DEPARTAMENTO DE ELECTRÓNICA, TELECOMUNICAÇÕES E INFORMÁTICA
LICENCIATURA EM ENG. DE COMPUTADORES E INFORMÁTICA

# REDES DE COMUNICAÇÃO I

## LAB GUIDE 02

## ETHERNET, ARP AND BASIC IPV4 ROUTING

### Objectives

- Physical Interfaces and Ethernet Addresses
- IPv4 protocol (addressing, forwarding, fragmentation and reassembly)
- IPv4 Address Resolution Protocol
- ICMP (ping, arp and traceroute commands)
- Familiarization with Wireshark protocol analyser
- Familiarization with equipment configuration
- Introduction to IP Routing

### Duration

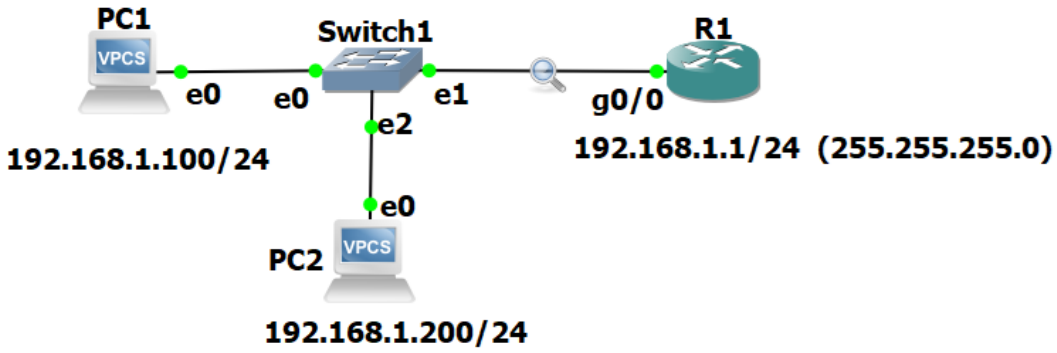
3 weeks

In the end of the class, send your report to your Professor.

# Part 1

## 1. Initial Experiments

1. Use the network configuration from Guide 1 (Part C):




a) Cisco:

Router# **configure terminal** // conf t
Router(config)# **interface GigabitEthernet0/0** // Enter interface configuration mode
Router(config-if)# **ip address 192.168.1.1 255.255.255.0** // Assign IPv4 address
Router(config-if)# **no shutdown** // Enable the interface
Router(config-if)# **exit** // ^Z
Router# show run // View the current router configuration
Router# write // save the configuration
Router# show ip interface brief //verify interfaces status (ip address and status/protocol)

b) **Configuration of the VPCs (configuring and IP address):**

On the VPC1 Console: PC1> ip 192.168.1.100/24
On the VPC2 Console: PC2> ip 192.168.1.200/24
PC1/PC2> save (to save the configuration)

2. Run the command ping –t (non stop ping) from the PC1 to the router (ping 192.168.1.1 -t ).

3. Run Wireshark in the link between the switch and the router and start a capture of all packets.

4. Run the Statistics ➔ Endpoints tool and verify that the PC captures packets from/to PC/Router.

5. Run the Statistics ➔ Conversations tool to visualize the communications among the different pairs of hosts. At this point you may execute a similar ping from PC2 to the router.

6. For future analysis, you may save the wireshark capture on your local hard disk (stop the capture and save with a file extension ".cap" or ".pcap"). Stop all pings before saving the capture.

7. Analyze the saved capture. **What do you conclude on the ICMP packet periodicity? Observe how the Sequence Number field of ICMP packets is used for round-trip-time (RTT) estimation done by the ping command.**

8. Observe now in the saved capture the different encapsulation levels: the ICMP packets are encapsulated on IP datagrams and the IP datagrams are encapsulated on Ethernet frames. **Register the following information:**
    a. **PC Ethernet/MAC address:**
    b. **Router Ethernet/MAC address:**
    c. **Hexadecimal code (Type field of Ethernet header) that identifies an IP datagram:**
    d. **Hexadecimal code (Protocol field of IP header) that identifies an ICMP packet:**
    e. **Hexadecimal code (Type field of ICMP header) that identifies the two ICMP packet types (Echo Request and Echo Reply):**

9. On the PCs, execute the command "arp" and check if it returns "arp table is empty". If not, wait until it expires.

10. Run the ping command from PC1 to the Router.

11. Run the command arp to display the ARP table of the PC1. **Check that the IP address of the Router has an associated Ethernet address.**

12. Start a new capture with Wireshark. Repeat the experiment from point 9 and 10 and, then, stop the capture.

13. Analyzing the captured packets, explain how ARP protocol is used by the PC to discover the Ethernet address of the Router before exchanging the ICMP packets. Register the following information of the captured ARP packets:

ARP Request
- Ethernet header
  - **Origin MAC/Ethernet/Hardware Address:**
  - **Destination MAC/Ethernet/Hardware Address:**
- ARP Packet
  - **Origin MAC/Ethernet/Hardware Address:**
  - **Origin IP Address:**
  - **Destination MAC/Ethernet/Hardware Address:**
  - **Destination IP Address:**

ARP Response
- Ethernet header
  - **Origin MAC/Ethernet/Hardware Address:**
  - **Destination MAC/Ethernet/Hardware Address:**
- ARP Packet
  - **Origin MAC/Ethernet/Hardware Address:**
  - **Origin IP Address:**
  - **Destination MAC/Ethernet/Hardware Address:**
  - **Destination IP Address:**

14. **On the PC, run again the command ping to the Router. Check how long it takes the Router entry to disappear from the ARP table.** Remember from the theoretical classes the reasons for the fact that these ARP table entries are not permanent (depending on the operating system, the arp expiration time is different).

### Padding

In order to work properly, Ethernet requires a minimum size data field of 46 bytes. If the protocol running on top of Ethernet delivers a chunk of less than 46 bytes, Ethernet adds dummy bytes to guarantee its minimum size (**this process is named padding**).

15. Start a new capture with Wireshark

16. On PC1 execute the command "ping 192.168.1.1 –l 8" to the Router.

17. Stop the capture.

18. **Observe the padding process on the captured ARP and ICMP packets** (NOTE: Wireshark does not show the padding bytes in packets generated by the VPC; therefore, the padding process can be observed only in the packets received by the VPC)

19. Repeat points 15 to 18, but now executing the command "ping 192.168.1.200 size 36" on the router. (note that, on the VPC, the size refers to the ICMP Data size, while on the Cisco Router, the size refers to the total size of the IP packet)

**20. Verify that you are able to see the padding on all the Ethernet headers of the ICMP packets.**

### Fragmentation

The IP protocol includes a fragmentation and reassembly mechanism in order to transmit IP packets whose size is larger than the MTU (Maximum Transmission Unit) of the network (typical Ethernet MTU = 1500 bytes).

21. Start a new capture with Wireshark.

22. On PC1 execute the following commands to the Router:

    a. ping 192.168.1.1 –l 2000
    b. ping 192.168.1.1 –l 3100

23. Now repeat the pings from the router to the VPC, also using 2000 and 3100 bytes of data:

    a. ping 192.168.1.100 size 2028
    b. ping 192.168.1.100 size 3128

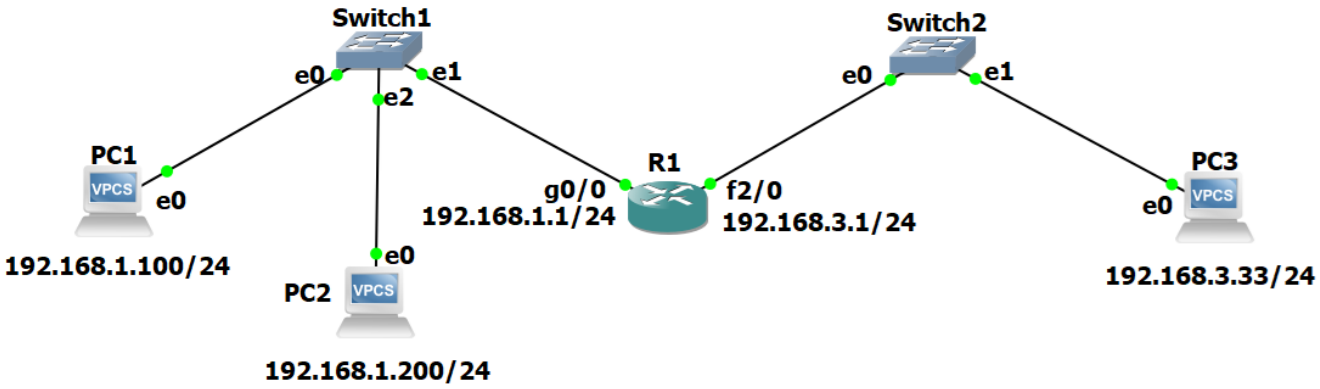
**24.** Analyze the captured packets and explain the fragmentation process**. In particular, explain:**

   **a. why each packet is fragmented in either 2 or 3 fragments;**
   **b. the content of the IP header fields that enable the recovery of the complete packet at the destination;**
   **c. the packet size of each fragment.**

# Part 2

## 2. Routing Basics

2.1. Expand the previous network by adding a new switch and VPC.




Configure the second router port (f2/0 – FastEthernet 2/0) accordingly and configure the PC3 ip address

c) Cisco:

R1# configure terminal // conf t
R1(config)# interface f2/0 // Enter interface configuration mode
R1(config-if)# ip address 192.168.3.1 255.255.255.0 // Assign IPv4 address
R1(config-if)# no shutdown // Enable the interface
R1(config-if)# exit // ^Z
R1# write // save the configuration
R1#sh ip interface brief //verify that the interfaces are configured (ip address) and "up" (status/protocol)

b) Configuration of the VPCs (configuring and IP address):

On the VPC3 Console: PC3> ip 192.168.3.33/24

**Register and justify the routing table of the Router. (R1#show ip route)**

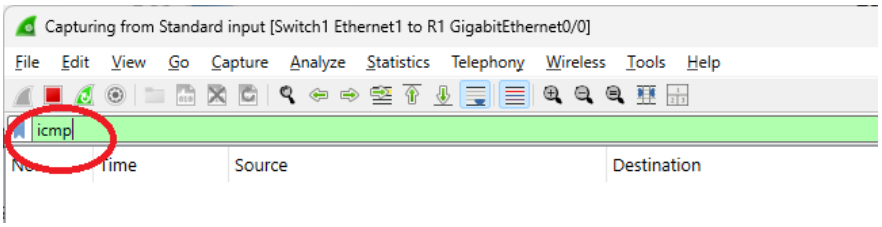
2.2. Start a capture with Wireshark between Switch1 and R1.

Execute the ping command from PC1 to PC3.
Repeat the experiment but now executing the ping command from the PC3 to PC1.
**Register and justify both the results and the captured packets.**

2.3. Configure the appropriate Default Gateway PC3.

PC3> ip 192.168.3.33/24 192.168.3.1

Start a new Wireshark capture with a display filter for ICMP packets.




Execute the ping command from PC3 to PC1.
**Register and justify both the ping command result and the observed captured packets.**

2.4. Configure the appropriate Default Gateway at PC1.

Start a new capture with a display filter for ICMP packets.

Execute the ping command from PC1 to PC3.

**Register and justify the ping command result.**

Register also the following addresses of the ICMP Echo Request and Echo Reply packets and identify to which equipment interfaces each one of them belong:

**ICMP Echo Request**

| | | |
|---|---|---|
| Ethernet packet header | Source MAC Address: | "Owner": |
| | Destination MAC Address: | "Owner": |
| IP packet header | Source IP Address: | "Owner": |
| | Destination IP Address: | "Owner": |

**ICMP Echo Reply**

| | | |
|---|---|---|
| Ethernet packet header | Source MAC Address: | "Owner": |
| | Destination MAC Address: | "Owner": |
| IP packet header | Source IP Address: | "Owner": |
| | Destination IP Address: | "Owner": |

2.5. Router arp table

R1#show arp

**Register and justify the ARP tables of the Router.**

2.6. Remember:

From the theoretical classes that Routers forward IP packets based on the IP addresses of their IP headers (routers do not change the packet IP addresses). Nevertheless, routers are clients of each Ethernet segment. ➔ Therefore, the MAC addresses of the Ethernet header are specified with the MAC addresses of the communicating hosts on each Ethernet segment.

Having in mind this behaviour, and without making any capture, predict what were the following addresses of the ICMP packets exchanged between the Router and the PC3 on the previous experiment (if needed, check the addresses on the equipment console):

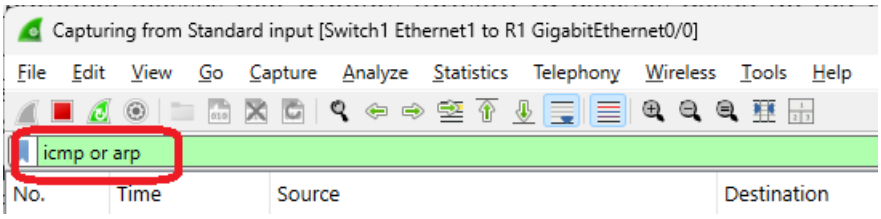
**ICMP Echo Request**

| | | |
|---|---|---|
| Ethernet packet header | Source MAC Address: | "Owner": |
| | Destination MAC Address: | "Owner": |
| IP packet header | Source IP Address: | "Owner": |
| | Destination IP Address: | "Owner": |

**ICMP Echo Reply**

| | | |
|---|---|---|
| Ethernet packet header | Source MAC Address: | "Owner": |
| | Destination MAC Address: | "Owner": |
| IP packet header | Source IP Address: | "Owner": |
| | Destination IP Address: | "Owner": |

2.7. Start a new capture with a display filter for ICMP and ARP packets




Execute the ping command from PC3 to the IP address 192.168.1.10 (an inexistent IP address of the left network).

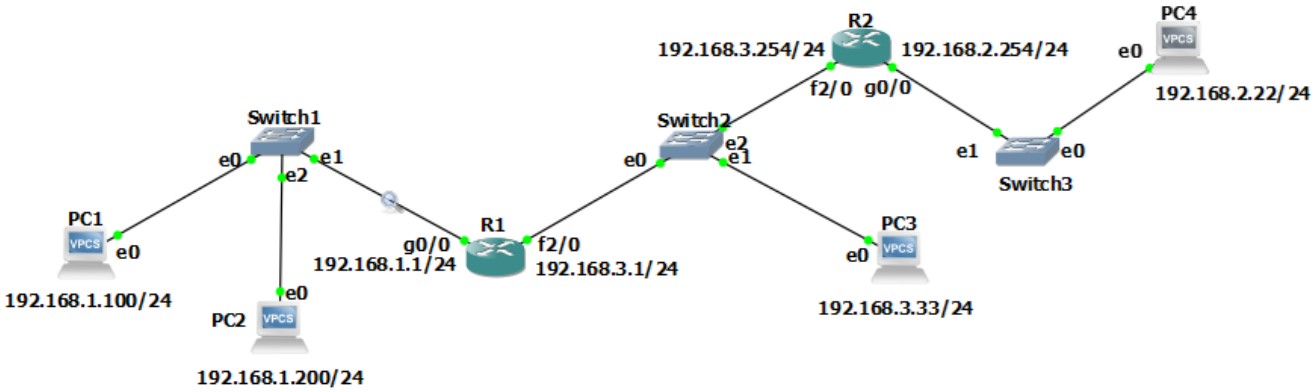
**Register the captured packets and explain the obtained results.**

2.8. With Wireshark still capturing

Execute the ping command from PC3 to the IP address 194.100.1.1.

**Register the captured packets. Justify the observed packets** (take into consideration that the Router has no entry for this IP address nor its network).

2.9. Add a new router (R2)




Configure the new router interfaces:

ip address of g0/0 and then "no shutdown"

ip address of f2/0 and then "no shutdown"

Configure PC4 ip address and gateway

**2.10. Register R1 routing table and compare with the results from point 2.1**

Observe that the routing table is the same, which means that the Router must be configured with something else (a routing protocol) to be able to reach the new IP network on the right (192.168.2.0/24).

2.11. Start a capture with Wireshark between Switch1 and R1

Execute the *ping* command from PC1 to the IP address 192.168.3.150 (an inexistent address of an existing network).

**Register and justify the captured packets.**

**Predict what has happened in this experiment in the other side of R1** (in the network 192.168.3.0), taking into consideration the results of experiments 2.3 and/or 2.4.

2.12. Start a capture with a display filter for ICMP packets.

Execute the ping command from PC1 to the IP address 192.168.2.254 (an existing address of a network that is not known yet by your Router R1).

**Register and justify the captured packets.**

**Predict what has happened in this experiment on the other side of R1** (in the network 192.168.3.0/24) taking into consideration the results of experiment 2.8.

## Static Routing

2.13. Configure a static route in R1 and another in R2 in order for each of them be able to reach the farthest network.

In order to configure the static route, use the following commands:

```
R1#configure terminal
R1(config)#ip route 192.168.2.0 255.255.255.0 192.168.3.254
(Define the path to network 192.168.2.0/24 through R2)

R2#configure terminal
R2(config)#ip route 192.168.1.0 255.255.255.0 192.168.3.1
(Define the path to network 192.168.1.0/24 through R1)
```

**Register both routers routing tables.** (Rx# show ip route)

Observe that, now, the routing protocol enabled the routers to add information on their routing tables concerning the new network.

**Execute the ping command from PC1 to PC4 address (192.168.2.22) to verify the connectivity between PC1 and the new network.** Note that you must have the gateway configured at PC4.

2.14. Start a capture with a display filter for ICMP packets. Then, run on PC1 the following ping commands:

```
ping 192.168.2.22 -T 1
ping 192.168.2.22 -T 2
ping 192.168.2.22 -T 3
```

**Based on the analysis of the result obtained at PC1 and the captured packets for each case, explain the behaviour of the routers with the different TTL (Time-To-Live) values sent by the PC.**

2.15. Start a capture with a display filter for ICMP packets and execute the trace route command:

```
PC1>trace 192.168.2.22 -P 1
```

**Based on the analysis of the captured packets, explain how the trace (traceroute, tracert) command works. In particular:**

**(i) identify how the PC identifies each router in the path;**

**(ii) observe that the PC sends three ICMP Echo Request packets for each growing value of TTL in order to obtain a better estimation of the round trip time;**

**(iii) determine how the PC stops the process.**

**2.16. Verify and justify the differences obtained when executing in your PC the command trace for the IP addresses 192.168.2.22 (PC4) and 192.168.2.254 (R2).**

**END**