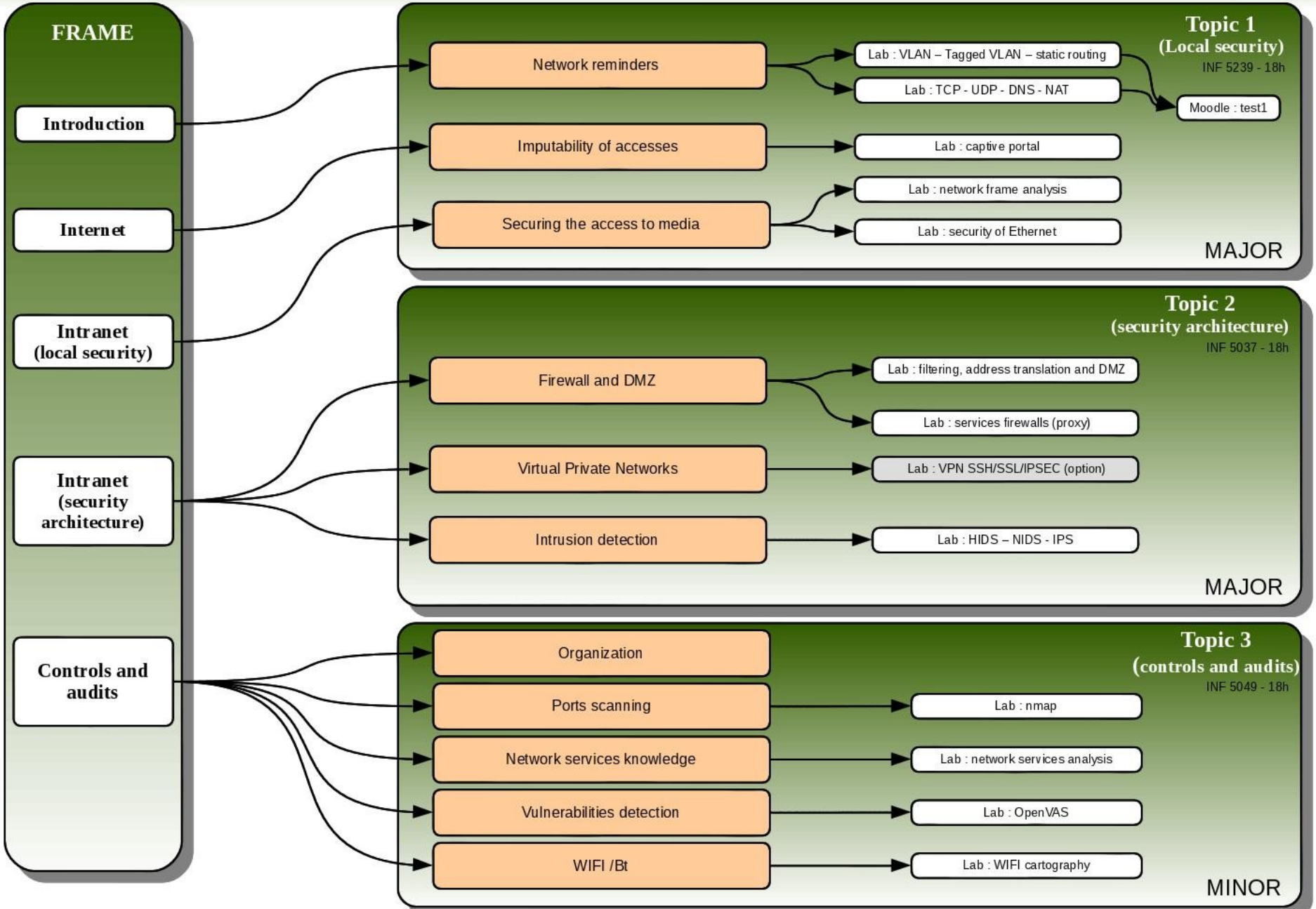
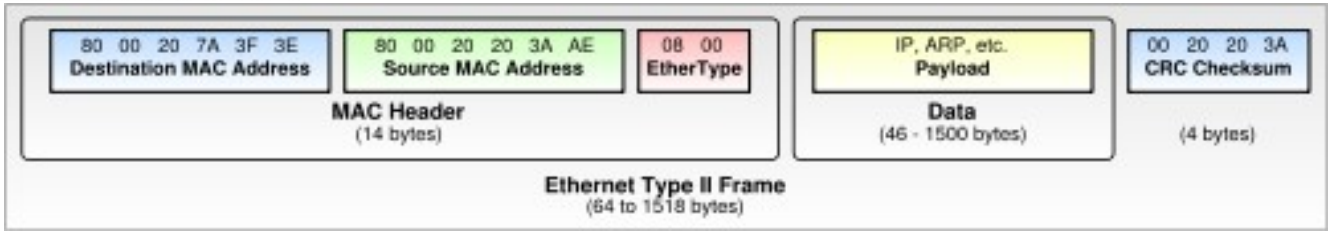
Network reminders

By Roxy

Course 5A - « network security »



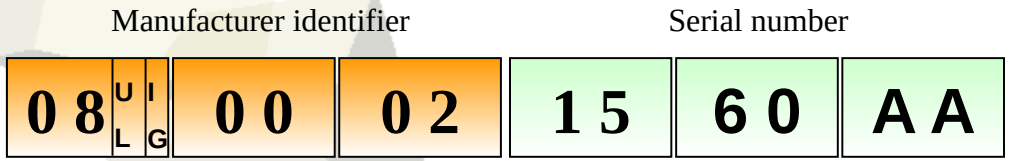


An Ethernet NIC give the frame to the OS only if the destination MAC address is its own MAC address.

Exception for :

- The broadcast frames ;
- The multicast frames with pre-recorded addresses (manufacturers frames) ;
- When the NIC is in promiscuous mode.

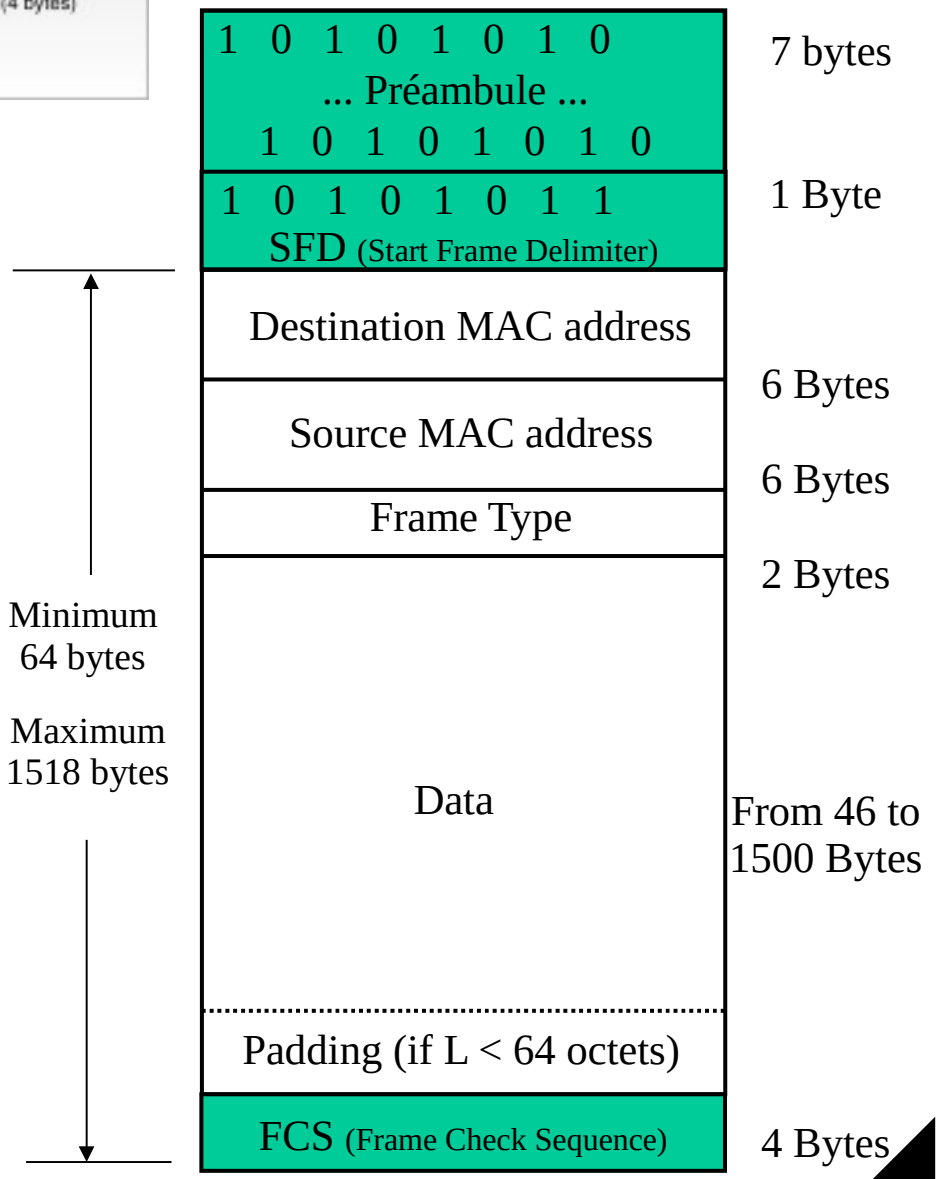
Physical address : IEEE (802.1)



Bit U/L: 0 = U (Universal address (managed by IEEE)
1 = L (Local address)

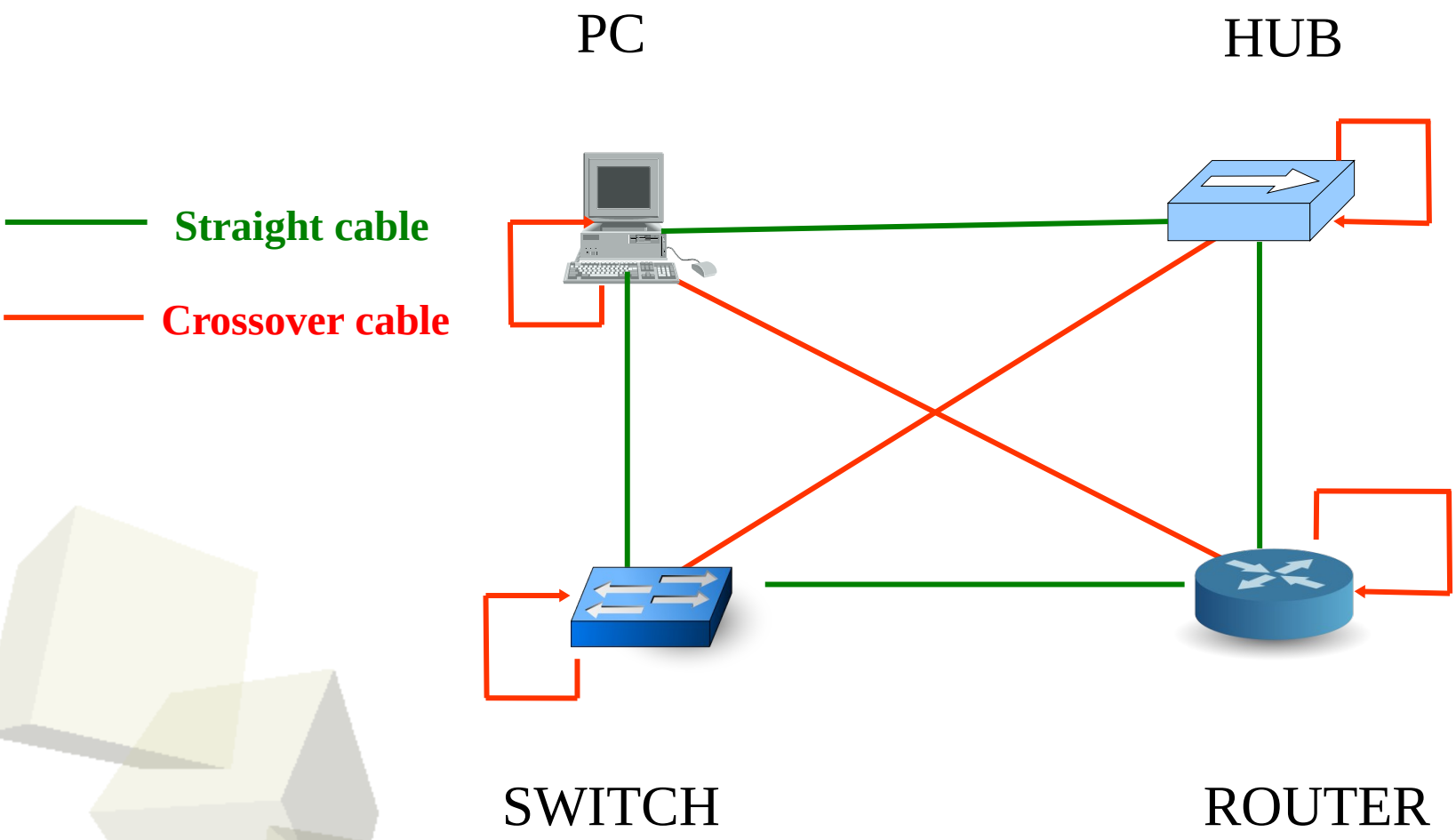
Bit I/G: 0 = I : individual address (Unicast)
1 = G : Group address (Multicast)

Ethernet frame



Never shown in frames analysis software

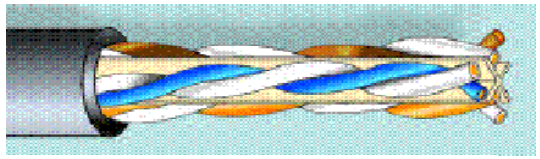
The wiring



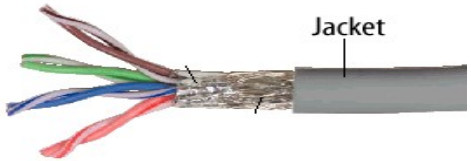
Wires with Twisted pairs

Protection systems

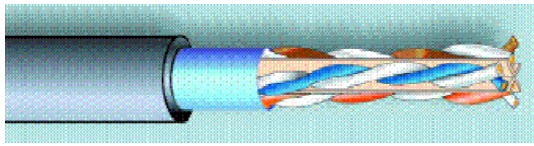
Unshielded



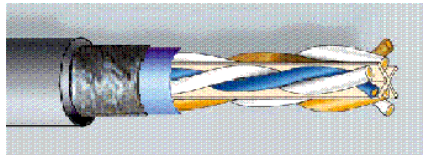
General Shielded : *protection against high frequency*



General Foiled : *protection against low frequency*

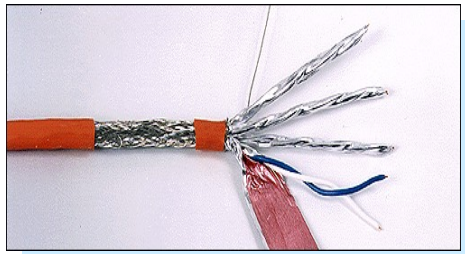


General shielded and foiled (SF)



Foiled Twisted Pair (FTP)

Dénomination	Wire	Pair
U / UTP		
U / FTP		foiled
F / UTP	foiled	
F / FTP	foiled	foiled
SF / UTP	Foiled + shielded	
S / FTP	shielded	foiled



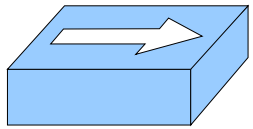
Ethernet offers

100 Base TX

- Speed : 100 Mégabits/s
- Coding : Baseband
- The support : 2 twisted pairs

	NOM	Longueur du segment	TYPE
Fast Ethernet	100 Base TX	100 m	2 paires, catégorie 5
	100 Base T2	100 m	2 paires, catégorie 3
	100 Base T4	100 m	4 paires, catégorie 3
	100 Base FX	2 000 m	Fibre optique
Giga Ethernet	1000 Base LX	550 m	FO
	1000 Base SX	5000 m	FO
	1000 Base T	100 m	4 paires torsadées, catégorie 3
10 Giga Ethernet	10G Base LR	25 km	FO monomode
	10G Base ER	40 km	FO monomode
	10G Base SR	100 m	FO multimodes
	10G Base LRM	300 m	FO multimodes
	10G Base T	100 m	4 paires torsadées, catégorie 6

CSMA/CD & HUB :



- How does it work ?
- Half duplex or full duplex mode ?
- What others L2 technologies share the media ?

SWITCH :

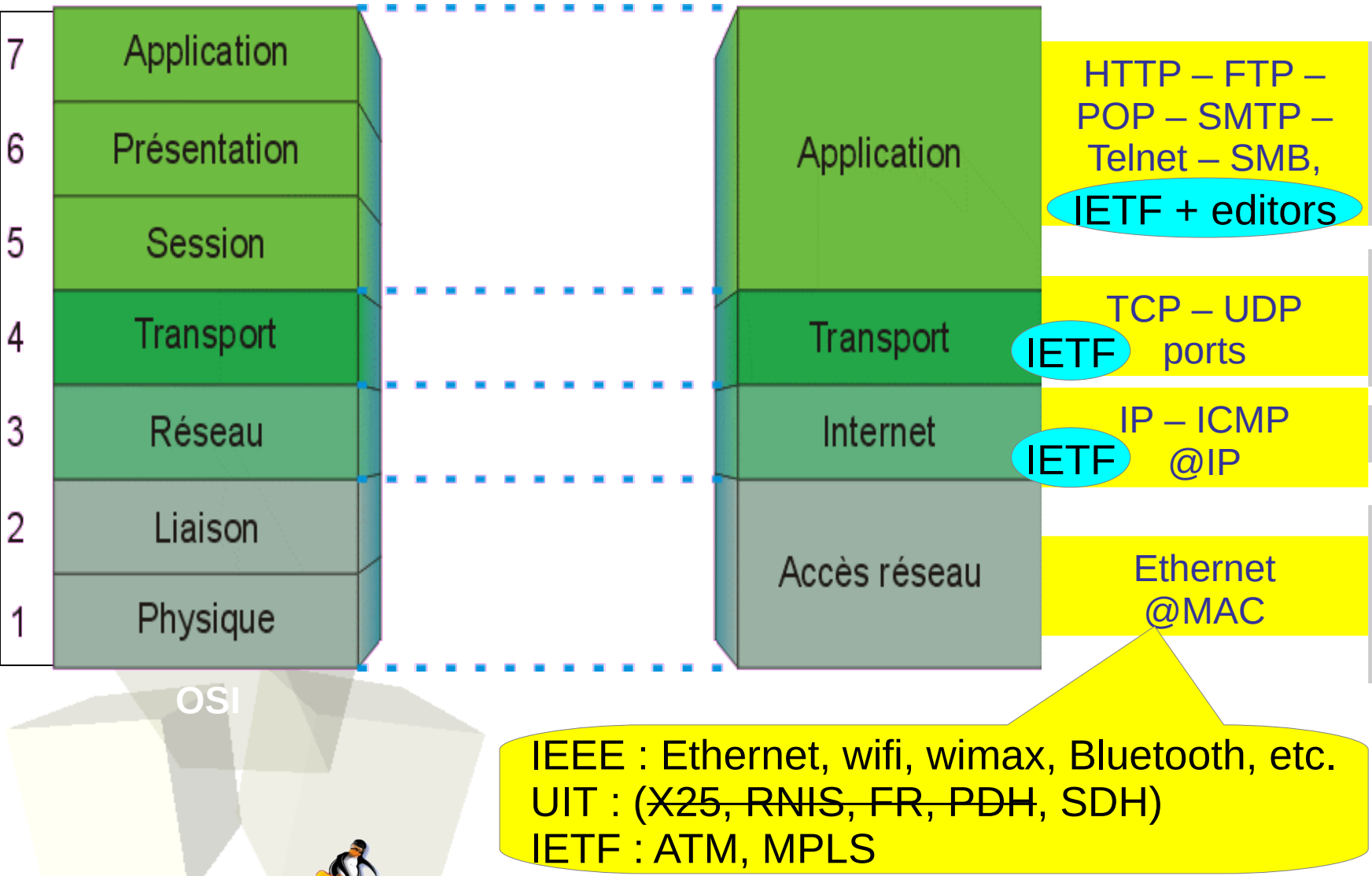
- Is there any collisions ?
- Half duplex or full duplex mode ?
- Auto-negotiation : which norm ? Why ?
- How many switches in cascade ?
- Inner workings ? How many memory ? --> (**slides**)

VLAN :

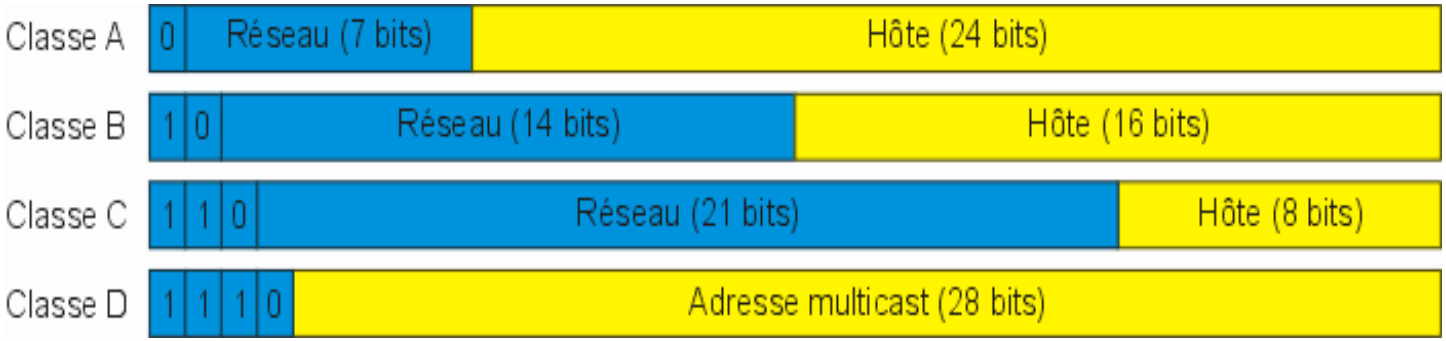
- What's the main goal?
- What's 802.1q --> (**slides**)

IP/Ethernet

- Broadcast and Multicast IP : Which differences for Ethernet ?


OSI / ISO
TCP-IP
Applications
7 Application
6 Présentation
5 Session
4 Transport
3 Réseau
2 Liaison
1 Physique
OSI
Application
Transport
Internet
Accès réseau
HTTP – FTP – POP – SMTP – Telnet – SMB,
IETF + editors
Web navigation
Files transfert
Messaging
shares
TCP – UDP
IETF ports
From 0 to 65535
80, 20&21, 110, 25, 22, 135, etc.
IP – ICMP
IETF @IP
router
Ethernet
@MAC
NIC
Modem
switch – Hub
Repeater
IEEE : Ethernet, wifi, wimax, Bluetooth, etc.
UIT : (X25, RNIS, FR, PDH, SDH)
IETF : ATM, MPLS

RFC IP-Class



0.0.0.1 to 127.255.255.254 (netmask /8)
128.0.0.1 to 191.255.255.254 (netmask /16)
192.0.0.1 to 223.255.255.254 (netmask /24)

224.0.0.1 to 239.255.255.254

Now, we prefer using the subnetting system without class segmentation (and the CIDR notation). Ex : 10.10.10.0/24, 200.10.0.0/16 (= 200.10/16), 192.168.10.1/25

3 private address classes (can't be found on Internet)

In the class A : from 10.0.0.0 to 10.255.255.255 (/8)

In the class B : from 172.16.0.0 to 172.31.255.255 (/12)

In the class B : from 192.168.0.0 to 192.168.255.255 (/16)

1 address class for the loopback

In the class A : from 127.0.0.1 to 127.255.255.255 (/8)

Network reminders

Can we attribute these IP addresses to an equipment ?

223.56.3.0
18.255.255.254
126.127.127.127
127.126.126.1
145.145.255.255
18.254.254.255
0.0.0.0
255.0.0.0
191.255.255.255
192.192.0.0

Network reminders

Can we attribute these IP addresses to an equipment ?

223.56.3.0	No (network IP@)
18.255.255.254	Yes
126.127.127.127	Yes
127.126.126.1	No (IP@ for loopback and test)
145.145.255.255	No (broadcast IP@)
18.254.254.255	Yes, only if the Netmask is the default class one (/8)
0.0.0.0	No
255.0.0.0	No (network IP@)
191.255.255.255	No (broadcast IP@)
192.192.0.0	No (network IP@)

Network reminders

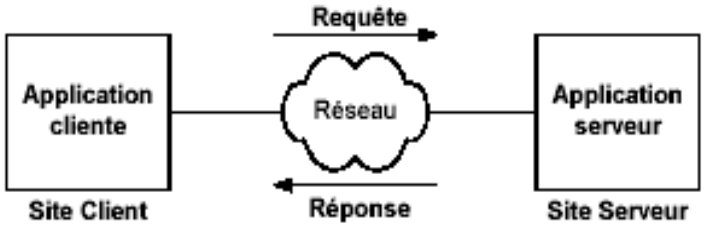
Can these devices communicate with each other ?

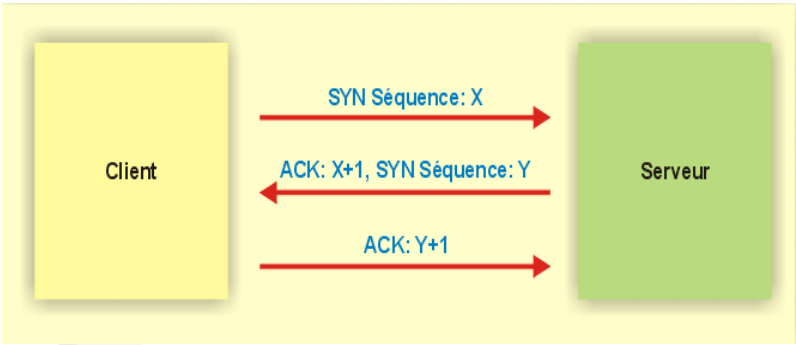
IP@ Eq-1	Netmasq Eq-1	O / N	IP@ Eq-2	Netmasq Eq-2
13.0.0.0	255.0.0.0		13.0.0.1	255.0.0.0
127.0.127.1	255.0.0.0		127.0.127.2	255.0.0.0
125.3.3.3	255.255.0.0		125.0.0.1	255.0.0.0
192.168.1.2	255.255.255.0		192.168.1.254	255.255.255.0
10.10.10.130	255.255.255.240		10.10.10.141	255.255.255.240

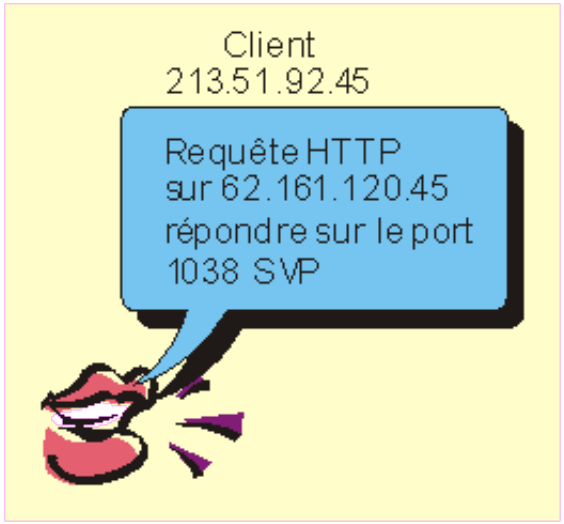
Network reminders

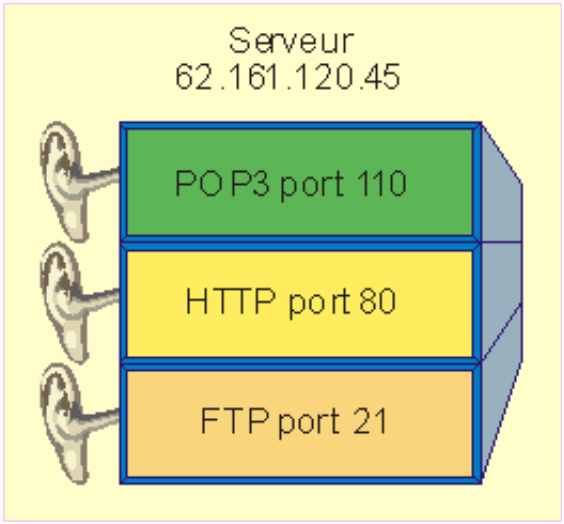
Can these devices communicate with each other ?

IP@ Eq-1	Netmasq Eq-1	O / N	IP@ Eq-2	Netmasq Eq-2
13.0.0.0	255.0.0.0	N	13.0.0.1	255.0.0.0
127.0.127.1	255.0.0.0	N	127.0.127.2	255.0.0.0
125.3.3.3	255.255.0.0	N	125.0.0.1	255.0.0.0
192.168.1.2	255.255.255.0	O	192.168.1.254	255.255.255.0
10.10.10.130	255.255.255.240	O	10.10.10.141	255.255.255.240



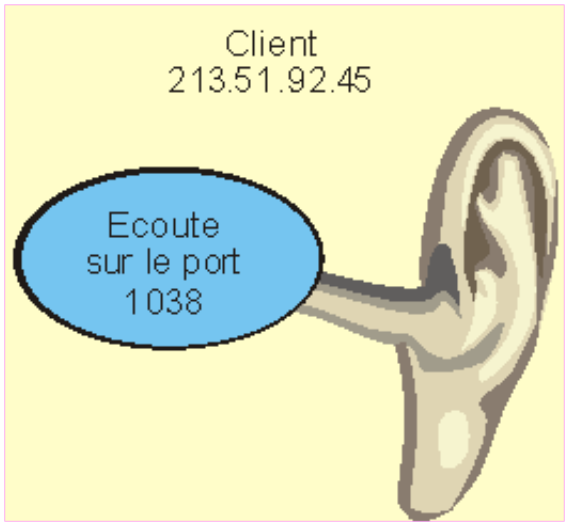


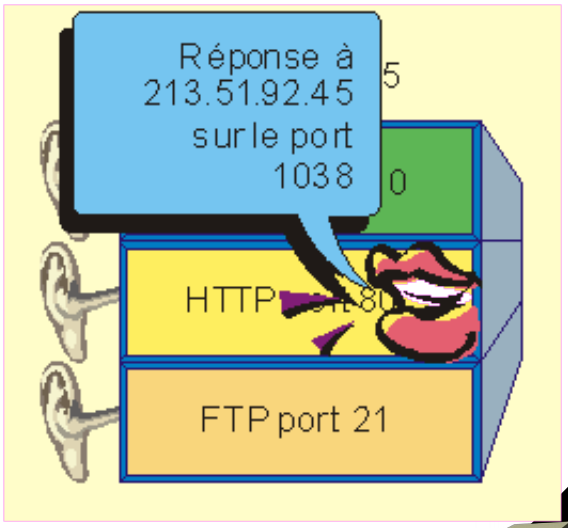




Well known ports

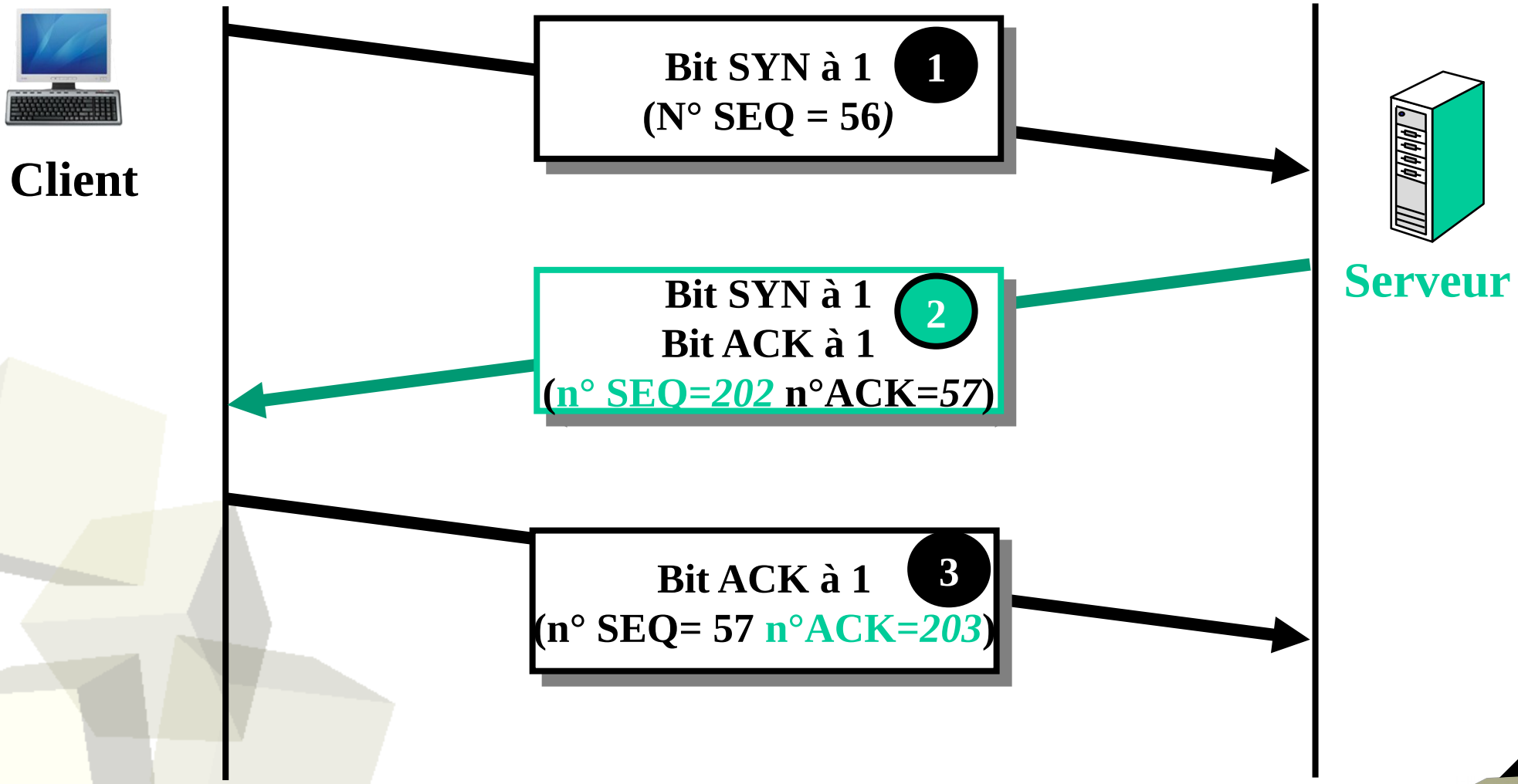
ftp-data	20/tcp	File Transfer [Default Data]
ftp-data	20/udp	File Transfer [Default Data]
ftp-data	20/sctp	FTP
ftp	21/tcp	File Transfer [Control]
ftp	21/udp	File Transfer [Control]
ftp	21/sctp	FTP
ssh	22/tcp	SSH Remote Login Protocol
...		





Établissement de la connexion (handshaking)

- Utilisation des bits SYN et ACK
- Le n° de séquence est généré par l'horloge système (aléa)



Transfert des données

- Gestion des acquittements lors du transfert
- Le n° de séquence correspond à l'indice du 1er octet

20 octets à émettre

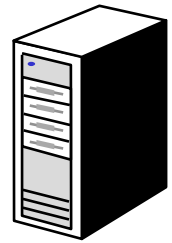
Ack attendu 120

100 octets à émettre

Ack attendu 220

80 octets à émettre

Ack attendu 300



50 octets à émettre

Ack attendu 300

60 octets à émettre

Ack attendu 360

n°seq=100 n°ack=0 (+20 octets)

n°seq=250 n°ack=120 (+50 octets)

n°seq=120 n°ack=300 (+100 octets)

n°seq=300 n°ack=220

n°seq=220 n°ack=360

n°seq=360 n°ack=300

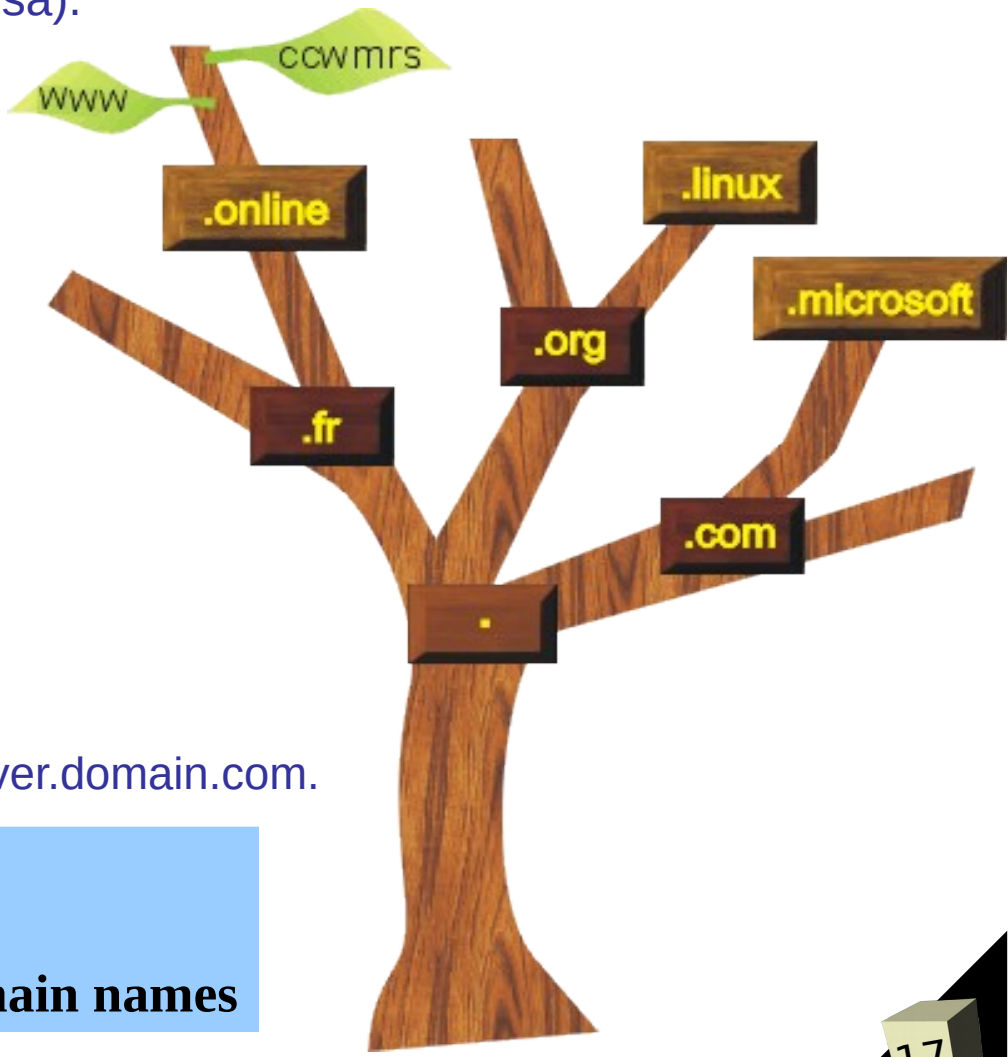
The « Domain Name System » is a network service on port UDP 53. It allows to associate :
- a Full Qualified Domain Name (FQDN) and its aliases to a IP address (and vice-versa) ;
- the IP address of the mail servers of a domain name ;
- a service name to a IP address (and vice-versa).

```
$ORIGIN          domain.com
server1  IN      A       10.0.1.5
server2  IN      A       10.0.1.6
ftp              IN      CNAME server1
www              IN      CNAME server1
smtp             IN      CNAME server2
sipserver        IN      CNAME server2
                 IN      MX      10
smtp.domain.com.
```

```
$ORIGIN 1.0.10.in-addr.arpa

5       IN      PTR server1.domain.com.
6       IN      PTR server2.domain.com.
```

```
_sip._tcp.domain.com. 86400 IN SRV 0 5 5060 sipserver.domain.com.
```

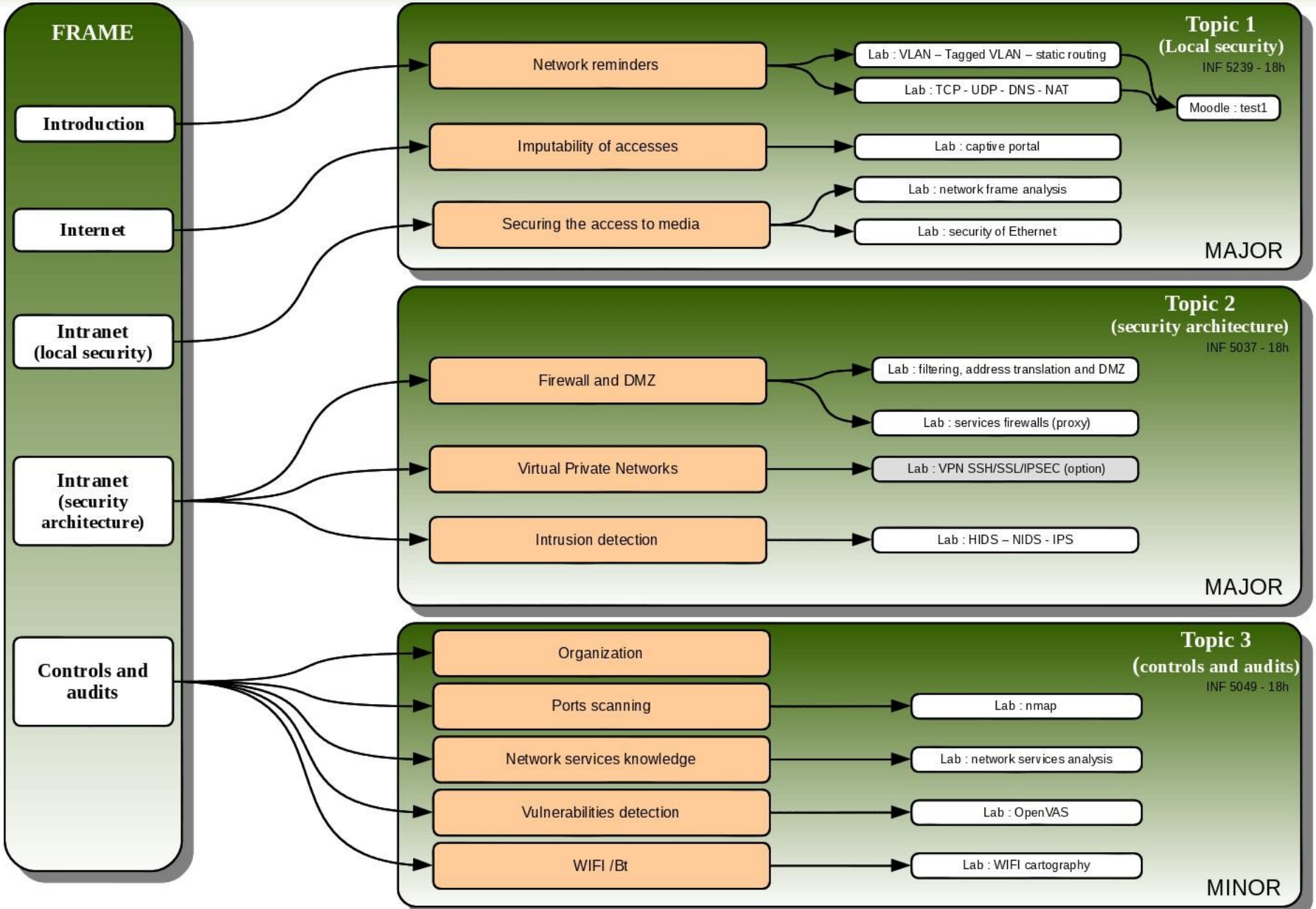


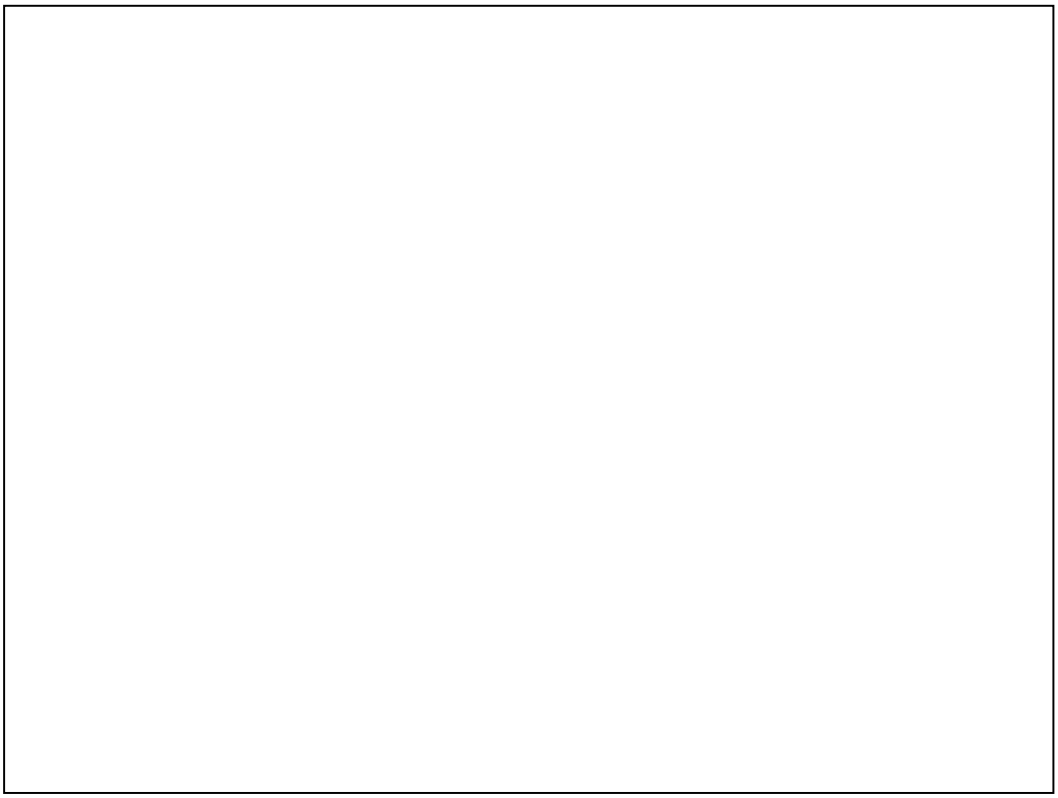
Strategic in the Internet architecture
13 root servers including 7 in USA
1998 : creation of l'ICANN to manage domain names

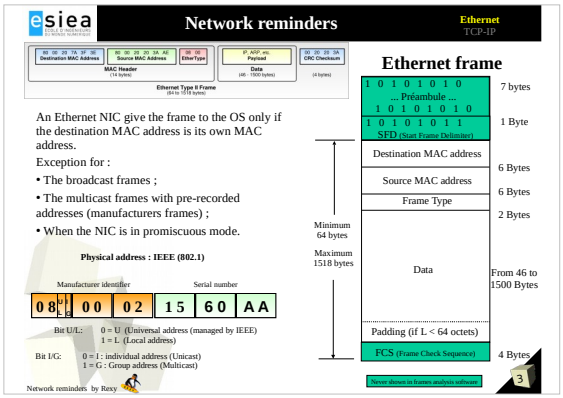
Network reminders

By Roxy

Course 5A - « network security »







LA TRAME ETHERNET II :

Longueurs de la trame :

- minimum 64 octets :
  - adresses + Frame Type + données + FCS;
  - bourrage si nécessaire;
  - préambule non compris;
- maximum 1518 octets ;
  - adresses + Frame Type + données + FCS;
  - préambule non compris.

Le préambule :

- il est constitué de 8 octets;
- c’est une suite de 0 et de 1 qui permet au récepteur de synchroniser son horloge.

Adresse de destination :

- adresse MAC du destinataire;
- placée en début de trame elle permet aux récepteurs de savoir immédiatement s’ils doivent traiter ou non la trame;
- elle est de type « unicast », « multicast » ou « broadcast ».

Adresse source :

- identifie l’émetteur de la trame;
- c’est toujours une adresse unicast.

Le Frame Type :

- indique le protocole de niveau supérieur transporté.

Les données :

- elles contiennent le paquet de niveau supérieur;
- la valeur max de 1500 octets a été définie de manière arbitraire à la création du standard Ethernet, ce qui évite à une station de monopoliser le support de transmission.

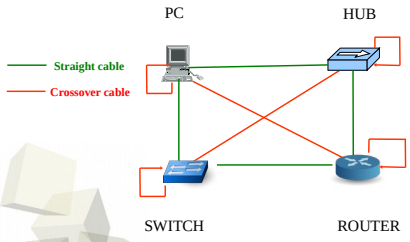
Le bourrage :

- il est appliqué si la taille des données est insuffisante pour obtenir une longueur de trame de 64 octets.

Le FCS :

- c’est un champ de 4 octets qui permet de vérifier l’intégrité de la trame;
- il est calculé à partir des champs adresses, longueur de données et données.

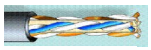
The wiring



Wires with Twisted pairs

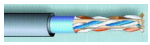
Protection systems

Unshielded



General Shielded : ***protection against high frequency***

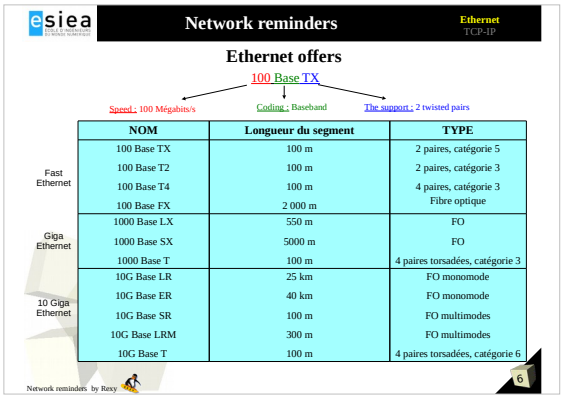
General Foiled : ***protection against low frequency***



General shielded and foiled (SF)

Dénomination	Wire	Pair
U / UTP		
U / FTP		foiled
F / UTP	foiled	
F / FTP	foiled	foiled
SF / UTP	Foiled + shielded	
S / FTP	shielded	foiled

Foiled Twisted Pair (FTP)



Les offres Ethernet

L'IEEE a adopté une nomenclature pour identifier les caractéristiques de chaque évolution d'Ethernet.

Les différentes offres Ethernet (802.3) sont détaillées dans la norme : IEEE 802.3-2008.

Les offres à 10 Mbps :

- Câble coaxial :
  - 10 Base 5, coaxial épais, 500 m, 1er du nom;
  - 10 Base 2, coaxial fin, 185 m, Plus souple que le 10 Base 5;
- Paire torsadée :
  - 10 Base T, paires torsadées, 100 m;
- Fibre optique :
  - 10 Base F, fibre optique, 2000 m, Inter-site et Inter-bâtiment

.

Les offres Fast Ethernet

Au début des années 1990, il a fallu offrir des débits plus importants (Voix, Données, Images).

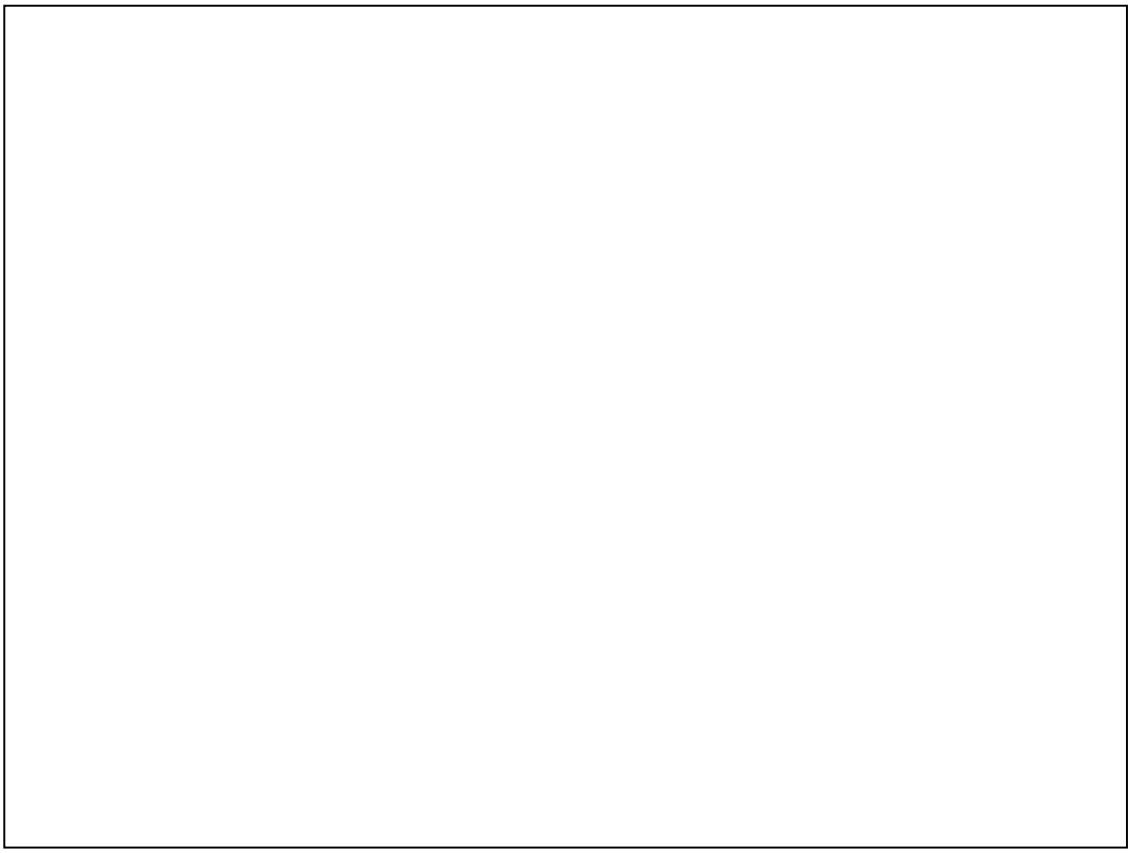
En juin 1995 normalisation de Fast Ethernet, compatible avec Ethernet et qui conserve les caractéristiques de taille de trames :

- 100 Base FX, 2 Fibres optiques, 400 m, ST ou SC (2 km selon longueur d'onde et fibre), codage 4B/5B;

- 100 Base TX, 2 paires torsadées, 100 m, à partir de câble cat 5, codage 4B/5B;

- 100 Base T2, 2 paires torsadées, 100 m, à partir de câble cat 3, modulation d'impulsion en amplitude à 5 niveaux;

- 100 Base T4, 4 paires torsadées, 100 m, à partir de câble cat 3.



Définition :

En mode « simplex » le communication n’est effectuée que dans un sans (exemple : les émetteurs TV)

En mode « Half-duplex », la communication est effectuée dans les deux sens par alternat (exemple : le Talkie Walkie).

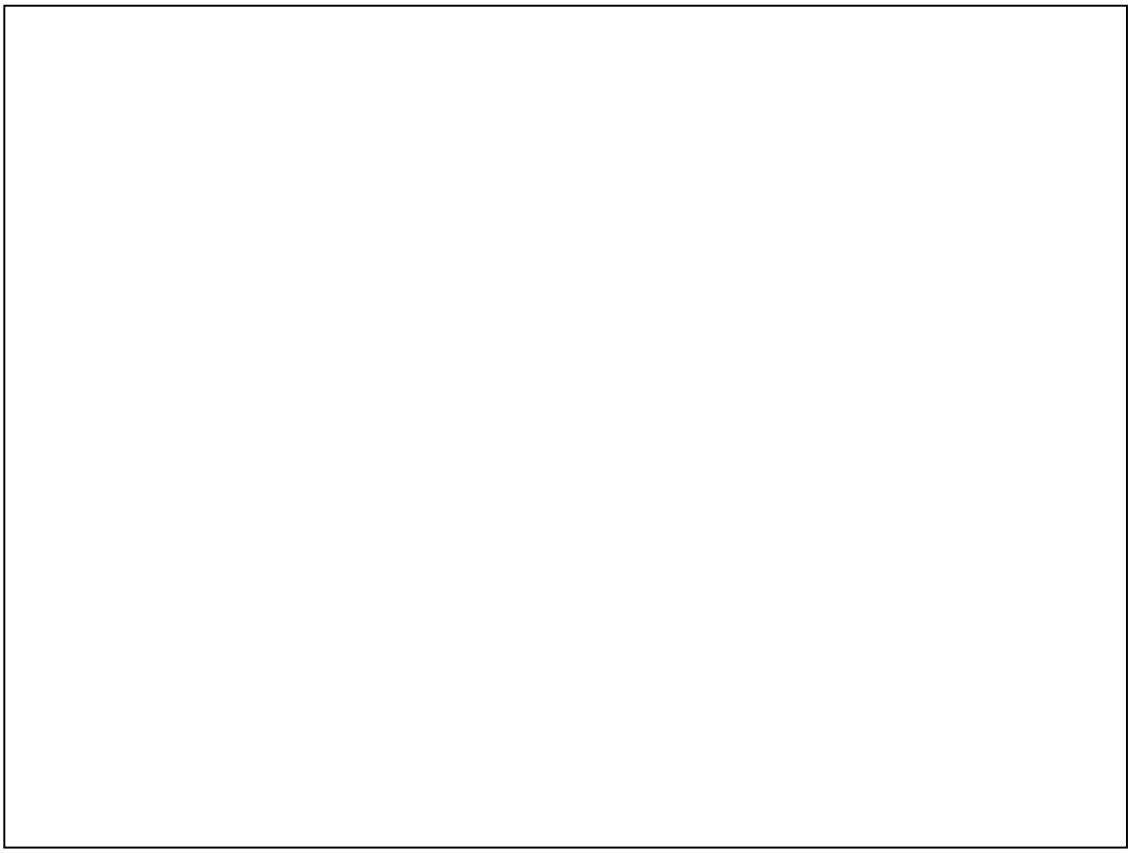
En mode « Full-Duplex », la communication est effectuée dans les deux sens simultanément (exemple : la téléphonie).

L’auto-négociation permet à deux extrémités Ethernet de s’accorder automatiquement sur les caractéristiques des échanges (Half ou Full duplex, 10 ou 100 Mb/s, avec ou sans contrôle de flux, etc.).

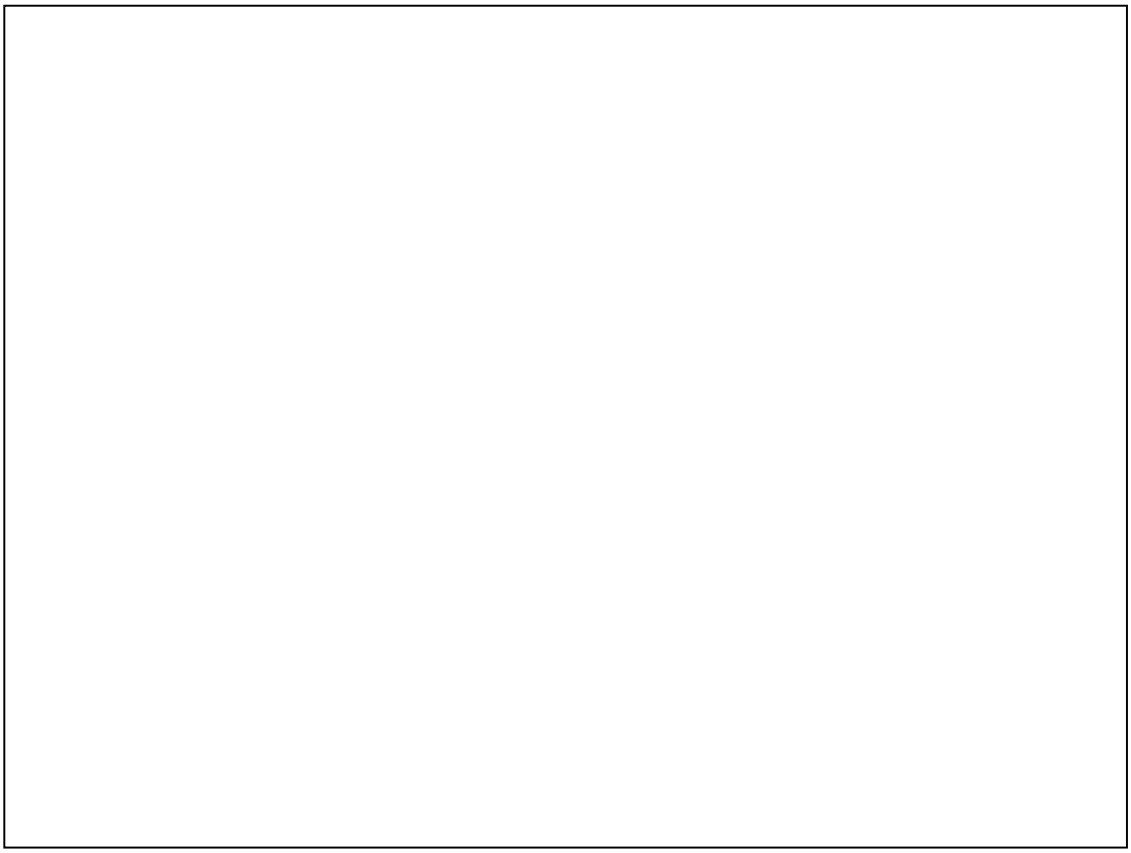
L’unicast est un mode de transmission dans lequel l’information est envoyée d’un émetteur à un récepteur (1 vers 1).

Le « Broadcast » ou « diffusion » est un mode de transmission dans lequel l’information est envoyée d’un émetteur à l’ensemble des récepteurs en écoute (1 vers N).

Le « MultiCast » est un mode de transmission dans lequel l’information est envoyée d’un émetteur vers un groupe de récepteurs en écoute (1 vers M (avec M qui est un sous-ensemble de N)).



Le modèle OSI définit sept couches. TCP/IP est basé sur le modèle DOD, qui ne comporte que quatre couches, mais en cohérence avec le modèle OSI.
Le protocole de plus bas niveau (couches 1 & 2 ou accès réseau) assure la bonne gestion du médium (détection de collisions - CSMA/CD) et permet l'acheminement des informations entre émetteur et destinataire. Les réseaux de type Ethernet qui sont utilisés sur la majorité des réseaux locaux respecte la norme IEEE 802.3. Dans ces réseaux, les carte possèdent une adresse unique : l'adresse MAC.
IP permet le routage des informations entre réseaux, c'est ici que l'adresse IP est utilisée. ICMP est un protocole de « contrôle » il met à disposition des messages de dépistage d'erreur et de signalisation.
TCP et UDP sont les protocoles orientés transport de données. UDP est dit « sans connexion » et TCP « est dit « avec connexion ». Ces protocoles permettent à ceux de la couche supérieure de transporter leurs données de façon fiable.
Les protocoles applicatifs sont des protocoles de haut niveau, destinés à permettre le dialogue entre applications serveurs et clientes.



En IPV4, le plan d’adressage a été divisé en plusieurs classes afin de pouvoir déployer des réseaux locaux de différentes tailles (2¨8, 2¨^16 et 2^24 stations).

Pour chacune de ces classes, des plages ont été réservées pour les réseau locaux privés.

Can we attribute these IP addresses to an equipment ?

223.56.3.0
18.255.255.254
126.127.127.127
127.126.126.1
145.145.255.255
18.254.254.255
0.0.0.0
255.0.0.0
191.255.255.255
192.192.0.0

10

Network reminders

Can we attribute these IP addresses to an equipment ?

223.56.3.0	No (network IP@)
18.255.255.254	Yes
126.127.127.127	Yes
127.126.126.1	No (IP@ for loopback and test)
145.145.255.255	No (broadcast IP@)
18.254.254.255	Yes, only if the Netmask is the default class one (/8)
0.0.0.0	No
255.0.0.0	No (network IP@)
191.255.255.255	No (broadcast IP@)
192.192.0.0	No (network IP@)

Can these devices communicate with each other ?

IP@ Eq-1	Netmasq Eq-1	O / N	IP@ Eq-2	Netmasq Eq-2
13.0.0.0	255.0.0.0		13.0.0.1	255.0.0.0
127.0.127.1	255.0.0.0		127.0.127.2	255.0.0.0
125.3.3.3	255.255.0.0		125.0.0.1	255.0.0.0
192.168.1.2	255.255.255.0		192.168.1.254	255.255.255.0
10.10.10.130	255.255.255.240		10.10.10.141	255.255.255.240

12

Can these devices communicate with each other ?

IP@ Eq-1	Netmasq Eq-1	O / N	IP@ Eq-2	Netmasq Eq-2
13.0.0.0	255.0.0.0	N	13.0.0.1	255.0.0.0
127.0.127.1	255.0.0.0	N	127.0.127.2	255.0.0.0
125.3.3.3	255.255.0.0	N	125.0.0.1	255.0.0.0
192.168.1.2	255.255.255.0	O	192.168.1.254	255.255.255.0
10.10.10.130	255.255.255.240	O	10.10.10.141	255.255.255.240

13

65535 ports sont disponibles que ce soit en TCP ou en UDP.

Les ports situés en dessous de 1024 sont communément appelés « well-known ports ».

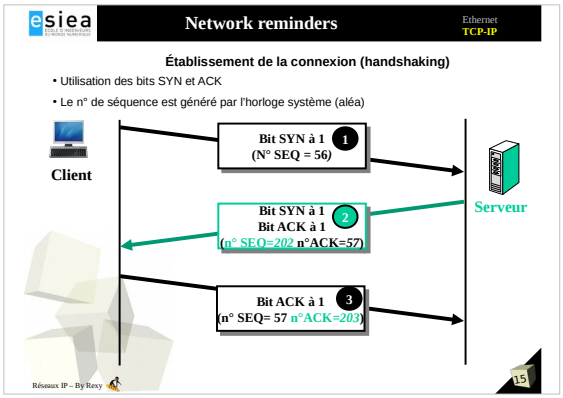
Quand un client ouvre une connexion vers un serveur, il ne doit pas ouvrir un port sortant inférieur à 1024.

Les services les plus connus :

- HTTP (Hyper Text Transfer Protocol), port TCP 80, permet de naviguer sur le Web et de rapatrier des pages web contenant du texte, des images, des liens vers d'autres pages (ou URL), mais qui peuvent aussi contenir des lignes de code exécutable sur le système.

- les protocoles de transfert de fichiers comme FTP (File Transfer Protocol), ports TCP 20 et 21, pour les téléchargements.

- les services de messagerie comme SMTP (Simple Mail Transfer Protocol), port TCP 25, pour l'envoi de courrier et POP (PostOffice Protocol), port TCP 110, ou IMAP (Internet Message Access Protocol), port TCP 143, pour la récupération.
- les services d'accès à distance pour la télémaintenance comme Telnet, port TCP 23, RSH (Remote SHell) ou SSH (Secure SHell), port TCP22.
- d'autres services sont moins visibles, comme DNS (Domain Name System), port UDP 53 ou DHCP (Dynamic Host Configuration Protocol). Ils permettent respectivement de gérer et d'attribuer des adresses logiques (IP) sur les réseaux.



•La connexion :

La connexion TCP est dissymétrique :

- chaque équipement est responsable de ses propres demandes de connexion et de leur gestion.

Une connexion TCP peut être de deux types :

- active, lorsque TCP initie la demande de connexion;
- passive dans le cas TCP est en attente d'une demande de connexion.

- Utilisation du bit SYN :

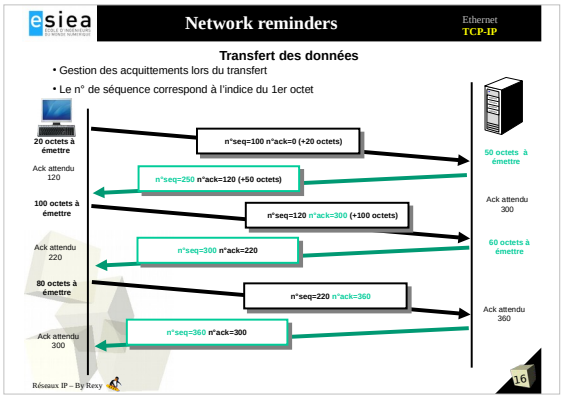
  Lors de la demande de connexion, le client génère un message dont le bit SYN de l'en-tête TCP est à 1. Le numéro de séquence doit être unique pour qu'il ne soit pas confondu par le serveur qui va traiter cette demande. Il est obtenu grâce à un système local (situé sur la station hébergeant le client) d'horloge.

- Utilisation du bit ACK:

  Ensuite, le serveur répond par un acquittement : Utilisation du bit ACK, valeur = 1.

  Il acquitte le message en ajoutant 1 à la valeur du champ séquence précédent et en le positionnant dans le champ acquittement.

  Il génère son propre numéro de séquence.



1. Le transfert des données :

   Dès que la connexion est établie, l'échange des données peut commencer. Il peut débuter pendant la phase de connexion.

   Pour assurer la bonne gestion de la liaison, il s'agit pour chaque extrémité de la connexion d'indiquer à son correspondant l'identité du segment transmis (n° de séquence) et le segment en attente (n° d'acquittement).

   La taille du premier segment TCP émis est au maximum de 556 octets (20 d'en-tête + 536 de données), ceci afin de s'assurer que le destinataire est capable de traiter une taille supérieure.

1. Le contrôle de flux :

   Il permet d'adapter le débit en émission en fonction de la capacité de réception du destinataire.

   Dans TCP, le contrôle de flux est effectué lors des acquittements en utilisant le champ fenêtre qui contient le nombre d'octets que le récepteur peut recevoir :

   - lorsque ce champ est à 0, l'émetteur ne doit plus envoyer de données car le récepteur ne pourra pas les traiter :
   - dans ce cas, l'émetteur teste périodiquement le récepteur;
   - lorsqu'il peut à nouveau recevoir, le récepteur averti l'émetteur par un message d'acquittement dont le champ fenêtre contient la taille de la zone mémoire disponible;
   - le champ fenêtre va donc indiquer à l'émetteur combien de données il va pouvoir traiter en émission.

   Le champ acquittement de l'en-tête TCP, d'une valeur de 4 octets indique la valeur du premier octet qui est attendu dans le prochain message. A chaque acquittement, cette valeur est incrémentée du nombre d'octets reçus.

1. La temporisation – Retransmission des segments :

   Dans son mode de fonctionnement en mode connecté, le protocole TCP mesure en permanence le délai écoulé entre l'émission d'un segment et la réception de son acquittement pour l'adapter aux conditions de trafic. Ce délai est appelé Round Trip Time.

   Si les données ne sont pas acquittées, elles sont retransmises. La valeur du RTT influence de manière importante les performances de TCP :

   - si le RTT est trop petit, des retransmissions inutiles vont avoir lieu;
   - si il est trop grand, le réseau ne sera pas optimisé.

   Cette valeur est à adapter en fonction du type de réseau utilisé. Sur un réseau local, les délais de propagations sont plus courts (quelques ms) que sur un WAN (quelques secondes avec des liaisons satellites).