SE331: Introduction to Computer Networks **Recitation 12**
Semester 1 5785 **29 Jan 22025**
Lecturer: Michael J. May **Kinneret College**

ICMP, ARP, DHCP, DNS

1 ICMP Demonstration

We'll use `tracert`, `mtr`, and `ping` to see how ICMP messages work.

Try the following operations with Wireshark running:

- `ping www.google.co.il`
- `ping www.luc.edu`
- `tracert www.google.co.il`
- `tracert www.luc.edu`
- `mtr www.google.co.il`
- `mtr www.luc.edu`

Find the ping packets in the first two pings. What data are in the packets?

Find out how `tracert` works. Why are there so many ICMP packets sent as part of the tracing procedure?

2 ARP Demonstration

We will the recitation session with a short demonstration of ARP. The demonstration will be done using the Wireshark packet sniffer tool on the Kinneret wireless network. I will show the students how my laptop sent out ARP packets toward the default gateway and how it responded to ARP queries to itself.

Steps to be done today:

- Show the `arp` program which Windows has to let them see the ARP cache maintained by their machines.
- We'll run the following commands in Windows:
  - arp -a
- Use the Wireshark sniffer tool to guide the students through the trace.

3 DHCP

Let's analyze a DHCP recording to get a better idea of how the protocol steps work as described in class. Open the DHCP.pcapng file that can be found on Moodle. Answer the following questions about the trace.

3.1 DHCP Discover

1. Find the DHCP Discover packet. Who is the packet's sender? How can you identify the sender? What identifiers does the sender put in?
2. What is the transaction ID for the request?
3. What information is the sender asking for? (Hint: Look at the Parameter Request List).

4. Who is the recipient of the DHCP Discover packet? Why?
5. Based on all of this, what can you conclude is the purpose of the DHCP Discover packet?

3.2 DHCP Offer

6. Find the DHCP Offer message in the trace. Who sends it? Who is the recipient?
7. Which fields would help the intended recipient of the Offer message to identify that it's for them?
8. What IP address does the Offer message offer? How long is the address given for?
9. There are two fields in the Offer - Renewal Time Value and Rebinding Time Value. What values do they have? What are they used for?

   (Hint: Look at RFC 2131 section 4.4.5 for details: `https://datatracker.ietf.org/doc/html/rfc2131#section-4.4.5`)
10. What responses does the Offer give for the information requested by in the DHCP Discover message?

3.3 DHCP Request

11. Find the first DHCP Request message (time 2.109). Who sends the message? Who receives the message?
12. What fields are different between the Request Message and the Discover message? Where do the new values come from?

3.4 DHCP ACK

13. Find the first DHCP ACK message (time 2.141). Who sends the message? Who receives the message?

3.5 DHCP Renewal

14. Find the DHCP Request message at time 59.195. Who sends the message? Who receives the message?
15. Based on the timing of the message, why did the sender not send the Request message directly to the original server?
16. Which IP address is the client requesting?
17. Find the DHCP ACK message at time 59.258. Who sends the message? Who receives it?

3.6 DHCP Renewal Take 2

18. Find the DHCP Request message at time 90.305. Who sends the message? Who receives the message?
19. How does this request differ from the request at 59.195? What is the reason for the difference?

4 DNS

The next part of the recitation will be done using DNS and `nslookup`. Steps to be done today:

1. Review the concepts of a "name server", a "zone", and a "name"
2. Make it clear that a name server is a server responsible for mapping the names in a zone to IP addresses
3. Name servers can also answer questions about names not in the their zone, but they may not be 100% certain about them

4. Use the `nslookup` tool to discover the name servers responsible for `www.illinois.edu`. There are four of them. The `-type=NS` option will tell you which name servers are responsible for the names in `illinois.edu`.
5. Use `nslookup` to ask for the IP address of `www.illinois.edu` without specifying any particular name server. The response will be from the Kinneret name server will include the line "non-authoritative response".
   - It implies that the response did not come from the name server responsible for `www.illinois.edu`, but rather from some other name server (perhaps a cache somewhere on the way).
6. Use `nslookup` to ask one of the `illinois.edu` name servers for the IP address for `www.illinois.edu`. The response should not include the "non-authoritative" line.
7. Go through a similar series of steps for the Kinneret network.
8. Try the above steps for the domain `mit.edu` and the website `www.mit.edu`. You will find that the results are quite different. Look for the phrase `akam` in the name servers - that's a sign that the website is hosted by the content distribution network (CDN) called "Akamai". You can learn more about the CDN at `https://www.akamai.com/`.

Next we will look at the DNS cache for the computer. Run the following commands in Windows:

- ipconfig /displaydns
- ipconfig /flushdns
- After flushing, we'll surf to a web site and then rerun the displaydns command to see the difference.

5 nslookup

`nslookup` is an older tool used for DNS lookup. It's a DNS client program found in Windows and Linux. As a review of using `nslookup`, let's perform the following steps.

1. Use `nslookup` to find the IP addresses of `www.illinois.edu`. What is it?
2. In the previous query, you used `nslookup` to ask for the IP address of `www.illinois.edu` without specifying any particular name server. Notice that the response included the line "non-authoritative response". Who responded to the query? Why does the response include a warning that it's not authoritative?
3. Use `nslookup` tool to discover the name servers responsible for `www.illinois.edu`. There are 3 of them. Use the `-type=NS` option to request name server responses. Write down the name server names and IP addresses.
4. Use `nslookup` to ask one of the `illinois.edu` name servers for the IP address for `www.illinois.edu`. The response should not include the "non-authoritative" line.
5. Try the above steps for the domain `mit.edu` and the website `www.mit.edu`. Why are the domains and IP addresses so different for the two domains?

6 About dig

`dig` is a Linux based tool which lets you perform a bunch of operations on DNS servers which are more complicated to do using `nslookup`. We'll perform the following operations using `dig` in class and see what the results are:

1. `dig`

2. `dig kinneret.ac.il`
3. Open the URL `https://apps.db.ripe.net/db-web-ui/#/query?searchtext=88.218.117.88` and see who is in charge of 88.218.117.88
4. `dig my.kinneret.ac.il`
5. Open the URL `https://whois.arin.net/rest/net/NET-104-16-0-0-1/pft?s=104.22.3.77` and see who is in charge of 104.22.3.77
6. `dig +short my.kinneret.ac.il`
7. `dig kinneret.ac.il ns`
8. `dig +short kinneret.ac.il ns`
9. `dig +trace kinneret.ac.il`
10. `dig 52.112.150.212.in-addr.arpa`
11. `dig 88.117.218.88.in-addr.arpa`