Cybercrime

Informatique Légale et Multimédia – ILM 2021/2022

Dr. Bourebia Soumia

Mohamed Seddik Ben Yahia university, Jijel

Email: soumia.bourebia@univ-jijel.dz

Informatique Légale et Multimédia - ILM

- Course title : **Cybercrime**
- Credits : **6**
- Coefficients : **3**

Chapter 1 : the Cybercrime Phenomena

Defining Cybercrime

Refers to criminal acts committed using the Interne tor another computer network as a component of the crime.

- **How can computers and networks be involved in crimes?**

1. The computer or network can be the tool of the crime (used to commit the crime).

2. The computer or network may be the target of the crime (the "victim").

3. The computer or network may be used for purposes related to the crime (e.g., to keep records of illegal drug sales).

Crimes That Use the Net VS Crimes That Depend on the Net

Crimes That Use the Net : computer network is somehow involved Or traditional crimes which can be increased in scale by using computers.

Crimes That Depend on the Net : the crime is unique and came into existence with the emergence of the Internet **(**can only be committed through the use of online devices)

1. **Examples :**

Unauthorized access, Hacking, Distributed Denial-of-Service (DDOS) attacks , drug sales,

Categorizing Cybercrime

- **Typology of cybercrime**

- **Because the term "cybercrime" is used to describe a wide variety of offenses, it is difficult to develop a typology or classification system for this type of crime. However, an interesting attempt should be noted:**

- **the system proposed by the Council of Europe Convention on Cybercrime, which distinguishes four types of offences:**

-offences against the confidentiality, integrity and availability of computer data and systems

- Offences related to content

- offences related to intellectual property rights

offences against the confidentiality, integrity and availability of computer data and systems

- All crimes classified in this category violate (at least) one of the three legal principles of confidentiality, integrity and availability.

Overview of the most common offences classified in this category:

1- Illegal access (hacking, cracking):

Hacking is the illegal access to a computer. It is one of the oldest computer crimes. with the development of computer networks (especially the Internet), this offence has become a become a widespread phenomenon.

offences against the confidentiality, integrity and availability of computer data and systems

The following examples illustrate some of the infractions that fall under the category of " hacking ":

- cracking a password or breaking into password-protected websites

- exploiting a software or hardware flaw to illegally obtain a password to enter a computer system

- creation of " spying " websites (spoofing) websites designed to trick users into revealing to reveal their passwords

- installation of keyboard recording hardware or software (e.g., "keyloggers"), which records all typed input and, therefore, all passwords entered on the computer and/or device

offences against the confidentiality, integrity and availability of computer data and systems

2- Data spying :

-Computer systems often contain sensitive data. If the system is connected to the Internet, a hacker can try to retrieve this data through the network.

-To enter their victims' computer systems, hackers use various techniques, including :

- the use of software designed to scan for unprotected ports
- use of software designed to bypass protection measures
- social engineering";

offences against the confidentiality, integrity and availability of computer data and systems

2- Data spying :

Example: Phishing, for example, has recently become a major crime in cyberspace. It refers to the attempt to fraudulently appropriate sensitive data (e.g. passwords) by pretending to be a trustworthy person or company (e.g., a financial institution).

offences against the confidentiality, integrity and availability of computer data and systems

3- Illegal interception:

To obtain information, hackers can also intercept communications (e-mail for example) or data transfers (transfer to a server or access to an external storage medium via the Web).

offences against the confidentiality, integrity and availability of computer data and systems

Data Integrity Violation:

Hackers can violate the integrity of data in a variety of ways:

- by removal;

- by manipulation;

Offences related to content

- This category covers content that is considered illegal, such as xenophobia and insulting religious symbols.
- As a solution to this offence, there are several types of filtering systems. For example, Internet service providers can install programs which, after analysis, blacklist specific websites visited. Another solution is to install filtering software on the user's computer

offences related to intellectual property rights

- One of the most important functions of the Internet is the distribution of information. Companies, for example, use the Internet to disseminate information about their services and products.

- In terms of piracy, they face the same risks on the Internet as they do off-line: their brand image and graphic design can be used to sell counterfeit products. Counterfeiters copy logos and products;

Chapter 2 : Cyber attacks

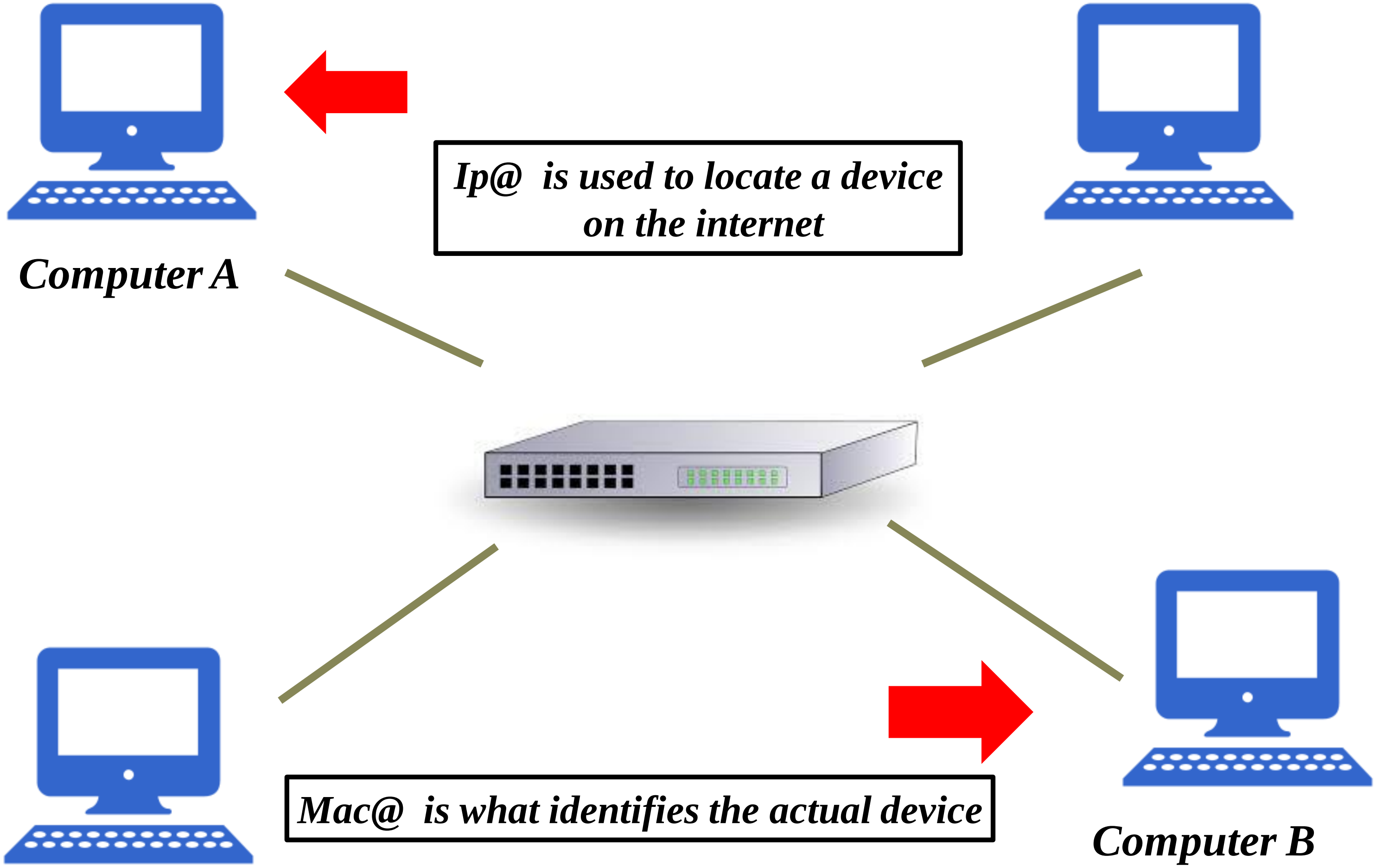
ARP spoofing

- ***What is ARP protocol ?***

Adress resolution protocol: used to resolve IP adresses to Mac Adresses. Computers on a local network need Mac@ to communicate with each other.

- ***Operating principle?***

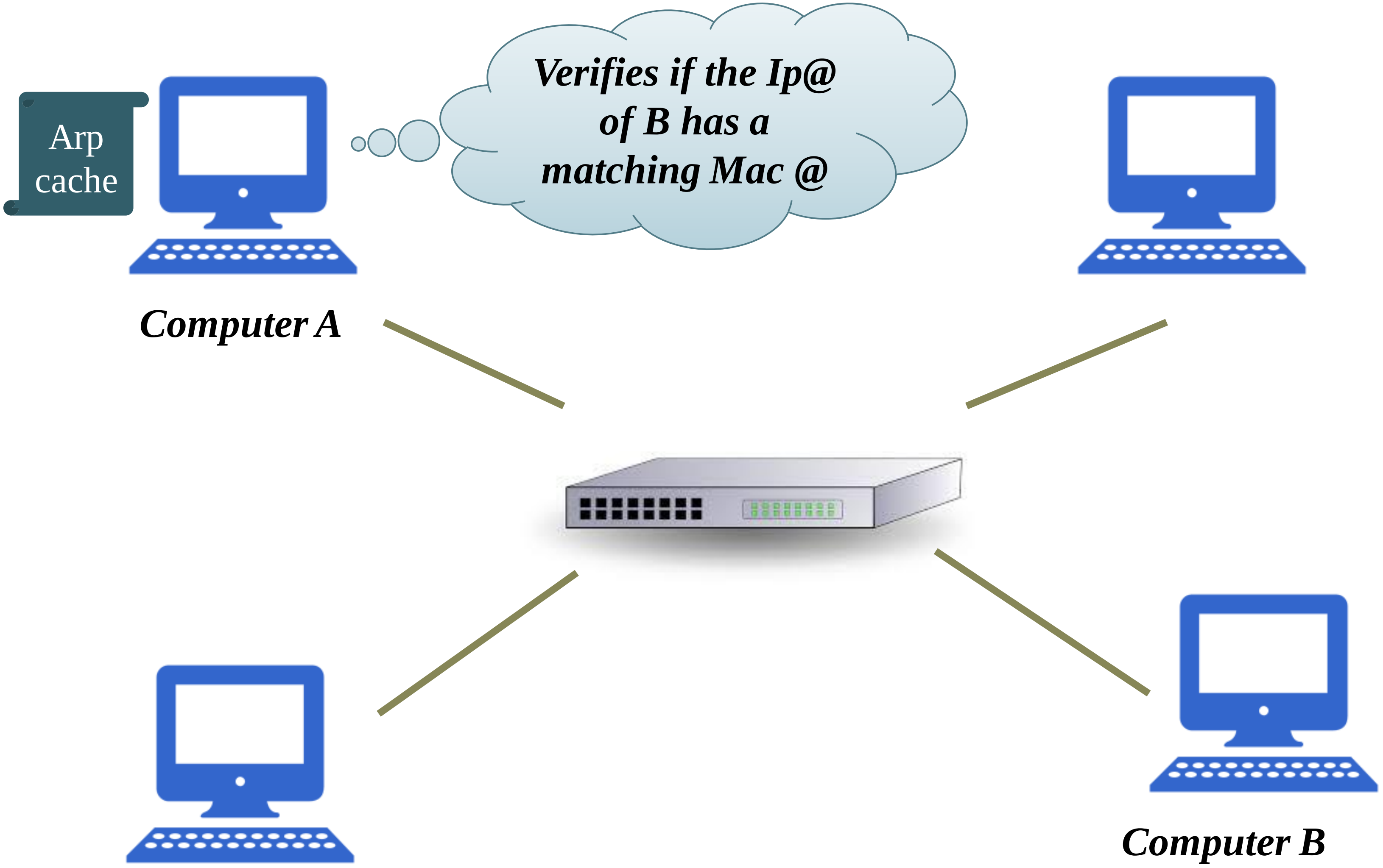
ARP Protocol



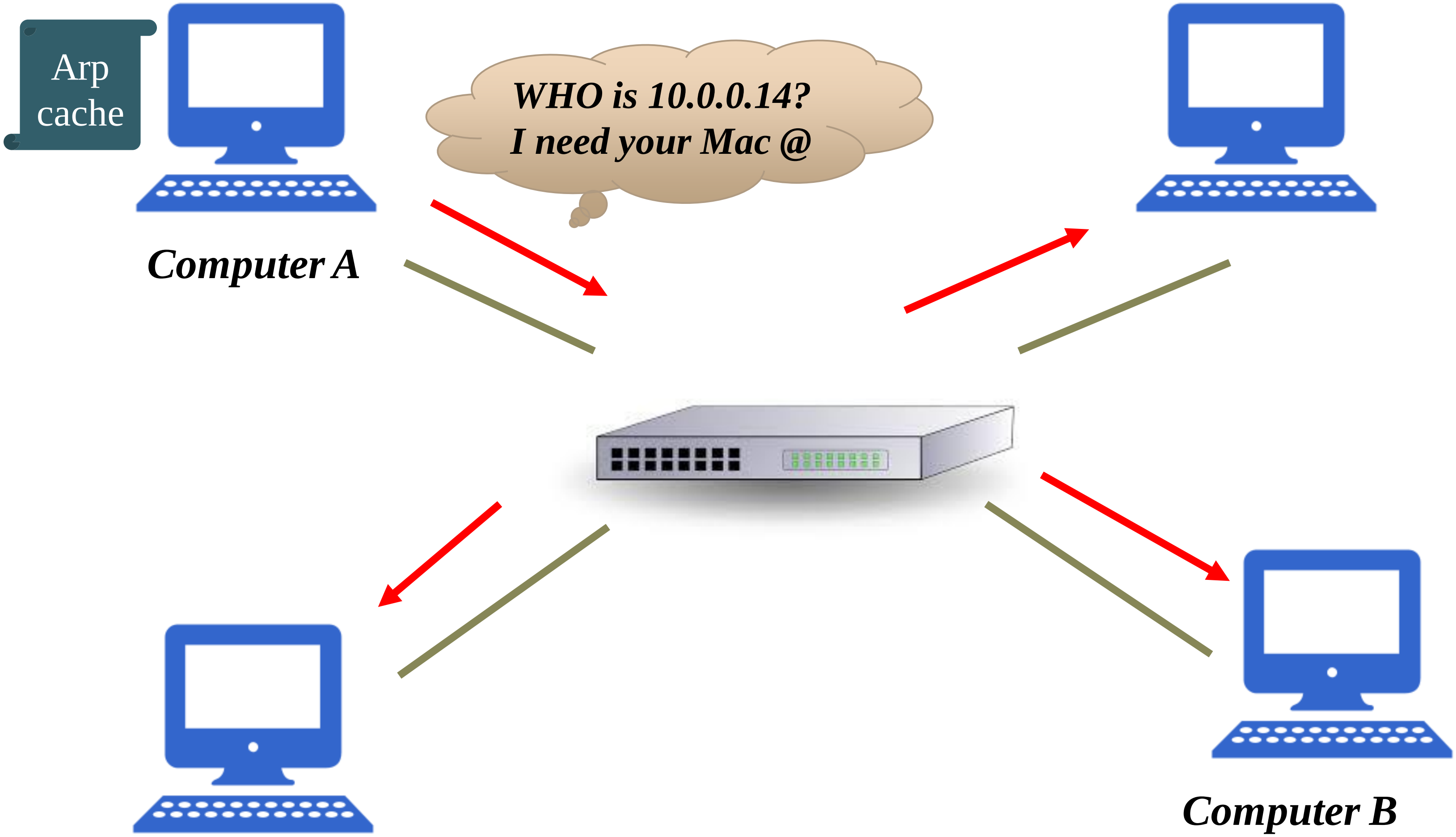
Ip@ is used to locate a device on the internet

Mac@ is what identifies the actual device

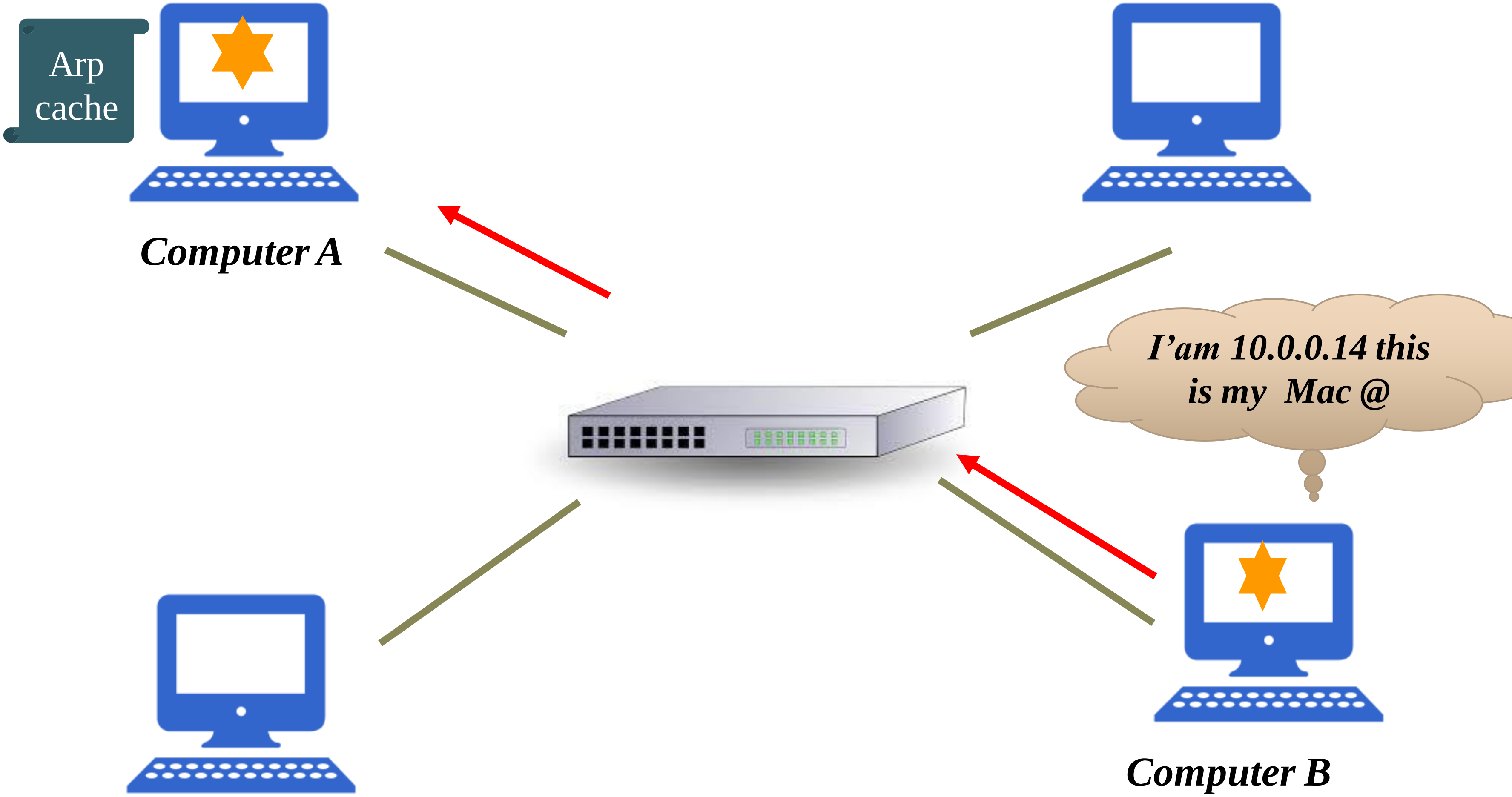
ARP Protocol



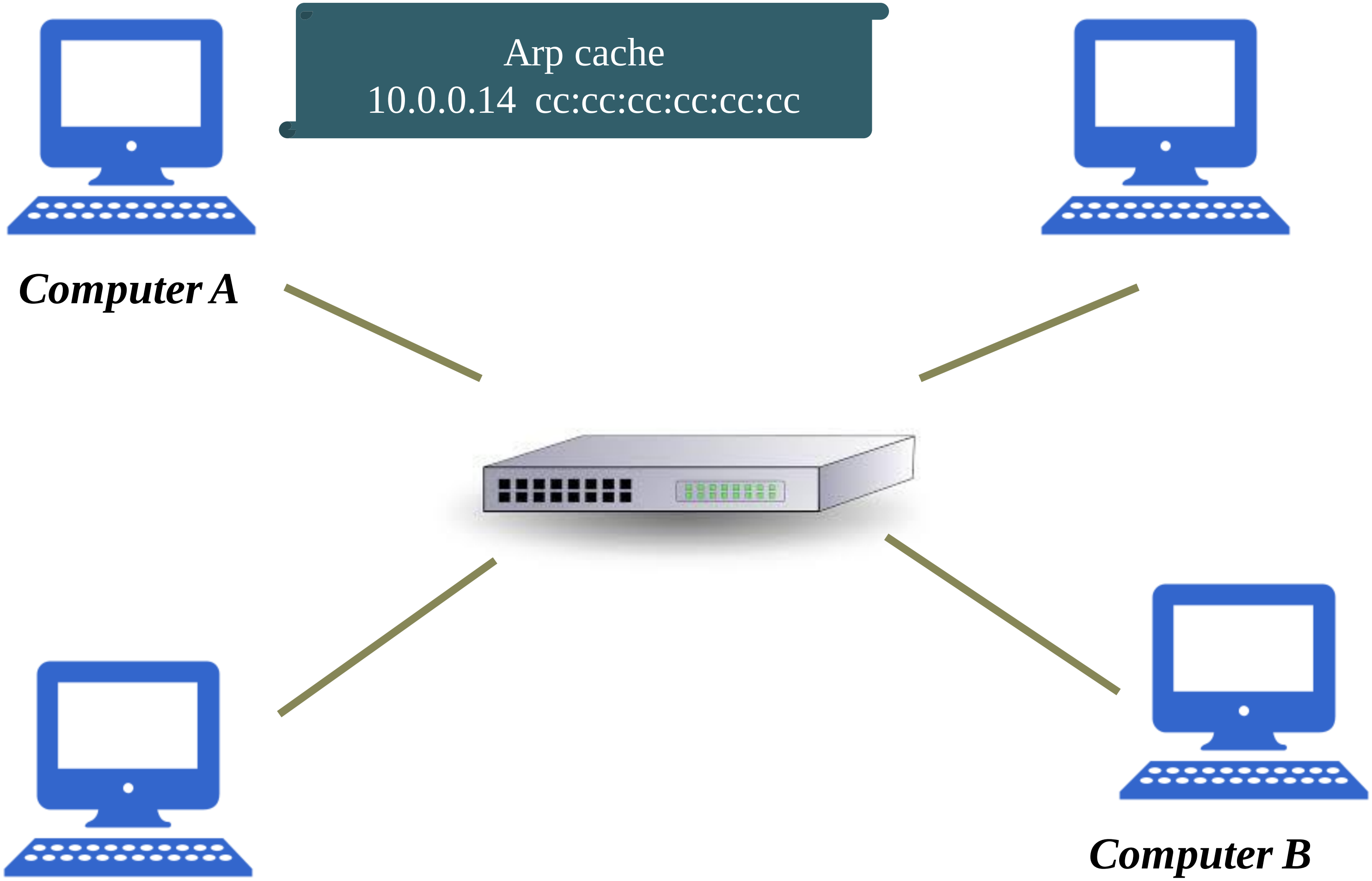
ARP Protocol



ARP Protocol

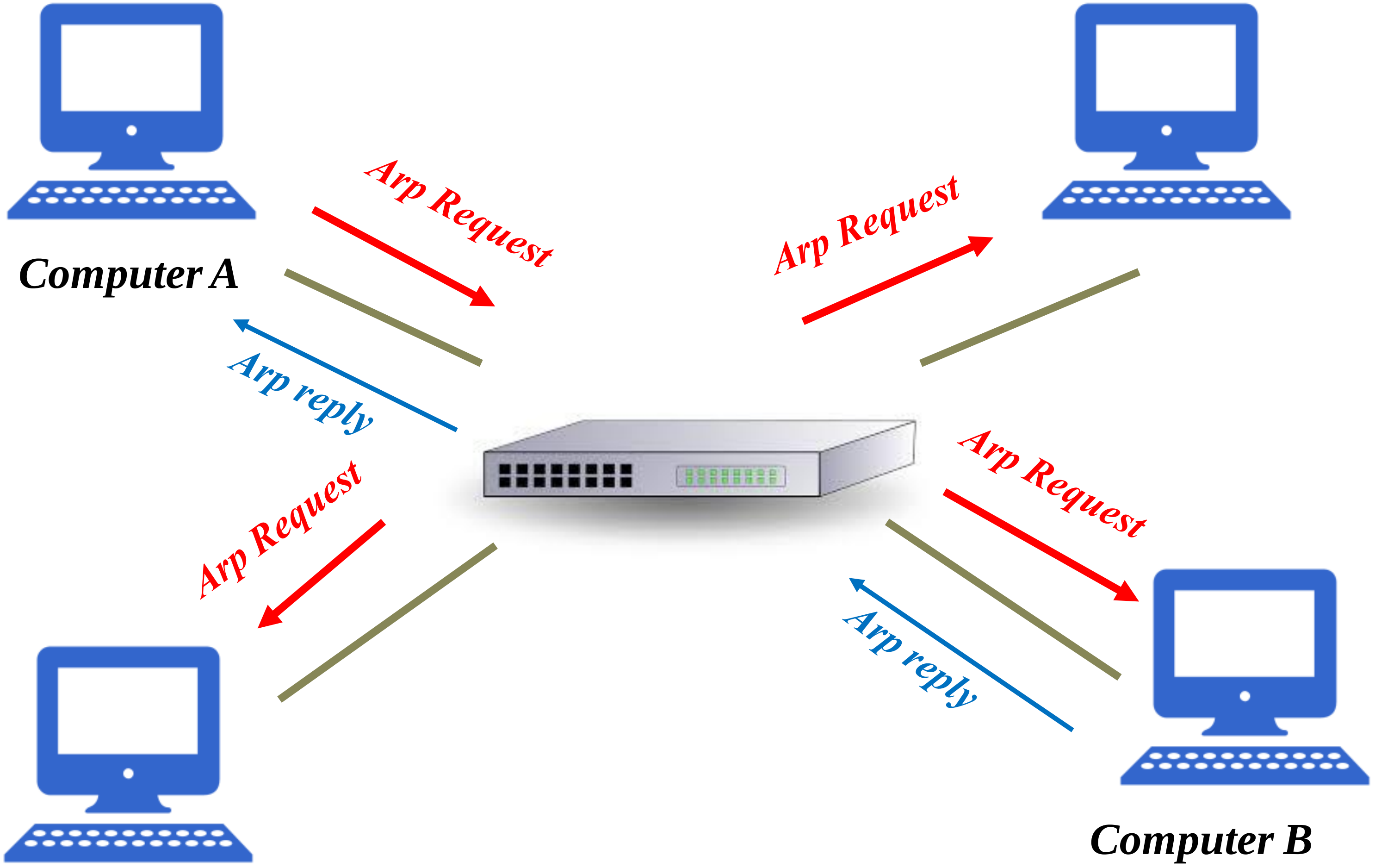


ARP Protocol



Arp cache
10.0.0.14 cc:cc:cc:cc:cc:cc

ARP Protocol



ARP spoofing (ARP cache poisoning)

- ***The aim of the attack?***

Associate the attacker's Mac adress with an other host's Ip adress. Such as the default getway, causing any trafic meant for the Ip adress to be sent to the attacker.

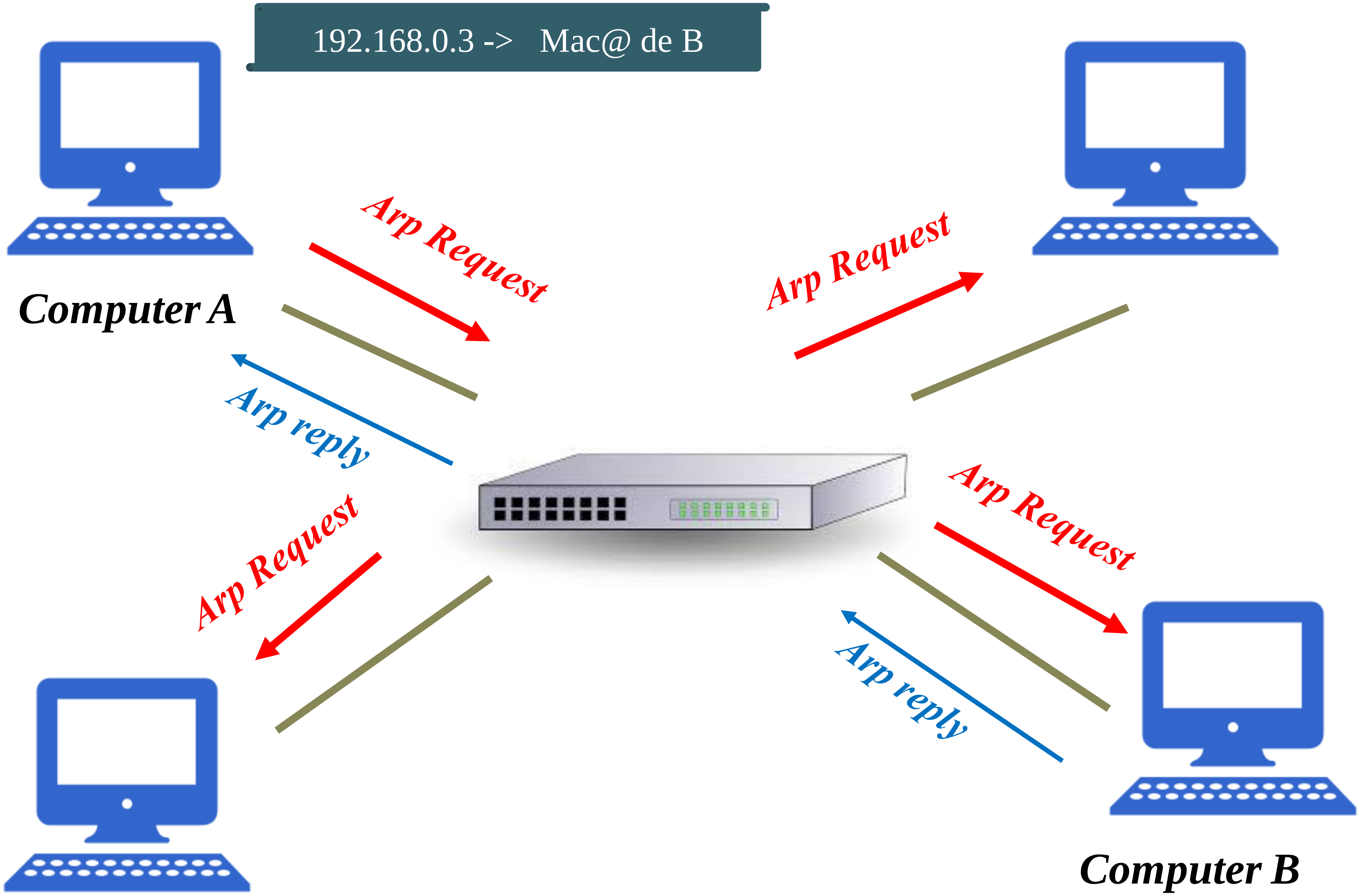
Ideally, a machine makes an ARP broadcast, and the destination machine responds by providing its MAC address.

- ***what if I also decided to respond with my own MAC address?***

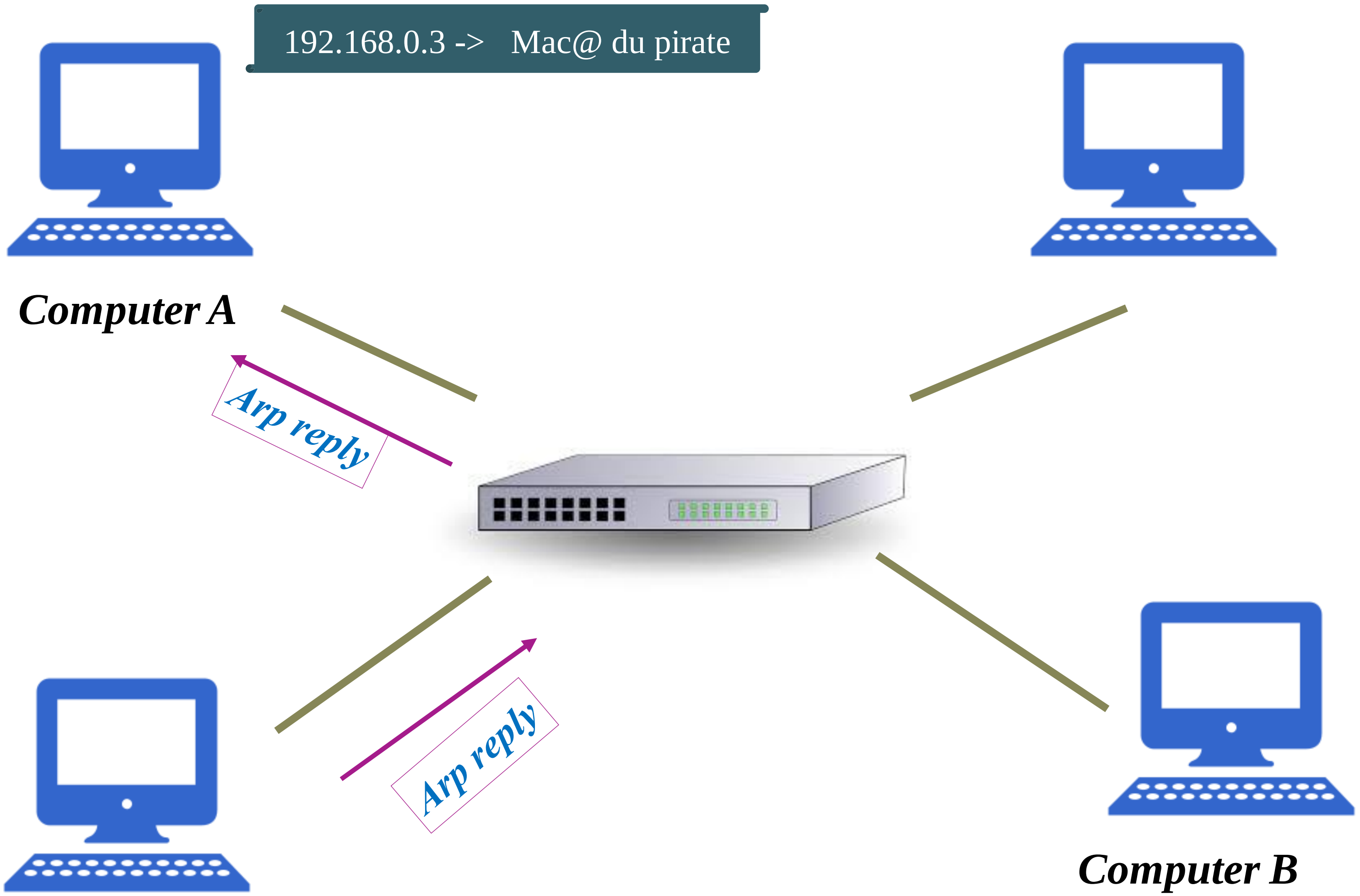
the last answer will be taken into account

.

ARP Protocol



ARP Protocol



192.168.0.3 -> Mac@ du pirate

Computer A

Arp reply

Arp reply

Computer B

pirate

Pirate does the same thing with computer B

ARP spoofing (ARP cache poisoning)

- ***problems?***

- ***if one of the machines sends an ARP response to the other after the attacker, the ARP table will be updated and the attack will no longer work;***

- ***after some time, thc ARP table will empty and the attack will not work***

- ***Note:*** ***we won't have to wait for an ARP request to answer..***

the hacker can " flood " the destination machine with ARP responses to make sure that his table is never properly updated.

.

Attack targeting DNS

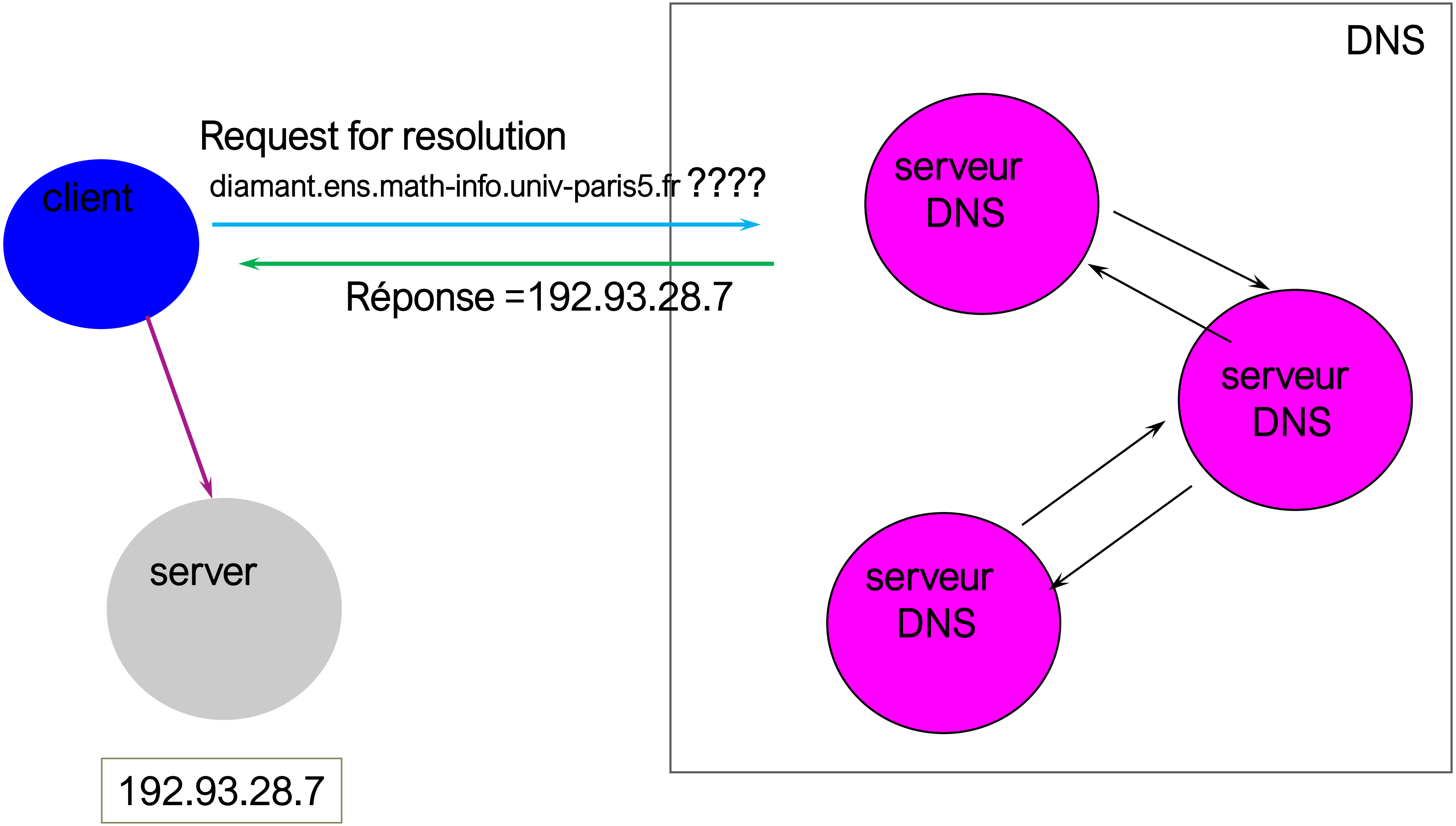
1. *Introduction to DNS (Domain Name System)*

- ***Domain Name System, it translates Internet domain names into IP addresses.***

- ***A tree structure***

  - ***DNS is structured in the form of a tree, with a " root " from which the different " branches " depend.***
  - ***At the first level of the tree there are the "Top-Level Domains", such as: .fr, .com etc.***
  - ***At the second level, there are the "classic" domain names such as “google.com".***

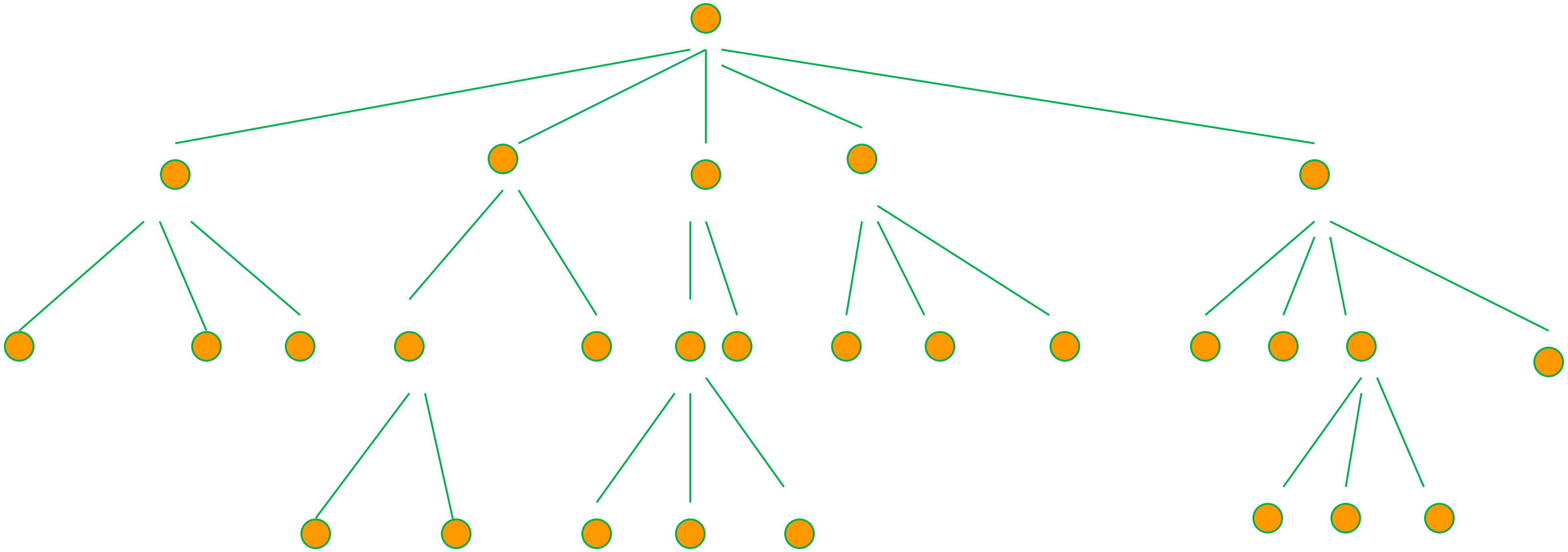
Concept


DNS
Request for resolution
diamant.ens.math-info.univ-paris5.fr ????
client
Réponse =192.93.28.7
serveur DNS
serveur DNS
serveur DNS
server
192.93.28.7

.

Domain name space

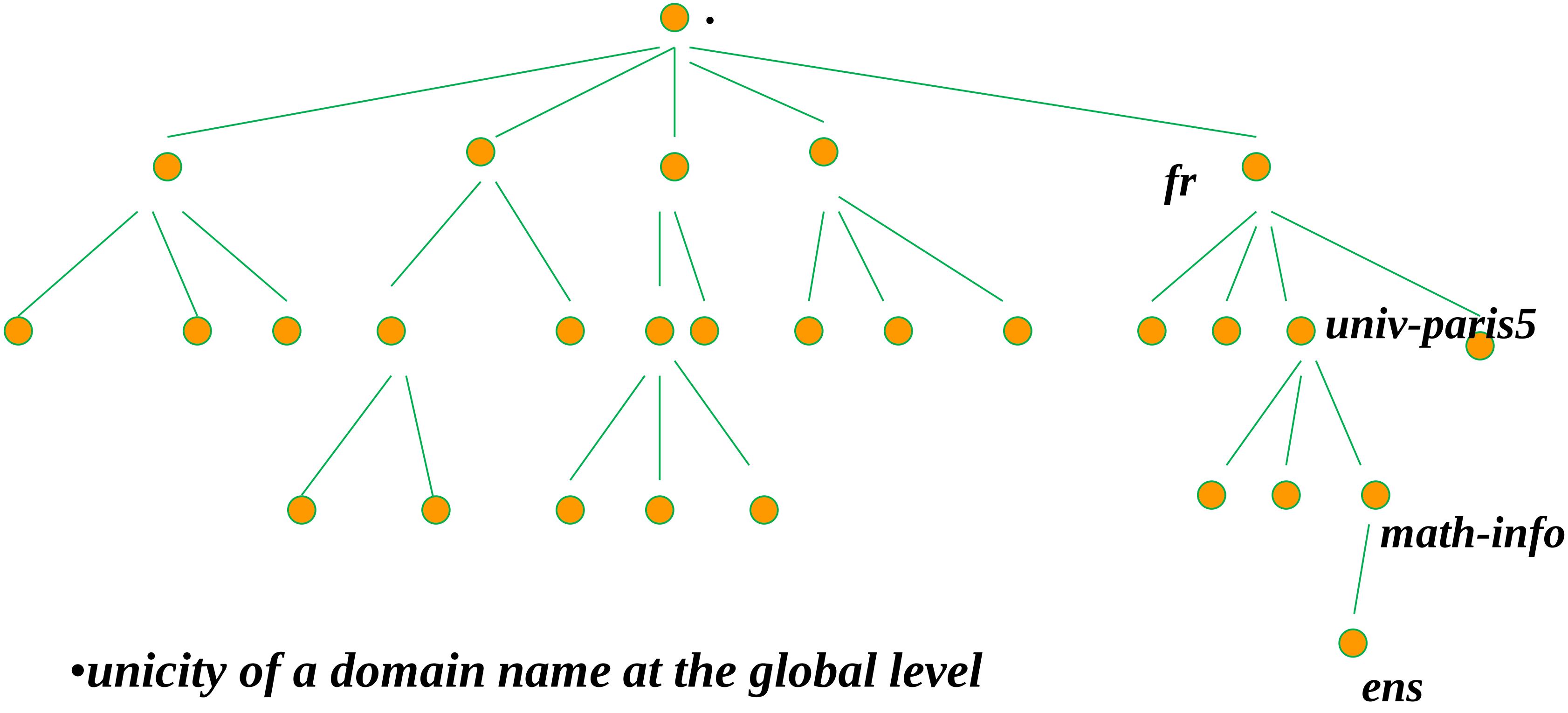
- *Each data unit in the DNS database is indexed by a name*
- *The names represent a path in a tree called the domain name space*



- *Each node is identified by a name*
- *the root is identified by «.»*
- *there are 127 levels at most*

Domain name space

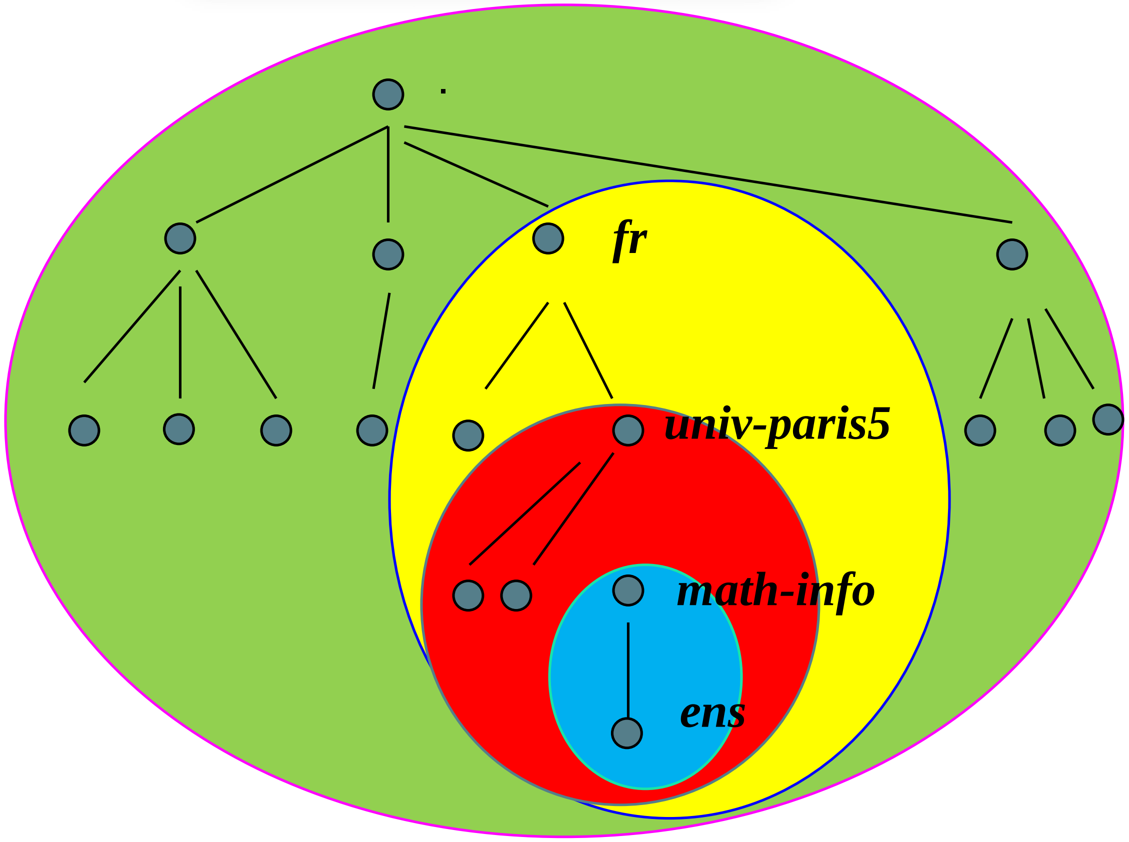
- *A domain name is the sequence of labels from the node of the corresponding tree to the root*



•*unicity of a domain name at the global level*

Domain

- *A domain is a sub-tree*



🟢 *Complete domain*

🟡 *Domain fr*

🔴 *Domain univ-paris5*

🔵 *Domain Math-info*

Domains and sub-domains

- *the domain " fr " includes the node fr* and *all nodes contained in all subdomains of fr*
- *A domain name is an index in the DNS database*
- *The DNS system imposes few naming rules:*
  - ✓ *names < 63 characters*
  - ✓ *upper and lower case letters are not significant*
  - ✓ *no imposed meaning for the names*

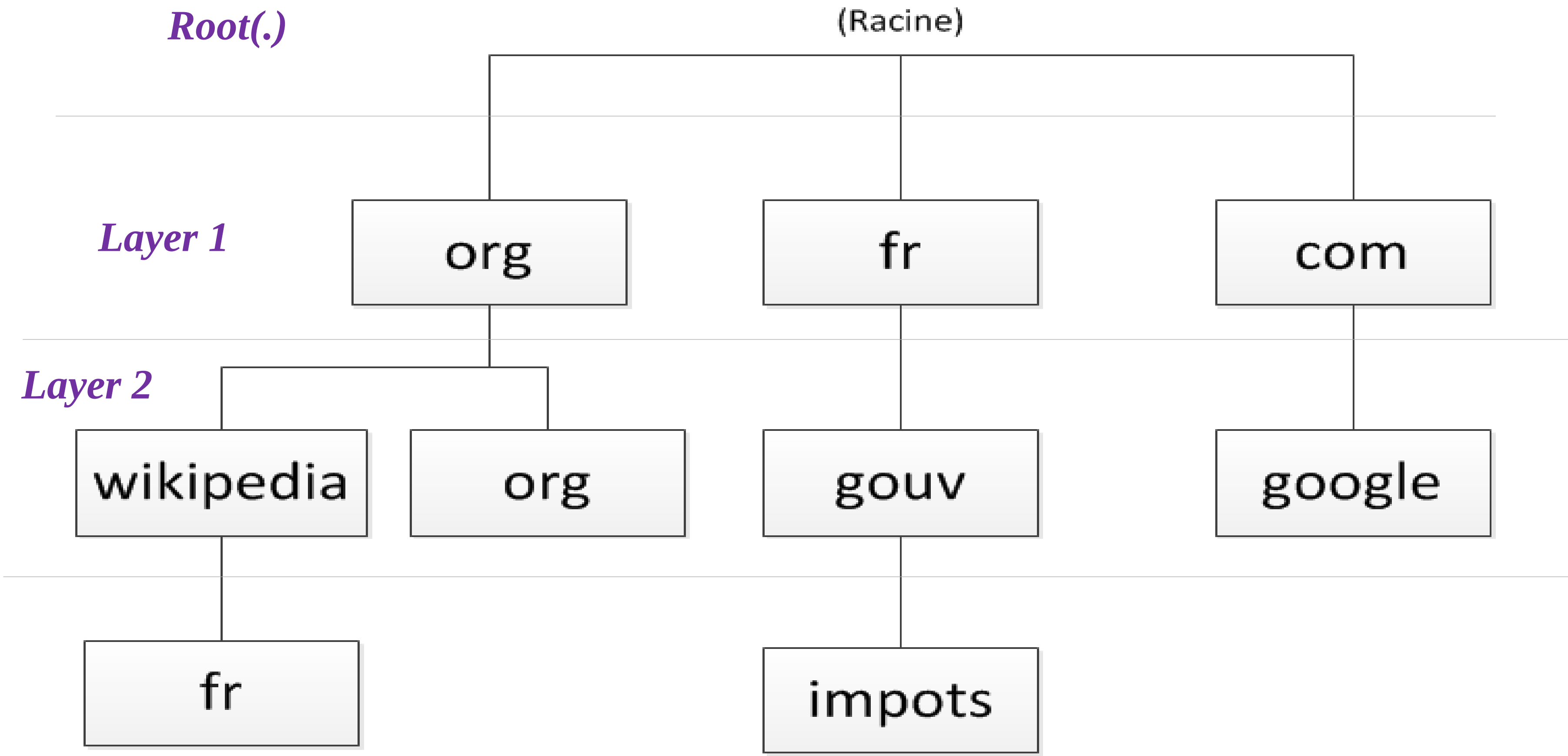
.

Domains and sub-domains

- ***7 predefined root domains :***
  - ✓ ***com: commercial organizations; ibm.com***
  - ✓ ***edu : education related organizations ; mit.edu***
  - ✓ ***gov: government organizations; nsf.gov***
  - ✓ ***mil: military organizations; army.mil***
  - ✓ ***net: Internet network organizations; worldnet.net***
  - ✓ ***org: non-commercial organizations; eff.org***
  - ✓ ***int: international organizations; nato.int***

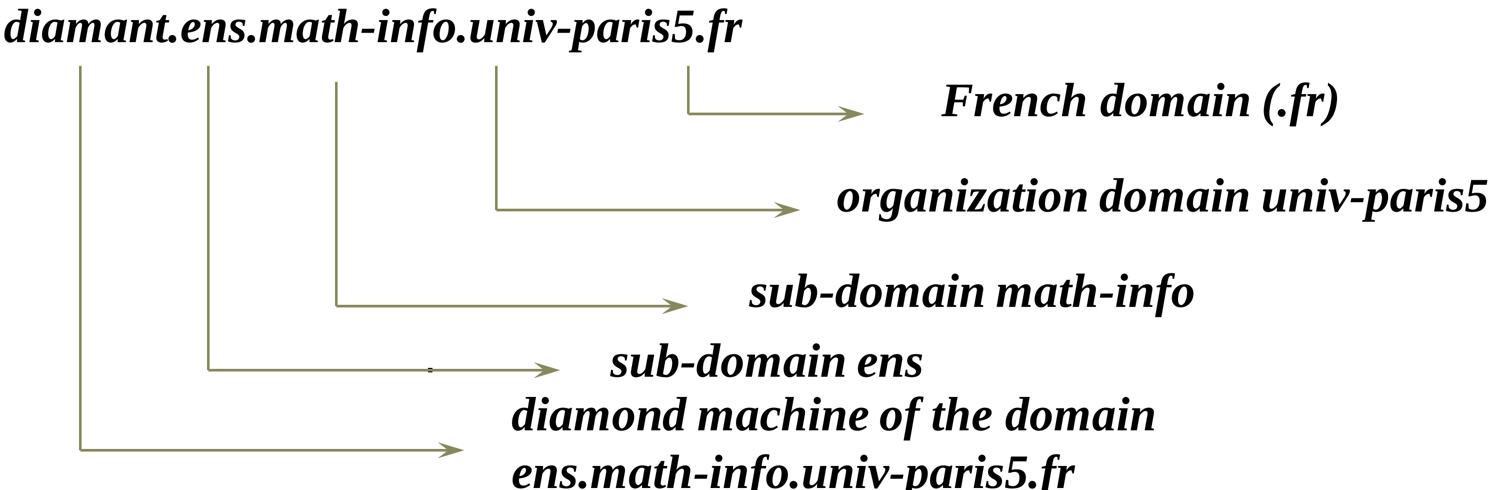
.

the Internet name tree



Reading domain names

- *Unlike IP addressing, the most significant part is on the left side of the syntax:*



diamant.ens.math-info.univ-paris5.fr

French domain (.fr)

organization domain univ-paris5

sub-domain math-info

sub-domain ens

diamond machine of the domain ens.math-info.univ-paris5.fr

Delegation

- ***The DNS system is fully distributed***
- ***The underlying mechanism is domain delegation: each domain has an associated administrative responsibility***
- ***An organization responsible for a domain can***
  - ***split the domain into sub-domains***
  - ***delegate the sub-domains to other organizations :***
    - ***who in turn become responsible for the sub-domain(s) delegated to them***

.

Delegation

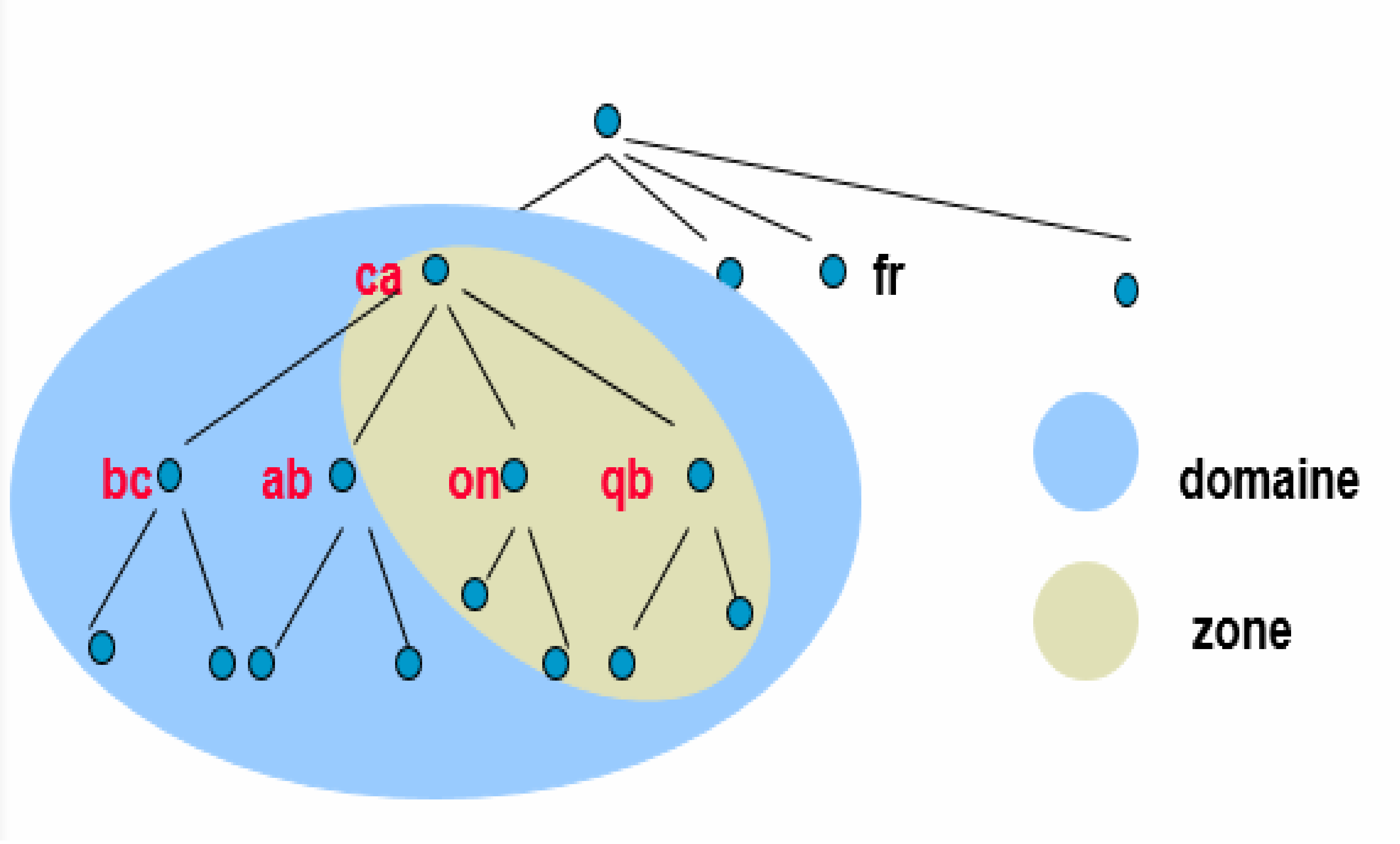
- *The parent domain then contains only a pointer to the delegated subdomain*
    - *univ-paris5.fr (in theory) could be managed by the organization responsible for the .fr domain which would then manage the data of univ-paris5.fr*
    - *univ-paris5.fr is delegated to the organization Université Paris 5 which manages the data specific to its domain*
    - *math-info.univ-paris5.fr is delegated to the organization UFR Mathématiques et Informatique which manages the data specific to its domain*

Name servers

- *The software that manages the data in the domain name space is called a name server.*
- *Name servers store data specific to a portion of the domain name space in a zone.*
- *The name server has "administrative authority" over that zone.*
- *A name server can have authority over multiple zones.*

.

Name servers



Name resolution

- ***Root servers know which name servers have authority over all root domains***
- ***The root servers know at least the name servers that can resolve the first level (.com, .edu, .fr, ...)***

.

Questions

- ***Explain what dns root servers and TLDs (top level domains) are and what they are used for***
- ***Can a zone be managed by several dns servers? What is the point of doing this?***
- ***How do Servers handle requests for other domains?***
- ***How many domains in www.google.com?***
- ***What is the host name part in: http:// www.google.com?***

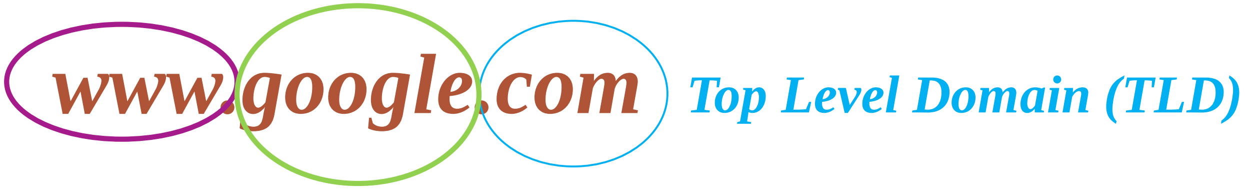
DNS

- *what happens if the dns does not know the domain?*

The dns server will interogate other DNS servers on internet

- *Adress internet?*

-A tree with branches:
A domain name consists of several parts



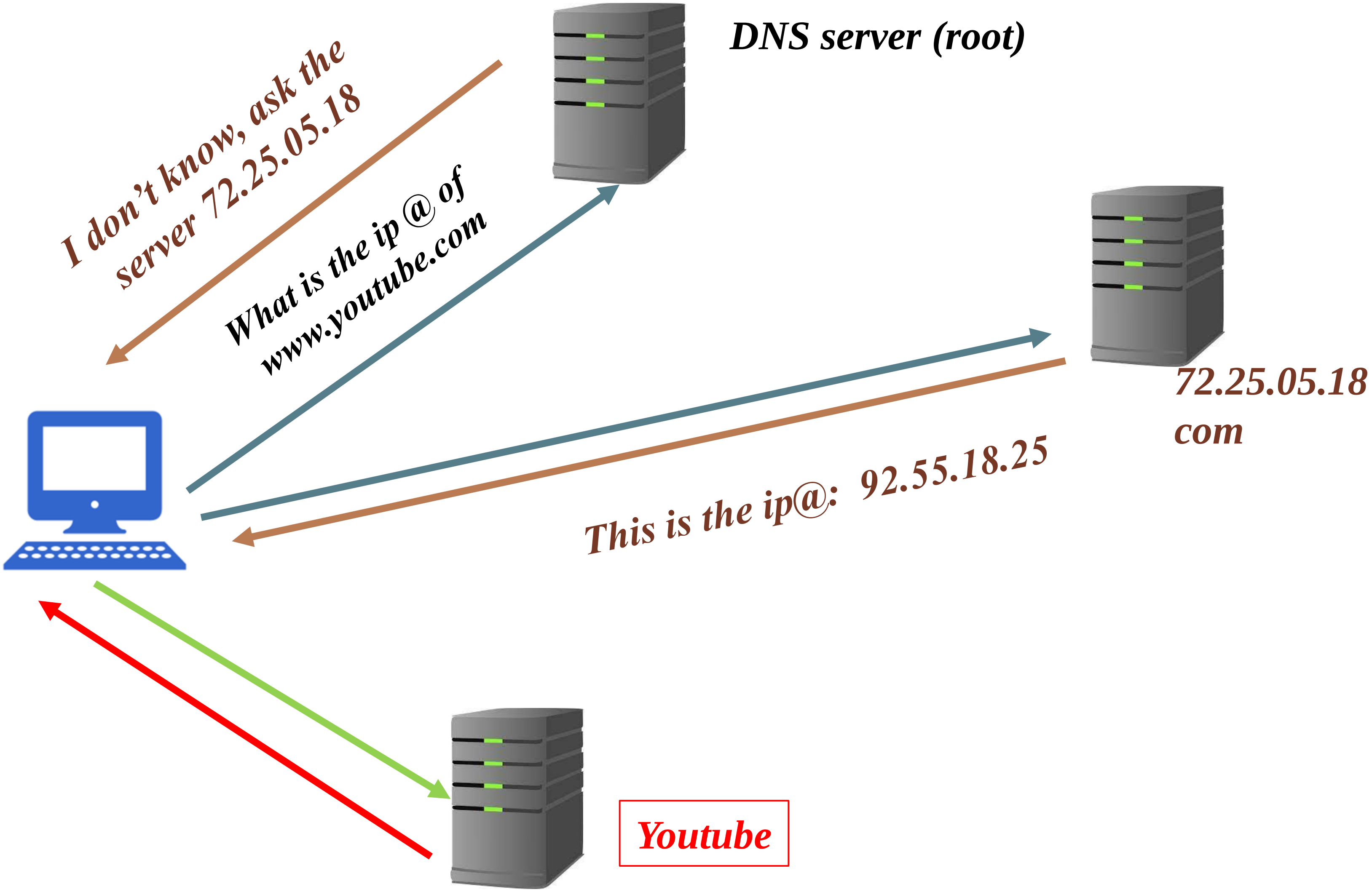
www.google.com

Top Level Domain (TLD)

all existing sites

www is the name of a machine in the google.com domain.

Example



DNS server (root)

I don't know, ask the server 72.25.05.18

What is the ip @ of www.youtube.com

72.25.05.18 com

This is the ip@: 92.55.18.25

Youtube

Major DNS attack types

- ***DoS and DDos***

attackers flood internet servers with so many requests that they simply can't answer them all, and the system crashes as a result.

- ***DoS***

A simple DoS attack uses one computer and one internet connection to flood a remote server.

- ***DDoS***

In a DDoS attack, multiple computers and internet connections target a site

.

Major DNS attack types

1. Protocol attacks: This attack cripples actual server resources or other network equipment like firewalls

2. Application layer attacks: To crash the web server, the attacker sends requests that seem harmless but actually exploit the target's vulnerabilities.

3. Flood attacks: Floods aim to make a server unavailable to real traffic by 'flooding' the targeted server's resources.

.

Major DNS attack types

- ***DNS amplification attacks***

flood a target with DNS response traffic.

- ***HOW?***

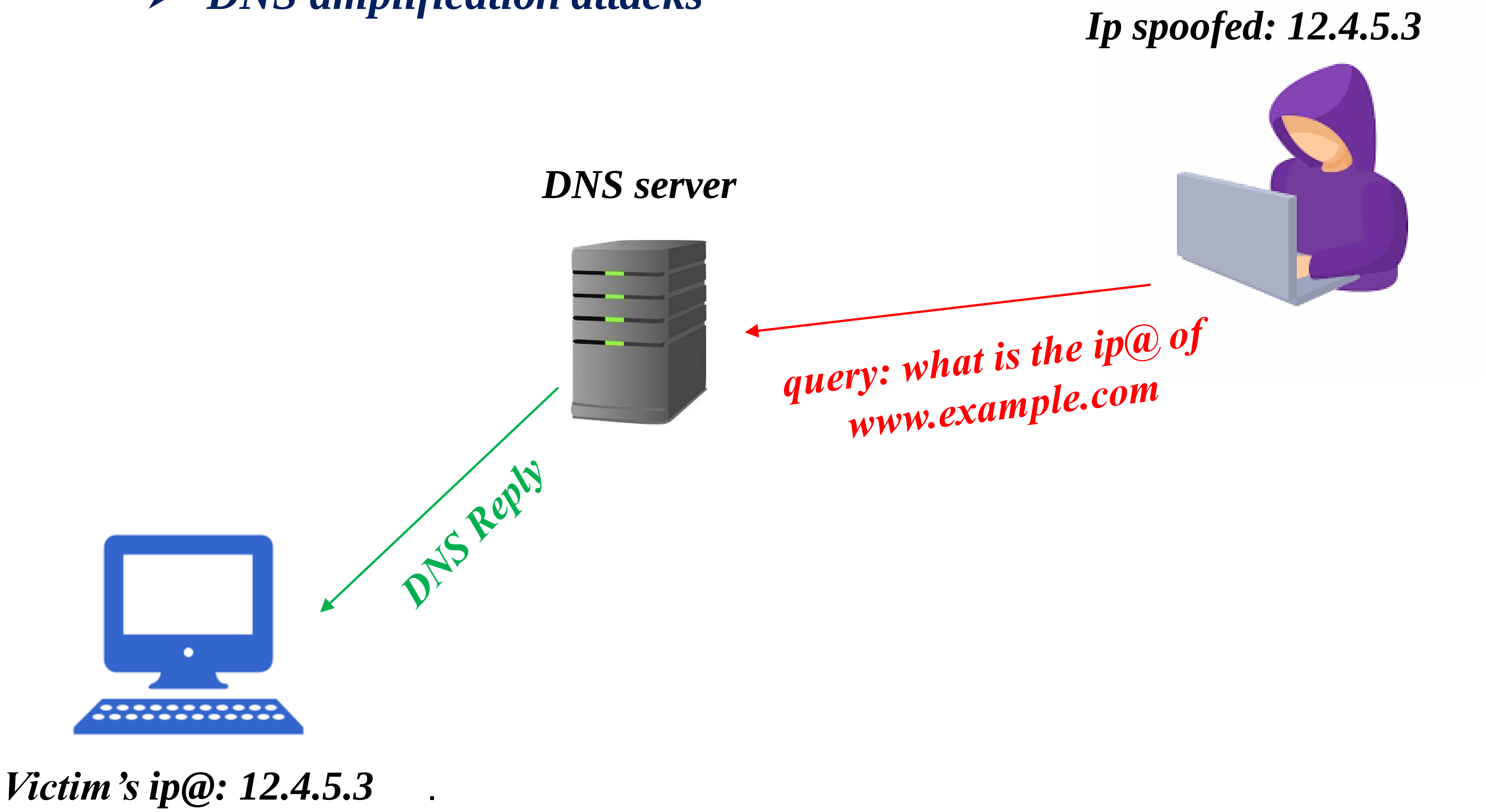
-The attacker sends a DNS lookup request to a DNS server with the source address spoofed to be the target's address.

-When the DNS server sends the DNS record response, it is sent to the target instead.

.

Major DNS attack types

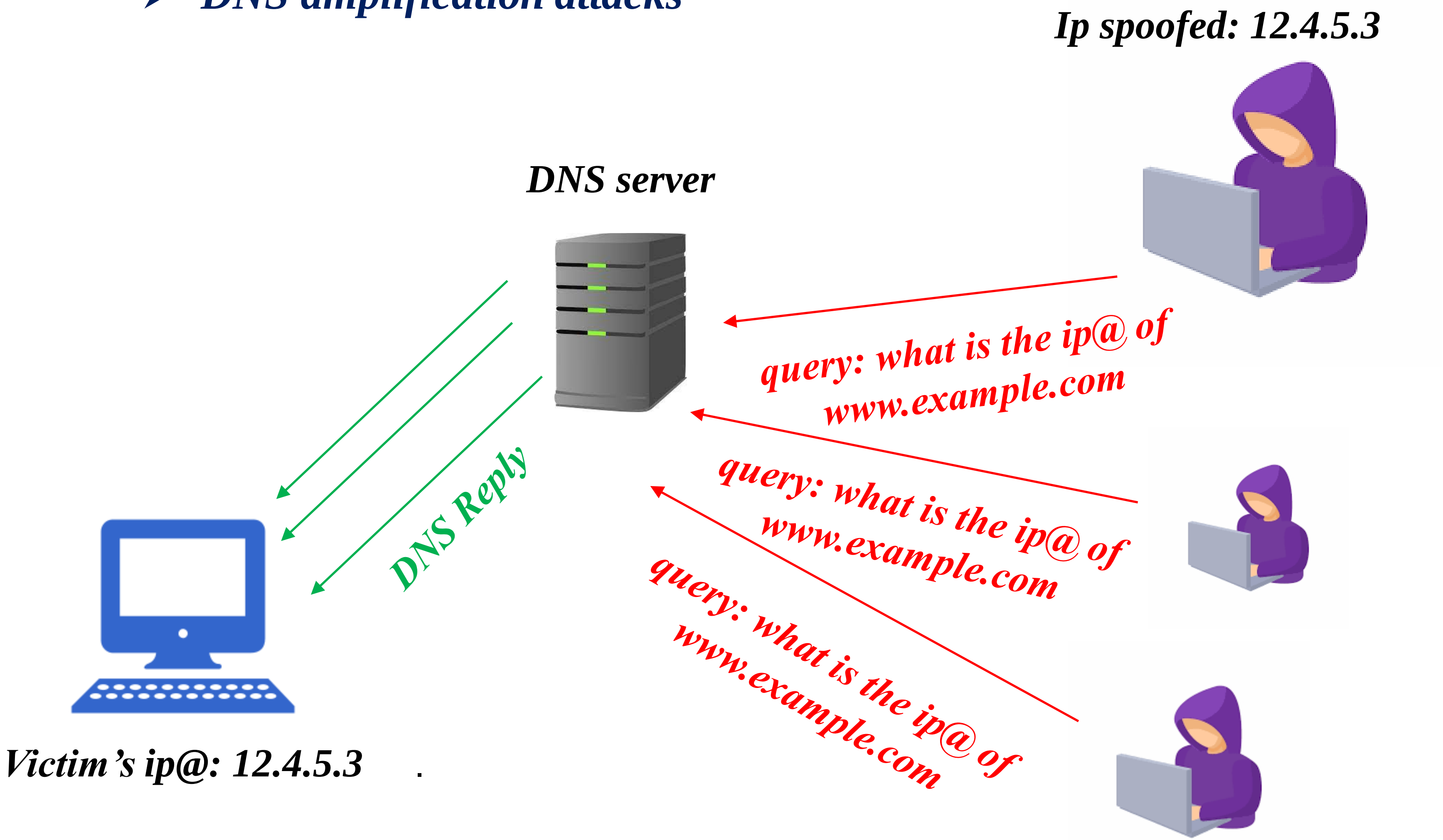
- ***DNS amplification attacks***



.

Major DNS attack types

- ***DNS amplification attacks***



Ip spoofed: 12.4.5.3

DNS server

query: what is the ip@ of www.example.com

query: what is the ip@ of www.example.com

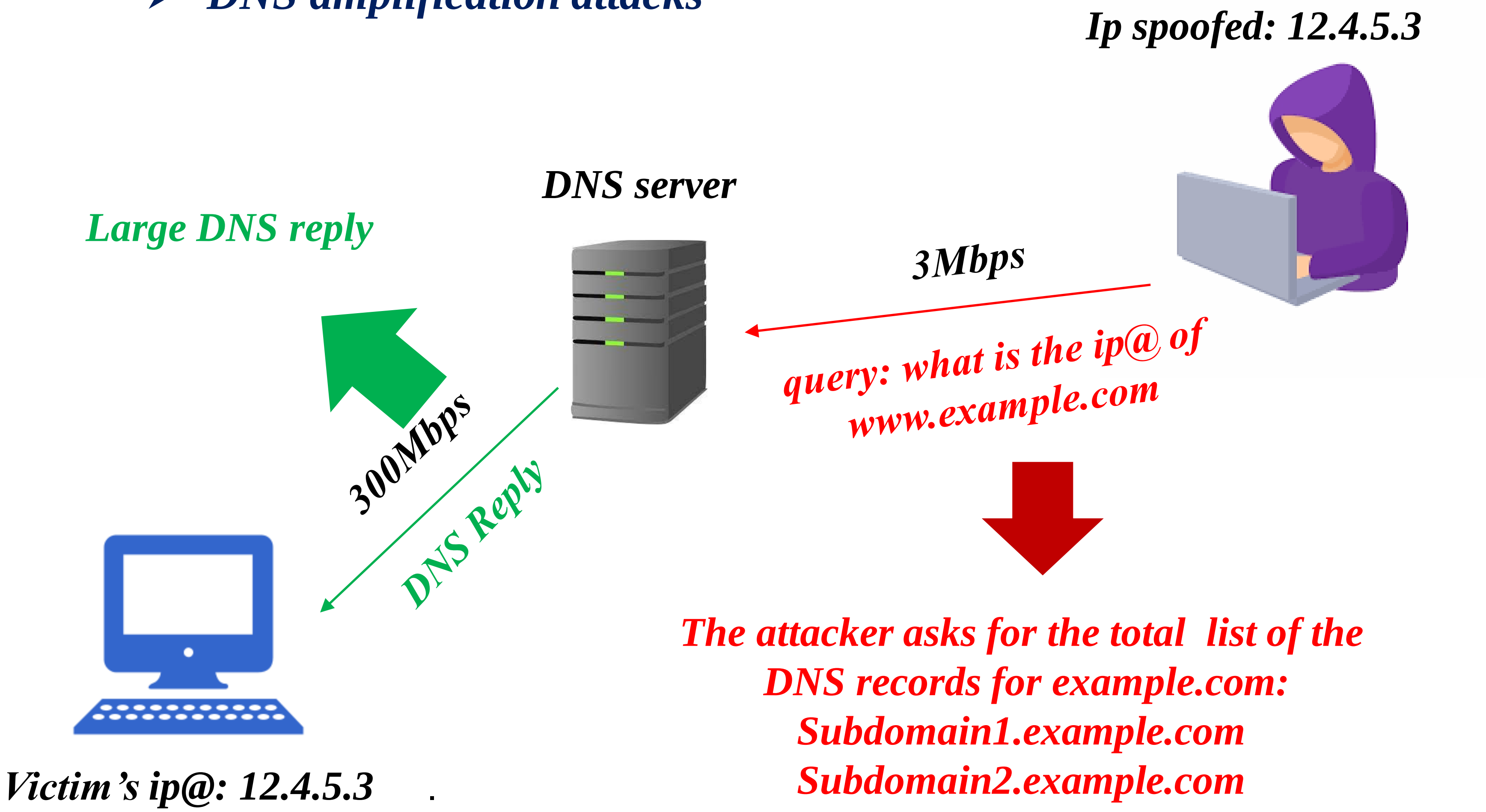
query: what is the ip@ of www.example.com

DNS Reply

Victim's ip@: 12.4.5.3

Major DNS attack types

- *DNS amplification attacks*



Ip spoofed: 12.4.5.3

DNS server

Large DNS reply

3Mbps

query: what is the ip@ of www.example.com

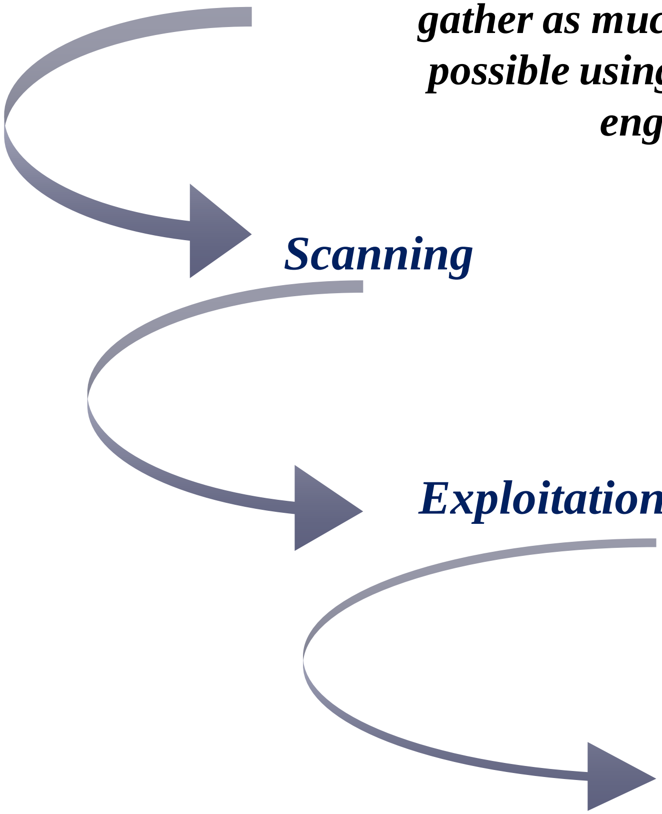
300Mbps

DNS Reply

Victim's ip@: 12.4.5.3 .

The attacker asks for the total list of the DNS records for example.com:
Subdomain1.example.com
Subdomain2.example.com
Subdomain3.example.com

The different steps of an attack



Target identification

gather as much information about the target as possible using public information and without engaging in hostile action.

Scanning

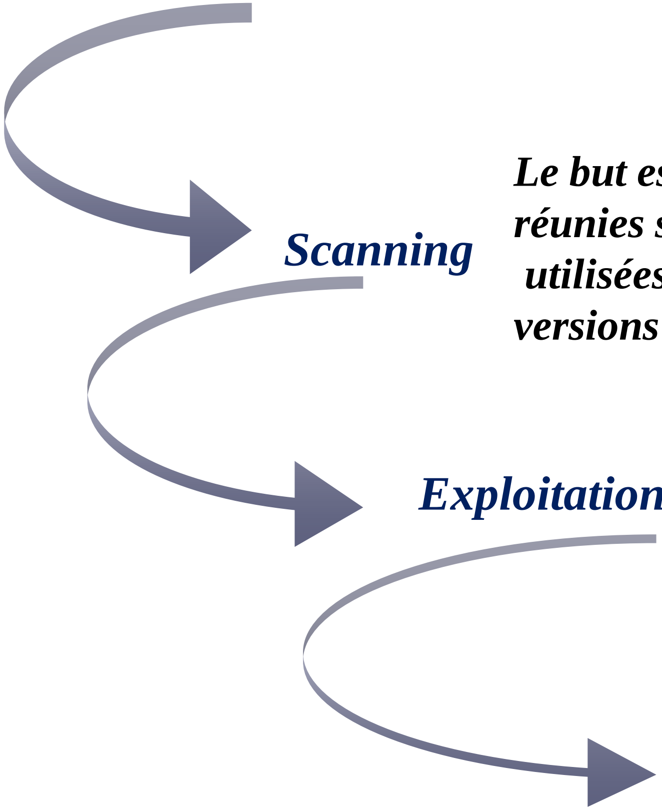
Exploitation

Progression

.

The different steps of an attack

Target identification



Scanning

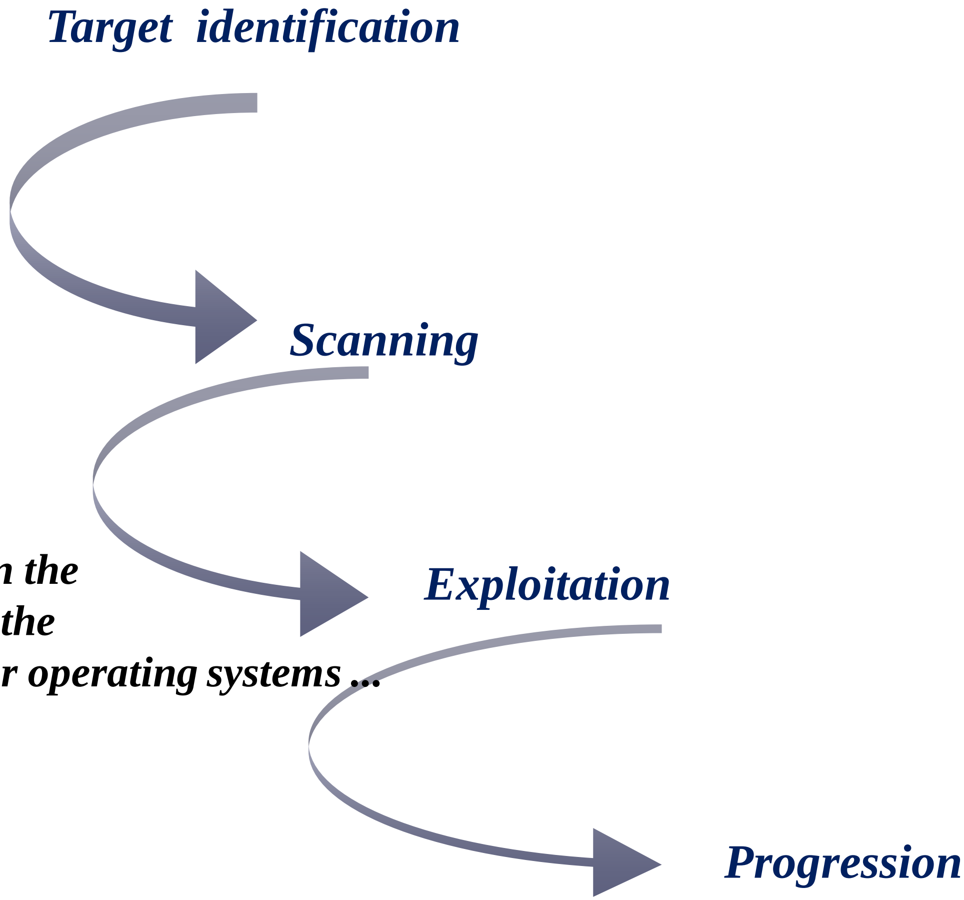
Le but est de compléter les informations réunies sur une cible.: les adresses IP utilisées, les services Accessibles; OS, versions des services, règles de pare-feu…

Exploitation

Progression

.

The different steps of an attack



Target identification

Scanning

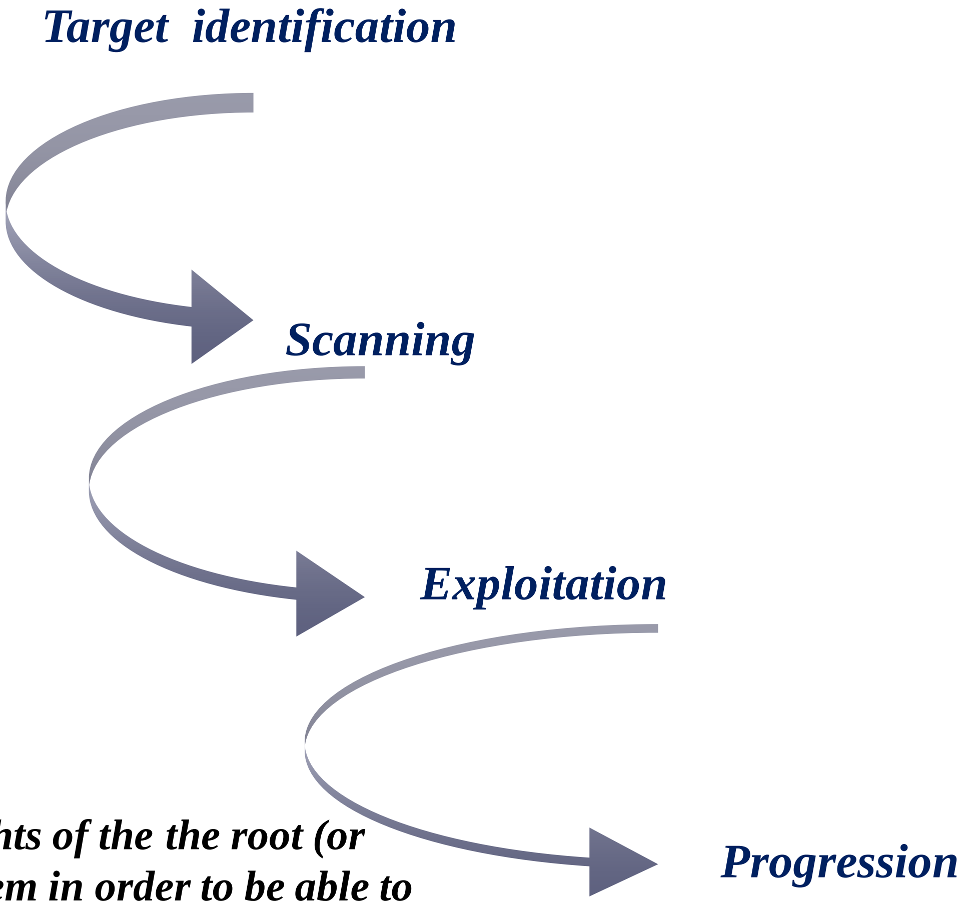
Exploitation

Progression

exploits the flaws identified in the target's elements, whether at the protocol level, ,applications or operating systems ...

.

The different steps of an attack



Target identification

Scanning

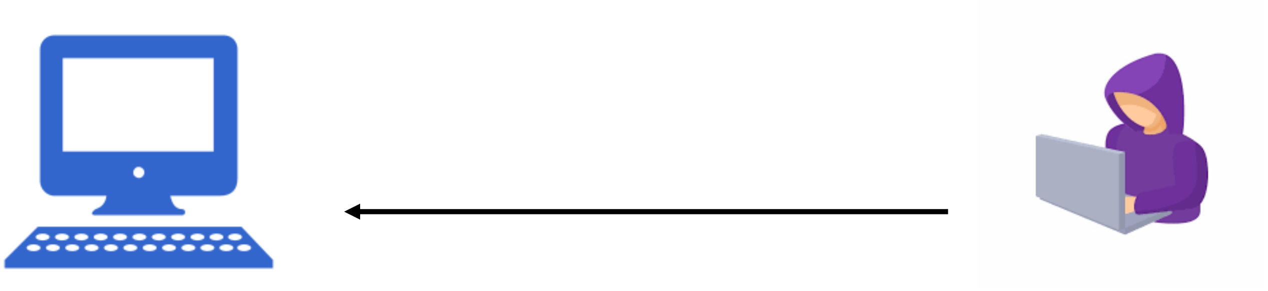
Exploitation

Progression

The goal is to obtain the rights of the the root (or system) user rights on a system in order to be able to do whatever he wishes (inspection of the machine, recovery of information, cleaning traces...).

Types of attacks

- ***Direct attacks***



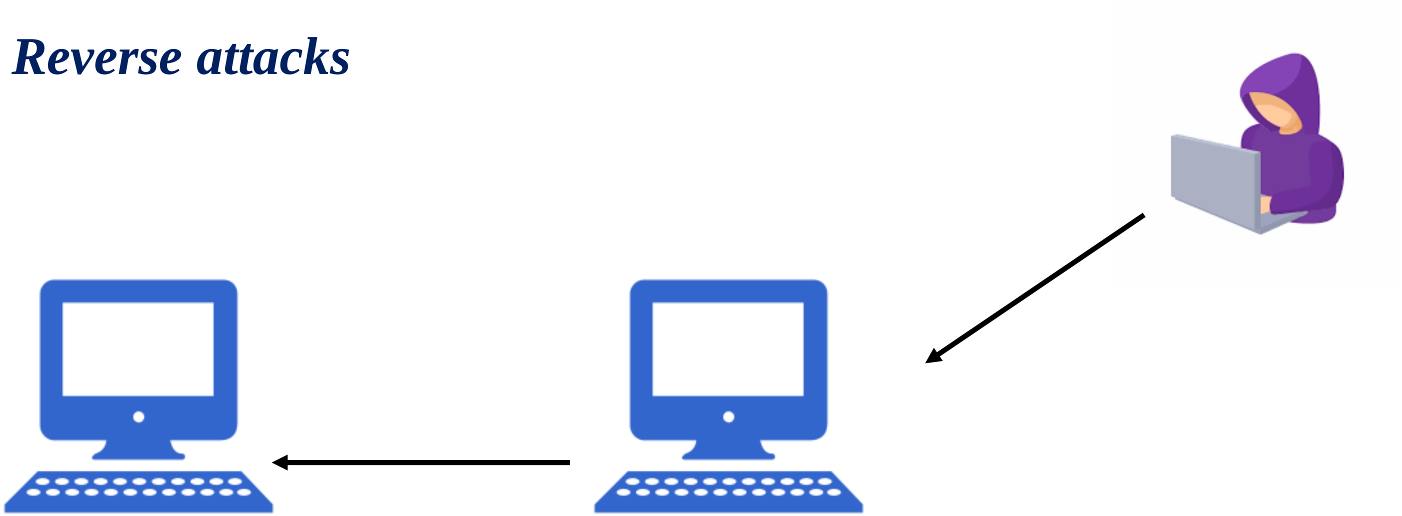
The simplest of the attacks to carry out:

1. ***The hacker attacks directly his victim from his computer***
2. ***the hacking programs they use directly send the packets to the victim***

.

Types of attacks

- ***Reverse attacks***



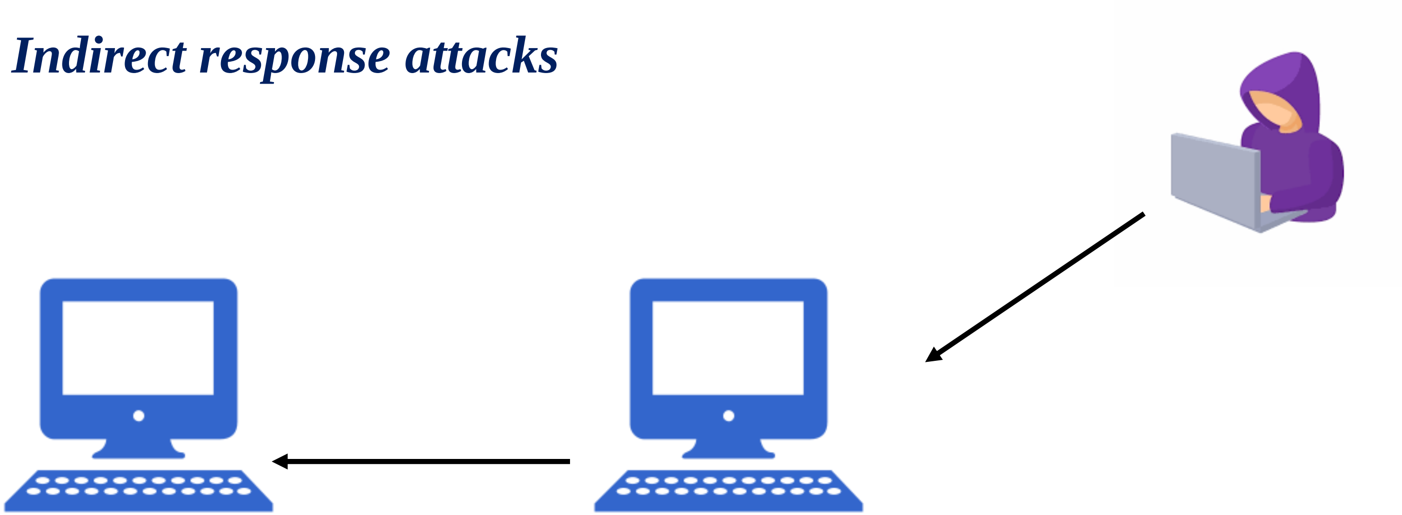
Attack a machine through another machine

1. ***hide the traces***

.

Types of attacks

➢ ***Indirect response attacks***



attack derivatived from the rebound attack.

1. ***Instead of sending an attack to the intermediate computer to be reflected, the attacker will send it a request.***
2. ***And it is this response to the request that will be sent to the victim computer.***

.

Password attacks

- ***Needs***

Protect secret information

- ***Attack methods***

1. ***Brute force attack***
2. ***Dictionary attack***
3. ***Hybrid attack***

- ***tools that allow the hacker to obtain the users' passwords of users:***

1. ***key loggers***
2. ***Social engineering***
3. ***Spying***

Malicious program (malware)

- ***What is it?***

Unwanted software installed in your system without your consent.

- ***subcategories***

1. ***Ransomware***
2. ***Spyware***
3. ***Macro viruses***
4. ***Polymorphic viruses***
5. ***Stealth viruses***
6. ***Trojan horse***
7. ***Logic bombs***
8. ***Worm*** .
9. ***Injectors***

Ransomware

It is a malicious software that takes data hostage while waiting for the payment of a ransom.

- ***Contents are then totally or partially encrypted, so as to make them unusable without the decryption key.***
- ***The hacker asks to be paid in cryptocurrency, such as Bitcoin for example.***

.

Spyware

programs installed to collect information about users, their browsing habits or their computer.

- monitor everything you do without your knowledge and send this data to the cyber-attacker(s).

-They are usually set up when you download a free application..

.

Polymorphic viruses

virus that modifies its own representation during replication.

-This action prevents them from being detected by antivirus software.

- ***Difficulty in identifying virus-specific binary sequences(signature).***

.

Stealth viruses

These types of viruses take control of certain system features to hide themselves.

- ***These viruses can be spread in the same way as any other virus, through malware, attachments or installations created via various websites…***

.

Trojan horse

Apparently legitimate program, but with malicious intent.

-Cybercriminals use so-called social engineering techniques to trick you into loading and running this Trojan Horse. For several purposes:

1. ***Steal, delete, block, modify or copy personal or sensitive content***
2. ***Spy,***
3. ***Steal passwords...***

Logic bombs

Malicious software added to an application. These are programmed devices that are triggered at a specific time.

-This type of virus is capable of being triggered at a specific time in the near future, and on a large number of machines.

.

Worm

It is malware that replicates itself on multiple computers using a computer network. Worms have the ability to duplicate themselves once they have been executed. The most common propagation is through email attachments.

.

Hameçonnage (phishing)

-These types of attacks combine social engineering and technical skills.

-It involves sending emails that appear to come from trusted sources in order to collect personal data or entice victims to take action

.

SQL (Structured Query Language) injection

A recurring problem affecting websites that use databases

-These attacks occur when a cybercriminal executes a piece of SQL (standard computer language) code to manipulate a database and access potentially sensitive content.

.

Most common injection attacks:

- ❑ *How injection attacks work:*
  - problem

No strict separation between the instructions of a program and the data entered by a user.

↓

attackers can insidiously place instructions telling the program to perform actions of their choice

↓

manage to place, in classic entries, data interpreted as instructions.

Most common injection attacks:

- ❑ ***How injection attacks work:***
  - **The success of the operation is based on three elements:**

    Identify the technology on which the web application is based.

    List all possible user inputs.

    Find the vulnerable user input.

.

Most common injection attacks:

- ***SQL injection :***

SQL: Structured Query Language

Objective: access to databases

SQL syntax = database statements + user input.

↓

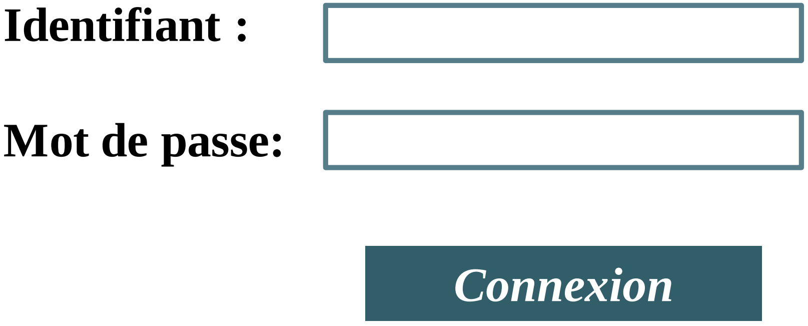
Can be interpreted as instructions

Most common injection attacks:

❑ ***SQL injection :***

Example :

Simple web application requiring authentication



Most common injection attacks:

- ***SQL injection :***

Example :

Simple web application requiring authentication

```
CREATE TABLE user_table (
  id INTEGER PRIMARY KEY,
  username VARCHAR(32),
  password VARCHAR(41)
);
```

Hashing of password

id	username	password

Most common injection attacks:

- ❑ ***SQL injection :***

Example :

Simple web application requiring authentication

SELECT id FROM user_table WHERE username=’Alice’
AND
password=PASSWORD(’monMotDePasse’)

If such a user exists in this database table, this SQL command will return the associated ID number.

Most common injection attacks:

❑ *SQL injection :*

Example of Java code :

```
String username = req.getParameter("username");
String password = req.getParameter("password");
String query = "SELECT id FROM user_table WHERE " +
    "username = ’" + username + "’ AND " +
    "password = PASSWORD(’" + password + "’)";
ResultSet rs = stmt.executeQuery(query);
int id = ñ1; // la valeur ñ1 signale un utilisateur non authentifié
while (rs.next())
      id = rs.getInt("id");
```

Most common injection attacks:

❑ ***SQL injection :***

Example of Java code :

```
String query = "SELECT id FROM user_table WHERE " +
    "username = ’" + username + "’ AND " +
    "password = PASSWORD(’" + password + "’)";
```

What happens if we enter 'OR 1=1 -- for the username, with the password x?

Most common injection attacks:

- ❑ *SQL injection :*

Example of Java code :

```
String query = " SELECT id FROM user_table WHERE username = ”  OR
1=1 -- ’AND password = PASSWORD(’x’)
```

=

```
SELECT id FROM user_table WHERE username = ” OR 1=1
```

Most common injection attacks:

❑ ***SQL injection :***

Example of Java code :

```
String query = " SELECT id FROM user_table WHERE username =‘ ‘ OR
1=1 -- ’AND password = PASSWORD(’x’)
```

=

```
SELECT id FROM user_table WHERE username = ‘ ‘ OR 1=1
```

In this situation, the attacker placed the SQL statements (' OR 1=1 --) instead of the data in the username field.

Most common injection attacks:

- ❑ ***SQL injection :***

it is possible to insert other instructions:

```
OR 1=1; DROP TABLE user_table; --
```

```
SELECT id FROM user_table WHERE username=‘ ‘  OR 1=1; DROP
TABLE user_table; -- ’AND password = PASSWORD(’x’);
```

Most common injection attacks:

- ❑ ***SQL injection :***

Prevention against SQL injection

1-Clean user input
2-Use prepared statements

Types of pirates

- *There are many types of "attackers" classified according to their experience and their motivations:*

  - *white hat hackers*
  - *black hat hackers*
  - *script kiddies*
  - *Phreakers*
  - *Carders*
  - *Crackers*

Types of pirates

- *There are many types of "attackers" classified according to their experience and their motivations:*

- ***white hat hackers***
- *black hat hackers*
- *script kiddies*
- *Phreakers*
- *Carders*
- *Crackers*

hackers in the noble sense of the term, whose goal is to help improve computer systems and technologies

Types of pirates

- *There are many types of "attackers" classified according to their experience and their motivations:*

- *white hat hackers*
- *black hat hackers*
- *script kiddies*
- *Phreakers*
- *Carders*
- *Crackers*

more commonly known as hackers, individuals who break into computer systems for harmful purposes

Types of pirates

- *There are many types of "attackers" classified according to their experience and their motivations:*

- *white hat hackers*
- *black hat hackers*
- ***script kiddies***
- *Phreakers*
- *Carders*
- *Crackers*

young network users using programs found on the Internet, usually in a careless way, to damage computer systems for fun.

Types of pirates

- *There are many types of "attackers" classified according to their experience and their motivations:*

- *white hat hackers*
- *black hat hackers*
- *script kiddies*
- ***Phreakers***
- *Carders*
- *Crackers*

hackers who are interested in the telephone network in order to make free calls.

Types of pirates

- *There are many types of "attackers" classified according to their experience and their motivations:*

- *white hat hackers*
- *black hat hackers*
- *script kiddies*
- *Phreakers*
- ***Carders***
- *Crackers*

mainly attack credit card systems (bank cards in particular) to understand how it work and to exploit its flaws. The term carding refers to the hacking of chip cards.

Types of pirates

- *There are many types of "attackers" classified according to their experience and their motivations:*

- *white hat hackers*
- *black hat hackers*
- *script kiddies*
- *Phreakers*
- *Carders*
- ***Crackers***

people whose goal is to create software tools to attack computer systems or to break the copy protections of paid software. A "crack" is thus a program created as that modifies the original software in order to remove its protections.

Components and Architectures for network security

Introduction

***Network security** refers to all activities aimed at protecting the company's network.*

- ***Network security activities and components are designed to protect :***

1- Usability

2-Integrity

3- Fiability

4- Network and data security

Components and Architectures for network security

Introduction

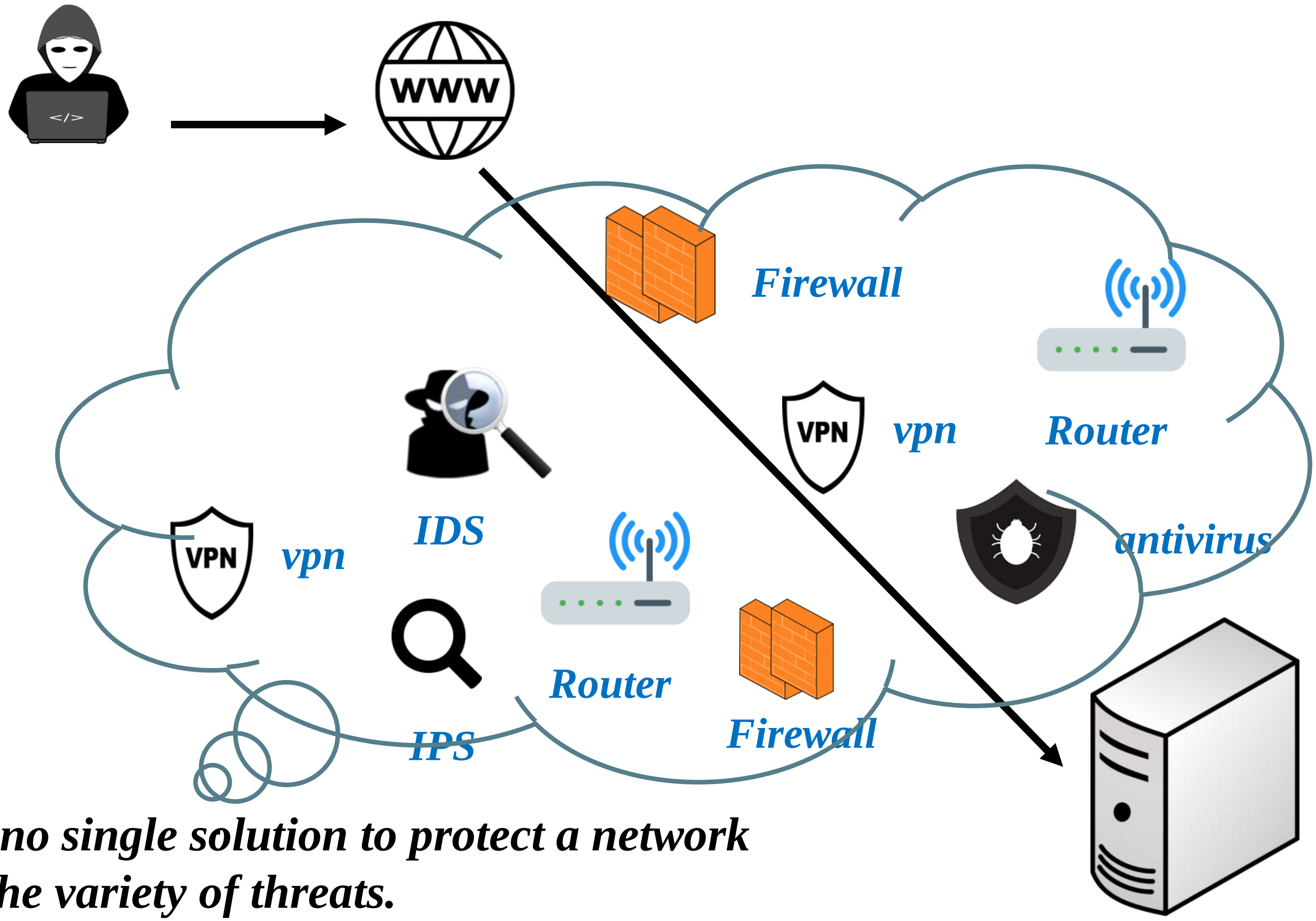
The implementation of an effective network security policy aims at protecting against a variety of threats and prevents any penetration or propagation on a network.

security policy?

- ***Implementation of several layers of security.***
- ***If one of the layers is compromised or fails the others are still standing..***

.

Components and Architectures for network security



- *There is no single solution to protect a network against the variety of threats.*

Network threats

- ***Denial of Service (DoS) attacks***
- ***Viruses, worms and Trojan horses***
- ***Spyware and adware***
- ***Data interception and and identity theft identity theft***

.

Network security components

- ***A network security system consists of several components:***
  - ***Firewall***
  - ***Intrusion detection system (IDS)***
  - ***Intrusion Prevention System (IPS)***
  - ***Antivirus and antispyware***
  - ***Virtual Private Network (VPN)***

- ***All components work together, which minimizes maintenance and improves safety.***

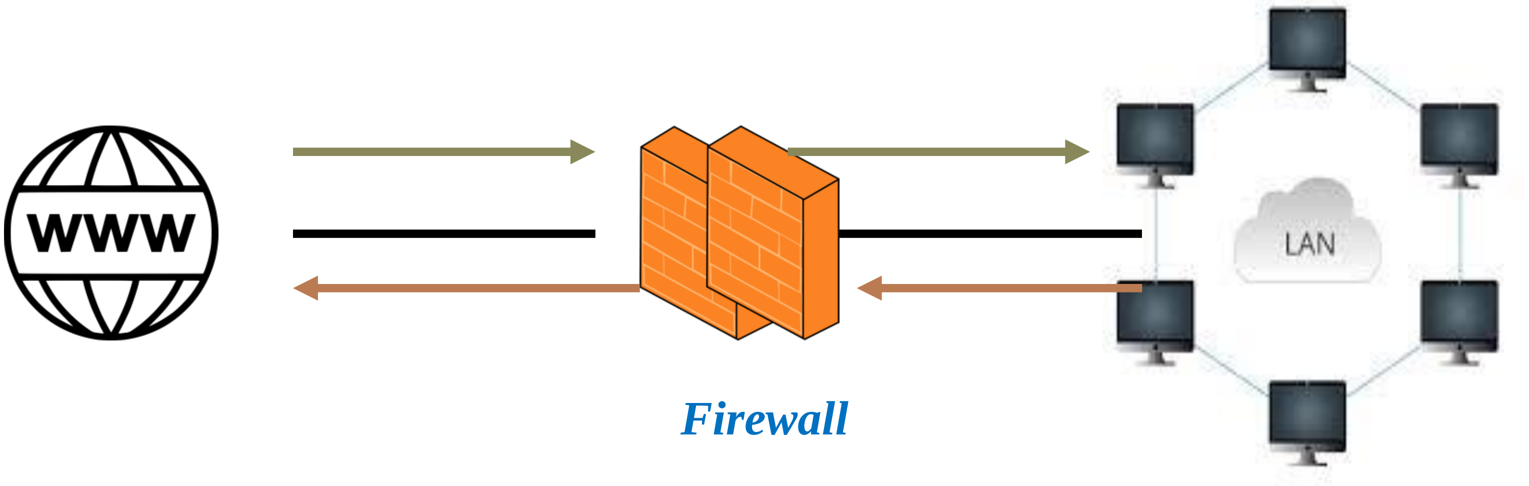
.

Firewalls

- ***A firewall is used to restrict access to a network from another network.***
- ***A firewall has at least two network interfaces:***
  1. ***for the external network or Internet***
  2. ***for the network to be protected (LAN)***

.

Firewalls



.

Firewalls

- ***A software firewall can be installed on any machine and with any operating system .***
- ***Firewalls can filter messages based on:***
  - ***Traffic type (protocol)***
  - ***Source and destination addresses***
  - ***Port numbers.***

.

Operating mode of Firewall

- *A firewall is a device used to enforce security policies (control the flow of network traffic) within a network or between multiple networks.*

- *It can be software or hardware dedicated to examine all messages entering or leaving the network and block all messages that do not meet the specified security criteria.*

.

Operating mode of Firewall

○ ***A firewall system contains a set of predefined rules allowing:***

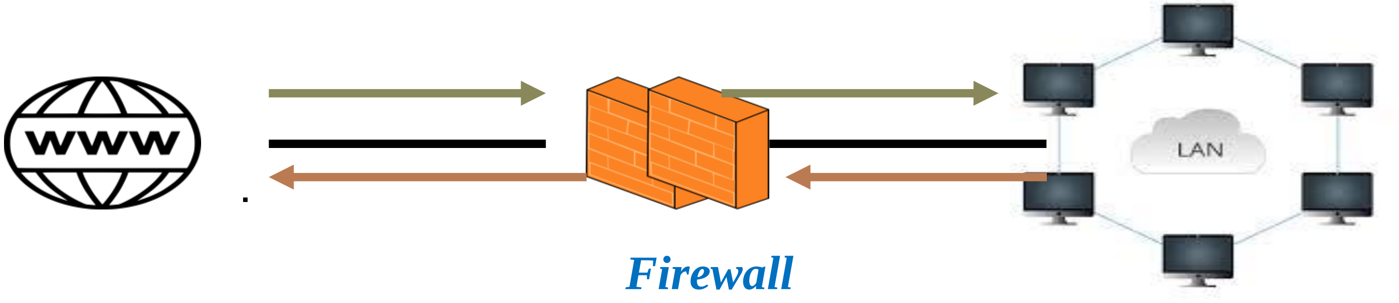
- ✓ ***Allow the connection (allow) ;***
- ✓ ***Block the connection (deny);***
- ✓ ***Reject the connection request without notifying***
- ✓ ***the sender (drop).***

.

Firewall Architecture

I. *Simple architecture:*

- *Bastion host is a machine designed and configured to protect network resources from external attacks.*
- *This machine provides a single point of entry and exit to the Internet or external network.*
- *It has two interfaces:*
  - ➢ *Public interface connected directly to the Internet.*
  - ➢ *Private interface connected to the local network.*



Firewall Architecture

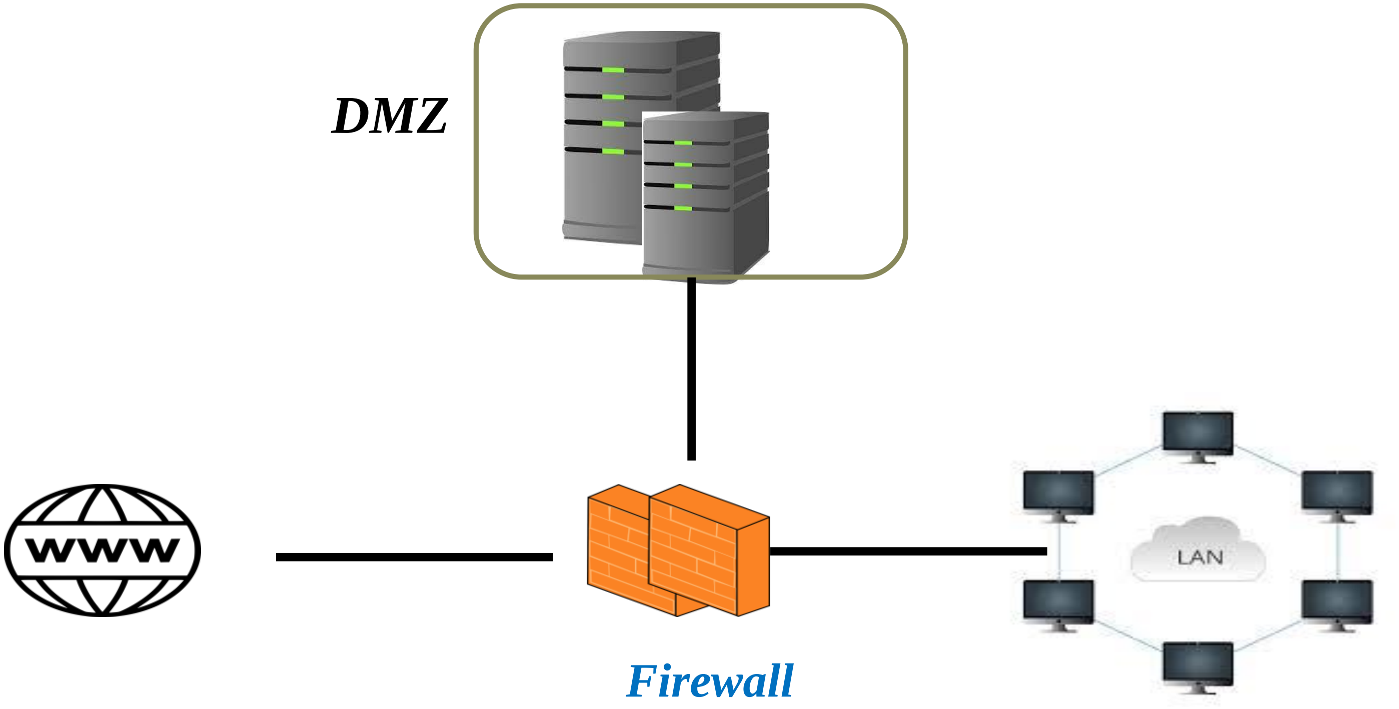
II. Screened subnet firewall:

- ***allows companies to offer services securely for Internet users.***
- ***All servers hosting public services (accessible from the Internet) are placed in the demilitarized zone (DMZ).***
  - ***The DMZ is separated from the Internet and the Intranet by the firewall.***
  - ***The DMZ services respond to requests from the public network.***

.

Firewall Architecture

II. Screened subnet firewall:



.

Firewall Architecture

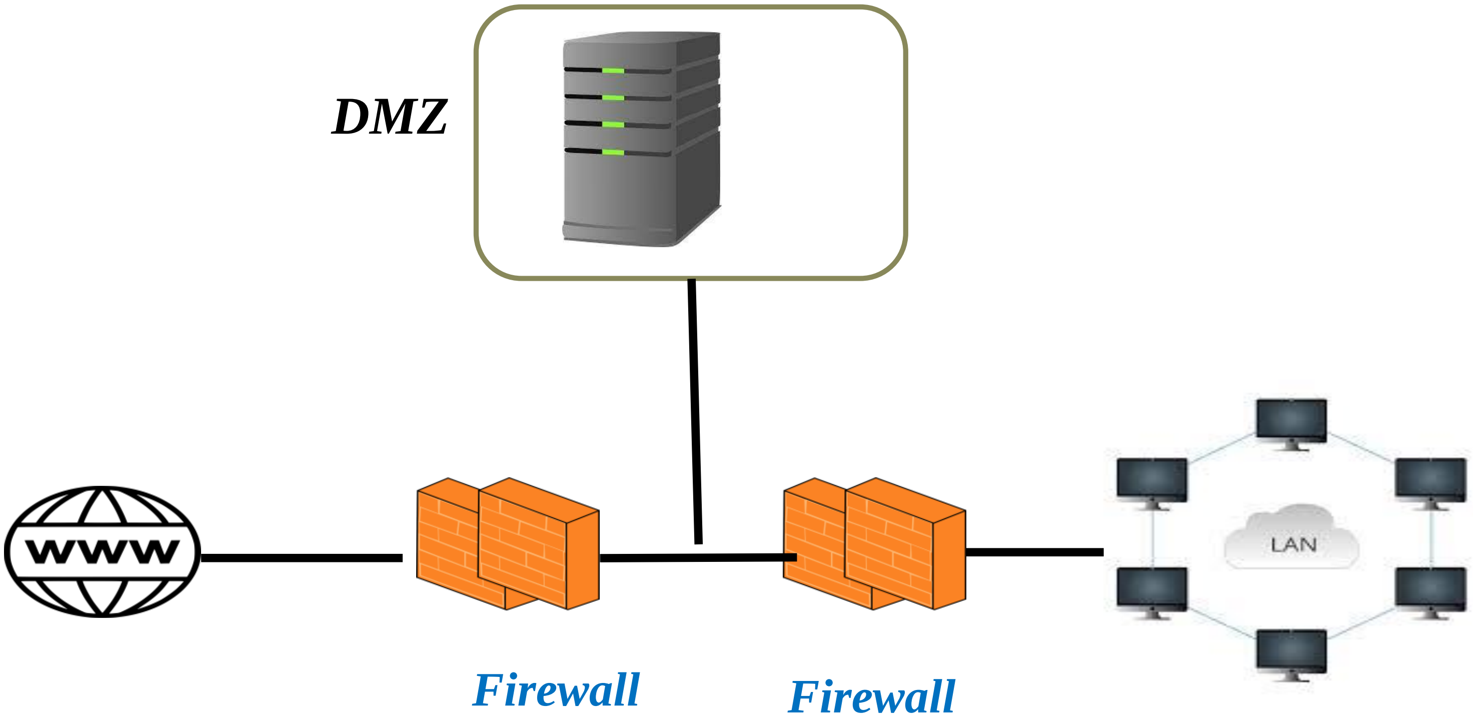
III. Multi-homed firewall:

- ***refers to an architecture of two or more networks.***
- ***Multi-homed firewall is equipped with three or more network interfaces to subdivide the network based on the specific security objectives of the organization.***
- ***Each interface is connected to a separate network segment.***

.

Firewall Architecture

III. Multi-homed firewall:



DMZ

Firewall

Firewall

What is a DMZ?

A DMZ is a machine or network placed as a neutral network between the private network (Intranet) and the public network (Internet) to prevent any access from the public network to the resources and data of the private network.

.

Firewalls evolution

1) ***Packet Filter***
2) ***Application Proxy Filter***
3) ***Stateful Inspection***
4) ***Adaptive Response***
5) ***Kernel Proxy***

Packet Filter Firewall/ Simple Filtering

1) IP addresses identify the sending and target machines.
2) The type of packet and the port number give an indication of the type of service being transported.

Rule	Action	Ip_S	IP_D	Protocol	Port_s	Port_D
1	Accept	192.168.10.20	any	tcp	any	25
2	Accept	any	192.168.10.03	tcp	any	80
3	Deny	any	any	any	any	any

Packet Filter Firewall/ Simple Filtering

Limitations:

- ***No user authentication***
- ***Performance problem if there are too many rules***
- ***This type of filtering is not resistant to certain IP Spoofing / IP Flooding or DoS attacks.***

.

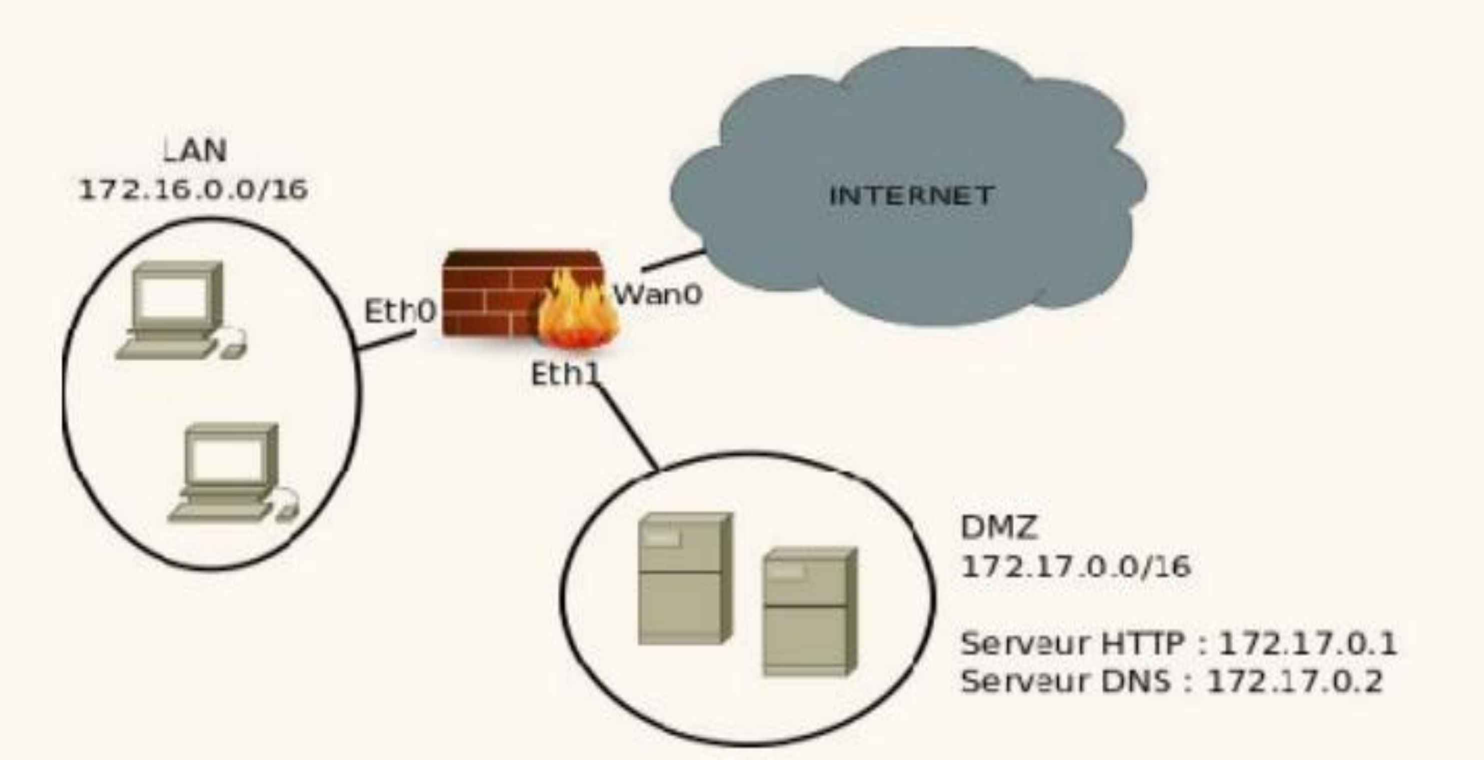
Packet Filter Firewall/ Simple Filtering

Exercise 1:

- ***A company has a firewall to limit access to and from machines on its internal network. The company's network architecture also includes a demilitarized zone (DMZ) for the deployment of the company's Web and DNS servers. servers. The security policy applied by the firewall is described in Table 1.***

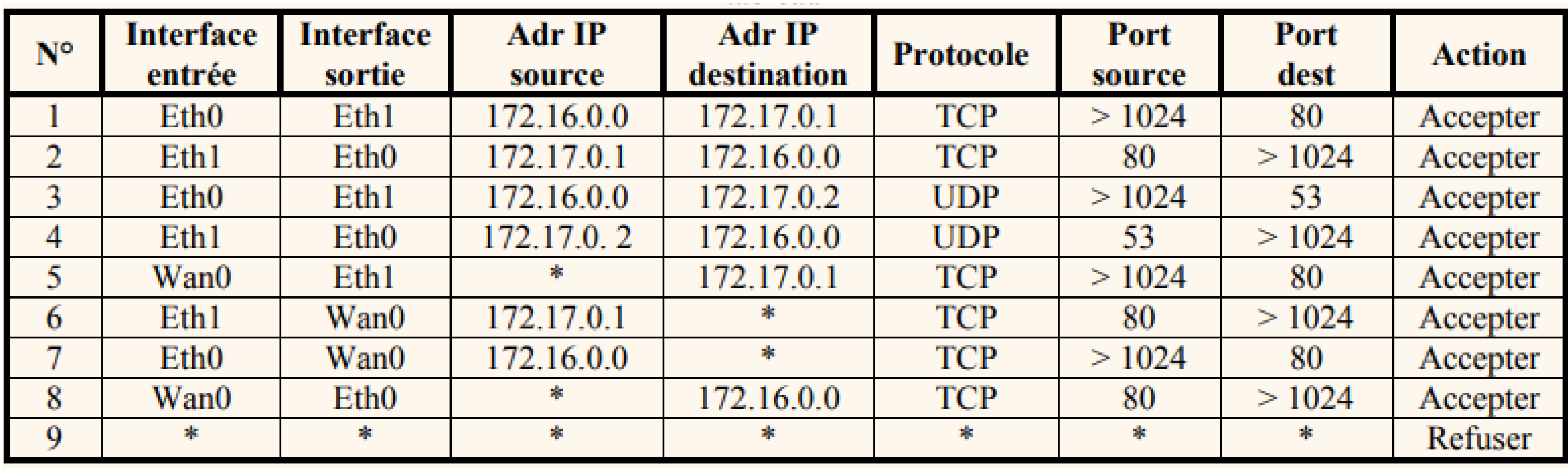
.

Packet Filter Firewall/ Simple Filtering



.

Packet Filter Firewall/ Simple Filtering



N°	Interface entrée	Interface sortie	Adr IP source	Adr IP destination	Protocole	Port source	Port dest	Action
1	Eth0	Eth1	172.16.0.0	172.17.0.1	TCP	> 1024	80	Accepter
2	Eth1	Eth0	172.17.0.1	172.16.0.0	TCP	80	> 1024	Accepter
3	Eth0	Eth1	172.16.0.0	172.17.0.2	UDP	> 1024	53	Accepter
4	Eth1	Eth0	172.17.0. 2	172.16.0.0	UDP	53	> 1024	Accepter
5	Wan0	Eth1	*	172.17.0.1	TCP	> 1024	80	Accepter
6	Eth1	Wan0	172.17.0.1	*	TCP	80	> 1024	Accepter
7	Eth0	Wan0	172.16.0.0	*	TCP	> 1024	80	Accepter
8	Wan0	Eth0	*	172.16.0.0	TCP	80	> 1024	Accepter
9	*	*	*	*	*	*	*	Refuser

1. *Give the corresponding policy for each pair of rules (1-2), (3-4), (5-6) and (7-8)*
2. *Specify the rule that will check each of the following packets and say whether the packet will be accepted or rejected*

-IP s : 172.16.0.30 | IP D : 12.230.24.45 | Prot : TCP | Port sce :1045 | Port dest : 443

-IP s : 172.16.0.5 | IP D : 172.17.0.2 | Prot : UDP | Port sce :6810 | Port dest : 53

-IP s : 140.10.2.1 | IP D : 172.17.0.1 | Prot : TCP | Port sce :8000 | Port dest : 80

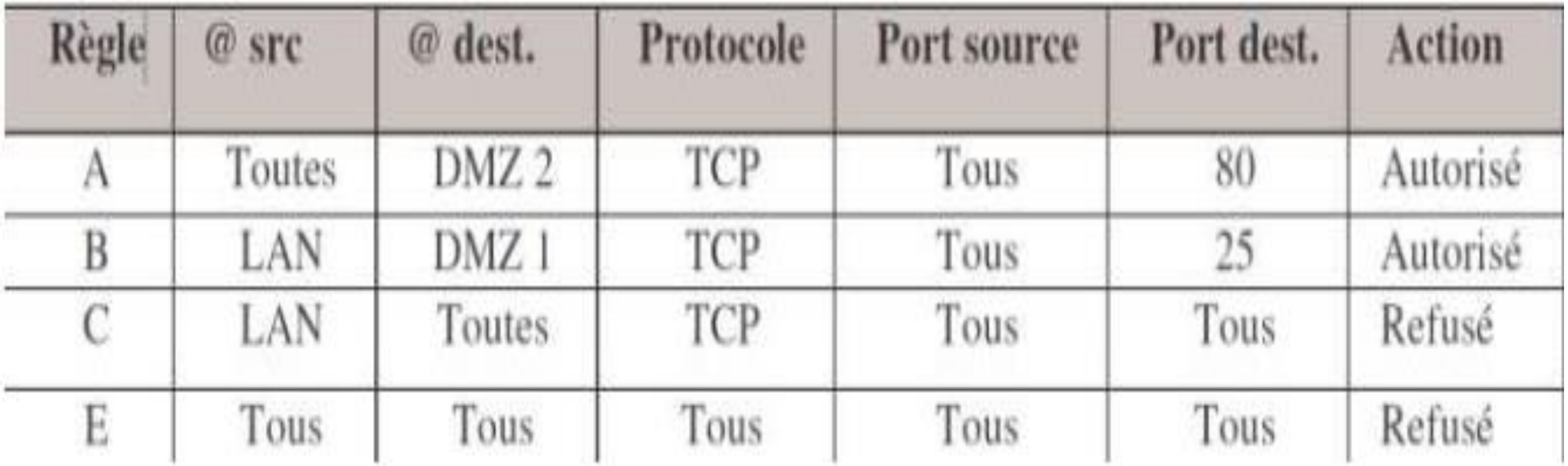
- IP s : 172.17.0.1 | IP D : 1.2.3.4 | Prot : TCP | Port sce :80 | Port dest : 9999

.

Packet Filter Firewall/ Simple Filtering

Exercise 2

Below, rule A of the firewall allows machines on the private LAN to access DMZ2 while rule C should forbid it. How can this be fixed?

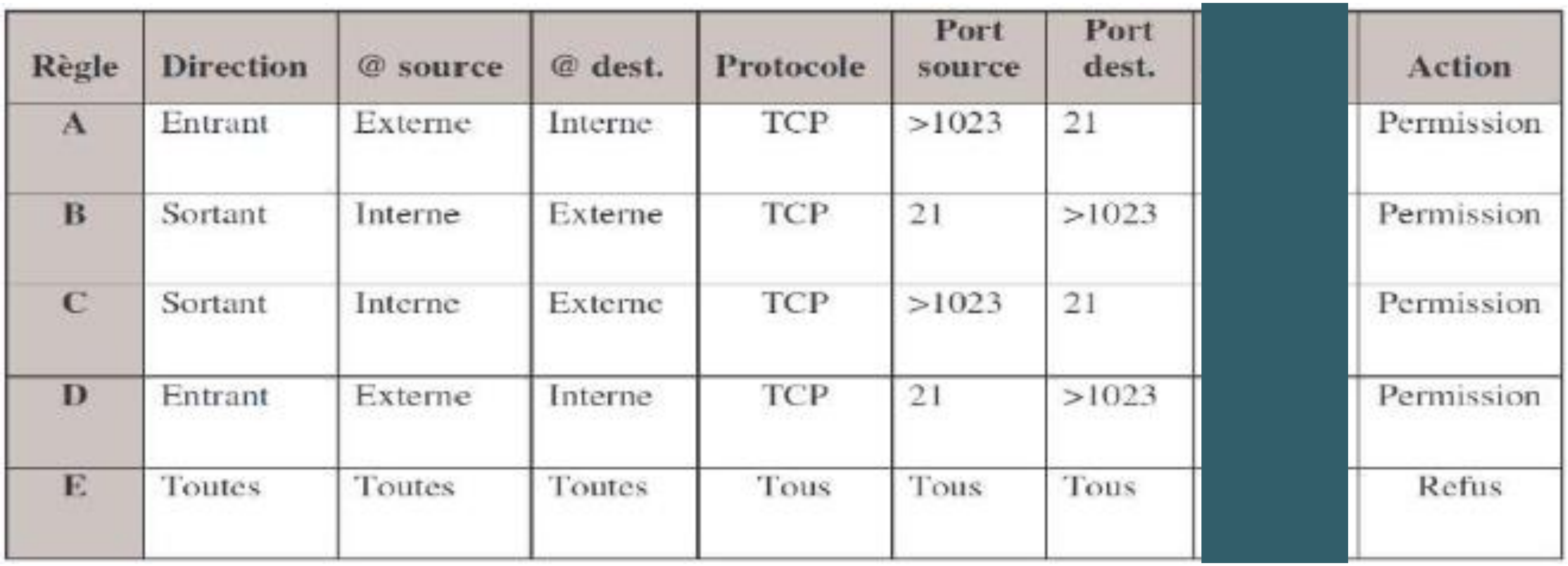


Règle	@ src	@ dest.	Protocole	Port source	Port dest.	Action
A	Toutes	DMZ 2	TCP	Tous	80	Autorisé
B	LAN	DMZ 1	TCP	Tous	25	Autorisé
C	LAN	Toutes	TCP	Tous	Tous	Refusé
E	Tous	Tous	Tous	Tous	Tous	Refusé

.

Packet Filter Firewall/ Simple Filtering

The following table represents a set of filtering rules on a firewall.

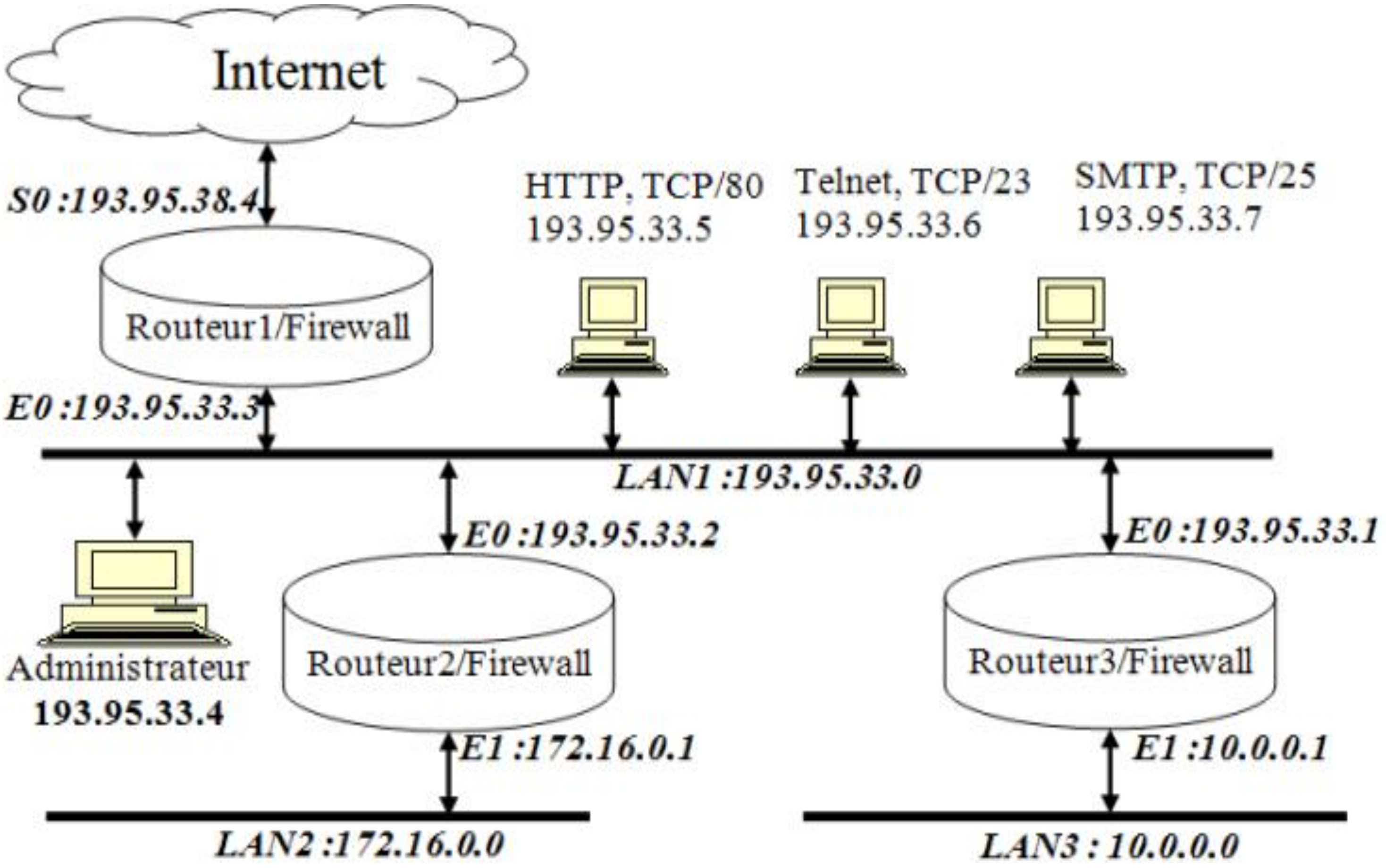


Règle	Direction	@ source	@ dest.	Protocole	Port source	Port dest.	[redacted]	Action
A	Entrant	Externe	Interne	TCP	>1023	21	[redacted]	Permission
B	Sortant	Interne	Externe	TCP	21	>1023	[redacted]	Permission
C	Sortant	Interne	Externe	TCP	>1023	21	[redacted]	Permission
D	Entrant	Externe	Interne	TCP	21	>1023	[redacted]	Permission
E	Toutes	Toutes	Toutes	Tous	Tous	Tous	[redacted]	Refus

- ***Are FTP transfers to an internal server still allowed?***
- ***FTP transfers to an internal server are only allowed if the connection is initiated from outside?***
- ***Are FTP transfers to an external server always allowed?***
- ***FTP transfers to an external server are only allowed if the connection is initiated from the inside?***
- ***Are SMTP mail transfers allowed in both directions?***

Packet Filter Firewall/ Simple Filtering

Let's consider the network architecture shown in figure 1 where LAN1 is the network of servers accessible from outside and inside the company.



Packet Filter Firewall/ Simple Filtering

In which routers should filtering rules be implemented in each of the following cases:

- ***Allow internal and external users to access the HTTP, FTP and SMTP servers on LAN1***
- ***Allow the administrator machine to access the different LANs.***
- ***Allow LAN1 users to access the Internet***

.

Packet Filter Firewall/ Simple Filtering

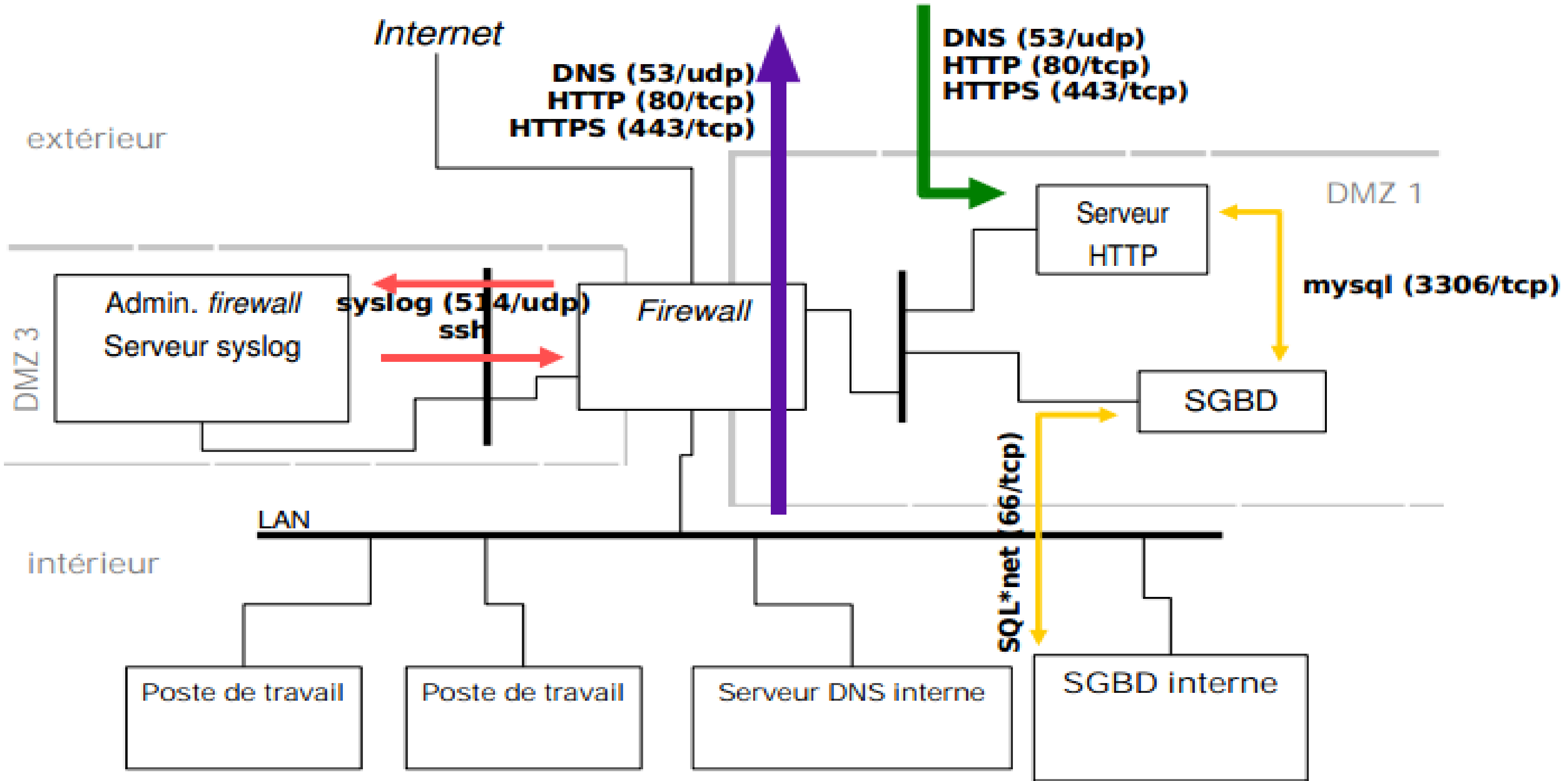
Complete the following table allowing external users to access the LAN1' s http server and allowing LAN1 users to access the external web servers.

Action	*Ip_S*	*IP_D*	*Protocol*	*Port_s*	*Port_D*

.

Packet Filter Firewall/ Simple Filtering

Complete the following table allowing external users to access the LAN1' s http server and allowing LAN1 users to access the external web servers.



Internet
extérieur
DNS (53/udp)
HTTP (80/tcp)
HTTPS (443/tcp)
DNS (53/udp)
HTTP (80/tcp)
HTTPS (443/tcp)
DMZ 1
Serveur
HTTP
mysql (3306/tcp)
DMZ 3
Admin. firewall
Serveur syslog
syslog (514/udp)
ssh
Firewall
SGBD
SQL*net (66/tcp)
LAN
intérieur
Poste de travail
Poste de travail
Serveur DNS interne
SGBD interne