Shaun Lim
Aldrich Go

Packet Tracer - Investigate the TCP/IP and OSI Models in Action

Objectives

Part 1: Examine HTTP Web Traffic

Part 2: Display Elements of the TCP/IP Protocol Suite

Background

This simulation activity is intended to provide a foundation for understanding the TCP/IP protocol suite and the relationship to the OSI model. Simulation mode allows you to view the data contents being sent across the network at each layer.

As data moves through the network, it is broken down into smaller pieces and identified so that the pieces can be put back together when they arrive at the destination. Each piece is assigned a specific name (protocol data unit [PDU]) and associated with a specific layer of the TCP/IP and OSI models. Packet Tracer simulation mode enables you to view each of the layers and the associated PDU. The following steps lead the user through the process of requesting a web page from a web server by using the web browser application available on a client PC.

Even though much of the information displayed will be discussed in more detail later, this is an opportunity to explore the functionality of Packet Tracer and be able to visualize the encapsulation process.

Instructions

Part 1: Examine HTTP Web Traffic

In Part 1 of this activity, you will use Packet Tracer (PT) Simulation mode to generate web traffic and examine HTTP.

Step 1: Switch from Realtime to Simulation mode.

In the lower right corner of the Packet Tracer interface are buttons that toggle between **Realtime** and **Simulation** mode. PT always starts in **Realtime** mode, in which networking protocols operate with realistic timings. However, a powerful feature of Packet Tracer allows the user to “stop time” by switching to Simulation mode. In Simulation mode, packets are displayed as animated envelopes, time is event driven, and the user can step through networking events.

a. Click the **Simulation** mode icon to switch from **Realtime** mode to **Simulation** mode.

b. Select **HTTP** from the **Event List Filters**.

   1) HTTP may already be the only visible event. If necessary, click the **Edit Filters** button at the bottom of the simulation panel to display the available visible events. Toggle the **Show All/None** check box and notice how the check boxes switch from unchecked to checked or checked to unchecked, depending on the current state.

   2) Click the **Show All/None** check box until all boxes are cleared and then select **HTTP** from the Misc tab of the Edit Filters window. Click the X in the upper right hand corner of the window to close the **Edit Filters** window. The Visible Events should now only display HTTP.

Step 2: Generate web (HTTP) traffic.

Currently the Simulation Panel is empty. There are five columns listed across the top of the Event List within the Simulation Panel. As traffic is generated and stepped through, events appear in the list.

Note: The Web Server and Web Client are displayed in the left pane. The panels can be adjusted in size by hovering next to the scroll bar and dragging left or right when the double-headed arrow appears.

a. Click **Web Client** in the far left pane.

b. Click the **Desktop** tab and click the **Web Browser** icon to open it.

c. In the URL field, enter **www.osi.local** and click **Go**.

Because time in Simulation mode is event-driven, you must use the **Capture/Forward** button to display network events. The capture forward button is located at the left hand side of the blue band that is below the topology window. Of the three buttons there, it is the one on the right.

d. Click **Capture/Forward** four times. There should be four events in the Event List.

Look at the Web Client web browser page. Did anything change?

The web page should've loaded

Step 3: Explore the contents of the HTTP packet.

a. Click the first colored square box under the **Event List** > **Type** column. It may be necessary to expand the **Simulation Panel** or use the scrollbar directly below the **Event List**.

The **PDU Information at Device: Web Client** window displays. In this window, there are only two tabs (**OSI Model** and **Outbound PDU Details**) because this is the start of the transmission. As more events are examined, there will be three tabs displayed, adding a tab for **Inbound PDU Details**. When an event is the last event in the stream of traffic, only the **OSI Model** and **Inbound PDU Details** tabs are displayed.

b. Ensure that the **OSI Model** tab is selected.

Under the **Out Layers** column, click **Layer 7**.

What information is listed in the numbered steps directly below the **In Layers** and **Out Layers** boxes for Layer 7?

1. The HTTP client sends a HTTP request to the server

What is the **Dst Port** value for **Layer 4** under the **Out Layers** column?

80

What is the **Dest. IP** value for **Layer 3** under the **Out Layers** column?

192.168.1.254

What information is displayed at Layer 2 under the **Out Layers** column?

1. The next-hop IP address is a unicast. The ARP process looks it up in the ARP table.

2. The next-hop IP address is in the ARP table. The ARP process sets the frame's destination MAC address to the one found in the table.

3. The device encapsulates the PDU into an Ethernet frame.

c. Click the **Outbound PDU Details** tab.

Information listed under the **PDU Formats** is reflective of the layers within the TCP/IP model.

Note: The information listed under the **Ethernet II** section of the Outbound PDU Details tab provides even more detailed information than is listed under Layer 2 on the **OSI Model** tab. The **Outbound PDU Details** provides more descriptive and detailed information. The values under **DEST MAC** and **SRC MAC** within the **Ethernet II** section of the **PDU Details** appear on the **OSI Model** tab under Layer 2, but are not identified as such.Questions:

What is the common information listed under the **IP** section of **PDU Details** as compared to the information listed under the **OSI Model** tab? With which layer is it associated?

They both show the source IP and destination IP. It is associated with layer 3.

What is the common information listed under the **TCP** section of **PDU Details**, as compared to the information listed under the **OSI Model** tab, and with which layer is it associated?

They both show the source port and destination port. It is associated with layer 4.

What is the **Host** listed under the **HTTP** section of the **PDU Details**? What layer would this information be associated with under the **OSI Model** tab?

The Host is www.osi.local. It is associated with layer 7.

d. Click the next colored square box under the **Event List** > **Type** column. Only Layer 1 is active (not grayed out). The device is moving the frame from the buffer and placing it on to the network.

e. Advance to the next HTTP **Type** box within the **Event List** and click the colored square box. This window contains both **In Layers** and **Out Layers**. Notice the direction of the arrow directly under the **In Layers** column; it is pointing upward, indicating the direction the data is travelling. Scroll through these layers making note of the items previously viewed. At the top of the column the arrow points to the right. This denotes that the server is now sending the information back to the client.

Comparing the information displayed in the **In Layers** column with that of the **Out Layers** column, what are the major differences?

The major difference I can see is the values of the (source IP and destination IP) and the (source MAC address and the destination MAC address) have swapped. (192.168.1.1 and 192.168.1.254 src, and dst respectively becomes 192.168.1.254 for the src and 192.168.1.1 for the dst), same thing happens with the src and dst MAC addresses.

f. Click the **Inbound and Outbound PDU Details** tab. Review the PDU details.

g. Click the last colored square box under the **Info** column.

How many tabs are displayed with this event? Explain.

There are only 2 tabs (OSI and Inbound PDU Details). The web server relays information back to the web client, the web client receives the reply from the web server. There will be no further communication between the web server and web client, so there are only In Layers, which means we get the Inbound PDU Details, but not the Out Layers.

Part 2: Display Elements of the TCP/IP Protocol Suite

In Part 2 of this activity, you will use the Packet Tracer Simulation mode to view and examine some of the other protocols comprising of TCP/IP suite.

Step 1: View Additional Events

a. Close any open PDU information windows.

b. In the **Event List Filters** > **Visible Events** section, click **Show All/None**.

What additional Event Types are displayed?

ARP, BGP, Bluetooth, CAPWAP, CDP, DHCP, DHCPv6, DNS, DTP, EAPOL, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPSec, ISAKMP, IoT, IoT TCP, LACP, LLDP, Meraki, NDP, NETFLOW, NTP, OSPF, OSPFv6, PAgP, POP3, PPP, PPPoED, PTP, RADIUS, REP, RIP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, USB, VTP

These extra entries play various roles within the TCP/IP suite. Address Resolution Protocol (ARP) requests MAC addresses for destination hosts. DNS is responsible for converting a name (for example, **www.osi.local**) to an IP address. The additional TCP events are responsible for connecting, agreeing on communication parameters, and disconnecting the communications sessions between the devices. These protocols have been mentioned previously and will be further discussed as the course progresses. Currently there are over 35 possible protocols (event types) available for capture within Packet Tracer.

c. Click the first DNS event in the **Type** column. Explore the **OSI Model** and **PDU Detail** tabs and note the encapsulation process. As you look at the **OSI Model** tab with **Layer 7** highlighted, a description of what is occurring is listed directly below the **In Layers** and **Out Layers** ("1. The DNS client sends a DNS query to the DNS server."). This is very useful information to help understand what is occurring during the communication process.

d. Click the **Outbound PDU Details** tab.

What information is listed in the **NAME** field: in the DNS QUERY section?

NAME (VARIABLE LENGTH):www.osi.local

e. Click the last DNS **Info** colored square box in the event list.

At which device was the PDU captured?

Web Client

What is the value listed next to **ADDRESS**: in the DNS ANSWER section of the **Inbound PDU Details**?

192.168.1.254

f. Find the first **HTTP** event in the list and click the colored square box of the **TCP** event immediately following this event. Highlight **Layer 4** in the **OSI Model** tab.

In the numbered list directly below the **In Layers** and **Out Layers**, what is the information displayed under items 4 and 5?

1. The device receives a TCP ACK segment on the connection to 192.168.1.1 on port 1025.

2. Received segment information: the sequence number 1, the ACK number 1, and the data length 20.

3. The TCP segment has the expected peer sequence number.

4. The TCP connection is successful.

5. The device sets the connection state to ESTABLISHED.

TCP manages the connecting and disconnecting of the communications channel along with other responsibilities. This particular event shows that the communication channel has been ESTABLISHED.

g. Click the last TCP event. Highlight Layer 4 in the **OSI Model** tab. Examine the steps listed directly below **In Layers** and **Out Layers**.

What is the purpose of this event, based on the information provided in the last item in the list (should be item 4)?

4. The device sets the connection state to CLOSED.

Purpose: The web server closes the connection.

Challenge Questions

This simulation provided an example of a web session between a client and a server on a local area network (LAN). The client makes requests to specific services running on the server. The server must be set up to listen on specific ports for a client request. (Hint: Look at Layer 4 in the **OSI Model** tab for port information.)

Based on the information that was inspected during the Packet Tracer capture, what port number is the **Web Server** listening on for the web request?

Port 80

What port is the **Web Server** listening on for a DNS request?

Port 53