Lab 9: Layer 2, 3, 4 and 7 protocols

What you will do:

Capture, inspect, and understand various PDUs.

Things that you will need to know or learn:

1. Topology of the existing lab infrastructure (i.e., How is everything hooked up?)
2. How the TCP 3-way handshake works and the operation of key fields & flags in the TCP header, i.e. sequence number, acknowledgement number, flags
3. Layer 4 port numbers for the layer 7 applications
4. How to use Wireshark to capture & **filter** network traffic (Skill exercised during lab time)
5. How to identify key fields in a Wireshark capture: IP addresses, port numbers, transport layer header values, and application layer header and data fields. (Skill exercised by lab)

What you need to submit and when:
This lab must be done individually. You can ask your classmates for help if you want to, but be sure YOU understand in the end.

1. Complete the in-lab part of the exercise (see below).
2. Complete the "Lab 9 – Quiz" on BrightSpace before due time.

Required Equipment:
- Laptop
- Linksys Router
- Ethernet Cables
- Access to the Eagle Network

Notes:

- There will be questions based on your **understanding** of this material on your final exam.

- The marks associated with this lab are small. The marks associated with the final exam are large. Rushing through this lab just to get the marks is of NO value to **you**. Actually understanding what you did is of LARGE value to **you**.

- It is your responsibility to use your lab time to explore and learn.

Topology Diagram

This is the Eagle Server network t*opology* or layout. Although it may appear that the two routers serve no real purpose, they are included to provide multiple hops between client & server and allow a greater variety of configuration.

You should become very familiar with this topology so that you don't need to constantly flip back to it. Transcribe the IP addresses from the table below onto the diagram, with an IP address next to each device.
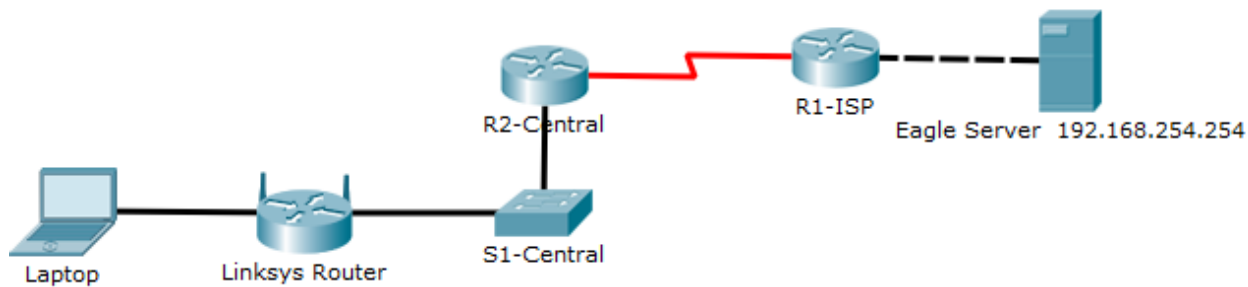
Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1-ISP	S0/0/0	10.10.10.6	255.255.255.252	N/A
	Fa0/0	192.168.254.253	255.255.255.0	N/A
R2-Central	S0/0/0	10.10.10.5	255.255.255.252	N/A
	Fa0/0	172.16.255.254	255.255.0.0	N/A
Eagle Server	Ethernet	192.168.254.254	255.255.255.0	192.168.254.253
PC	Ethernet	192.168.1.x	255.255.255.0	192.168.1.1

Protocols that you will be exploring in this lab:

ARP: Address Resolution Protocol = A Layer 2 protocol that is used to find an unknown MAC address when the IP address is known.

TCP: Transmission Control Protocol = Connection oriented "reliable" layer 4 protocol with flow control and ordered data reconstruction.

UDP: User Datagram Protocol = Connectionless "unreliable" layer 4 protocol with NO flow control or data reconstruction

DNS: Domain Name System = A Layer 7 protocol that is used to resolve host names to IP addresses. Example: www.google.com = 173.194.43.82

HTTP: Hypertext Transfer Protocol = Layer 7 protocol that transfers files that make up the web pages of the World Wide Web.

DHCP: Dynamic Host Configuration Protocol = A layer 7 protocol used to automatically assign an IP address, subnet mask, default gateway, and DNS server addresses to a host.

READ ALL OF THE INSTRUCTIONS FOR EACH TASK BEFORE STARTING THE TASK

This lab is divided into two sections. First you will get the required Wireshark captures. Once you have them all, you will then go back and examine the captures. You are doing this so you can explore the captures on your own laptop if you run out of time.

PART 0 – Preparation

Task 0: Preparation Tasks

1. Download this document to your laptop.
2. Disable your wireless network adapter.
3. Disable your firewall.
4. Reset your Linksys router to factory defaults
5. Connect your laptop to one of your router's Ethernet port
6. Connect your router's Internet port to the Eagle Network (red RJ45 jack).
7. Make sure your Laptop has a valid IP address from your Linksys router (192.168.1.0/24)
8. Make sure your router's Internet Network Adapter has a valid IP address from the red network (172.16.0.0/16).

PART I – Capture the required traffic

Task 0: Configure Linksys Router

1. By default most SOHO routers act as their LAN's DNS server. For this lab we need to change that. **Login to the router and on the "Basic Setup" page locate the "Static DNS 1" fields. Change this to 192.168.254.254.**
2. Save the settings
3. Release and renew you PC's IP address. Confirm that (using ipconfig /all) you now have 192.168.254.254 as your first DNS server address
4. Open a command prompt and clear your DNS entries by typing **ipconfig /flushdns**. You are doing this to force your PC to make a DNS query.
5. Type **ipconfig /displaydns** to show your DNS entries. As you just flushed the DNS entries, there should be none.
6. Ping eagle-server (by the host name, not by IP address) **ping eagle-server.example.com**
7. Type **ipconfig /displaydns** to show your DNS entries again. As you just used ICMP to test your connection to the eagle-server using the host name rather than the IP address, you should now see a DNS entry for the eagle-server. Look for "A (Host) Record"

Task 1: Capture ARP and DNS Operations using Wireshark

1. Create batch file that will flush your DNS cache and then ping the Eagle-Server by its hostname.

Suggested batch file:

arp –d *	*(clears ARP cache)*
ipconfig /flushdns	*(clears DNS cache)*
arp -a	*(views ARP cache is clear)*
ipconfig /displaydns	*(views DNS cache is clear)*
ping eagle-server.exa…….	*(pings eagle server by name)*
arp -a	*(views new ARP cache entry)*
ipconfig /displaydns	*(views new DNS cache entry)*
pause	*(READ THE OUTPUT)*

Note: don't cut and paste this,
type it out

2.   Start a new Wireshark capture.

3.   With the Wireshark capture running, run your batch file.

4.   Stop the Wireshark capture and **save your captured data** as: **Lab9-1-ARP-and-DNS.pcap**.

5.   Take a moment to look over the output that resulted from running the batch file. Make sure there were no errors. Does the output make sense?

6.   Open your capture file and filter to show only ARP and DNS traffic (arp || dns).

6.1. Can you see **your** ARP request and the corresponding reply?

6.2. Can you see **your** DNS query and the corresponding reply?

If you see the above information, close your capture and continue. Otherwise, repeat the task. Ask for help if you need to.

Task 2: Capture HTTP traffic

1.   Start another (new) Wireshark capture.

2.   AFTER starting a new Wireshark capture, use a web browser to connect to **http://eagle-server.example.com**

3.   Navigate to a second web page by entering the following URL:
http://eagle-server.example.com/page2.html

4.   <u>Close the web browser,</u> then stop the Wireshark capture. Save your capture data as **Lab9-2 HTTP.pcap.**

5.   Open your saved capture.

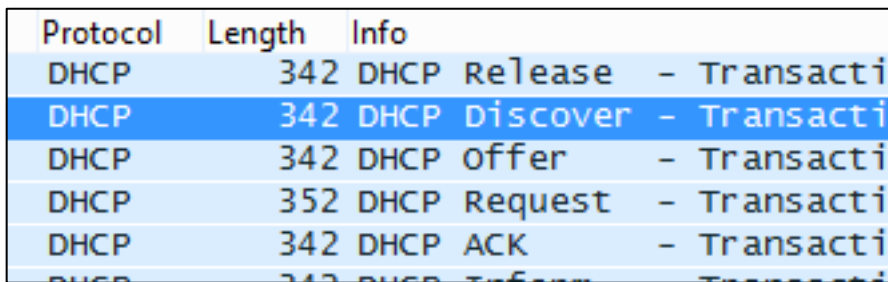5.1. Filter to show the captured http traffic. If your capture was successful, you should see:

Protocol	Info
HTTP	GET / HTTP/1.1
HTTP	HTTP/1.1 200 OK (text/html)

IF you don't see this, **clear your browser's cache** and repeat the steps. Be sure to start the capture before you load the web page.

5.2. If you see the http Packets above, close your capture and continue. Otherwise, repeat the task. Ask for help if you need to. *Remember, you need to clear the browser's cache before you try again. Otherwise the webpage will be cached on your PC and you will not capture the required http traffic.*

Task 3: Capture a DHCP exchange

1. Still using the Eagle Server network, start another (new) Wireshark capture.

2. With your Wireshark capture running, <u>release and renew</u> your IP Address. (2 commands) You should do this with a batch file as well. Your capture will be cleaner.

3. Stop the Wireshark capture. Save your capture data as **Lab9-3 DHCP.pcap**.

4. Filter for "**bootp**" and examine what was captured. You should see (at least) a DHCP Discover, Offer, Request and Acknowledgement.

Protocol	Length	Info
DHCP	342	DHCP Release - Transacti
DHCP	342	DHCP Discover - Transacti
DHCP	342	DHCP Offer - Transacti
DHCP	352	DHCP Request - Transacti
DHCP	342	DHCP ACK - Transacti

5. If you see the DHCP Packets, close your capture and continue. Otherwise, repeat the task. Ask for help if you need to.

PART II – Inspect the captured traffic

Inspect your captured ARP & DNS traffic

1. Open your ARP and DNS capture file and filter to show only ARP and DNS traffic.

- Why did pinging the Eagle Server allow you to capture both ARP and DNS packets?
- Identify <u>**your**</u> ARP REQUEST and ARP REPLY
- Identify the DNS QUERY
    - o Identify the source port
    - o Identify the destination port
    - o Does the layer 7 DNS protocol use TCP or UDP at layer 4?
- Identify the DNS RESPONSE
    - o Identify the source port

o   Identify the destination port
- How was the source port chosen on the client? (It's in the textbook)
- How was the destination port chosen on the server? (It's in the textbook)
- What is the name of the DNS server that responded? (Expand the DNS response and read it)

Inspect your captured HTTP traffic

1. Open your HTTP capture file and filter for the layer 7 protocol, http.
   - Which layer 4 protocol is used for http?

2. Change your filter so you see both http and the correct layer 4 traffic.

- Identify the 3 packets used for the 3-way handshake.
    o   Can you find the flags that are set for each stage of the process?
    o   Which flags are set for each stage?

- Can you find the packet where you requested the 1ˢᵗ web page? (GET /)
    o   What were the source and destination ports?
    o   Can you explain why these ports were used?

- Can you find the acknowledgement for that packet?
    o   What were the source and destination ports?
    o   Was the acknowledgment sent by the layer 4 or the layer 7 protocol?

- Can you find the packet where you requested the 2nd web page? (GET /page2.html)
    o   What were the source and destination ports?
    o   Did the client use the same source port as it did for the 1ˢᵗ web page?
    o   Is this the same layer 4 sessions, or a different one?

Inspect your captured DHCP traffic (Optional)

1. Open your DHCP capture file and filter for bootp

   - Can you figure out why you filtered for bootp rather than dhcp?
   - What is the source layer **2** address in the DHCP discover packet?

   - What is the destination layer **2** address in the DHCP discover packet?
     - What type of address is this? (Unicast / Multicast / Broadcast?)
     - Why did your PC use that destination layer 2 address in the request?
       (Think… Does your PC know the address of the DHCP server?)

   - What is the source layer **3** address in the DHCP discover packet?
     - Why did your PC use that as the source layer 3 address in the request?

   - What is the destination layer 3 address in the DHCP discover packet?
     - What type of address is this? (Unicast / Multicast / Broadcast?)
     - Why did your PC use that as the destination layer 3 address in the request?

   - Can you find the IP address that the server offered you in the DHCP offer packet?

When you get an IP address from a DHCP server, you get it for a certain amount of time. This is called a lease. Essentially, you borrow your IP address for a certain amount of time before you have to renew it. If the lease expires before you renew it, you could lose that IP address to another PC…

   - How long is the lease that your PC was offered?
   - How long will your PC wait until it renews the lease?
   - Does it wait until the lease expires to renew?
   - What other information is being offered in the lease? (explore)

Please demo to your instructor.

You will need your capture files for the Lab9 Quiz.
     Lab9-1 ARP and DNS.pcap
     Lab9-2 HTTP.pcap
     Lab9-3 DHCP.pcap
     Lab9-Answer-Sheet.docx

PART III – Clean up and Lab Quiz

1. Make sure you saved all the results you got during this lab period.
2. Re-enable Firewalls, Anti-virus, Wireless, etc.
3. Return all the equipment.
4. Complete "Lab 9 – Quiz" before your next scheduled lab period.