ECSE 308:
Introduction to
Communication Systems and Networks

L4:

Part 1: Internet Protocol (IP)

Part 2: Domain Name System (DNS)

Part 3: User Datagram Protocol (UDP)

Part 1: Internet Protocol (IP)

- The Internet Protocol (IP), is used to route packets from source to destination based on logical (IP) addresses.
- One of the tools that can be used to get better understanding of how this protocol works is tracert.
- The tracert utility in Windows is a client-server program that sends ICMP echo messages encapsulated in IP packets with TTL values 1,2,3, and so on.
- When a router receives one of these packets, it decrements the value of TTL field by one and if this value reaches zeros, it transmits an ICMP message (type 11 – TTLexceeded) to the sending host.
- Thus, the packet with TTL i leads the router on i hop away from the host to transmit an ICMP message back to the sender.
- As a result, by receiving these ICMP messages, the tracert learns the identities of the routers between the host and the destination.

  - Use nslookup to find the IP address of the default DNS
  - Open up the Wireshark.
  - Start Packet Capture.
  - Run Command Prompt and type:
  - *tracert –d DNS IP*
  - The –d option prevents *tracert* from resolving the IP addresses to their names.
  - Go back to the Wireshark and stop packet capture.
  - In the filter field, type *icmp* and click apply.

1. *How many ICMP packets are in the list plane?*
2. *How many probe packets are sent from the source to the destination for each TTL?*
3. *The last few echo-request ICMP packets are followed by the echo-reply ICMP packets. Compare one of them with the corresponding reply. Determine which fields are similar and which fields are different? Explain the reason.*
4. *What are the TTL values for these last few packets? Determine the number of routers between the source and destination based on these TTL values.*
5. *Examine the IP packet header of the last echo-request ICMP packet, what is the value in the "Protocol" field? What does this field indicate?*

6. *How many bytes are in this IP header? How many bytes are in the payload of this IP packet? Explain how you determined the number of payload bytes.*
7. *Has this IP packet been fragmented? Explain how you determined whether or not the packet has been fragmented.*

Part 2: Domain Name System (DNS)

- The DNS translates hostnames to IP addresses needed for locating and identifying computer services and devices with the underlying network protocols.
- The client's role in the DNS is relatively simple; a client sends a query to its local DNS server. If the local DNS server can resolve query by using locally cached information, the query is answered and the process is completed. Otherwise, the resolution process continues with the client querying a DNS server to resolve the name.
- **ipconfig:** *ipconfig* (for Windows) and *ifconfig* (for Linux/Unix) are among the most useful little utilities in your host, especially for debugging network issues. Here we will only describe ipconfig, although the Linux/Unix *ifconfig* is very similar. *ipconfig* can be used to show your current TCP/IP information, including your address, DNS server addresses, adapter type and so on.
- **Running ipconfig:**
    - Windows: open the Command Prompt and run ipconfig on the command line.
    - Linux/Unix: type the *ifconfig* command on the command line.
- ipconfig /all
    - Displays all current TCP/IP network configuration values
- ipconfig /displaydns
- A host can cache DNS records it recently obtained. To see these cached records, we can use this command. Each entry shows the remaining Time to Live (TTL) in seconds.
- ipconfig /flushdns
    - This command clears all entries of the DNS cache and reloads the entries from the hosts file.
- nslookup
    - This tool allows the user to query any specified DNS server for a DNS record.
    - To accomplish this task, nslookup sends a DNS query to the specified DNS server, receives a DNS reply from that same DNS server, and displays the result.
- Running nslookup:

    - Windows: open the Command Prompt and run nslookup on the command line.
    - Linux/Unix: just type the nslookup command on the command line.
- nslookup
    - This command identifies which DNS server the computer is currently configured to use for its DNS lookups.
- nslookup "hostname"
    - This command provides two pieces of information: (1) the name and IP address of the DNS server that provides the answer; and (2) the answer itself, which is the host name and IP address of "hostname".
- nslookup –type=NS "hostname"
    - This command specifies a DNS name server for the given hostname.
- nslookup "hostname" "dns server"
    - This command indicates that the query should be sent to the given DNS server rather than to the default DNS server.
- nslookup –option1 –option2 "hostname" "dns-server"
    - This is the general syntax of nslookup commands. As we have seen in the above, nslookup can be run with zero, one, two or more options. Furthermore, the dnsserver is optional as well; if it is not given, the query is sent to the default local DNS server.

8. Use *nslookup* to determine the IP address of www.cbc.ca. What is the IP address of this web server?
9. Use *nslookup* to determine the authoritative DNS servers for McGill.ca.

    - Start packet capture.
    - Run Command Prompt and enter the command:
    - nslookup www.ieee.org
    - Stop packet capture.

10. What are the destination port number for the DNS query message and the source port number of the DNS response message?
11. What is the destination IP address of the DNS query? Is this the IP address of your default local DNS server?
12. Examine the DNS query. What is the "Type" of the DNS query? What does

this “Type” mean?

13. Which bit in the “Flags” field indicates that the message is a query or a response?
14. Which field of the response message contains the IP address of www.ieee.org?
15. Provide a screenshot.
    - Start packet capture.
    - Run Command Prompt and enter the command:
    - nslookup –type=NS www.wireshark.org
    - Stop packet capture.
16. What is the destination IP address of the DNS query? What does this address correspond to?
17. Determine the “Type” of DNS query. What is the authoritative name server of www.wireshark.org. What is the role of an authoritative name server?
18. Provide a screenshot.

Part 3: User Datagram Protocol (UDP)

- Use ipconfig to clear the DNS cache in your host.
- Open your browser and clear your browser cache. (In Chrome/At the top right, click More /Click More tools /Clear browsing data./At the top, choose a time range. To delete everything, select All time./Next to "Cookies and other site data" and "Cached images and files," check the boxes/Click Clear data.)
- Use ipconfig to obtain your IP address.
- Open up the Wireshark and enter "ip.addr == your_IP_address" into the filter. This filter removes all packets that neither originate nor are destined to your host.
- Open up the Wireshark and start packet capture.
- With your browser, visit the Web page: http://www.ietf.org
- Stop packet capture.
- Hint: ip.addr == 132.206.42.35 && udp

19. What transport layer protocol is used to transfer the DNS query and the response message?
20. To setup the connection, how many UDP datagrams are exchanged between your computer and the server? Explain your answer.
21. Select the first DNS packet in your trace. From this packet, determine the header fields of UDP.
22. By consulting the displayed information in Wireshark's packet content field for the first DNS message, determine the length (in bytes) of each of the UDP header fields.
23. The value in the Length field indicates the length of what? Verify your claim with your captured UDP packet.
24. What is the maximum number of bytes that can be included in a UDP payload? (Hint: the answer to this question can be determined by your previous answer)
25. What is the largest possible source port number?
26. Determine whether a checksum is provided for the first DNS message or not. What is the usage of this field?
27. Determine the destination port number for the DNS query message and the source port number of the DNS response. What is the relationship between the two? Which port number is a well-known port number?
28. List two other well-known port numbers used by UDP.
29. Determine the IP address of your local DNS server (use ipconfig). Is it the same as destination IP address of the DNS query?

30. Examine the DNS response message. How many “answers” are provided in this message? What do each of these answers contain?
31. By checking the trace, determine whether UDP is a reliable protocol or not.
32. Explain your answer.
33. Why does DNS use UDP services?