universidade de aveiro
theoria poiesis praxis

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

REDES DE COMUNICAÇÃO I

LAB GUIDE 02

ETHERNET, ARP, IPV4 ADDRESSING AND SUBNETTING

Objectives

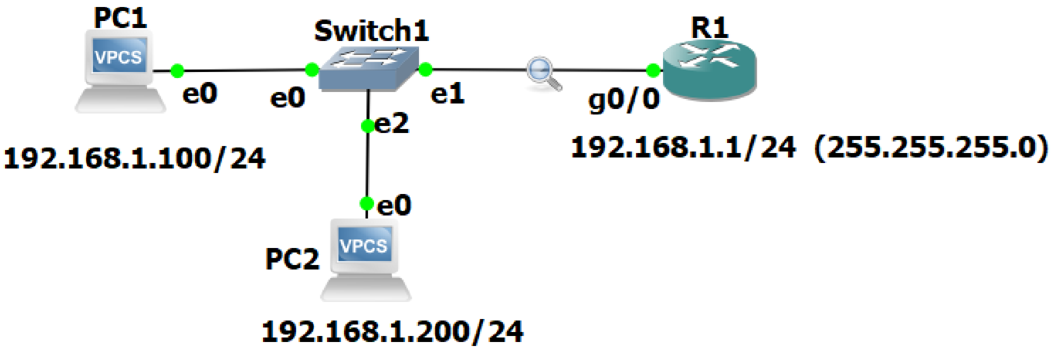
- Physical Interfaces and Ethernet Addresses
- IPv4 protocol (addressing, forwarding, fragmentation and reassembly)
- IPv4 Address Resolution Protocol
- ICMP (ping, arp and traceroute commands)
- Familiarization with Wireshark protocol analyzer
- Familiarization with equipment configuration
- Ethernet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

Duration

3 week

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
```

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 192.1681.1 -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 –l 2028
    b. ping 192.168.1.100 –l 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.