Fast Ethernet 0/1 (F0/1) | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |
| 1900 | Gigabit Ethernet 0/0 (G0/0) | Gigabit Ethernet 0/1 (G0/1) | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |
| 2801 | Fast Ethernet 0/0 (F0/0) | Fast Ethernet 0/1 (F0/1) | Serial 0/1/0 (S0/1/0) | Serial 0/1/1 (S0/1/1) |
| 2811 | Fast Ethernet 0/0 (F0/0) | Fast Ethernet 0/1 (F0/1) | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |
| 2900 | Gigabit Ethernet 0/0 (G0/0) | Gigabit Ethernet 0/1 (G0/1) | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |

**Note**: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.