

**DEPARTAMENTO DE ELETRÓNICA, TELECOMUNICAÇÕES E**

**INFORMÁTICA**

**LICENCIATURA EM ENGENHARIA DE COMPUTADORES E INFORMÁTICA**

# REDES DE COMUNICAÇÕES 1

**SELF-EVALUATION**

**Legenda:**

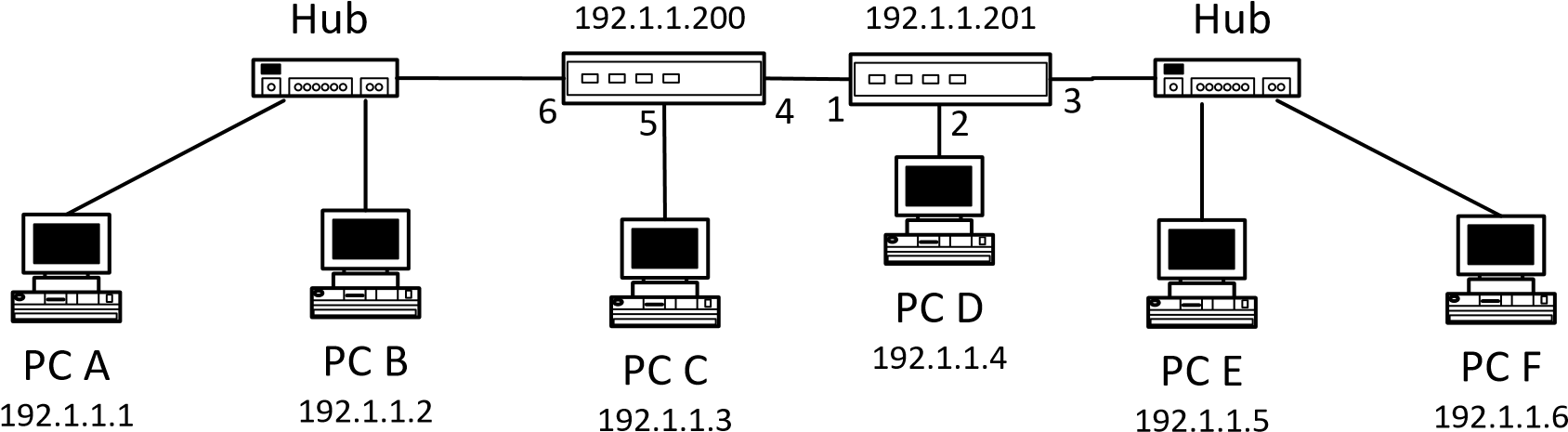
**Correto**

**Errado**

**Correção/Adição**

1. Consider the following network. The figure shows the assigned IP addresses to all network elements (with the netmask 255.255.255.0). The figure also indicates the number of the ports used on switches. Both PC B and PC C have WireShark permanently capturing all packets. The hub spreads everything it receives through all ports, so PC B can observe everything that traverses the links on the left part of switch A.

Switch A Switch B



(Wireshark) (WireShark)

The current MAC address table of Switch A is:

VID VLAN Name MAC Address Port Type

---- ---------------- ----------------- ---- ---------

1 default 00-0A-F4-3B-80-A5 6 Dynamic

1 default 00-0A-F4-3B-80-B0 4 Dynamic

1 default 00-0A-F4-42-CC-34 6 Dynamic

1 default 00-0A-F4-45-2D-23 4 Dynamic

1 default 00-0A-F4-45-2E-A7 5 Dynamic

1 default 00-0A-F4-46-2F-B5 4 Dynamic

1 default 00-1C-F0-A8-BD-C4 CPU Self

1 default 00-1C-F0-A9-12-F3 4 Dynamic

The current MAC address table of Switch B is:

VID VLAN Name MAC Address Port Type

---- ---------------- ----------------- ---- ---------

1 default 00-0A-F4-3B-80-A5 1 Dynamic

1 default 00-0A-F4-3B-80-B0 3 Dynamic

1 default 00-0A-F4-42-CC-34 1 Dynamic

1 default 00-0A-F4-45-2D-23 3 Dynamic

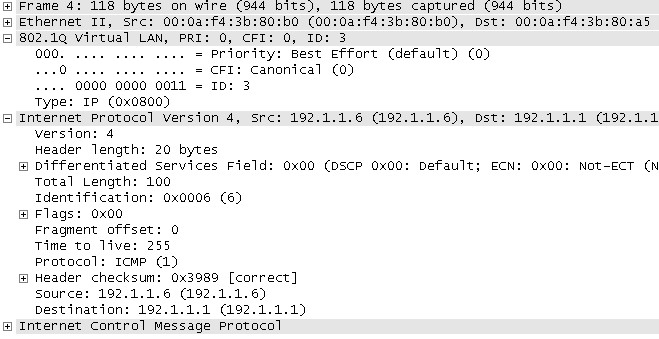
1 default 00-0A-F4-45-2E-A7 1 Dynamic

1 default 00-0A-F4-46-2F-B5 2 Dynamic

1 default 00-1C-F0-A8-BD-C4 1 Dynamic

1 default 00-1C-F0-A9-12-F3 CPU Self

In a run of a ping command on PC A to PC F, one of the ICMP packets captured on PC B was:



* 1. With the provided information, indicate and justify the Ethernet addresses of all switches and all PCs.

Ethernet addresses = MAC address

PCA = 00-0A-F4-3B-80-A5;

PC B = 00-0A-F4-42-CC-34;

PC C = 00-0A-F4-45-2E-A7;

PC D = 00-0A-F4-46-2F-B5;

PC E = 00-0A-F4-45-2D-23;

PC F = 00-0A-F4-3B-80-B0;

Switch A = 00-1C-F0-A8-BD-C4; Switch B = 00-1C-F0-A9-12-F3;

* 1. What type of ICMP packet is the one shown above? Justify.

ICMP Reply. Podemos chegar a essa conclusão observando a source e o destino do pacote onde, apesar de ter sido efetuado um ping do PC A até o PC F, o destino desse pacote é o PC A, logo não é uma ICMP Request, mas sim uma Reply já porque é a resposta do PC F ao PC A.

1. Consider the previous network. On each of the following experiments (2.1, 2.2, 2.3 and 2.4), consider an initial state where all MAC address tables and all ARP tables are empty (remember that both PC B and PC C have WireShark permanently capturing all packets). Assume that the execution of a ping command generates 5 ICMP Echo Request messages both on PCs and on switches. The hub spreads everything it receives through all ports, so PC B can observe everything that traverses the links on the left part of switch A. For each of the following experiments, indicate which packets are captured on PC B and on PC C:
   1. Running a ping command on PC D to the address 192.1.1.3.

PC B: ARP Request (Broadcast and switch flooding) (Who is 192.1.1.3)

PC C: ARP Request (Broadcast and switch flooding) (Who is 192.1.1.3) + ICMP Reply + ICMP Request

* 1. Running a ping command on PC A to the address 192.1.1.200.

PC B: ICMP Request + ICMP Reply

PC C: Nada switch rebroadcasts the ARP Request broadcast packet

* 1. Running a ping command on PC F to the address 192.1.1.4.

PC B: ARP Request (Broadcast and switch flooding) (Who is 192.1.1.4)

PC C: ARP Request (Broadcast and switch flooding) (Who is 192.1.1.4)

* 1. Running a ping command on Switch A to the address 192.1.1.10.

PC B: ARP Broadcast (Who is 192.1.1.10)

PC C: ARP Broadcast (Who is 192.1.1.10)

1. Starting on the initial state (where all MAC address tables and all ARP tables are empty), consider that experiments 2.1, 2.2, 2.3 and 2.4 were all run. Indicate and justify the resulting MAC address table of Switch A.

MAC address table of Switch A is:

VID VLAN Name MAC Address Port Type

---- ---------------- ----------------- ---- ---------

1 default 00-0A-F4-3B-80-A5 6 Dynamic 🡨 2.2; 2.4 🡪 PC A

1 default 00-0A-F4-3B-80-B0 4 Dynamic 🡨 2.3; 🡪 PC F

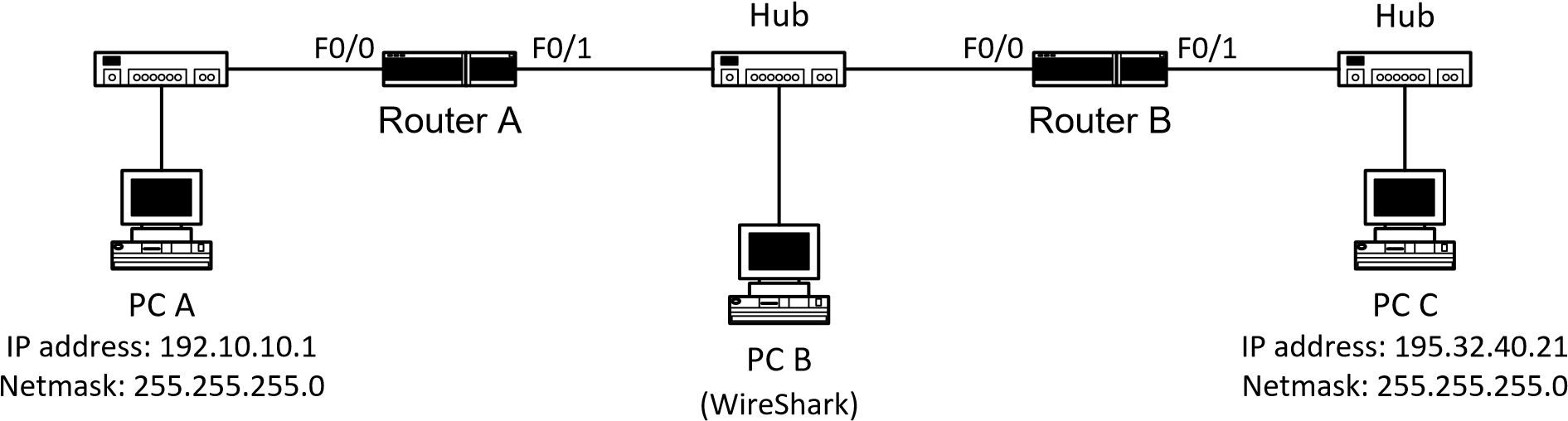
1 default 00-0A-F4-46-2F-B5 4 Dynamic 🡨 2.1; 🡪 PC D

1 default 00-1C-F0-A9-12-F3 4 Dynamic 🡨 2.1; 🡪 Switch B

1 default 00-0A-F4-45-2E-A7 5 Dynamic 🡨 2.1; 🡪 PC C

1 default 00-1C-F0-A8-BD-C4 CPU Self 🡪 Switch A

1. Consider the network shown in the following figure. The figure shows all IP addressing information of PC A and PC C and the name of the interfaces used on the routers. Routers have static routing. PC B is used only to capture packets through WireShark (and it is why it is connected through a hub, to be able to observe of packets in that link).



Def. Gateway: 192.10.10.20 Def. Gateway: 195.32.40.15

The current IP routing table of Router A is:

C 192.10.10.0/24 is directly connected, FastEthernet0/0

C 192.30.30.0/24 is directly connected, FastEthernet0/1

S 195.32.40.0/24 [1/0] via 192.30.30.2, FastEthernet0/1

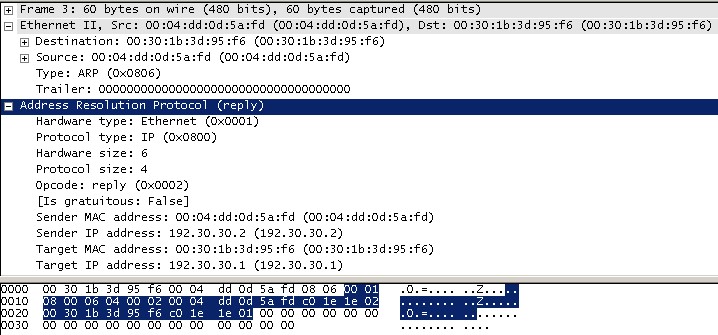
The current IP routing table of Router B is:

R 192.10.10.0/24 [1/0] via 192.30.30.1, FastEthernet0/0

C 192.30.30.0/24 is directly connected, FastEthernet0/0

C 195.32.40.0/24 is directly connected, FastEthernet0/1

In a run of a ping command on PC A to PC C, one of the packets captured on PC B was:



* 1. With the provided information, indicate and justify the IP addresses of all router interfaces.

Router A: F0/0 🡪 192.10.10.20; F0/1 🡪 192.30.30.1

Router B: F0/1 🡪 195.32.40.15; F0/0 🡪 192.30.30.2

* 1. What type of packet is the one shown above? Give an explanation for the reason why this packet was captured.

Arp Reply. Serviu para indicar ao Router A o endereço do router B.

1. Consider the previous network. Assume that the execution of a ping command generates 5 ICMP Echo Request messages both on PCs and on routers. Assume also that the ARP tables of all PCs and all routers are complete. On each of the following experiments, indicate which ARP and ICMP packets are captured on PC B (for the ICMP packets, indicate the IP origin and destination addresses):
   1. Running a ping command on PC A to the address 192.10.10.20.

Nada

* 1. Running a ping command on PC A to the address 192.30.30.1.

Nada

* 1. Running a ping command on PC A to the address 192.30.30.10.

ARP Request

* 1. Running a ping command on PC A to the address 192.30.30.2.

ICMP Requests(src: 192.10.10.1; dst: 192.30.30.2) + ICMP Replys(src: 192.30.30.2; dst: 192.10.10.1)

* 1. Running a ping command on PC A to the address of PC C.

ICMP Requests(src: 192.10.10.1; dst: 195.32.40.21) + ICMP Replys(src: 195.32.40.21; dst: 192.10.10.1)

* 1. Running a ping command on Router A to the address of PC C.

ICMP Requests(src: 192.30.30.1; dst: 195.32.40.21) + ICMP Replys(src: 195.32.40.21; dst: 192.30.30.1)

1. Consider the previous network. Consider that you run ping commands on PC A. For each of the following alternatives, indicate a possible ping command whose run generates the following answers:
   1. Reply from 192.30.30.2: TTL expired in transit.

Ping 192.30.30.3 Ping PC C com TTL 2

* 1. Reply from 192.10.10.20: Destination host unreachable.

Ping 192.10.10.21 ping 192.40.40.1

* 1. Request timed out.

Ping 192.30.30.3

1. Consider the previous network again. Consider that PCA has now only a private address, 192.168.1.1 with a default gateway to the router 192.168.1.254. With a pool for NAT public addressing of 193.1.1.128/29 to be used by Router A for the communication to the outside (from its interface F0/1), answer as true or false:
   1. The NAT pool has 16 addresses.

29 = 255.255.255.1111\_1000

2^6 = 64; 256/64 = 4; 2^3 = 8

Endereços da network de 4 em 4 com 8 endereços host possíveis em cada;

R.: Falso, são 8 endereços.

* 1. A translation table in the router can be:

Inside global | inside local | outside global | outside local

~~193.1.1.139~~ | 192.168.1.1 | 195.32.40.15 | 195.32.40.15

* 1. A translation table in the router can be:

Inside global | inside local | outside global | outside local

~~192.168.1.1~~ | 192.168.1.1 | 195.32.40.15 | 195.32.40.15

* 1. A translation table in the router can be:

Inside global | inside local | outside global | outside local

193.1.1.131 | ~~193.1.1.131~~ | 195.32.40.15 | 195.32.40.15

* 1. A translation table in the router can be:

Inside global | inside local | outside global | outside local

193.1.1.131 | 192.168.1.1 | 195.32.40.15 | 195.32.40.15

(NAT possível) (PC A) (Router B F1/0) (Router B F1/0)

Verdade

* 1. With NAT/PAT only 8 PCs can reach the Internet.

Falso.

1. Still in the previous network and with the PC A in a private network, 1) is it possible to allocate IPs through DHCP? 1) What can be the pool of addresses? 3) What is the source address used by the PC A to contact the DHCP server?

1)Sim; 2)Não sei; 192.168.1.1 – 192.168.1.100 as exemple; 3)0.0.0.0

1. Considering IPv6 in the previous network, answer as true or false:
   1. PC A has always a local IPv6 address FE80::/10.

Falso. Verdade.

* 1. PC A has always a global IPv6 address, such as 2001::/16.

Falso.

* 1. PC A can have an IPv6 address without the help of the router.

Verdade.

* 1. PC A can have several global IPv6 addresses.

Verdade.

* 1. PC A needs its MAC address to generate the local IPv6 address.

Falso.

* 1. PC A needs its IPv4 address to generate the local IPv6 address.

Falso.