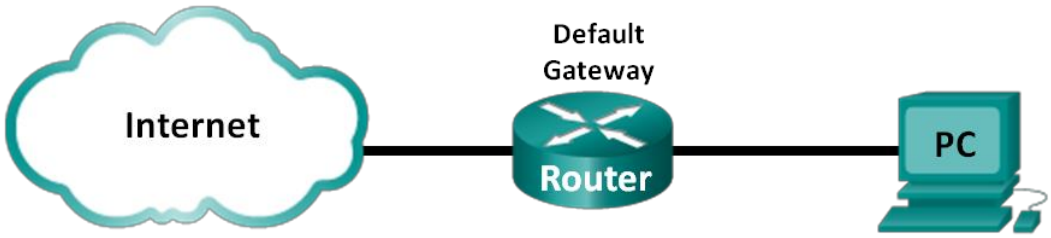
Topology



Background / Scenario

In this lab, you will use Wireshark to capture and examine packets generated between the PC browser using the HyperText Transfer Protocol (HTTP) and a web server, such as www.google.com. When an application, such as HTTP or File Transfer Protocol (FTP) first starts on a host, TCP uses the three-way handshake to establish a reliable TCP session between the two hosts. For example, when a PC uses a web browser to surf the Internet, a three-way handshake is initiated, and a session is established between the PC host and web server. A PC can have multiple, simultaneous, active TCP sessions with various web sites.

Required Resources

1 PC (Windows 7 or 8 with a command prompt access, Internet access, and Wireshark installed)

Part 1: Prepare Wireshark to Capture Packets

In Part 1, you will start the Wireshark program and select the appropriate interface to begin capturing packets.

Step 1: Retrieve the PC interface addresses.

For this lab, you need to retrieve your PC's IP address and its network interface card (NIC) physical address, also called the MAC address.

a. Open a command prompt window, type **ipconfig /all**, and press Enter.

```
Physical Address. . . . . . . . . : 00-1A-73-EA-63-8C
DHCP Enabled. . . . . . . . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::a858:5f3e:35e2:d38f%14(Preferred)
IPv4 Address. . . . . . . . . . . : 192.168.1.130(Preferred)
Subnet Mask . . . . . . . . . . . : 255.255.255.0
```

b. Write down the IP and MAC addresses associated with the selected Ethernet adapter. That is the source address to look for when examining captured packets.

The PC host IP address: 192.168.0.190

The PC host MAC address: 82:23:9d:e3:bc:01

Step 2: Install Wireshark and WinPcap

Part 2: Capture, Locate, and Examine Packets

Step 1: Capture the data.

a. Click the **Start** button to start the data capture.

b. Navigate to www.google.com. Minimize the browser and return to Wireshark. Stop the data capture.

Step 2: Locate appropriate packets for the web session.

a. Find the appropriate packet for the start of your three-way handshake. (Flags: Syn, Syn/Ack, Ack).

What is the IP address of the Google web server? 216.58.213.195

b. Filter tcp

Step 3: Examine the information within packets including IP addresses, TCP port numbers, and TCP control flags.

a. Click the **+** icon to the left of the Transmission Control Protocol in the packet details pane to expand the view of the TCP information.

b. Click the **+** icon to the left of the Flags. Look at the source and destination ports and the flags that are set.

What is the TCP source port number? 11038

How would you classify the source port? dynamic / private /ephermeral port

What is the TCP destination port number? 80

How would you classify the destination port? system or well-known port

Which flag (or flags) is set? Syn

What is the relative sequence number set to? 0

c. Do a. and b. for the whole three-way-handshake.