Active Class 3: It's always DNS, No It's 192.168.1.2

The learning objective of this class activity is to learn more about domain name system (DNS).

At the end of this activity, you should be able to:

1. Explain the operation of DNS.
2. Analyse DNS via Wireshark
3. Query DNS records using command line tool

This class activity is designed to be worked through active participation and collaborating with peers under the guidance of the teaching team in the class. The active classes are designed to be interactive, and they are here for you to extend your learning. However, these classes will only help you to enhance your learning if you come prepared. **To work on the class activities, you will be expected to have completed the Introduction module (Module 1) and the Application layer module (Module 2).** You need to have a basic understanding of layered model and application layer protocols including HTTP and DNS. If you are not familiar with any of the above, please head to the Module and 1 &2 in the CloudDeakin unit site and complete it before starting this active class.

The active classes are related to assessment tasks on OnTrack. After learning about different concepts from the content provided in the unit site, you will expand on this knowledge by working on activities designed to put these concepts in practice during the active classes and submit the completed task to OnTrack in the same week. The teaching team will guide and support your learning during these activities. This will help you manage your time and tasks better to avoid tasks piling up towards the deadlines. If you do not complete these activities in class, you will need to work on them in your own time, with limited support from us available.

The class activities are split into two parts. First, you will conduct a group discussion and a role play to understand the role and the process of DNS. Then, you will use the nslookup and Wireshark to analyse the DNS protocol.

Activity 1:

This activity is a group activity. Therefore, you need to form a group of four people. At your table (or in MS team chat) discuss the following questions and activities with your group members. Remember to take notes as they will help you prepare your task submissions.

1. What is the core Internet function provided by DNS?
2. Why do we need DNS?
3. What is the layer that DNS belong to?
4. Do you think a single DNS server is enough to support the entire network? Justify your answer. Provide alternate solution if we have any.

5. Discuss the steps involved in your browser to send a HTTP request message to the Web server, deakin.edu.au. Assume that this is the first time you access this webpage. You can continue the discussion as a role play.
    a. One group member can act as the web server, another as DNS servers (you need to decide how many DNS serves will be involved), and the remaining members can be the clients.
    b. First, Client 1 needs to view deakin.edu.au and initiate the conversation saying the right message to the right device (to the person who is acting as the right device). Use your knowledge about web browsing that we covered in Module 1 and the first part of Module 2. Assume that there is no DNS caching available.
    c. All the devices need to respond to each other with the correct messages in the right sequence. Make sure you record all the steps as you will need those notes to complete the activity 2.
    d. Now, after Client 1 accessed deakin.edu.au, Client 2 also needs to view deakin.edu.au. Discuss the steps involved in Client 2's web browser to be able to send a HTTP request message to the Web server.
    e. You can show all the steps in a timing diagram with the end systems and numbering the sequence of steps (similar to the activity you did in Active Class 1).

Actiivity2:

This is a group activity. Each group member can use a webserver from different continent (Example: cam.ac.uk from United Kingdom and universitystudy.ca from Canada) for the activity and compare the results.

1. You can send a DNS query message directly to some DNS servers. For this, we use "nslookup".
2. First use "nslookup" in command prompt in Windows or terminal in MacOS to identify the IP address of a Web server deakin.edu.au (in Australia). Note down the webserver and the IP address of that server.
3. What are the answers you received from nslookup?
4. What are the authoritative and non-authoritative answers?
5. Use nslookup to identify the authoritative DNS servers for a webserver of a university in USA.
6. Compare the answers in 2 and 5.
7. Let's trace DNS in Wireshark now. First,
    a. Use ipconfig in your command prompt/ terminal to empty the DNS cache in your host ipconfig /flushdns. (MacOS Mojave use: sudo killall -HUP mDNSResponder)
    b. Open google chrome and empty your browser cache.

c. Open Wireshark and start packet capture. Then, visit the Web page: http://www.discoverourtown.com in your browser and stop packet capture.

8. Now you are ready to analyze what you captured in Wireshark and explore more about DNS. Use the following questions as a guide for your analysis.
    a. Find the DNS query and response messages. Which transport layer protocol they have used? UDP or TCP?
    b. What are the destination port of the DNS query message and the source port of DNS response message?
    c. What is the IP address that the DNS query message was sent?
    d. Identify the IP address of your local DNS server using the terminal/command prompt. Are these two IP addresses identified in c and d the same?
    e. You can further explore the DNS query message. Can you identify the "Type" of DNS query? What does the query message contain?
    f. You can further explore the DNS response message. Can you identify the "Type" of DNS response?
    g. Are there any "answers" in the response message? If so, what are these answers?
    h. The web page that you have accessed contains a couple of images. Does the host request new DNS queries to access each image? Explain your answer.

Above and Beyond Tasks:

Those who are targeting for Credit and above can complete the following task as part of Task 4.1C and 5.2D to demonstrate your deeper understanding on the application layer.

- Explain E-mail (another popular application)
    - What is the principal application layer protocol used in e-mails?
    - What is the underlaying architecture and transport layer protocol used in e-mail application layer protocol?
    - Can you list down the basic steps involve in sending an e-mail from user A to B?