Network Architecture and Security

ECAM STRASBOURG-EUROPE 2018-2019

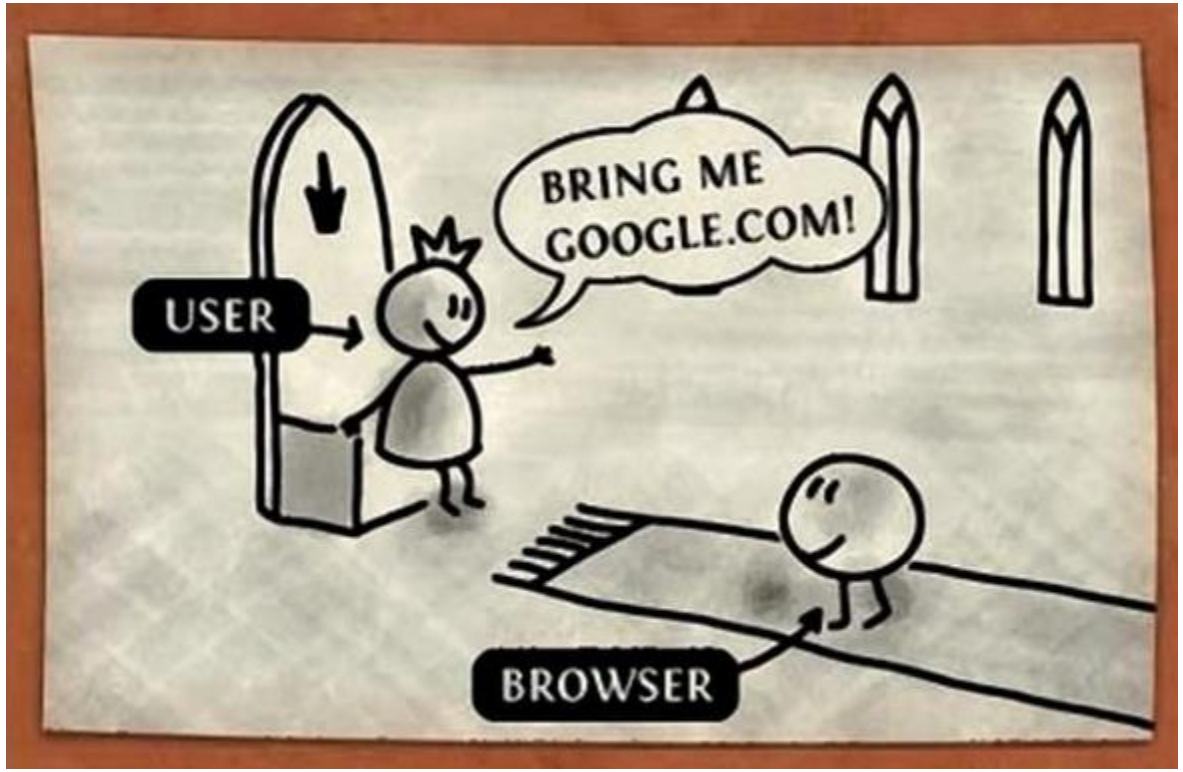
LECTURER: ROMAIN ORHAND (ROMAIN.ORHAND@ECAM-STRASBOURG.EU)

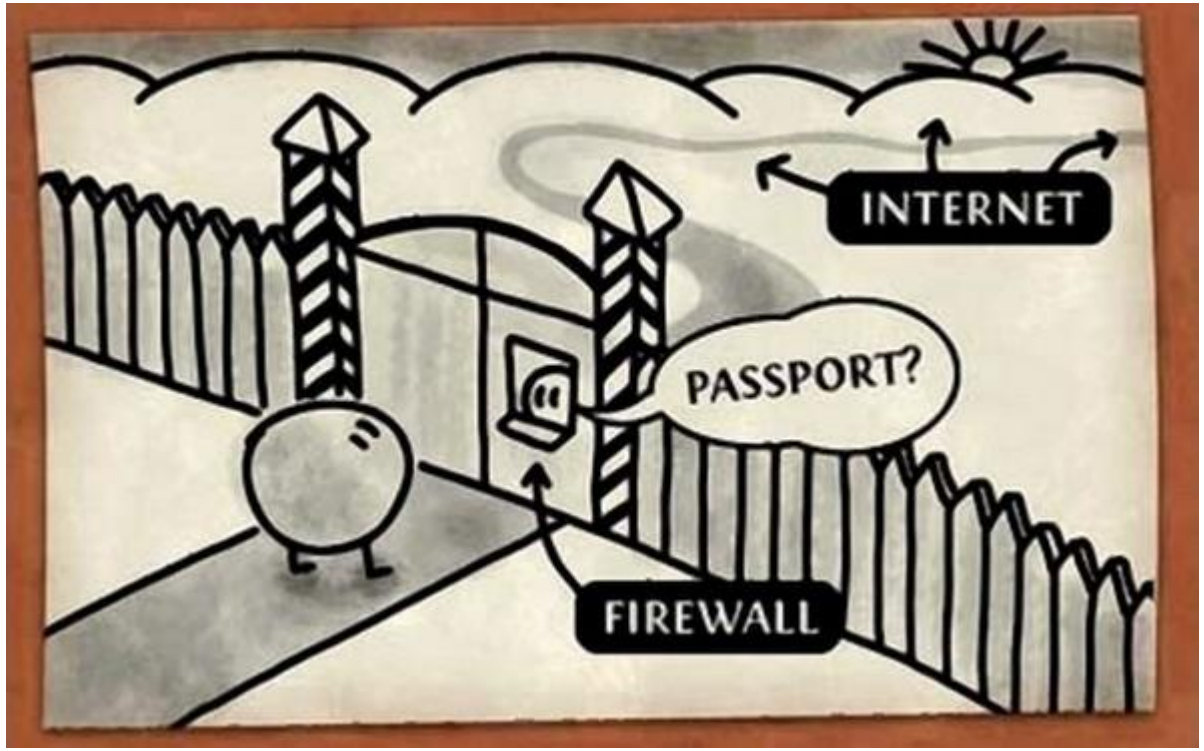
Objectives

- Designing a simple corporate network (including security appliances)
- Designing IP addressing scheme
- Having some knowledge of the OSI model
- Having some knowledge of TCP / IP
- Knowing some of the rudiments of cryptography

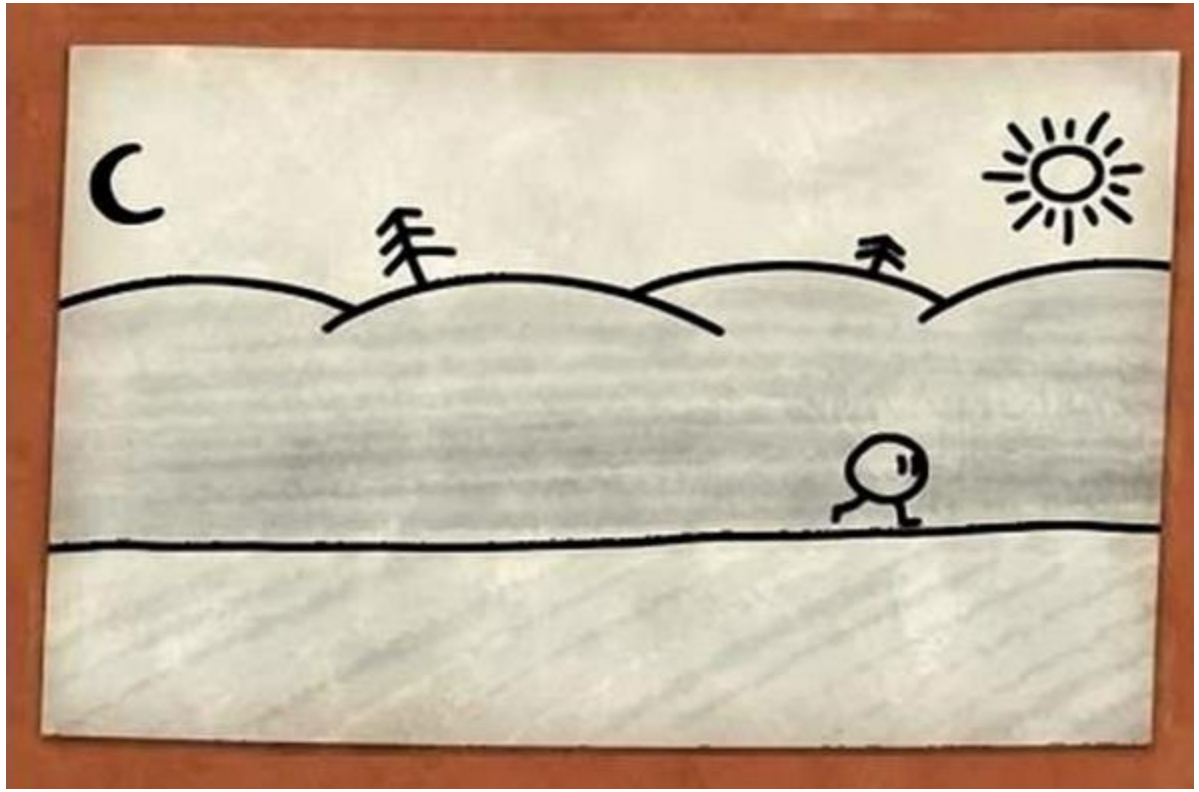
Introduction

ONCE UPON A TIME …


BRING ME GOOGLE.COM!
USER
BROWSER

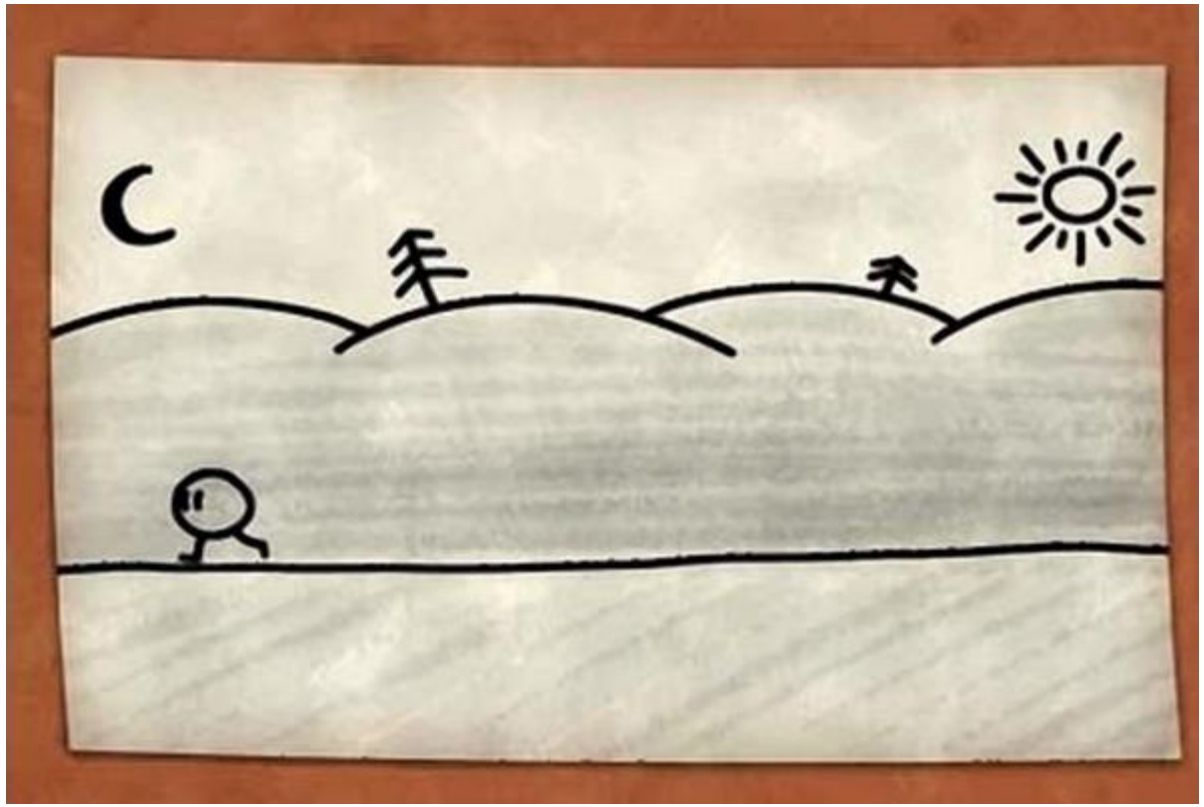

INTERNET
PASSPORT?
FIREWALL

DNS SERVER
23.45.67.89!
GOOGLE.COM?
12.34.56
98.76.5

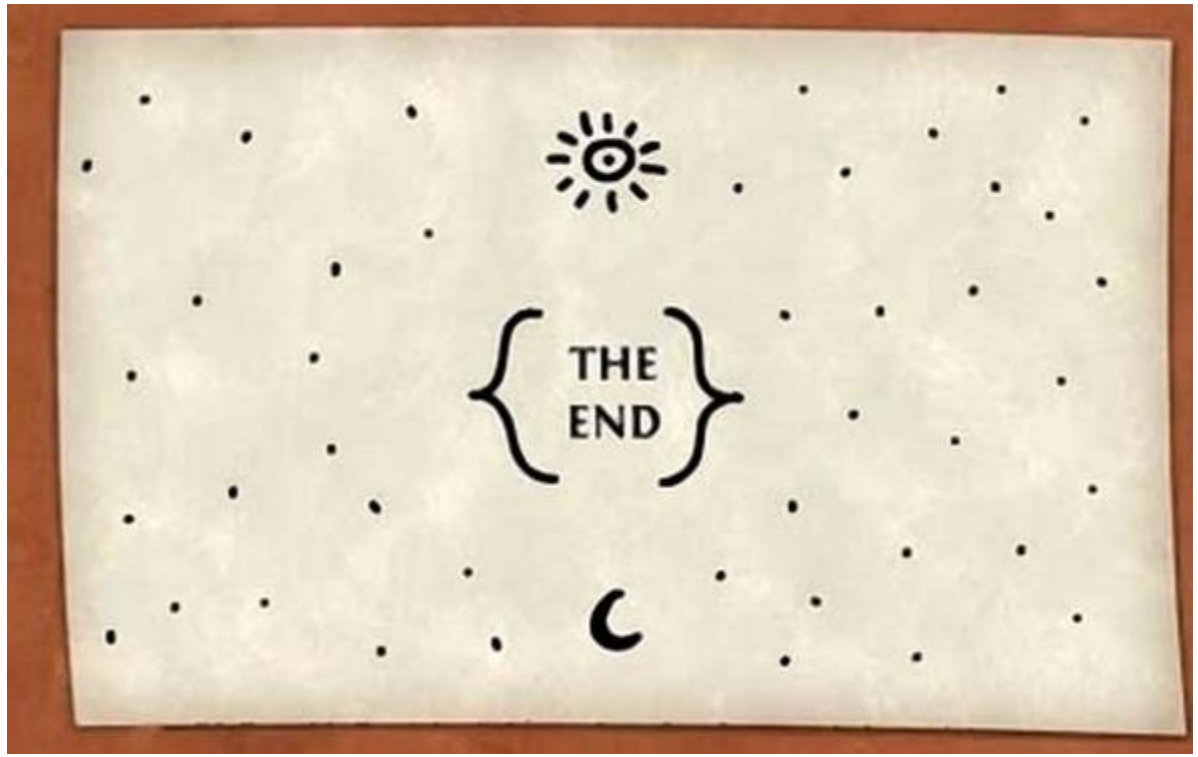


HOSTING SERVER
IP-ADDRESS
23.45.67.89
VIA 9GAG.COM

WEBSITE
SIGN IN!
I'M FEELING LUCKY!
ADVANCED SEARCH!
GOOGLE.COM?



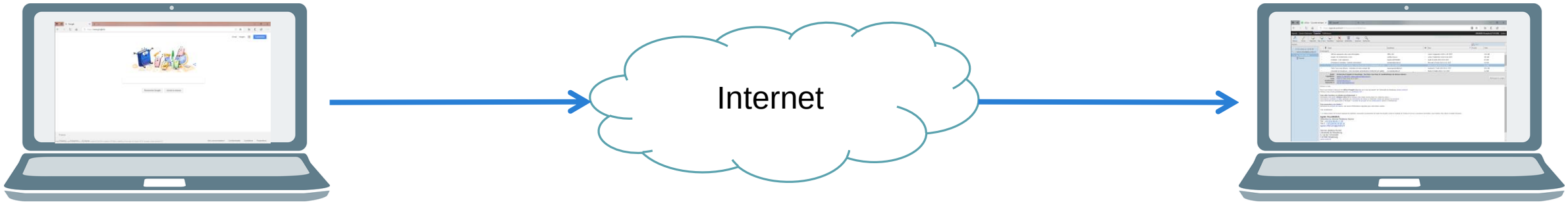
SIGN IN!
I'M FEELING LUCKY!
ADVANCED SEARCH!

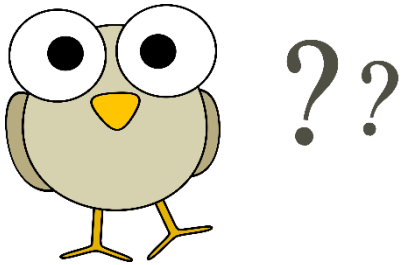

THE
END

Another Use Case

I WANT TO READ MY MAILS …

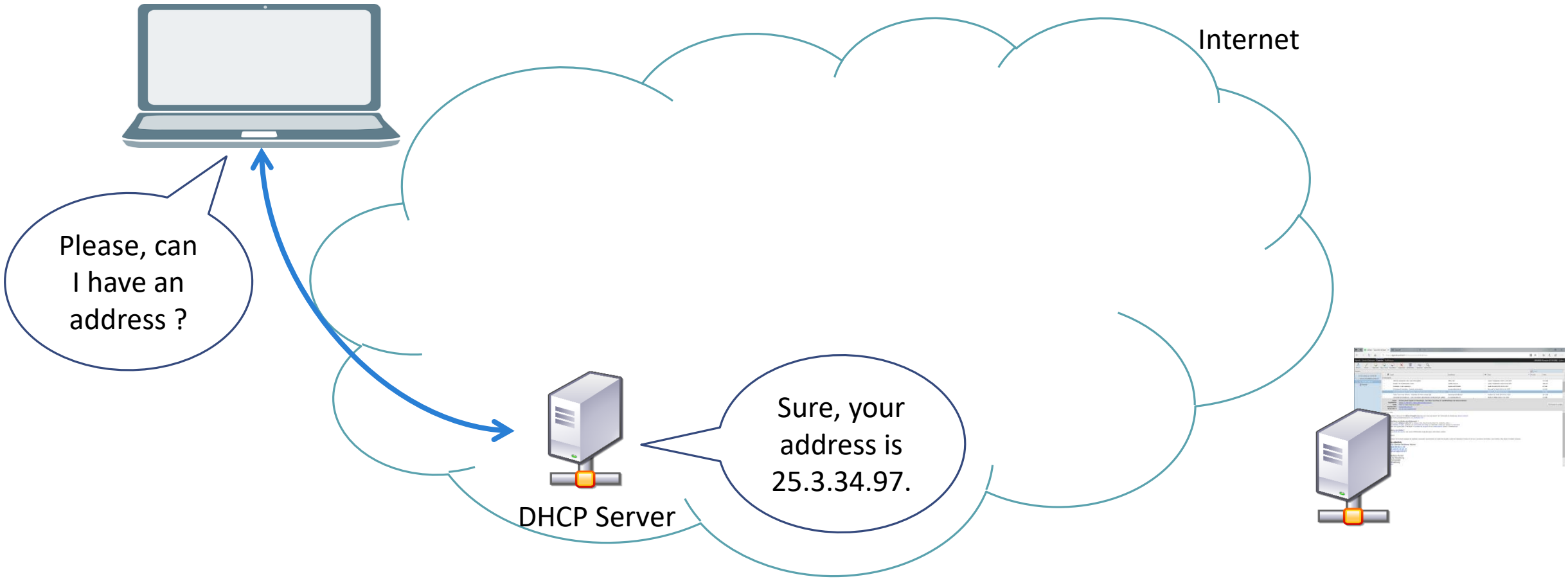
0. What I want



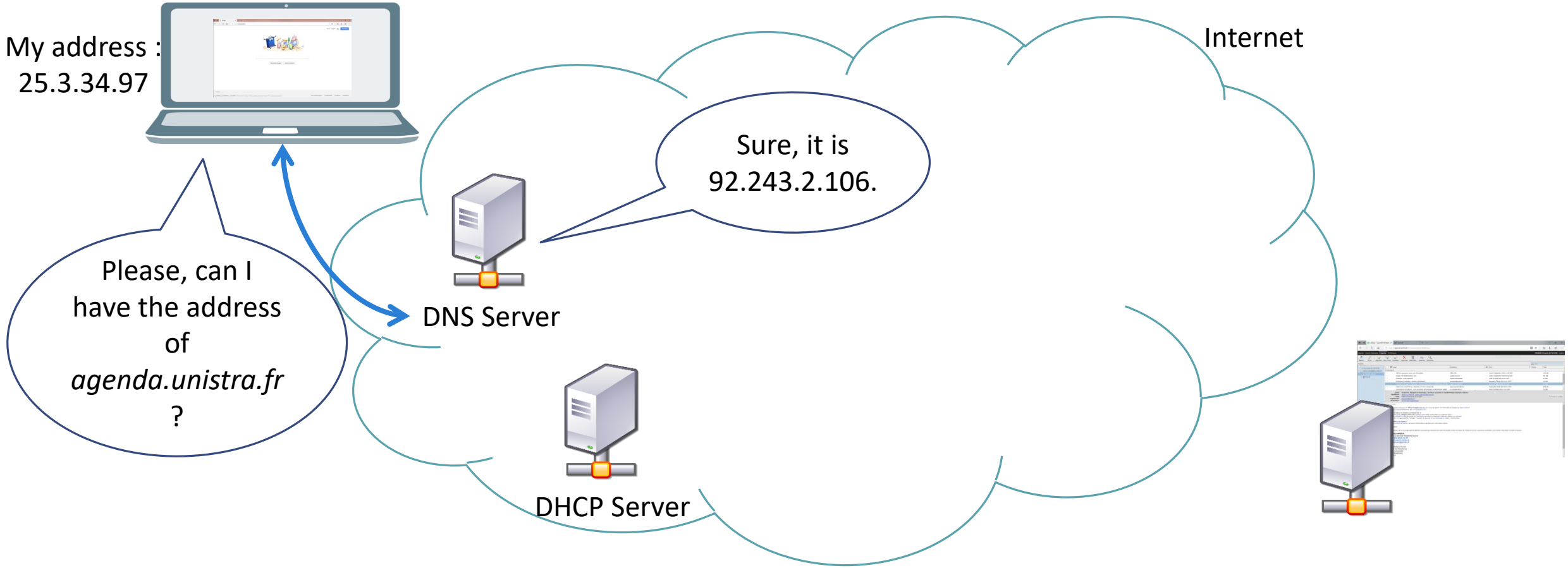


??

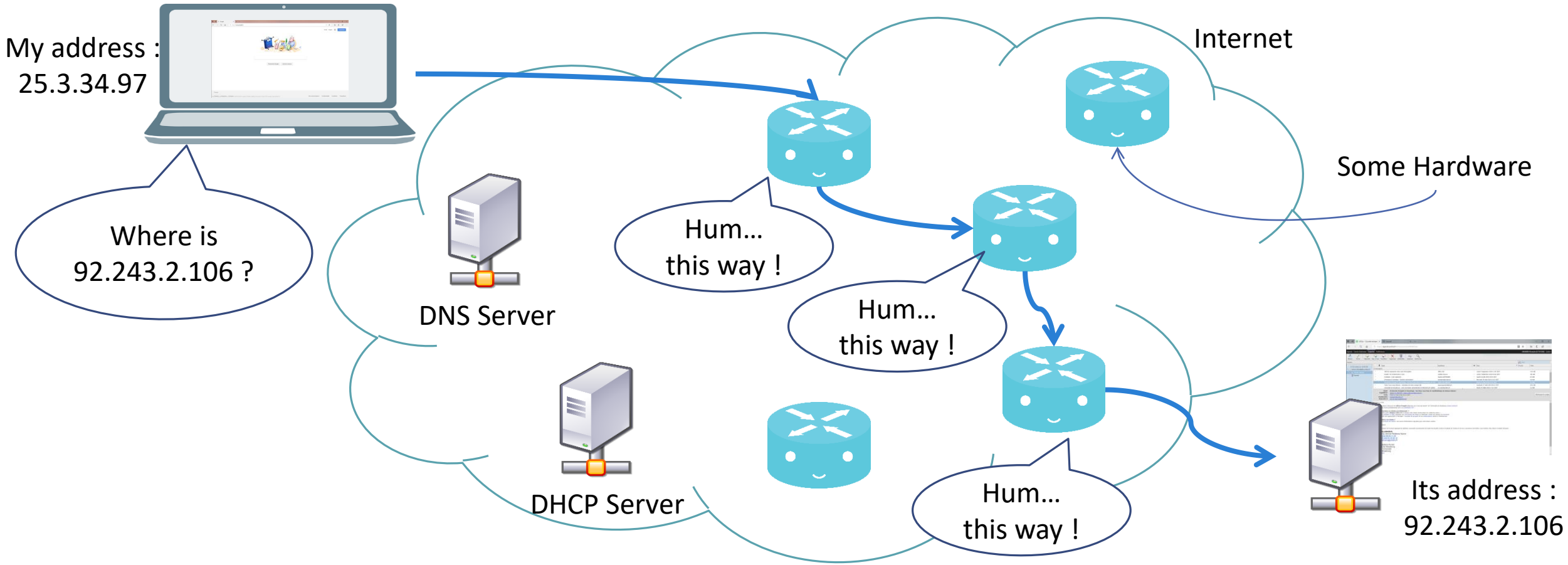
1. Getting an IP address - DHCP



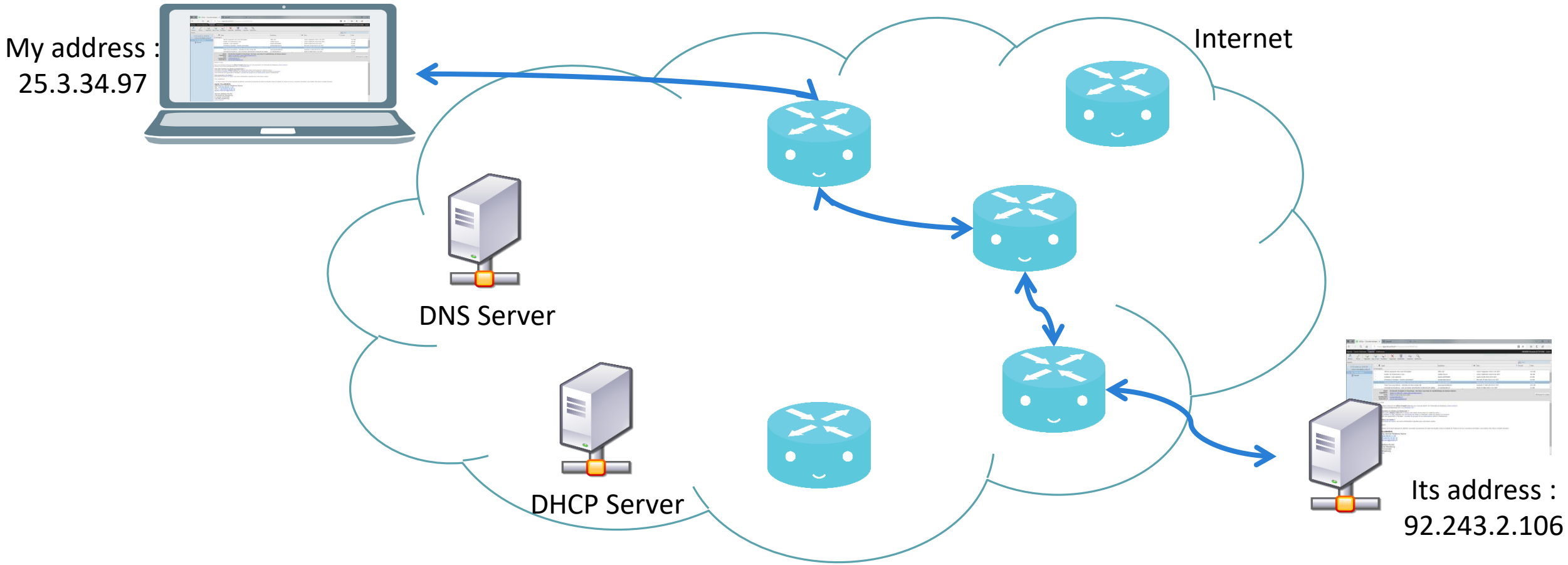
2. Getting the webmail server address - DNS



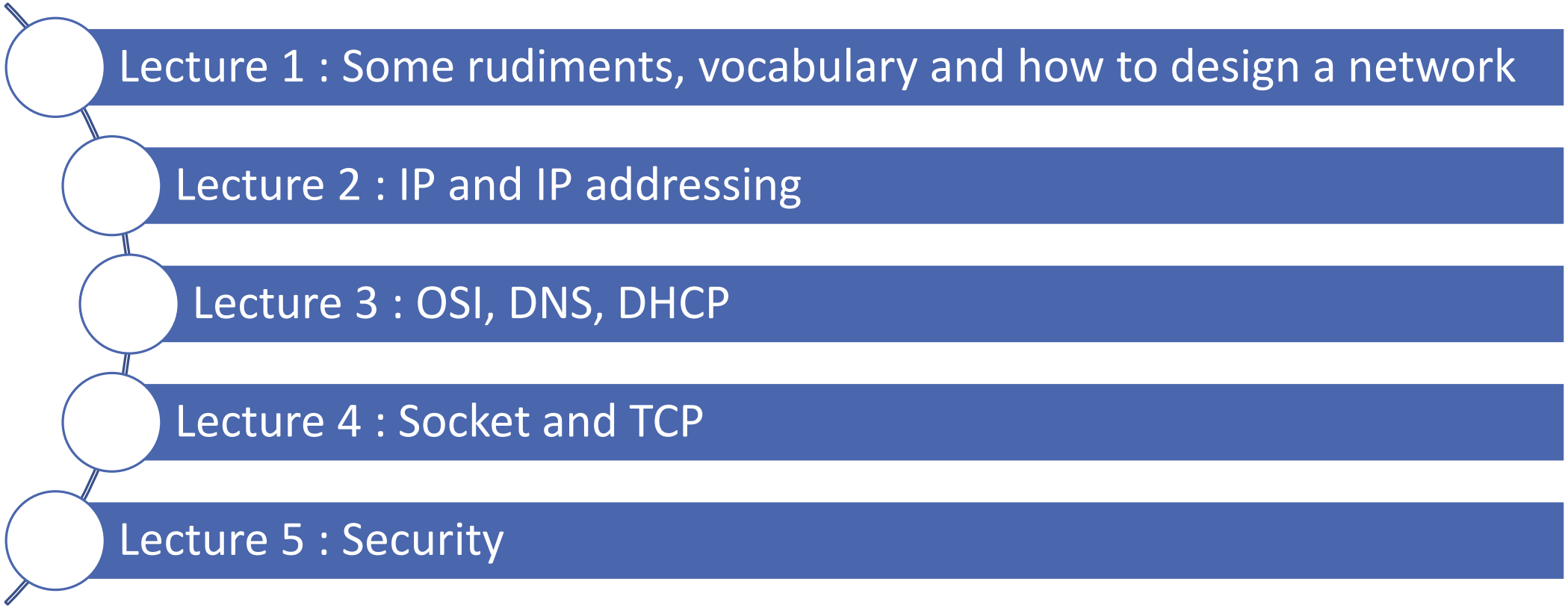
3. Finding its way out – TCP-IP routing



4. Getting access to webmail



The Lecture Outline



Some Concepts

THE NUMEROUS DEFINITIONS ARE COMING …

Just a reminder

A **name** indicates **what** we seek.

An **address** indicates **where** it is.

A **route** indicates **how** to get there.

IP address

Numerical label assigned to each device (e.g., computer, printer) participating in a computer network that uses the **Internet Protocol** for communication.

Format : U.V.Z.T where U, V, Z and T are between 0 and 255.

Example : 192.168.1.1

Two aims :

1. Host or network interface identification
2. Location addressing

What's behind ?

It is a **ROUTER !**

A router is a device that **forwards data packets between computer networks.**

When a data packet comes in one of the lines, the **router reads the address information** in the packet to determine its ultimate destination (**the routes**).

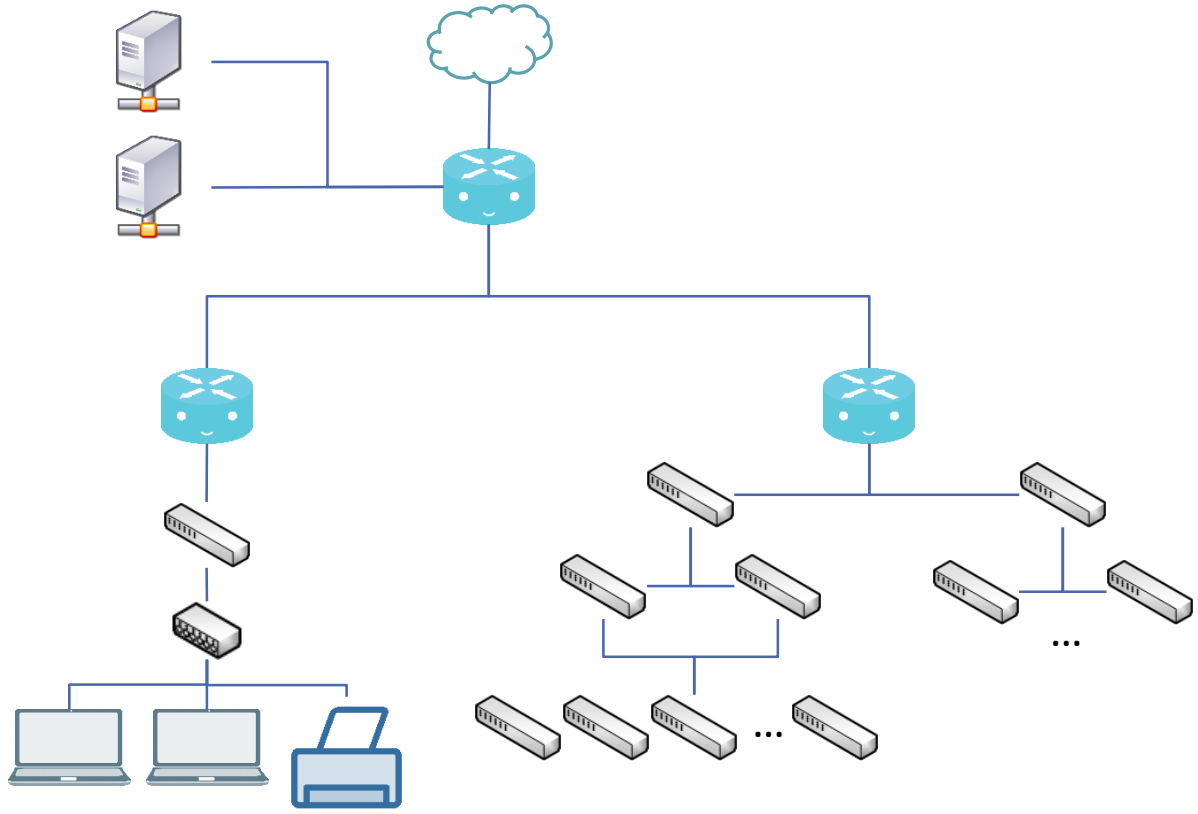
Between Routers, Routing

Routing **is the process of selecting a path for traffic** in a network or between or across multiple networks.

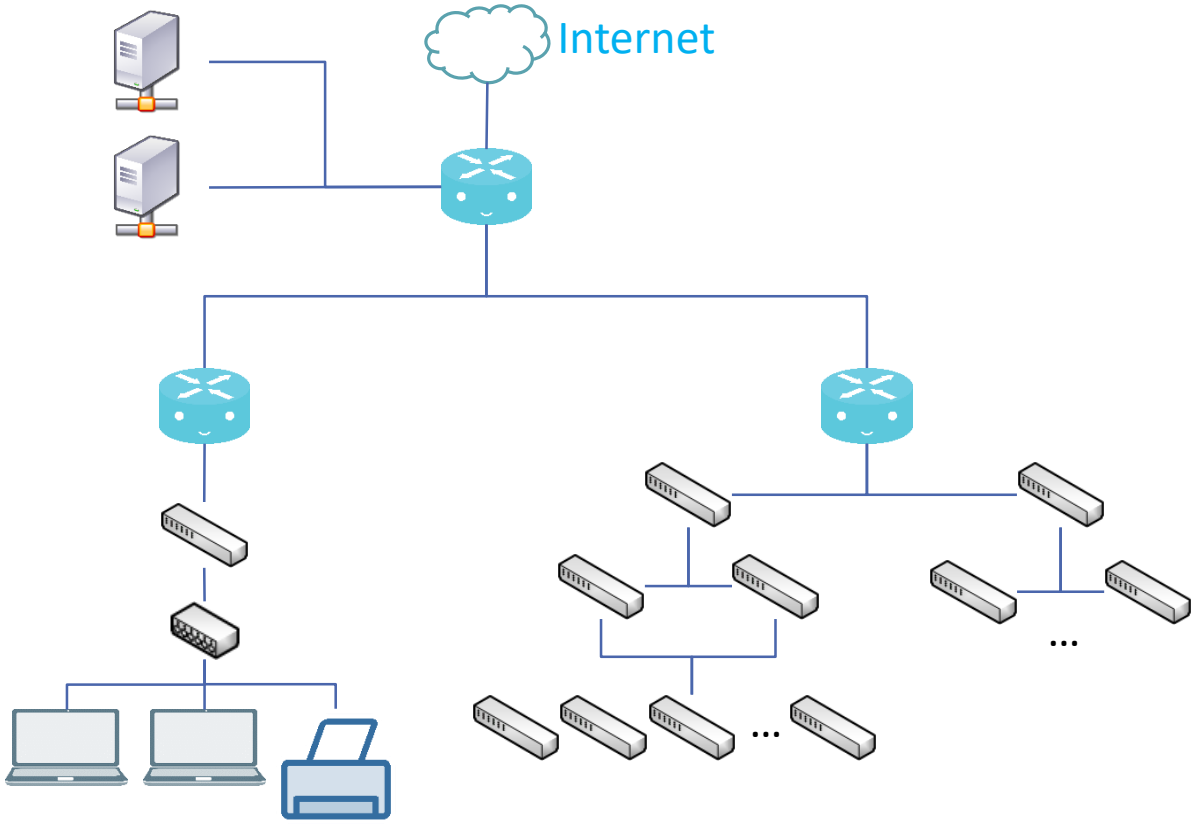
Routing schemes differ in **how** they deliver messages :

- Unicasting;
- Broadcasting;
- Multicasting…

An example of corporate network



Private Network



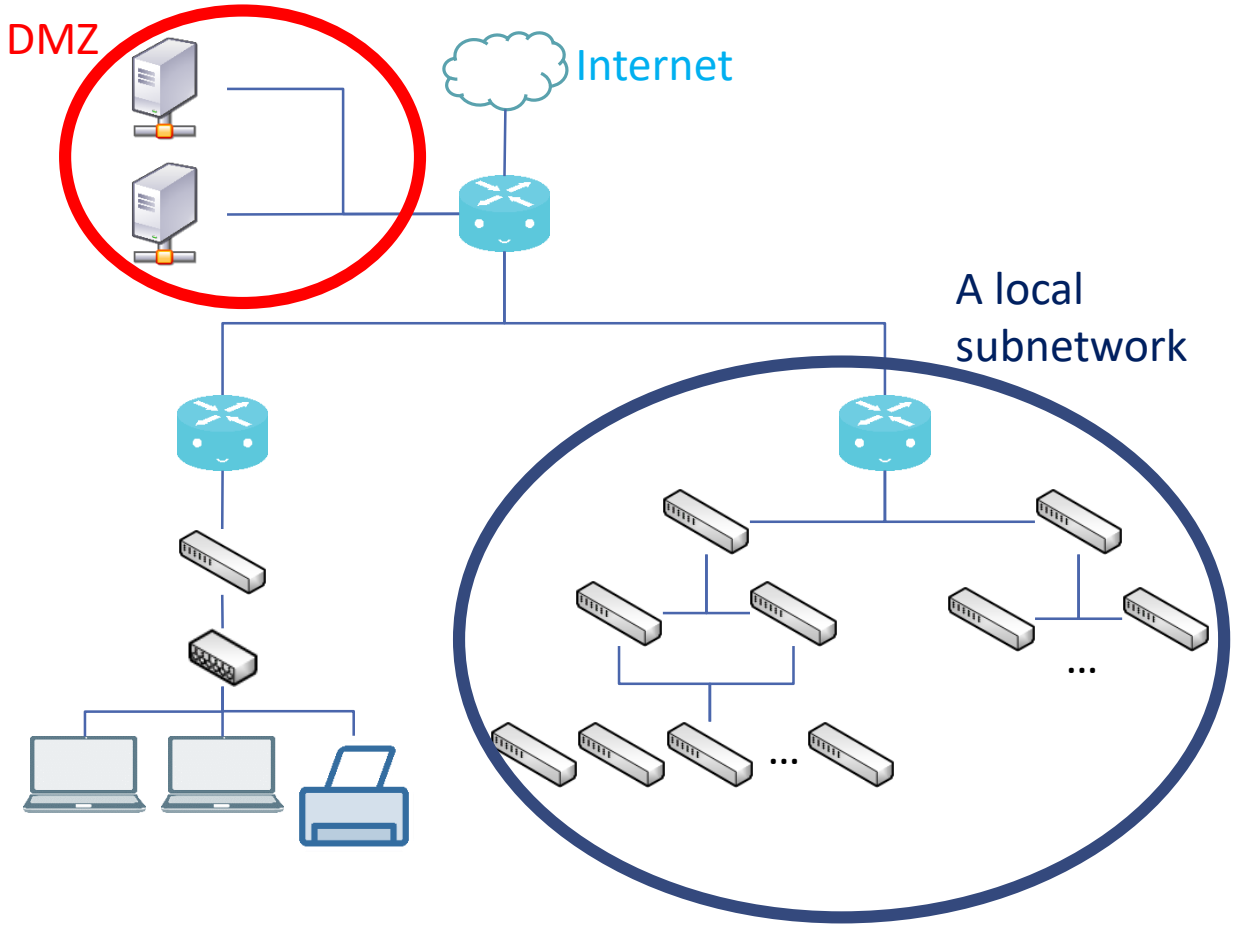
It is a network that uses **private IP address space defined by some specifications** (IPv4 and IPv6 ones).

IP packets addressed from them **cannot be routed through** the public internet.

Examples of IP addresses used :

- 10.0.0.0 to 10.255.255.255
- 172.16.0.0 to 172.31.255.255
- 192.168.0.0 to 192.168.255.255

DMZ – Delimitarized zone

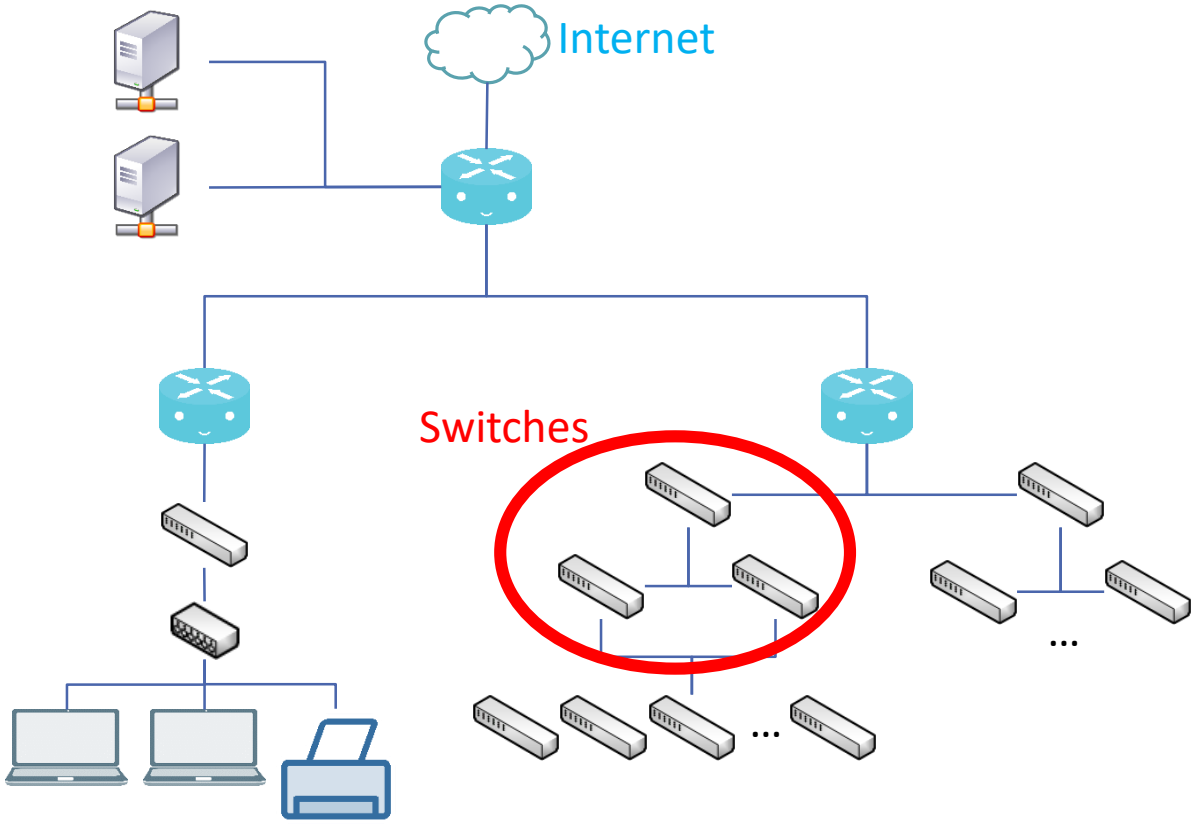


An isolated subnet separated from the **local network** and separated from **Internet by a firewall.**

Services are **embedded in the DMZ** so that they can be accessed from Internet such as a mailing service or a printing service.

Firewall is a **network security system** that monitors and controls incoming and outgoing network traffic based on predetermined security rules.

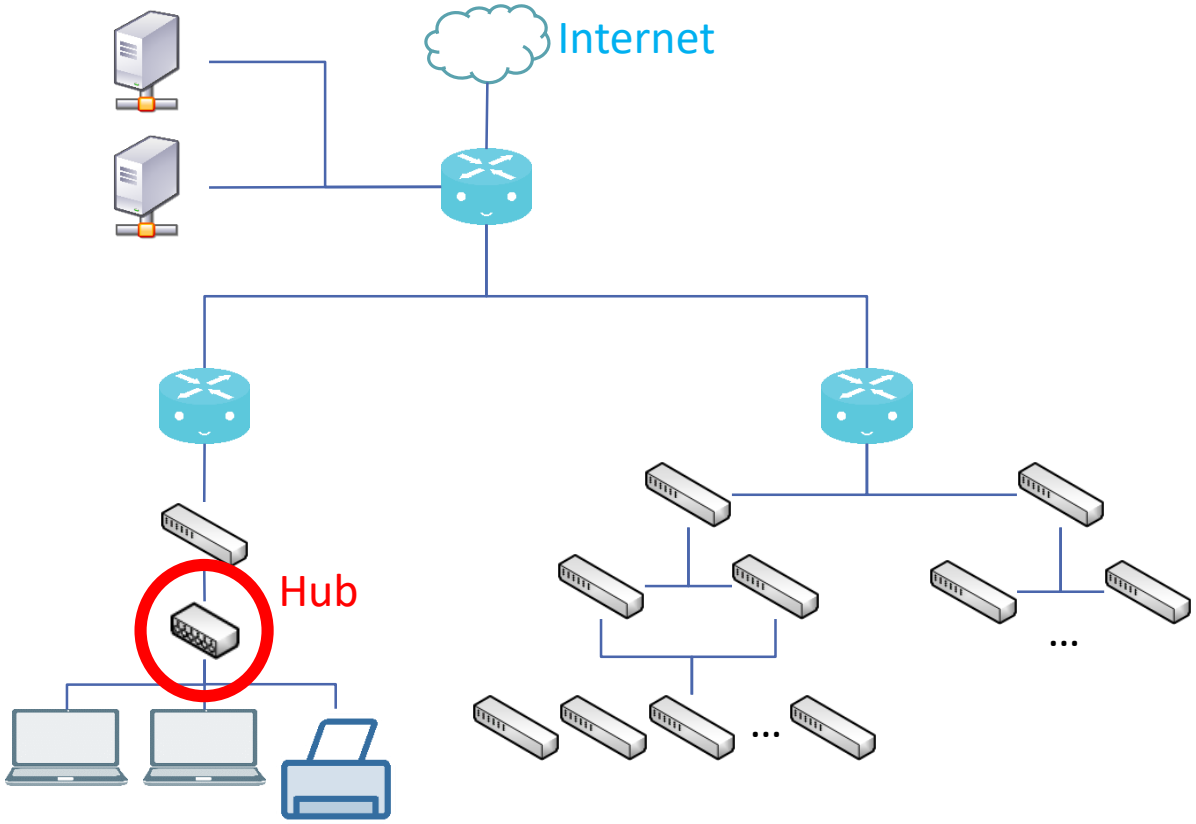
Switch



Switch is a computer networking device that links **network segments or network devices.**

It receives messages from **any devices** connected to it and then transmits the messages **only to the device** for which the message was meant.

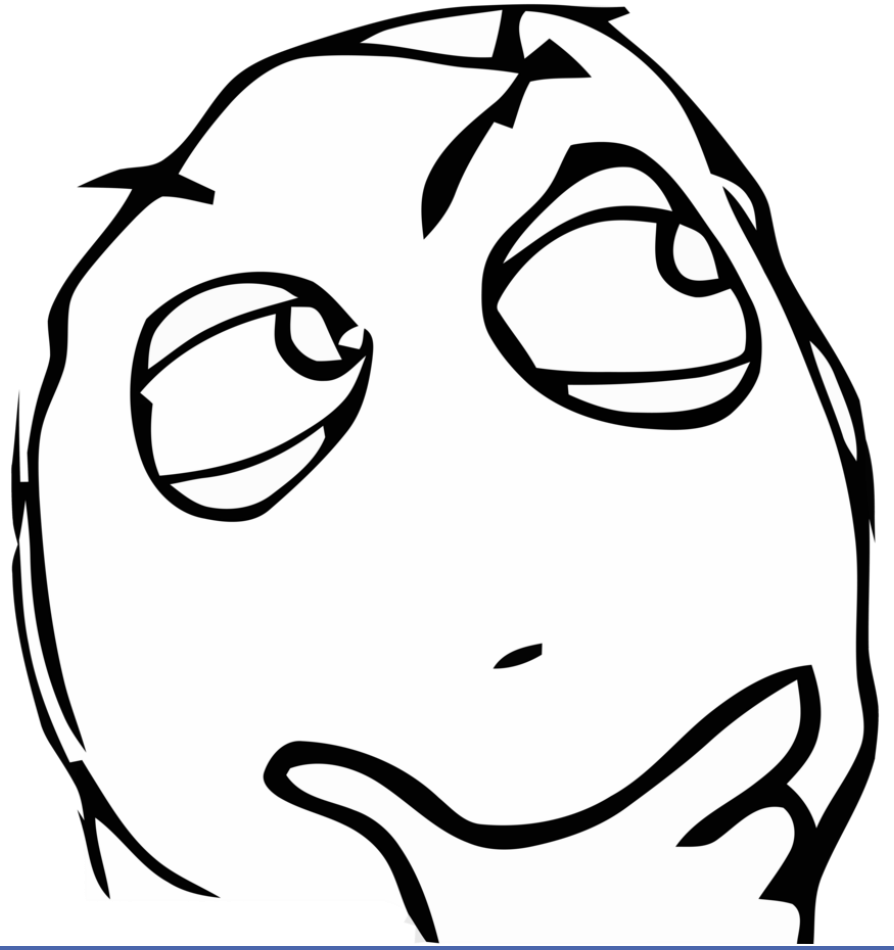
Hub



Hub is a device for connecting multiple Ethernet devices together and making them act as a **single network segment**.

It receives messages from **any devices** connected to it and then transmits the messages **to all devices except the sender**.

Any questions ?



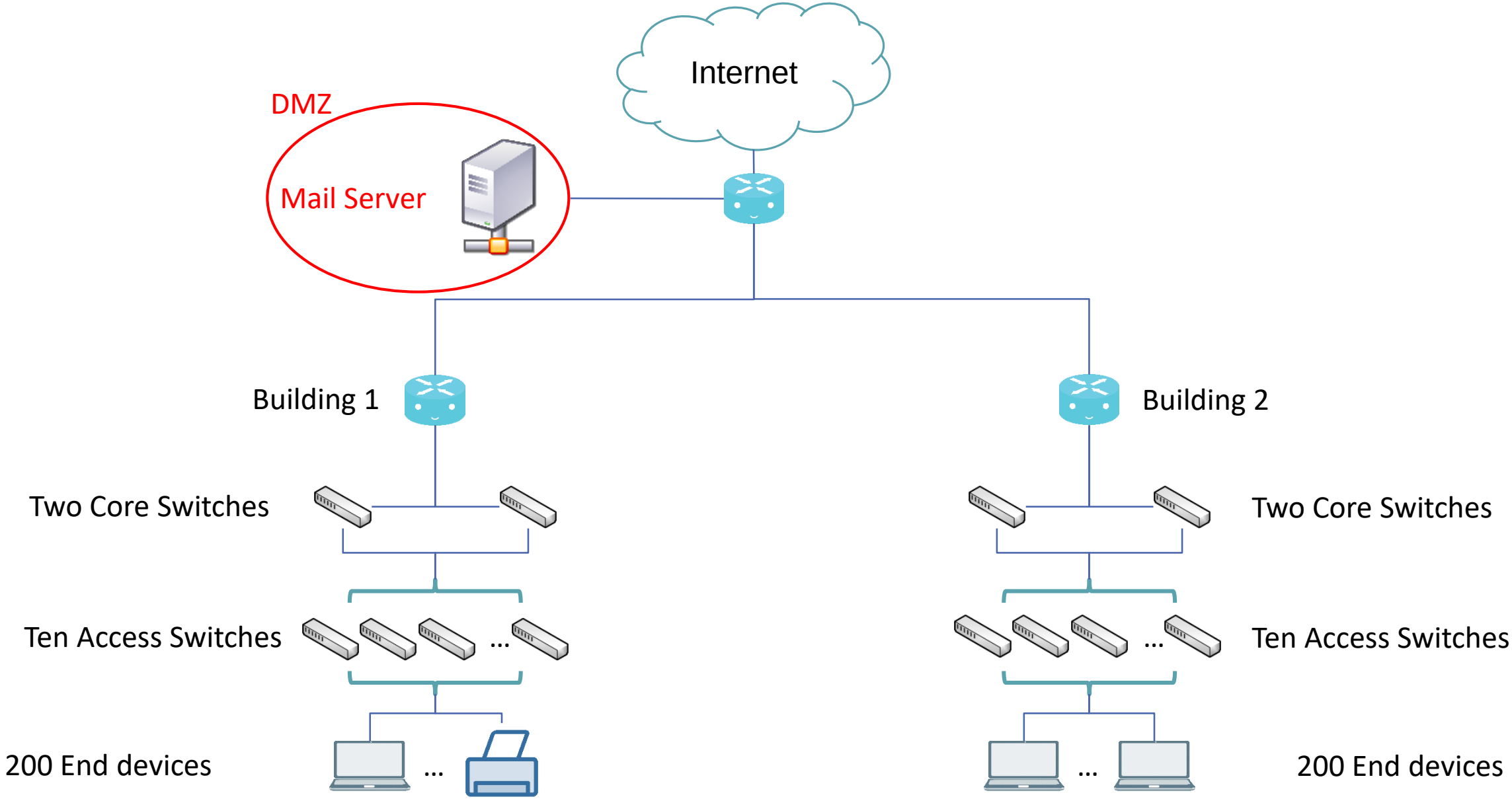
Exercices

Exercice 1

Design a local network with a mail server and two buildings having 200 end devices (PCs, printers, etc.) each.

Constraints are:

- The mail server is set in a DMZ (demilitarized zone)
- Three routers having each 4 ports are used: 1 between the enterprise network and the Internet, and one at each building.
- Each building is equipped with two core switches for redundancy and 10 access switches
- Switches all have 24 ports.


Internet
DMZ
Mail Server
Building 1
Building 2
Two Core Switches
Two Core Switches
Ten Access Switches
Ten Access Switches
200 End devices
200 End devices

Exercice 2

What are the differences between a switch, a router and a hub?

What about the next lecture ?

We will speak about IP addresses and IP addressing because the previous scheme is not complete =)

And so, you'll be able to (remember):

- Design a simple corporate network (including security appliances)
- Design IP addressing scheme