# UNIVERSITE LIBRE DE BRUXELLES

**ELEC-H-417**
**Communication Networks: protocols and architectures**

Full name : _____

Section: _____

- The exam duration is 3 hours.

- Please, write down your name on each answer sheet you submit.

## Short questions

1. (20 points) Give short answers. Write them on this sheet.

    (a) TCP implements a "pipelining" technique. What is its purpose ?

    _____

    _____

    (b) In IPv6, there is no broadcasting. How do routers share routing messages over adjacent links ?

    _____

    _____

    (c) What is the purpose of the 3-way handshake in TCP ?

    _____

    _____

    (d) Are link-state routing protocols scalable ? Why ?

    _____

    _____

    (e) In UDP, what does uniquely identify the destination application to communicate to ?

    _____

    _____

    (f) Cite 2 reasons for which TCP is suitable for a reliable file transfer.

    _____

    _____

    (g) Give two properties of a hash functions ?

    _____

    _____

# Architectures and Protocols

2. (20 points) **Network Address Translation** – Fig.1 depicts the general implementation of a residential internet access using a NAT box.

   (a) What is the purpose of NAT middleboxes ? Explain *in details* its functioning based on the scenario of Fig.1. For instance, consider that the computer at 10.0.1.1 connects to the webserver 164.15.59.200. Give, step by step, all transactions, the IP-layer headers of the packet, the content of the NAT table, etc.

   (b) Is it possible to reach a host in the "inside" zone from the "outside" zone ? Why/How ?

   (c) From a networking point-of-view, what is the maximum number of sessions that can be supported by a NAT box (consider that the RAM memory of the box is very large and not a limitation).
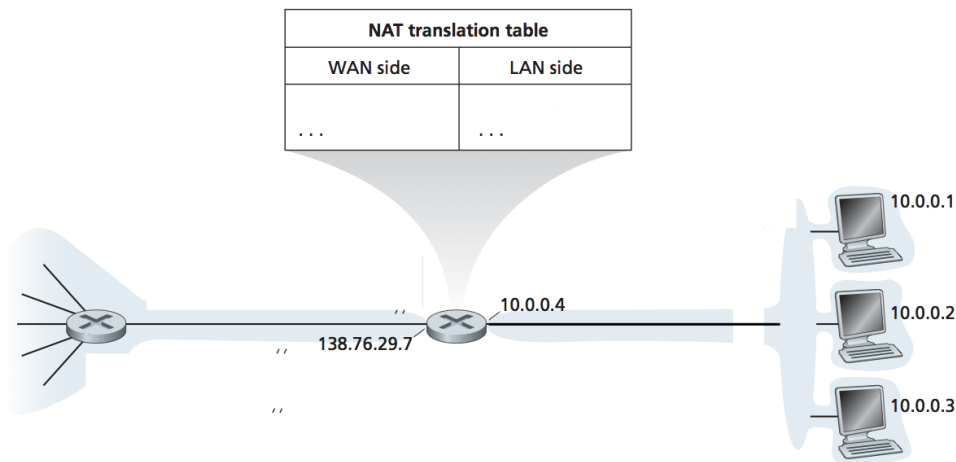


Figure 1: Network schema for a residential access using NAT box.

3. (20 points) **TCP pipelining** – [ Based on an example ]

   (a) What is the difference between flow control and congestion control ?

   (b) Consider a transmission scheme where one packet is sent and acknowledge at a time. The next packet cannot be sent before the acknowledgement of the current packet is received by the emitter. Compute the efficiency $\eta$, i.e., the ratio between the transmission time of a packet (in its local network) and the interval between the sending of two consecutive packets. Express it as a function of the packet length $L$ (unit: bits) and the line rate $R$ (unit: bits per second).

   (c) Define the round trip time RTT.

   (d) How does TCP set the maximum size of the pipeline $N_{max}$ ?

4. (20 points) **Security** – Consider two entities Alice and Bob wanting to securely communicate.

   (a) (1) Give (in details) the Diffie-Hellmann key exchange protocol. (2) What is a man-in-the-middle (MiTM) attack ? (3) Why is DH key exchange sensitive to MiTM attacks ?

   (b) Define a digital signature $\sigma$ of an identity $ID$ and its public key $K$.

   (c) How can Alice use her digital signature $\sigma$ with Bob to established a secure and authenticated communication channel with Bob ? What is the role of the Trusted Third Party (TTP) ?

5. (20 points) **Labs and IP routing** – One startup IT company is going to be expanded by establishing other 2 new Branches in Brussels. Every Branch will have 2 computers (PCs) connected to one switch (S) and one router (R). The network address at Ixelles Branch is 172.16.1.0/24, in Etterbeek Branch 172.16.2.0/24 and in Uccle Branch 172.16.3.0/24. By considering the following topology answer the questions:
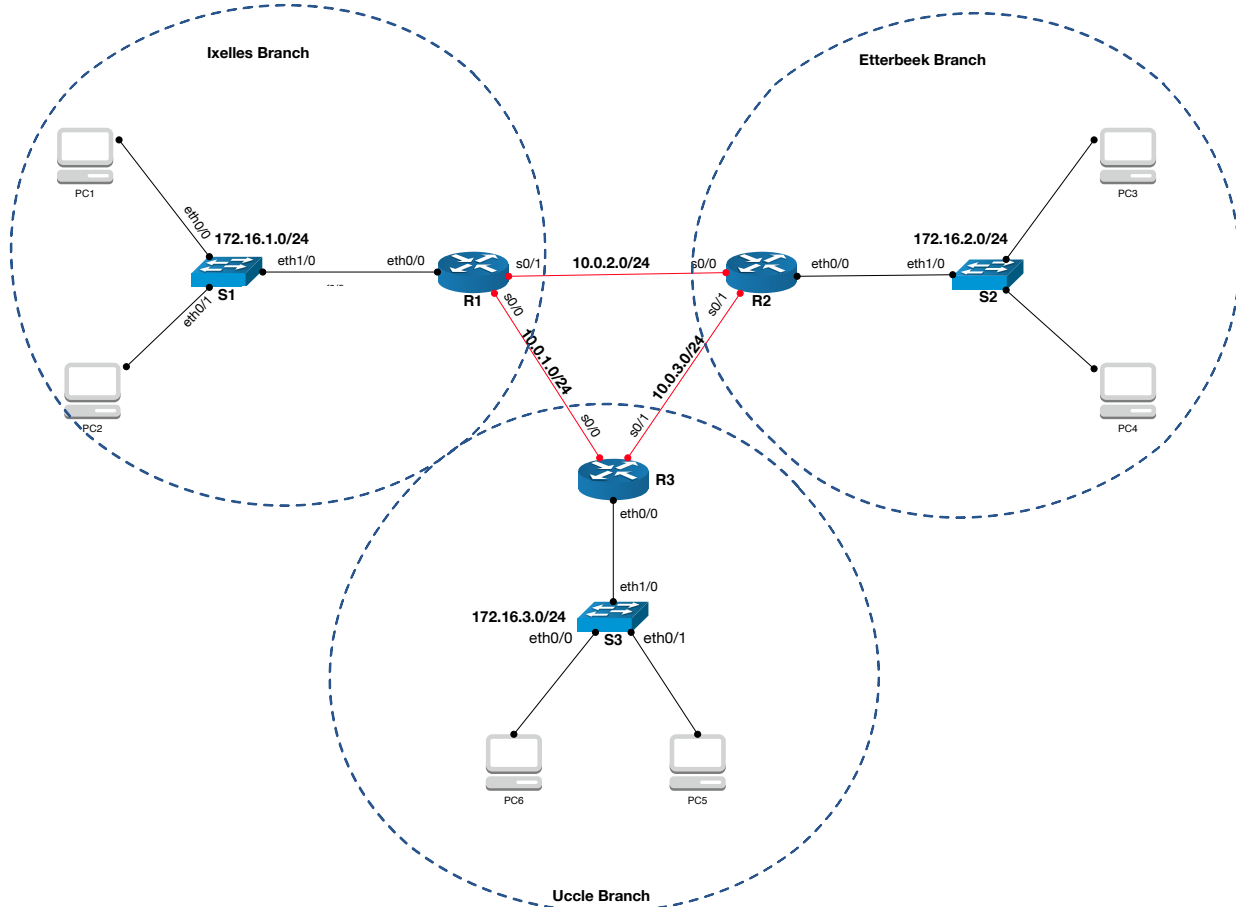


Figure 2: Company Network Topology

- Give the routing tables of the router R1.
- If the Ixelles Brach wants to communicate (a) with Uccle Branch and (b) with Etterbeek Branch, which steps should be considered? Specify the commands that should be executed and in which router. (Assume that we have static routing.)
- In the case where dynamic routing is considered, which will be the steps if we want to perform dynamic routing instead of static?

| Question: | 1 | 2 | 3 | 4 | 5 | Total |
|-----------|-----|-----|-----|-----|-----|-------|
| Points:   | 20  | 20  | 20  | 20  | 20  | 100   |
| Score:    |     |     |     |     |     |       |