Active class 9: Data-link Layer

The learning objective of this class is to learn about how the networks provide multiple access to multiple users over a shared channel, Address Resolution Protocol (ARP), and switches' Medium Access Control (MAC) address table.

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

1. Describe the data-link layer mechanisms that enable multiple users to access the network simultaneously: Link access
2. Explain and analyse the use of ARP and MAC address tables.

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 all the modules in the unit except the last module, i.e., Physical layer and connection module.** You need to have a good understanding of Data-Link Layer. If you are not familiar with any of the above, please head to 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 into 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.

To carry out the class activities, you need to form a group of four people. The class activities are split into three parts. First, you will conduct a role play to understand the use of medium access protocol. Then, you will use Cisco Packet Tracer to analyse the operation of ARP, ARP table and MAC table.

Activity 1: Investigating Multiple Access Control Protocols

We use different medium access protocols in the data link layer to enable packet transmission in a link with a given shared medium. We use WiFi on daily basis. In WiFi, we have a shared medium (wireless) to send packets that are generating in the host devices and to receive packets.

1. Let's do a small role play to understand the MAC protocol. Assume that your group forms a Wireless LAN (WLAN) that uses Wi-Fi technology (has a wireless access point (AP) and three wireless devices that connect to Wi-Fi AP). One member can be the Wi-Fi AP and other members are the hosts (could be laptops, smart watches, smart phones, etc.). Assume all the devices in the network would like to send packets to Internet simultaneously. For example, when you need to send a packet, you can say "I'm sending a packet". If another group member said the same thing at the same time, then a collision occurred, and both need to retransmit packets.

   Your group needs to act as a Wireless LAN and provides a mechanism to enable successful packet transmission. You can illustrate the protocol that you have designed in a timing diagram (Shows in Figure 1). You are not required to replicate the exact protocol used in WiFi. You can design your own protocol based on random access that allows hosts to communicate with WiFi AP with minimal collisions and act fast in case of a packet collision.

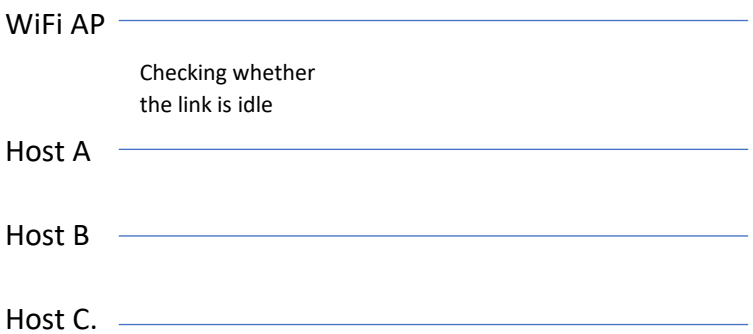
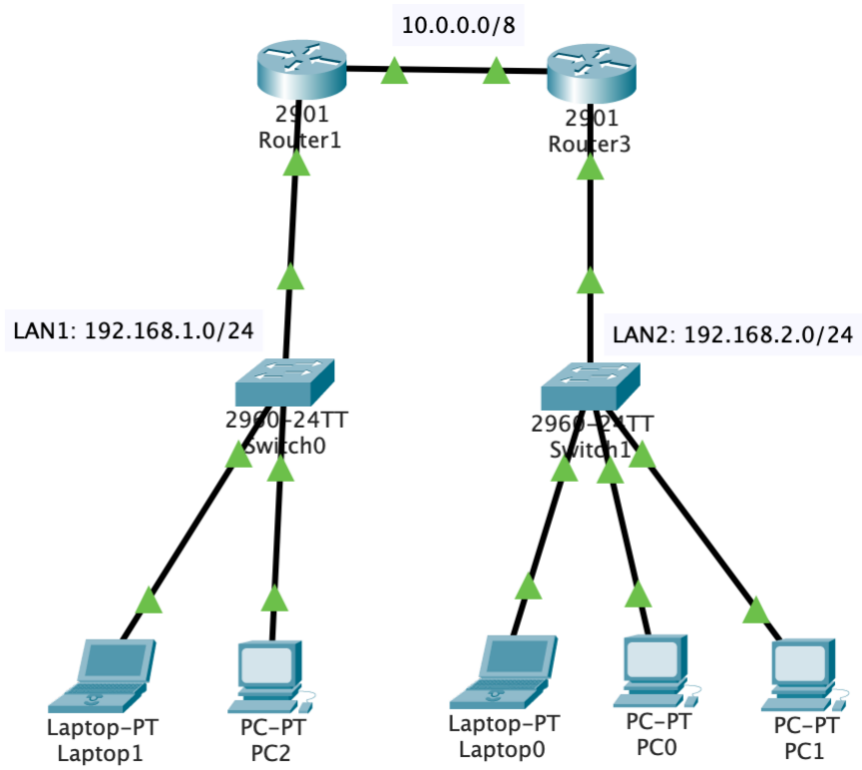


Figure 1: Timing Diagram of the Protocol

2. Once you have completed the above activity, discuss the following question with your group members.
   - What is the medium access control (MAC) protocol that can be used in WiFi?

Activity 2: ARP



Implement the above network in Cisco Packet Tracer. You can use static IP configuration to configure hosts and router interfaces. Make sure to take screenshots of your findings as you need to include those in the task submissions.

1. As a group, discuss what information Laptop1 in LAN1 requires to connect to PC2 In LAN1.
2. What protocol we can use to get the required information? Discuss the steps involved in getting the required information.
3. Use the simulation mode to check ARP in action by pinging PC2 from Laptop1.
    a. What are the types of messages that PC2 generated?
    b. Discover the message sequence of ARP and the message content (paying attention to the source IP, destination IP, source MAC address, and destination MAC address).
4. Each device maintains an ARP table. You can check the ARP table of devices using the command prompt and typing “arp -a”. Check and compare the arp tables in Laptop 1 and PC2.
5. Check the arp tables of router 1, router 2, PC0, PC1, and Laptop0. Keep notes of the content of each arp table. To show the arp table of a router, “show arp” command can be used in the router’s CLI.

6. Use the simulation mode again. Now, ping PC0 from Laptop1. Discover the arp message sequence and the message content in each link. Once the above steps are completed, ping PC1 from laptop0.
7. Check the arp tables of router 1, router 2, PC0, PC1, and Laptop0.
8. Compare your observations with the observations you recorded in step 5. Discuss your finding with your group members.

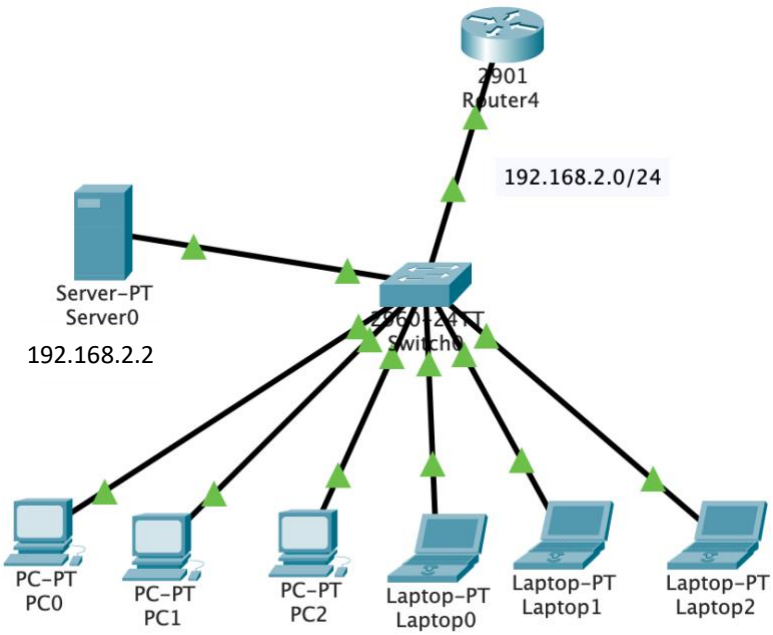
Note: if you want to delete the entries in arp table of a device, you can use "arp -d" command.

Activity 3: Mapping physical connections – MAC address table.

The MAC address table is used by an Ethernet Switch to store information about the MAC addresses associated with each physical port of the switch. Since the switch can direct the packets to a specific user in the same LAN using the MAC address table, it provides some privacy. However, the use of the MAC address table results in some vulnerability as there is only limited memory available. Attackers can flood switch with false MAC addresses which will overflow the table, making Switch to work as a HUB and breaking its privacy features. Therefore, in this activity, we will learn about the MAC address table.

Question to answer: How do Switches learn MAC addresses of its connected devices?

For this activity, you need to build and configure the following topology using a Cisco 2960 Switch.



1. After you configured the devices using static IP configuration,
   a) Record the MAC addresses of PCs/laptops/servers and Ethernet Ports of Switches.
   b) Record the arp table in PCs and laptops.
   c) Check the MAC address table of the switch. In switch's CLI, you can type the following command to show the MAC address table.

```
Switch>enable
Switch#show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
```

   d) Record your observations. If there are any records in the MAC table, explain your observation.
   e) Now, ping from PC1 and PC2 to Laptop0 and Laptop 1, respectively.
   f) Check the MAC address table of the switch. Explain your observations.
   g) Click on the "magnifying glass" icon and bring that on top of the switch. Click on the switch and select "MAC table". Resize the MAC address table and keep the table visible.
   h) Ping laptop2 from PC0 and check the changes in the MAC table. Explain your observation.
   i) Check the arp tables in all the PCs and laptops.

2. Clear the mac address table from the switch. You can do this by using "clear mac-address-table" command in CLI of the switch.
   a. Configure server as a DHCP server and use DHCP to obtain IP address for all PCs and laptops.
   b. Check the arp table of PCs and laptops. Compare you observation with what you have recorded in 1.b).
   c. Check the Mac table of the switch. Compare and explain you observation with what you have recorded in 1.c)

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 network layer.

1. Discuss the security issues associated with ARP identifying the types of attacks (200 – 300 words).