TÉCNICO LISBOA

Computer Networks — 2021/22		Assignment:	Lab 9
Understand ARP, DHCP, and VLANs		Issued:	2022-01-31
LANs – The Local Area Network		Submission Due:	2022-02-03
Authors:	Francisco Chamiça Pereira Prof. Luis D. Pedrosa	Comments Due:	2022-02-04
		Version:	1.0

Submission note. Answers to the questions in this assignment are to be submitted in Moodle (remember to store a local copy of the answers to avoid losing information). You should create a PDF file containing the answers, and submit the file to Moodle as an attachment to the submission form. Remember to include all relevant screenshots and diagrams in the PDF file itself.

1 Goals of the laboratory

- Understand ARP.
- Understand DHCP.
- Understand what are VLANs, their use, and how to configure a linux machine to behave as a VLAN compatible switch.

Reminder. Execute the command `git pull origin master` in `/home/rc/lab-files` to get the most up-to-date files. Then, execute `/home/rc/lab-files/lab-lans/setup.sh`.

2 ARP

By now, you should be familiar with IP addresses. They identify the two endpoints in a given communication between hosts. That said, communication for each hop between end-points is managed by the link layer, which uses MAC addresses–48-bit addresses typically represented in hexadecimal notation (*e.g.* `01:02:03:de:c0:de`), and are uniquely assigned to a network adapter. Every time a packet is forwarded from one router to the next, its Ethernet frame MAC addresses change accordingly. As such, there is a need for a protocol that provides translation between IP addresses into MAC addresses–the Address Resolution Protocol (ARP).

Each host stores an ARP table (cache) which contains not only mappings between IP addresses and MAC addresses, but also a time-to-live (TTL) field value indicating when the entry will expire. Whenever a host wants to discover the MAC address associated with a given IP, and it's not already in cache, it broadcasts an ARP request to the network asking for this missing information. ARP requests are broadcasted to the local network, using the special destination MAC address `ff:ff:ff:ff:ff:ff`. All nodes in the local network hear these requests and the node with the specified IP address responds, indicating its MAC address.

2.1 Exercise

Open `/home/rc/lab-files/lab-lans/arp.imn` in `Core`. You should see the network topology depicted in Figure 1.

Computer Networks — 2021/22		Assignment:	Lab 9
Understand ARP, DHCP, and VLANs		Issued:	2022-01-31
LANs – The Local Area Network		Submission Due:	2022-02-03
Authors:	Francisco Chamiça Pereira Prof. Luis D. Pedrosa	Comments Due:	2022-02-04
		Version:	1.0

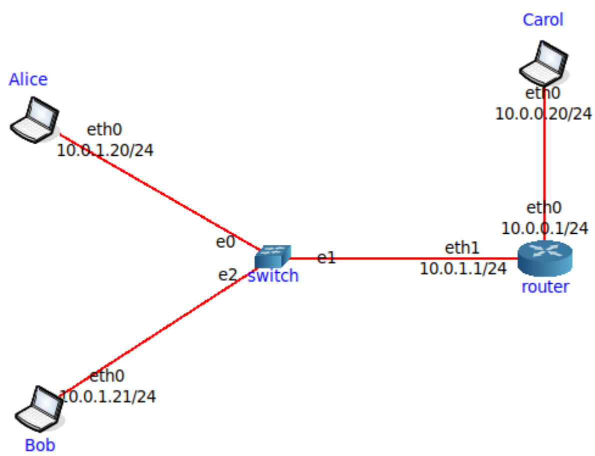

Figure 1: Network topology of `arp.imn`.

Q1 Catalog each interface with its corresponding IP (and subnet mask) and MAC addresses. Do this process for Alice, Bob, Carol, and the router.

Q2 Open `Wireshark` on interface `eth0` of Alice and filter by `arp || udp.port == 12345`. Now open a UDP port on Bob by running `netcat -ul 12345`, and send a UDP packet from Alice by running `echo "I'm sending a packet" | nc -u 10.0.1.21 12345` from her terminal. You should see a pair of ARP packets and one UDP packet. Provide a screenshot of the captured packets, and explain the purpose of each of them. Your justification should contain an explanation for (1) the source and destination MAC addresses of the ARP packets; (2) the role of each ARP packet; and (3) why the UDP packet is only sent after the ARP packets.

Q3 Run `arp` on Bob's terminal, which shows the current state of Bob's ARP table. What can you conclude from the output of the command?

Q4 Open `Wireshark` on interface `eth0` of Carol and filter by `arp || udp.port == 12345`. Now open a UDP port on Alice by running `netcat -ul 12345`, and send a UDP packet from Carol by running `echo "I'm sending a packet" | nc -u 10.0.1.20 12345` from her terminal. You should see a pair of ARP packets and one UDP packet. Provide a screenshot of the captured packets, and explain the purpose of each of them. Your justification should contain an explanation for (1) the source and destination MAC addresses of the ARP packets; (2) the role of each ARP packet; (3) why the UDP packet is only sent after the ARP packets; and (4) how is this situation different from **Q2**?

Computer Networks — 2021/22		Assignment:	Lab 9
Understand ARP, DHCP, and VLANs		Issued:	2022-01-31
LANs – The Local Area Network		Submission Due:	2022-02-03
Authors:	Francisco Chamiça Pereira Prof. Luis D. Pedrosa	Comments Due:	2022-02-04
		Version:	1.0

3 DHCP

In many situation, the users of a network do not want the hassle of individually configuring static IPs for their devices. As such, it is very common to resort to the DHCP protocol to dynamically assign IPs to hosts. DHCP, or Dynamic Host Configuration Protocol, is a client-server protocol composed of four steps:

1. *Server discovery*: A UDP packet sent by the node being configured (client) to discover the DHCP server. Being the first packet, the client is not yet configured and simply broadcasts the packet to the whole network (recall the special broadcast MAC address from the previous section).
2. *Server offer*: The DHCP server responds to the client with an offer message, containing both the offered IP address and the lease time (the amount of time for which the IP address will be valid).
3. *Request*: The original host will request/renew the offered IP address to the DHCP server.
4. *ACK*: Finally, the DHCP server accepts the requested parameters, and the host is finally associated with the new IP for the duration of the lease.

3.1 Exercise

Open `/home/rc/lab-files/lab-lans/dhcp.imn` in `Core`. You should see the network topology depicted in Figure 2.

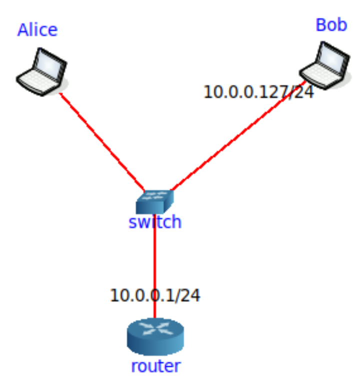

Figure 2: Network topology of `dhcp.imn`.

This LAN (`10.0.0.0/24`) contains a router running a DHCP server, the host Bob configured with a static IP value of `10.0.0.127/24`, and Alice, which is without an IP. Open

Computer Networks — 2021/22		Assignment:	Lab 9
Understand ARP, DHCP, and VLANs		Issued:	2022-01-31
LANs – The Local Area Network		Submission Due:	2022-02-03
Authors:	Francisco Chamiça Pereira Prof. Luis D. Pedrosa	Comments Due:	2022-02-04
		Version:	1.0

`Wireshark` on the router, filter by `arp || dhcp`, and execute the following command on Alice's terminal to run the DHCP client:

```
$ dhclient -nw -pf /var/run/dhclient-eth0.pid \
  -lf /var/run/dhclient-eth0.lease eth0
```

Q5 Which IP is offered by the DHCP server to Alice and how long is the lease?

Q6 Why does the router broadcast ARP requests before sending the DHCP offer to Alice?

4 VLANs

A virtual LAN (or VLAN) provides a logical grouping of devices in the same broadcast domain. The use of VLANs allows us to:

1. Isolate traffic between hosts associated with different VLANs;
2. Group together hosts to the same broadcast domain even if they are not connected to the same switch;

4.1 Port-based VLANs

Let's imagine that Alice, Bob, Charlie, and Dan belong to the same LAN, as can be seen in Figure 3.

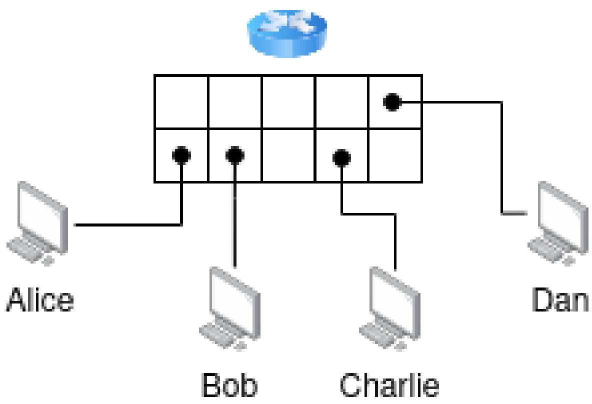

Figure 3: LAN

Now imagine that, for some reason, there is a need to logically separate Alice and Bob from Charlie and Dan. For example, although all of them share the same switch, Alice and Bob might belong to the Development Team whilst Charlie and Dan belong to Human Resources, and these two departments should not be able to see each other's traffic.

Additionally, maybe the network administrator might want to employ different firewall rules between the two departments.

In order to comply with these requirements, the switch can be configured with VLANs, as depicted by Figure 4. In the picture, the switch is configured with 2 VLANs: the green VLAN (containing Alice and Bob), and the blue VLAN (containing Charlie and Dan). This configuration allows Alice to communicate with Bob, and Charlie with Dan, but packets coming from Alice and Bob are not forwarded to Charlie and Dan (and vise-versa).

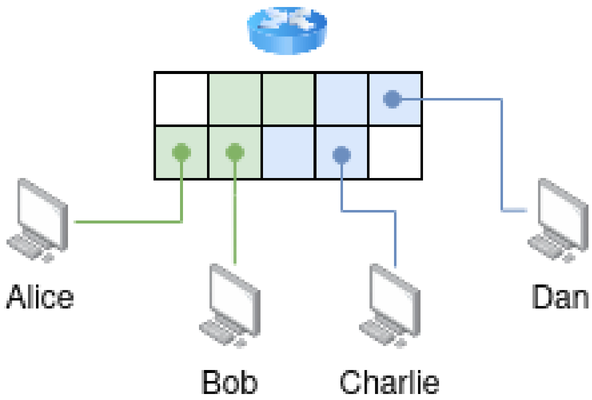

Figure 4: Switch configured with VLANs.

None of the hosts are aware of the existence of these VLANs. Figure 5 shows how they perceive the network: as if containing two not interconnected switches, one for Alice and Bob, and another for Charlie and Dan.

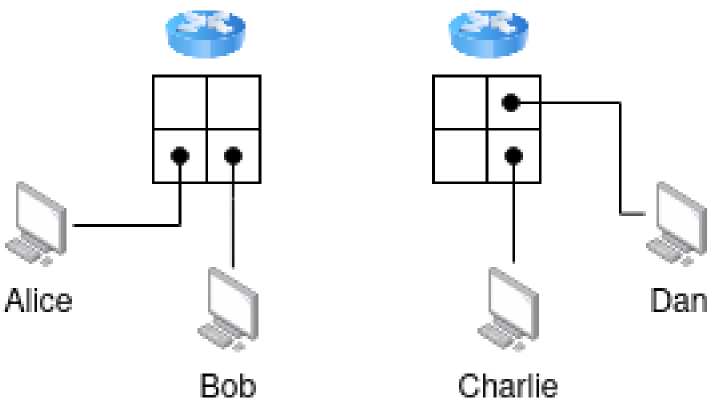

Figure 5: How the LAN is perceived by the users.

4.2 802.1Q

Imagine now that we wanted to extend our network into another building, and add one more person to the Development Team—Erin—and another to the Human Resources—Frank. Again, we would configure this second switch with both VLANs—green and blue—, and would connect Erin to a port associated with the green VLAN, and Frank to a port associated with the blue VLAN. This new configuration can be seen in Figure 6.

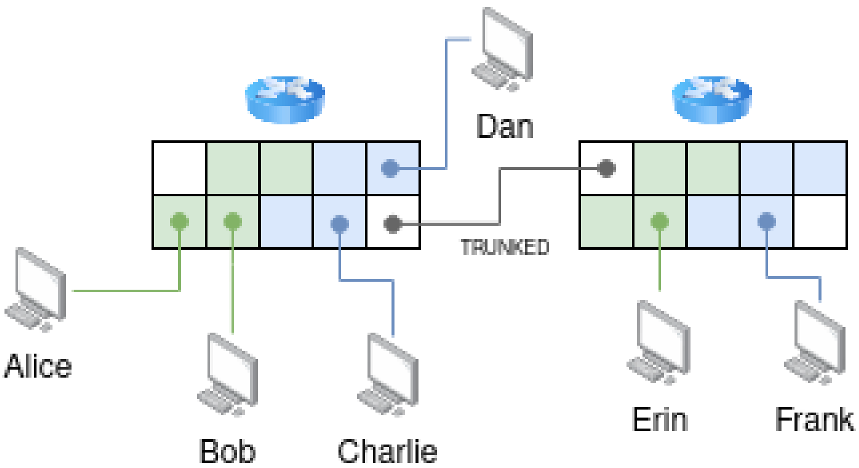

Figure 6: Tagged VLANs.

Naturally, both switches would need to be connected for Alice and Bob to communicate with Erin (and Charlie and Dan with Frank). However, when sending traffic between them, it is vital for the switches to identify from which VLAN the traffic came from, so that they can correctly forward it to the correct VLAN. As such, a mechanism called *tagging* (or *trunking*) is used. It is defined in the IEEE 802.1Q standard, and appends an additional 802.1Q header to the Ethernet frame containing the VLAN ID (a number identifying the VLAN). Figure 5 shows an Ethernet frame with the 802.1Q header field.

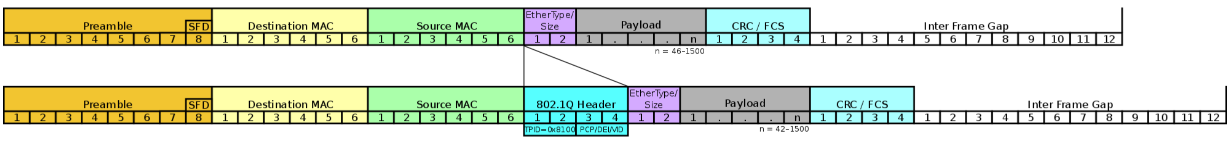

Figure 7: Ethernet frame with 802.1Q header (source: https://en.wikipedia.org/wiki/IEEE_802.1Q).

4.3 University departments

Consider a university with two departments: Mathematics and Physics. Both departments share the same building (building 1), and a single switch is used to connect all the hosts in both departments. This network topology is depicted in Figure 8. Open `/home/rc/lab-files/lab-lans/vlans_1.imn` in `Core` to load this network.

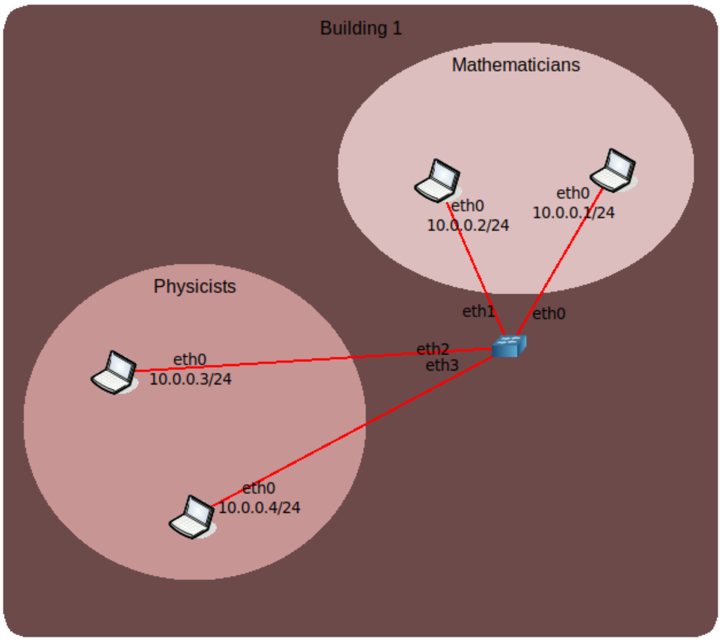

Figure 8: University with two departments: Mathematics and Physics.

Because both departments do not want to see each other's traffic, our goal now is to create two VLANs: one for the physicists, and another for the mathematicians. Instead of using a proprietary switch, they repurposed an already owned linux machine. If a proprietary switch were to be used, then the process of creating VLANs would be manufacturer-dependent (some switches provide a graphical web interface, others provide only a terminal-based interface).

Start the network emulator, and open the switch's terminal. Create two bridge interfaces representing each of the VLANs:

```
$ brctl addbr math
$ brctl addbr physics
```

Next, associate each switch interface with the matching bridge:

```
$ brctl addif math eth0
$ brctl addif math eth1
$ brctl addif physics eth2
```

```
$ brctl addif physics eth3
```

Run `brctl show` to confirm the creation of the bridges, and their association with the network interfaces.

Finally, set the link status of the bridges as `up`:

```
$ ip link set dev math up
$ ip link set dev physics up
```

Q7 Broadcast ICMP packets by running `ping 10.0.0.0 -b` from one of the *physicists*' host. Using `Wireshark`, check which of the switch's interfaces see the broadcasts and which don't. Explain what you see.

Suppose now that there are also mathematicians and physicists on building 2. As such, another switch was connected to the first one, and connected then to both the new physicist and mathematician, as can be seen in Figure 9. Open `/home/rc/lab-files/lab-lans/vlans_2.imn` in `Core` to load this network.

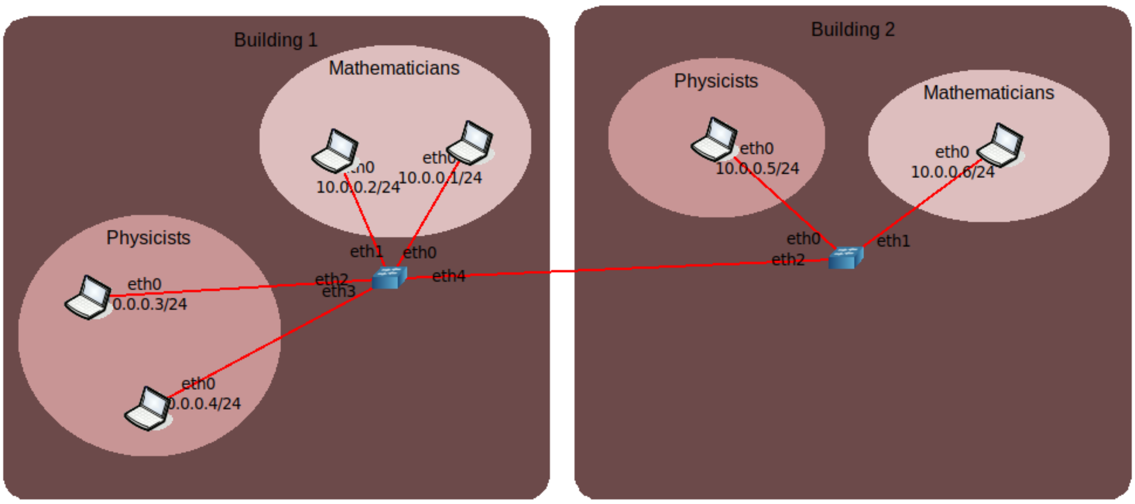

Figure 9: Univerity with two departments and two buildings.

Q8 Which interface from the switch in building 1 needs to tag the packets going through it with VLAN tags? Why?

Create the two required trunk mode VLANs in the first switch (`<TAGGED_IF>` refers to the interface answered in the previous question):

```
$ ip link add link <TAGGED_IF> name <TAGGED_IF>.100 type vlan id 100
$ ip link add link <TAGGED_IF> name <TAGGED_IF>.200 type vlan id 200
$ ip link set dev <TAGGED_IF>.100 up
$ ip link set dev <TAGGED_IF>.200 up
```

Run `ip address show` or `ifconfig` to confirm the creation of the VLAN interfaces in trunk mode.

Q9 As we did before, configure Linux bridges in both buildings to connect the *physicists* and the *mathematicians* among themselves. Create two bridges on each side–`math` and `physics`–and associate all the relevant interfaces to each of them. Associate bridge `math` with the VLAN tag value 100, and bridge `physics` with the VLAN tag value 200. Provide all the executed commands.

> **Hint.** When relevant, associate the VLAN interfaces (created in the previous exercise) with the bridges, and not the original interfaces. Additionally, don't forget to create the required trunk mode VLANs in the second switch on the relevant interface.

Q10 Broadcast ICMP packets by running `ping 10.0.0.0 -b` from the physics' machine with the IP `10.0.0.3/24`. Using `Wireshark`, check which of the *building 2 switch*'s interfaces see the broadcasts and which don't. Explain what you see.

Q11 Use `Wireshark` to capture a packet with a VLAN tag coming in to `eth2` on the *building 2 switch*. Take a screenshot showing the VLAN tag field and explain its value and meaning.

Q12 Is there any VLAN tag on the packets exiting through interfaces `eth0` and `eth1` from the *building 2 switch*? Explain.