Internet - Synthèse

Marc de Burlet
20/12/2016

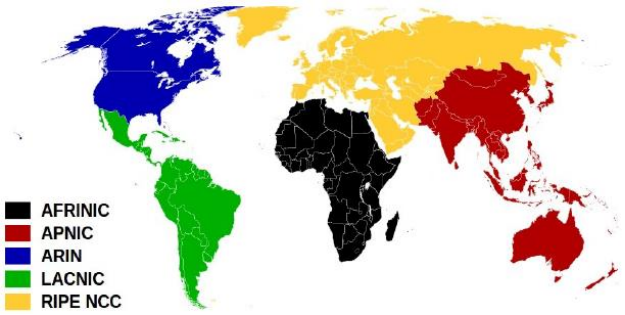
Table des matières

Introduction

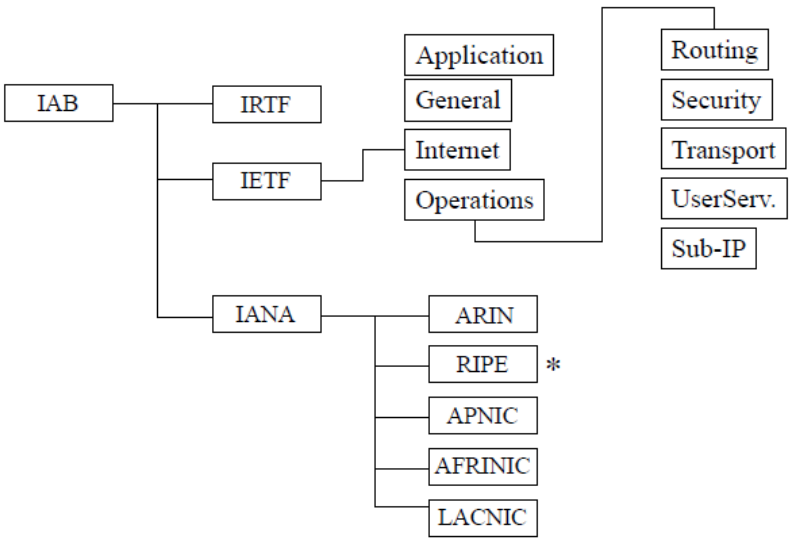
Les organisations de normalisation

- IAB (Internet Activities Board)
    - Chargé de coordonner et guider les protocoles et l'architecture d'Internet
    - Divisé en 3 entités (IRTF, IETF et IANA)

- IRTF (Internet Research Task Force)
    - Doit comprendre les technologies et comment les utiliser dans l'Internet.
- IETF (Internet Engineering Task Force)
    - Coordonne et gère l'évolution des protocoles utilisés dans l'Internet.
    - Publie les RFCs.
- IANA (Internet Assigned Numbers Authority)
    - Gestion et allocation des différents identifiants numériques nécessaires à la gestion et à l'utilisation de l'Internet.
    - Basé sur des groupes régionaux qui distribue les adresses IP (v4 et v6), les numéros d'AS etc..



- IEEE (Institute of Electrical and Electronic Engineers)
- ITU (International Telecommunication Union)



Les 7 couches OSI

Important à connaître!!!

Num	Nom de la couche	Type de données	Nom d'un élément	Exemple d'identifiant
7	Application	Flux	Gateway	Nom de machine, d'utilisateur, adresse mail …
6	Présentation			
5	Session			
4	Transport	Segments; paquets ou session	Switch niveau 4 (Layer 4 switch)	Socket (Port) (UDP ou TCP) (2 bytes)
3	Réseau (Network)	Paquets (Packets)	Routeur (Router)	Adresse IP (v4, 4 bytes; v6 16 bytes), …
2	Lien (Link – MAC)	Trames (Frames)	Pont (Bridge / Switch)	Adresse MAC (6 bytes) (Ethernet), DLCI (FR), VPI/VCI (ATM), …
1	Physique (Physical)	Bits	Répéteur (Repeater / Hub)	Numéro / nom d'une porte ou d'une interface…

On utilise l'encapsulation afin de mettre une couche dans une autre.

La couche 2 est divisée en 2 couches :

- LLC (Logical Link Control)
- MAC (Medium Access Control) qui couvre aussi la couche physique.

Les 5 couches TCP/IP

Num	Nom de la couche	Type de données	Exemple d'identifiant
5	Application	Flux	Nom de machine, d'utilisateur, adresse mail …
4	Transport	Segments; paquets ou session	TCP / UDP
3	Réseau (Network)	Paquets (Packets)	IP
2	Lien (Link – MAC)	Trames (Frames)	Ethernet, FR, ATM, …
1	Physique (Physical)	Bits	Numéro / nom d'une porte ou d'une interface…

Classification des réseaux

0,1 – 1m	**Internal Network** (au sein de la machine)
1m – 500m	**LAN** (Local Area Network)
500m – 50km	**MAN** (Metropolitan Area Network)
50km -	**WAN** (Wide Area Network)

Niveau 1 - La couche Physique

Les interfaces

DS0	64 Kbps
DS1	1.544 Mbps
DS2	6.312 Mbps (4 DS1)
DS3	45 Mbps (30 DS1)
E1	2.048 Mbps
E2	8.448 Mbps
E3	34.368 Mbps
E4	139.264 Mbps

OC-1c	51.840 Mbps
OC-3c	155.520 Mbps
OC-12c	622.080 Mbps
OC-48c	2.488.320 Mbps (2.5 Gbps)
OC-192c	9.953.280 Mbps (10 Gbps)
OC-768c	39.813.120 Mbps (40 Gbps)
OC-3072c	159.252.480 Mbps (160 Gbps)

Les interfaces Ethernet

- La vitesse est multipliée par 10 tous les 3 ans

Ethernet	10 Mbps	Années 90
Fast Ethernet	100 Mbps	2002 - 2003
Gig Ethernet	1 Gbps	2006 - 2007
10 Gig Ethernet	10 Gbps	2009 – 2010 (?)
100 Gig Ethernet	100 Gbps	Core only !
Terabit Ethernet	1 Tbps	Core only !

Les fibres

- Multimode
  - Approprié pour les courtes distances, LANs
  - Plusieurs longueurs d'onde (multi)
  - 50/125 µ, 62,5/125 µ
- Monomode
  - Approprié pour les longues distances, WANs
  - Une seule longueur d'onde (mono)
  - 9/125 µ

Ethenet over Power (CPL)

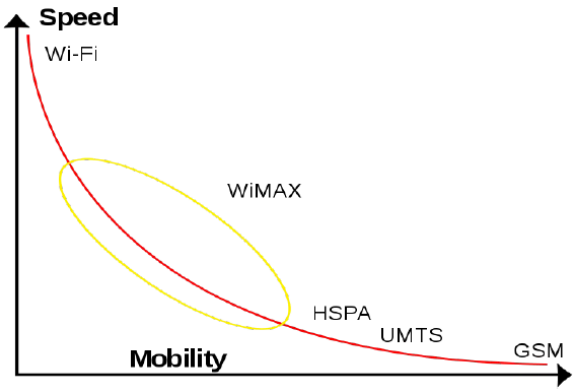
On fait passer de l'information Ethernet sur les câbles électriques qui sont souvent déjà présents. Cette technologie est de plus en plus utilisée en Belgique.

Power over Ethernet

Permet aussi de diminuer le nombre de câbles. Dans ce cas-ci, on fait passer du courant sur les câbles Ethernet.

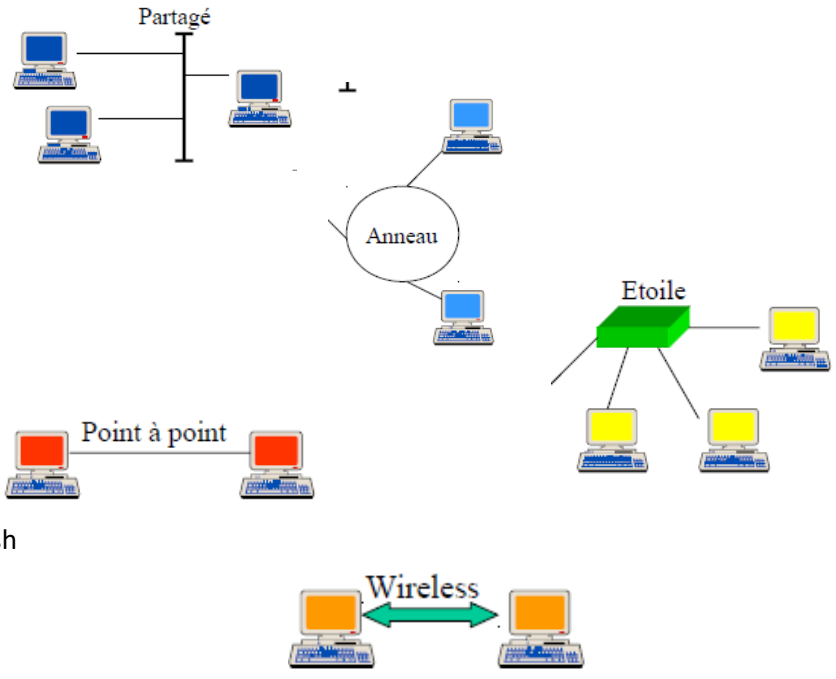
WiMAX

- Worldwide Interoperability for Microwave Access
- **But :** remplacer le « last mile » appartenant au Telecoms par une couverture sans fil
- Jusqu'à 40kmx
- Evite les petits obstacles (arbres, voitures,…) mais pas les grands (immeubles, collines, …)



Niveau 2 - La couche Lien

Topologies



- Shared media (partagé)
  - Ethernet
- Ring
  - Token ring
- Etoile
  - Ethernet/Satellite
- Point à point
  - ATM / FR / POS /X25
  - Partial Mesh / Full Mesh
- Wireless
  - 802.11 / Bluetooth

Trame Ethernet

1 2 3 4 5 6 7 8 9 1011 1213 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32

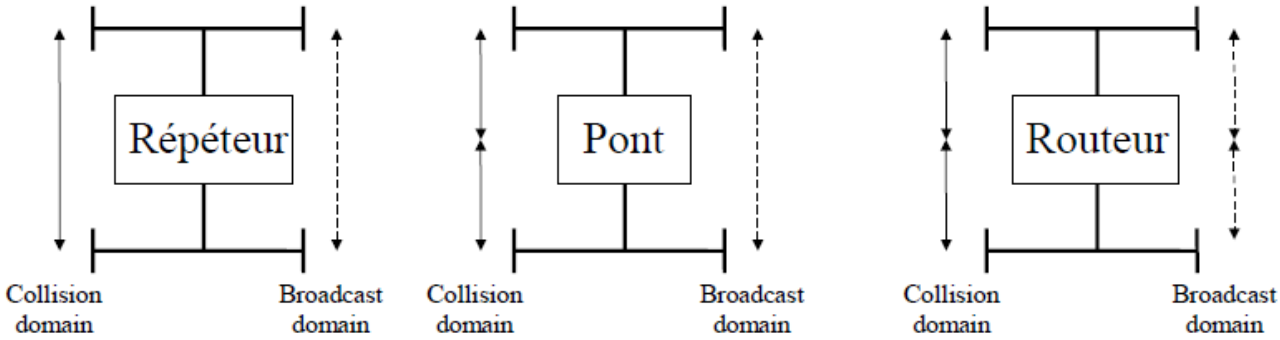
Destination Address	Source Address	Ether Type	Data (Variable length: 46 to 1500)	PAD	CRC

- Les longueurs sont en **bytes**
- Les adresses sont de niveau 2 : **MAC**
- **EtherType** : détermine le type de protocole utilisé pour les datas
- **PAD** : padding (seulement si la trame est trop courte)
- **CRC** (Cyclic Redundant Check)
- **Taille** : entre 64 et …
    - 1518 B dans le standard de base
    - 9000 B pour les Jumbo Frames
    - 64 000 B pour les Super Jumbo Frames (SJF)

Les types d'adresses

- **Unicast**
    - Envoyé à une adresse en particulier
    - Exemple : 00–dd–01–12–34–56
- **Broadcast**
    - Envoyé à toutes les machines du broadcast domain
    - Exemple : ff-ff-ff-ff-ff-ff
- **Multicast**
    - Envoyé à un ensemble de machines du broadcast domain mais pas toutes
    - Exemple : 01-00-5E-00-00-05

Répéteur, Pont et Routeur



Collision Domain = endroit où il peut y avoir une collision entre 2 paquets

Broadcast Domain = l'ensemble du réseau sur lequel un broadcast va être forwardé

Répéteurs

Il existe deux catégories de répéteurs :

- Classe 1
  - Convertissent le signal entrant (analogique) en signal digital, puis retransmettent le signal (analogique) sur les autres portes.

- Classe 2
  - Plus simple
  - Pas de conversion (le signal interne est aussi analogique)

Ponts

Il existe deux types de ponts :

- **Source – route bridge** (disparu avec le TR)
  - Développé par IBM
  - Utilisé en TR
  - La liste des ponts à parcourir est dans la trame
  - Une source peut envoyer une trame spéciale, d'exploration, pour trouver où est le destinataire
  - Connection-oriented

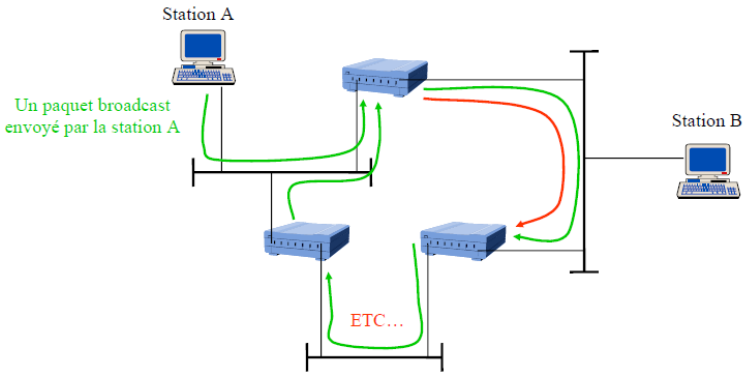
- **Transparent bridge** (tous les ponts actuels)
  - Développé par DEC
  - Utilisé en Ethernet
  - Basé sur des tables
  - Connectionless
  - STP

Transparent Bridging

5 modes de fonctionnement possibles (en fonction de l'adresse MAC source et destination):

1. **Learning** : création de la « Bridging table »
2. **Flooding**: en cas d'adresse inconnue ou de broadcast, envoi sur toutes les portes (à l'inverse des routeurs)
3. **Filtering**: si la source et la destination sont sur la même porte, ne rien faire (jeter le paquet)
4. **Forwarding**: envoi du paquet sur la bonne interface, déterminée par la table
5. **Aging** (après X secondes, suppression de la table)

STP (Spanning Tree Protocol)



Problème :

On risque d'avoir des boucles infinies avec le flooding du transparent bridging.

Solution :

- STP
- 5 états possibles pour une porte :
  - Blocking
  - Listening
  - Learning
  - Forwarding
  - Disabled
- Election d'un root bridge, basé sur la priorité la plus basse ou sur la plus petite MAC

Différence entre Switch et Bridge

Bridge

- Possède une seule porte d'entrée et une seule porte de sortie
- Peut bridger entre plusieurs topologies

Switch

- Possède plusieurs portes
- Peut « bridger »
- Débit plus important
- Les portes ont la **même topologie**

Store and forward vs Cut-through

Store and forward: Le device stocke la trame jusqu'à ce qu'il l'ait entièrement reçu, puis le renvoie.

Cut-through : Le device commence à renvoyer la trame dès qu'il sait qu'elle est l'adresse Mac de destination (après les 6 premiers bytes).

Adaptative cut-through : le device fait du cut-through, puis bascule en mode store and forward si un nombre trop grand d'erreurs est constaté.

Intermédiaire : Fragment Free : On attend les 64 premiers bytes (le header) et on vérifie sur ceux-là seulement. C'est donc un intermédiaire entre SF et CT qui évite les collisions.

	Store and forward	Cut through
Avantage	On est sûr de ne pas propager d'erreurs	Plus rapide
Désavantage	Plus lent, nécessite plus de buffers	On risque d'envoyer des trames corrompues, et donc de gaspiller de la bande passante

Niveau 3 – la couche Réseau

Adresse IPv4

4 chiffres compris entre 0 et 255, séparés par des points.

Normalement, une adresse par interface physique ou logique.

ARP (Address Resolution Protocol)

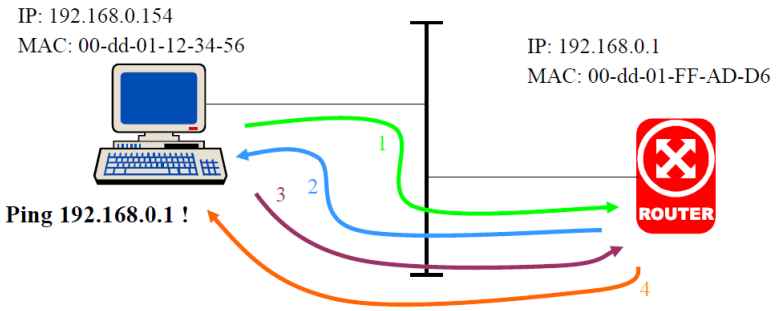
- Utilisé pour établir le lien (unique et univoque) entre une adresse de niveau 2 (**MAC**) et une adresse de niveau 3, **connaissant l'adresse de niveau 3**
- Le client envoie un « **ARP request** », **broadcast**, à tout le monde
- La machine concernée répond par un « **ARP Reply** ».
    - C'est un **unicast**, destiné uniquement à la machine qui a envoyé l'ARP request

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32

Hardware Type		Protocol type
Hardware address length	Protocol address length	Opcode
Source Hardware Address		
Source Protocol Address		
Destination Hardware Address		
Destination Protocol Address		

Fonctionnement

1. ARP Request (Broadcast)
2. ARP Reply (Unicast)
3. ICMP ECHO Request
4. ICMP ECHO Reply



Proxy ARP

- ⇨ Par défaut, les routeurs ne laissent pas passer les broadcasts
  - ⇨ Du proxy ARP peut être nécessaire si un broadcast domain est interrompu par un routeur
    - C'est dû à un mauvais design réseaux (un switch aurait dû être mis au lieu d'un routeur)

RARP (Reverse Address Resolution Protocol)

- ⇨ Utilisé pour établir un lien (unique et univoque) entre une adresse de niveau 2 (**MAC**) et une adresse de niveau 3, **connaissant l'adresse de niveau 2**
- ⇨ Peut être utilisé pour obtenir une adresse IP automatiquement (comme BOOTP ou DHCP), mais UNIQUEMENT l'**adresse IP.**
  - ⇨ Donc uniquement sur un LAN

Les paquets IP

IP est « **Best Effort** », il fait donc du mieux qu'il peut sans rien garantir

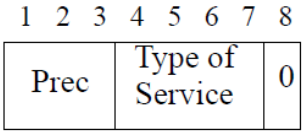
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32

Version	IHL	Type of Service	Total length
Identification		Flags	Fragment Offset
Time To Live	Protocol ID	Header Checksum	
Source Address			
Destination Address			
Options et données			

Default Gateway

- Quand une machine veut envoyer un paquet, elle doit comparer l'adresse destination avec sa propre adresse grâce au subnet mask (ET logique)
  - Si les deux machines sont sur le même réseau, on envoie directement (ARP)
  - Sinon, on s'adresse au default gateway (ARP aussi)

Le champ ToS (Type of Service)



- Défini dans la RFC 1349
- 3 premiers bits (precedence)
  - Définit le PHB, utilisé pour la gestion des queues
    - 111: network control (protocoles de routage)
    - 110: Internetwork control
    - 101: Critic / ECP
    - 100: Flash override
    - 011: Flash
    - 010: Immediat
    - 001: Priorité
    - 000: Routine (BE)
- 4 bits de ToS
  - Rarement implémenté car complexe
  - Beaucoup de CPU
    - 1000: D : Minimiser le délai
    - 0100: T : Maximiser le débit
    - 0010: R : Maximiser la fiabilité
    - 0001: C : Minimiser le coût financier
    - 0000: Service normal
    - 1111: Maximiser la sécurité

Le champ FLAG

Composé de 3 bits :

- 0 : Pas utilisé
- 1 :
  - 0 = may fragement
  - 1 = don't fragment
- 2 :
  - 0 = last fragment
  - 1 = other fragment coming

ICMP (Internet Control Message Protocol)

- Utilisé par les applications ping, traceroute et autres.
- RFC 792
- Tourne sur **IP** : **Protocol ID** numéro **1**

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32		
Type	Code	ICMP Header Checksum
ICMP DATA		

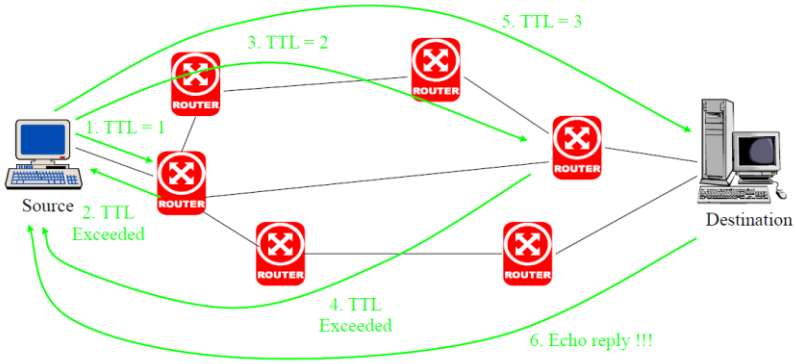
- Le type détermine le type de paquet
- Le code est déterminé par le type

Les types ICMP

- 0: Echo reply
- 3: Destination unreachable
- 4: Source quench
- 5: Redirect
- 8: Echo request
- 9: Router advertisement
- 10: Router solicitation
- 11: TTL exceeded
- 12: Parameter problem
- 13: Timestamp request
- 14: Timestamp reply
- 15: Information request
- 16: Information reply
- 17: Address mask request
- 18: Address mask reply
- 30: Traceroute
- 31: Conversion error
- 32: Mobile host redirect
- 33: IPv6 Where-are-you
- 34: IPv6 I-am-here
- 35: Mobile registration request
- 36: Mobile registration reply
- 37: Domain name request
- 38: Domain name reply
- 39: SKIP protocol
- 40: Security failures

Traceroute

Traceroute est une application basée sur ICMP.



⇨ On envoie des paquets vers la même destination avec des TTL (Time To Live) de plus en plus grand, en partant de 1

⇨ Permet de connaître **un** chemin vers une machine et donc d'avoir une **idée** du réseau.

⇨ Souvent limité à 32 hops, diamètre maximum de l'Internet de nos jours

Niveau 4 – La couche Transport

- Format :
    - Adresse : numéro de port (16 bits)

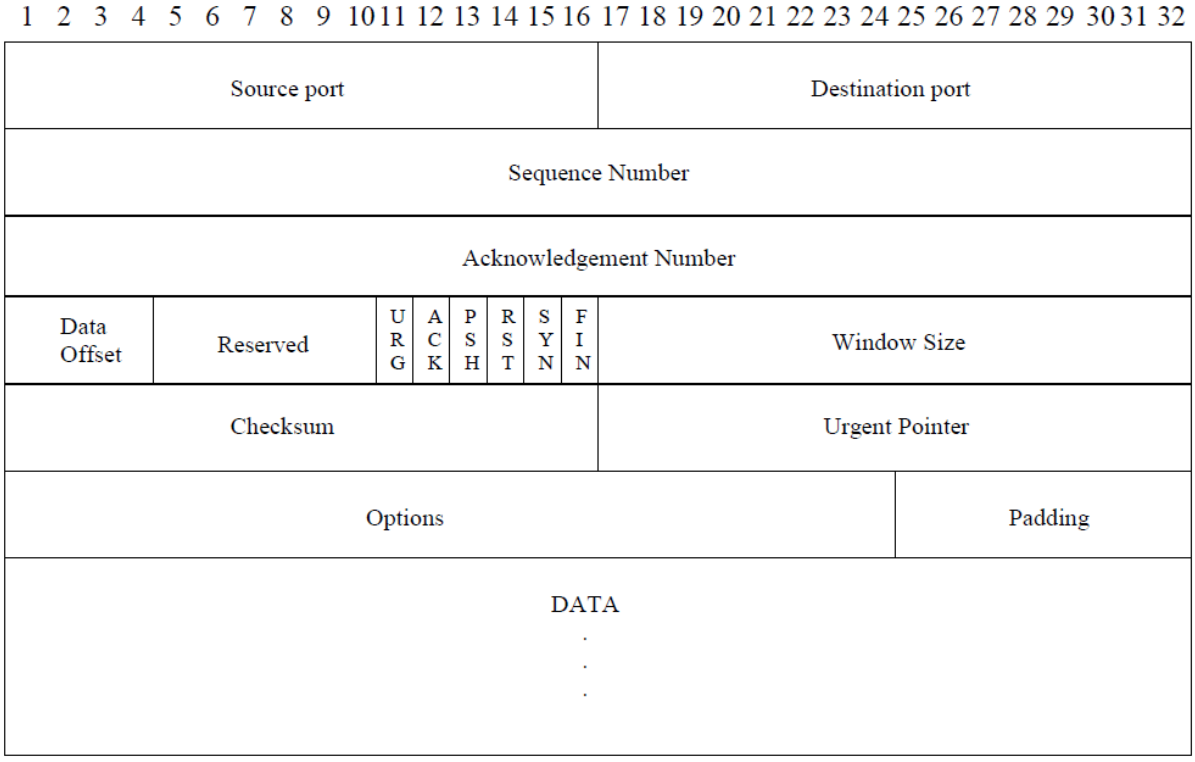
Ports

En théorie :

- Réservés : 0 – 1023 (IANA)
- Disponibles : 1024 – 65535

TCP (Transmission Control Protocol)

- RFC 793
- Basé sur la notion de **flux**, pas comme des paquets
- Fiable
- Orienté connexion
- Full duplex
- Basé sur des numéros de séquence



Session

- Etablissement d'une session de bout en bout
- Basé sur les « sliding windows »
- Offre un transfert d'information fiable en:
    - Renvoyant, si besoin est, des paquets perdus ou arrivant hors délais
    - Reséquençant les paquets, s'ils arrivent dans un ordre différent de celui dans lequel ils ont été envoyés
        - ➢ Le protocole est donc complexe

Sequence number & Acknowledgement number

Ce sont des nombres de 32 bits, indépendants l'un de l'autre, déterminant :

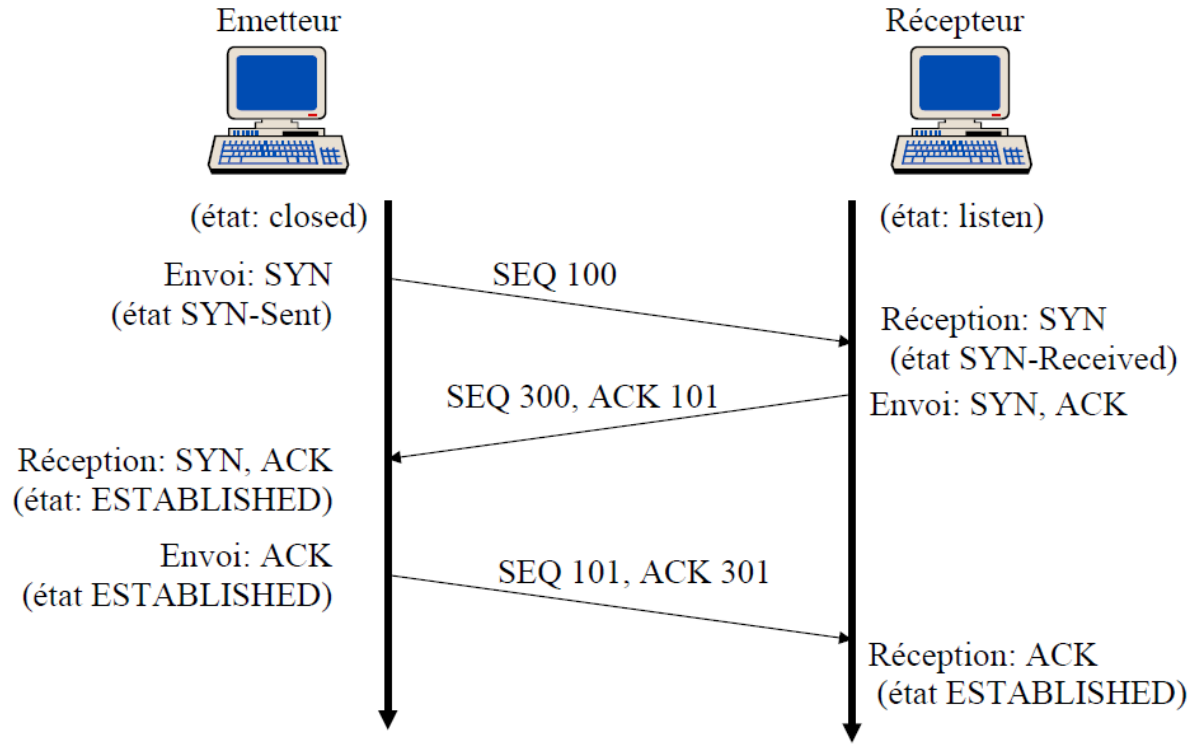
- Le numéro du premier byte du paquet envoyé (sequence number)
- Le numéro du dernier byte reçu (ack number)

Le champ **Windowd Size** indique le nombre de bytes disponibles pour recevoir des informations.

Ces informations sont utilisées pour l'implémentation des sliding windows

Three Way Handshake

Voir synthèse IPP pour plus d'info



Sliding windows

Voir synthèse IPP pour plus d'info

Afin d'éviter de noyer une machine plus lente avec des informations qu'elle n'arrive pas à traiter assez vite, on utilise un buffer pour transmettre plusieurs trames l'une à la suite de l'autre.

On a un problème si la trame est plus grande que le buffer.

On peut stocker plusieurs trames les unes derrière les autres si ces trames sont plus petites que le buffer.

Idéalement, l'application lit les données à la vitesse à laquelle elles arrivent.

Principaux protocoles TCP

- 20 – FTP (data)
- 21 – FTP (control)
- 22 – SSH
- 23 – Telnet
- 25 – SMTP
- 80 – HTTP
- 110 – POP3
- 143 – IMAP4
- 179 – BGP
- 646 – LDP

UDP (User Datagram Protocol)

- RFC 768
- Connexionless
- Non fiable
- Simple
- Offre que le checksum et le multiplexage par port

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32

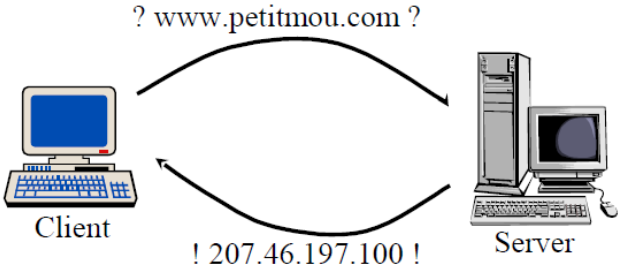
Source port	Destination port
Length	Checksum
DATA . . .	

Principaux protocoles UDP

- 53 – DNS
- 67 – Serveur DHCP
- 68 – Client DHCP
- 69 – TFTP
- 123 – NTP
- 161 – SNMP
- 520 – RIP
- 521 – RIPng
- 5060 – SIP
- Port négocié en SDP (partie de SIP) – RTP

DNS (Domain Name System (or Service))

- Couche 3,4 et 7
- Permet de faire le **mapping** entre une adresse symbolique et une adresse IP
- UDP (ou TCP) **Port 53**
- Notion de **FQDN** (Fully Qualified Domain Name)



- C'est une sorte de DB distribuée sur internet
    - La DB est hiérarchique car on sépare les niveaux par des points
- Quand une appli doit transformer un nom en adresse IP, elle devient un client du DNS
- On utilise une adresse symbolique car c'est plus simple à retenir

Notion d'autorité

- Chaque partie du DNS (client, DNS intermédiaire) fait partie d'un arbre et contrôle une partie de cet arbre.
- Un serveur DNS a autorité sur le sous-arbre qu'il contrôle
- Quand un serveur reçoit une demande pour un nom de domaine sur lequel il n'a pas autorité, il envoie la requête au niveau supérieur

Top-level domains (TLD)

- Générique
    - com
    - edu
    - gov
    - mil
    - net
    - org
    - …
- Par pays
    - Dans certains pays, il est impossible d'avoir un nom « .pays »
        - On passe donc par un sous-domaine (.co.uk)

Internationalized Domain Name (IDN)

- On peut utiliser les caractères **non-ascii** (éè…)
- On peut utiliser d'autres **alphabets** (cyrillique, arabre, …)
- On utilise donc **ToAscii** et **ToUnicode**
- Conversion en **PunnyCodes**
    - On utilise le prepend « xn--» (bücher.ch → xn--bcher-kva.ch)

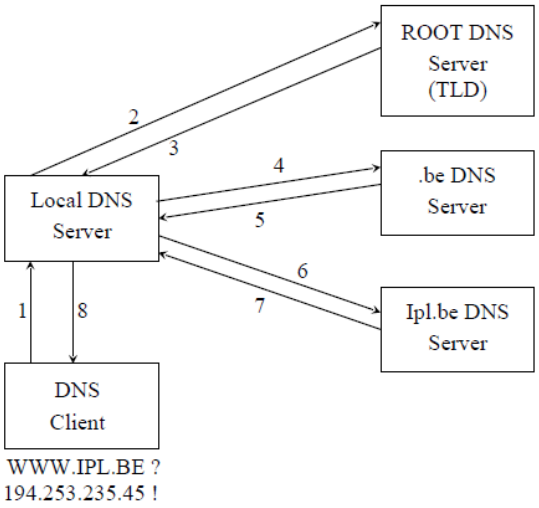
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32

Identification	Flags
Number of questions	Number of answers
Number of Authority RRs	Number of additional RRs
Question(s)	
Answer(s)	

Fonctionnement

- Le champ **Identification** permet de faire **corresponde les réponses aux demandes**
- Les **Flags** permettent de décrire l'état de la réponse, de savoir si une récursion est possible, si elle est « autoritaire » ou pas …
- Le **nombre de requêtes**
- Le **nombre de réponse** vaut 0 pour une requête et au moins 1 pour une réponse
- Chaque requête et chaque réponse a un type.
    - Les paquets contiennent un ou plusieurs **Ressource Records** (RR) qui décrivent ce type.

- Le client envoie une requête à son DNS local.
- Le DNS local n'a pas autorité pour ce nom, il envoie la requête à un 'root (top-level)' DNS
- Le root DNS renvoie l'adresse du sous-domaine au DNS local.
- Le DNS local renvoie la requête au DNS reçu etc…



Les types du DNS

- **A** : Adress record
    - Nom -> IPv4
- **AAAA** : Adress record
    - Nom -> IPv6
- **CNAME** : Canonical name
    - Alias
- **MX** : Mail Exchange
    - Mail servers
- **PTR** : Pointer
    - IPv4 -> nom (alias « reverse », puis inverse de A)
- **NS** : Name Server
    - Server DNS du domaine
- **SRV** : Serveur SIP
- …

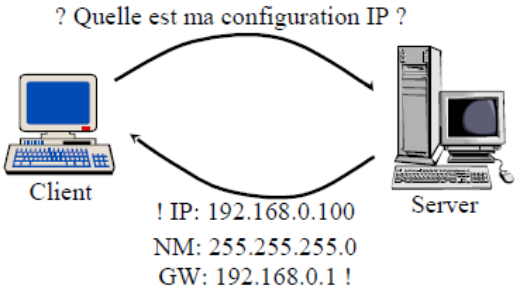
TTL (Time To Live)

- Les records DNS ont un TTL, afin de pouvoir contrôler la durée de la validité d'un record
- Plus long => moins de requêtes
- Plus court => plus de requêtes, mais plus de contrôle

De nouveaux types de RR ont été définis pour pouvoir renvoyer des adresses IPv6.

DHCP (Dynamic Host Configuration Protocol)

- Couche 3, 4 et 7
- RFC 2131
- **Port UDP 67** (Serveur)
- **Port UDP 68** (Client)
- Basé sur **BOOTP**



But : Permettre au client d'obtenir automatiquement sa configuration au niveau IP, en la demandant à un serveur.

- Les requêtes DHCP sont des paquets boradcast et les réponses peuvent l'être aussi
- **Lease** : les paramètres sont alloués pour une durée déterminée
- DHCP offre aussi une possibilité de récupération et de réallocation dynamique d'adresse grâce à un mécanisme de leasing.
- Les requêtes broadcast peuvent passer les routeurs avec l'option « **DHCP Helper** », « **BOOTP helper** » ou encore « **UDP helper** »
    - Sinon, le serveur doit être dans le même broadcast domain que le client

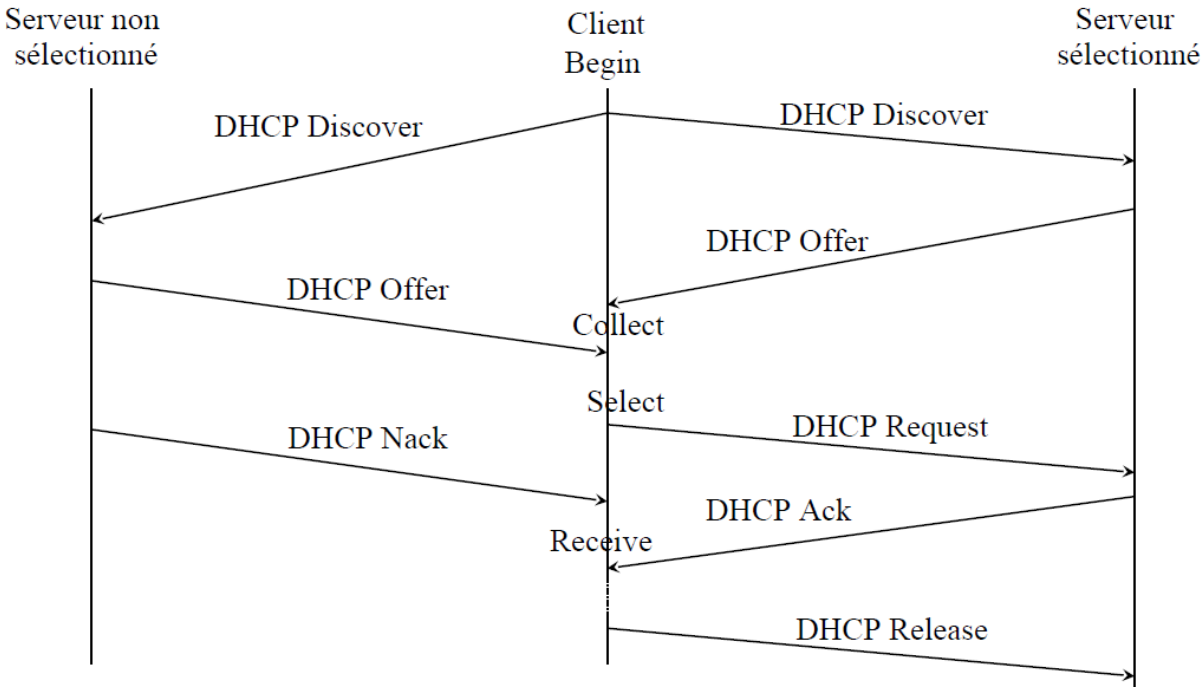
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32

Opcode	HW Type	HW Address Length	Hop Count
Transaction ID			
Number of seconds		Flags	
Client IP Address			
Your IP Address			
Server IP Address			
Gateway IP Address			
Client HW Address (16 Bytes)			
Server Hostname (64 Bytes)			
Boot Filename (128 Bytes)			
OPTIONS (> 4 Bytes) En particulier: DHCP Message Type			

Les champs

- **Opcode :** 1 = Bootrequest, 2= Bootreply
- **Filename :** 128 Bytes -> Limitation !
- **Client IP address :** utilisé lors du lease (pas pour l'acquisition de l'adresse)
- **Your IP address :** l'adresse assignée au client par le serveur
- **Server IP adress :** adresse du serveur assignant l'adresse

Fonctionnement



- **DHCPDISCOVER :** le client cherche les serveurs
- **DHCPOFFER :** Les serveurs répondent au client
- **DHCPREQUEST :** Réponse du client au serveur ou extension du lease
- **DHCPRELEASE :** Le client annonce au serveur qu'il n'a plus besoin de l'adresse
- **DHCPINFORM :** Le client informe le serveur qu'il a déjà une adresse
- **DHCPPACK :** Le serveur confirme l'allocation de l'adresse au client
- **DHCPNACK :** Le serveur indique au client que son adresse est incorrecte ou que son lease est expiré
- **DHCPDECLINE :** Le client annonce au serveur que l'adresse reçue est déjà utilisée

Routage

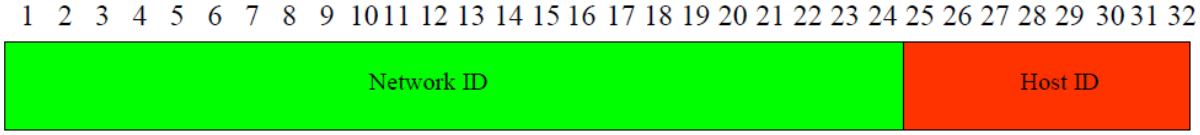
La table de routage

Prefix	Next hop	Age	Interface
192.168.5.0/24	10.5.5.5	13:57:16	Serial1/0
192.168.6.0/24	10.3.5.5	12:58:15	Ethernet0
…			
0.0.0.0/0	10.15.5.5	150:12:12	FastEthernet3

La modification du paquet

- La partie IP est modifiée (TTL décrémenté, checksum, ToS, fragment bit (IPv4 seulement))
- La partie MAC est **remplacée**
- La partie physique est parfois différente

L'adresse IP



Network ID: identifie le réseau	192.168.0.0
Host ID: identifie une machine sur un réseau	192.168.0.1
Subnet mask: délimite les deux parties	255.255.255.0
Broadcast vers toutes les machines de tous les réseaux.	255.255.255.255
Broadcast vers toutes les machines de notre réseau	192.168.0.255

- Le host ID « full 0 » est réservé pour représenter le numéro de réseau
  - 192.168.3.**0**/24
- Le host ID « full 1 » est réservé pour représenter toutes les adresses (broadcast) du réseau
  - 192.168.3.**255**

➢ Il y a donc toujours (2^n)-2 adresses disponibles, n étant le nombre de bits utilisés pour représenter le host ID

Les classes de réseaux

Type	L'adresse débute (en bits) par…	Le plus petit réseau	Le plus grand réseau	Nombre de réseaux	Nombre d'hôtes
A	0	0.0.0.0	127.255.255.255	2^7 = 128	2^24 = 16777216
B	10	128.0.0.0	191.255.255.255	2^14 = 16384	2^16 = 65536
C	110	192.0.0.0	223.255.255.255	2^21 = 2097152	2^8 = 256
D	1110	224.0.0.0	239.255.255.255	2^28 = 268435456	NA
E	1111	240.0.0.0	255.255.255.255	RESERVE	NA

Réseaux privés

Il existe au moins un réseau privé par classe:

- 10.0.0.0 – 10.255.255.255: 10.0.0.0/8
  - 1 Classe A
- 172.16.0.0 – 172.31.255.255: 172.16.0.0/16
  - 16 Classes B
- 192.168.0.0 – 192.168.255.255: 192.168.0.0 /16
  - 256 Classes C
- Et d'autres ! RFC 3330.

Réseaux réservés

0.0.0.0/8	128.0.0.0/16	192.88.99.0/24
10.0.0.0/8	169.254.0.0/12	192.168.0.0/16
14.0.0.0/8	172.16.0.0/16	198.18.0.0/15
24.0.0.0/8	191.255.0.0/16	223.255.255.0/24
39.0.0.0/8	192.0.0.0/24	224.0.0.0/4 (Multicast)
127.0.0.0/8	192.0.2.0/24	240.0.0.0/4 (class E)

Améliorations des classes

- **CIDR**
  - Classless InterDomain Routing
  - 1992
  - Les classes ne sont plus utilisées aujourd'hui
  - **Réseau Classless**
  - Le subnet mask n'est donc plus dérivé de l'adresse mais **doit** être transmis

- **VLSM**
  - Variable Length Subnet Mask
  - Permet d'assigner des adresses IP en fonction des besoins de chaque réseau, plutôt que d'utiliser des subnets de longueur identique
  - Les adresses (et les subnets) sont donc utilisées de manière plus efficace
- **LPM**
  - Longest Prefix Match
  - Notion très importante, permettant de choisir la meilleure entrée parmi plusieurs
  - On commence toujours par les subnets masks les plus longs, donc les adresses les plus précises
- **AS**
  - Autonomous System
- (Fragmentation)

Le default gateway

Algorithme pour envoyer un paquet

1. Quelle est mon adresse IP ?
2. Quel est mon subnet mask ?
3. Je fais un 'AND' entre les deux, j'obtiens A.B.C.D
4. Quelle est l'adresse IP de destination ?
5. Je fais un 'AND' entre l'adresse de destination et mon subnet mask, j'obtiens E.F.G.H
6. Si A.B.C.D = E.F.G.H, les deux machines sont dans le même réseau, je peux contacter mon correspondant directement (ARP vers IP destination).
7. Si A.B.C.D <> E.F.G.H, les deux machines sont dans des réseaux différents, je dois envoyer le paquet à mon default gateway (ARP vers GW).

Distance Vector vs Link State

- **Distance Vector**
  - Calcule la longueur d'un chemin (en termes de sauts)
  - Simpliste
  - Convergence lente
  - Diamètre
  - Ne tient pas compte de la bande passante, fiabilité, …

- **Link State**
  - Calcule la longueur d'un chemin (en termes de distance)
  - Complexe
  - Convergence rapide
  - Pas de diamètre
  - QoS possible

IGP - Interior Gateway Protocol

RIP – Routing Information Protocol

RIPv1

- RFC 1058
- IGP – Distance Vector
- Métrique utilisée : nombre de sauts (« **hops** »)
- Count to infinity
- Split horizon, poisoned revers
- UDP port 520

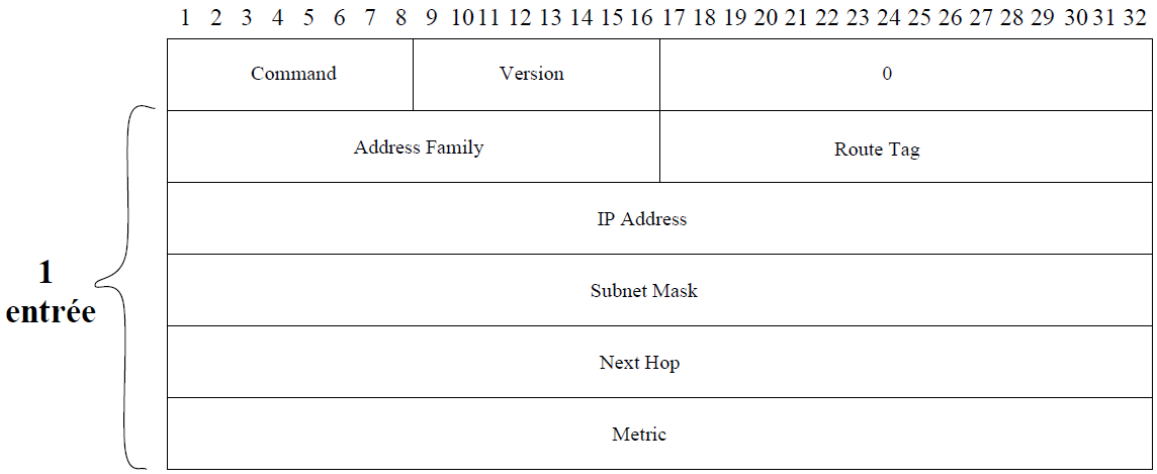
Fonctionnement

- Sont transmis: (destination, hop count)
- Broadcast de la table de routage toutes les 30 secondes (par défaut) (CPU, broadcast, band passante), soit un ensemble de paires
- Si une route n'est pas rafraîchie pendant plus de 6 updates (180 secondes par défaut), elle est éliminée de la table de routage
- Le Subnet Mask (SM) n'est pas transmis --> orienté classe

- Limite de 15 sauts
    - Diamètre de RIP = 16
- Amélirations
    - Split horizon
        - Un routeur n'annonce pas un réseau sur l'interface par laquelle il l'a reçu.
    - Poisoned reverse
        - Un routeur annonce un réseau sur l'interface par laquelle il l'a reçu avec métrique de 16 (infini)

RIPv2

- RFC 2453
- Utilisation d'une adresse **multicast** : 224.0.0.9
- Les updates contiennent:
    - Le préfixe
    - Le SM (possibilité de CIDR)
    - Le next hop
    - Le hop count
- Ajouts :
    - Authentification MD5
    - Route tag



Le champ Command

1. Request (partie ou toute la RT)
2. Response
3. Trace On (obsolète)
4. Trace Off (obsolète)
5. SUN reserved
6. Triggered request
7. Triggered response
8. Triggered acknowledgment
9. Update request
10. Update response update acknowledgement

OSPF – Open Shortest Path First

- RFC 2328
- IGP – Link state
- IP protocol ID 89
- Deux addresses multicast
    - Tous les DR (224.0.0.6)
    - Tous les SPF (224.0.0.5)

Améliorations par rapport à RIP

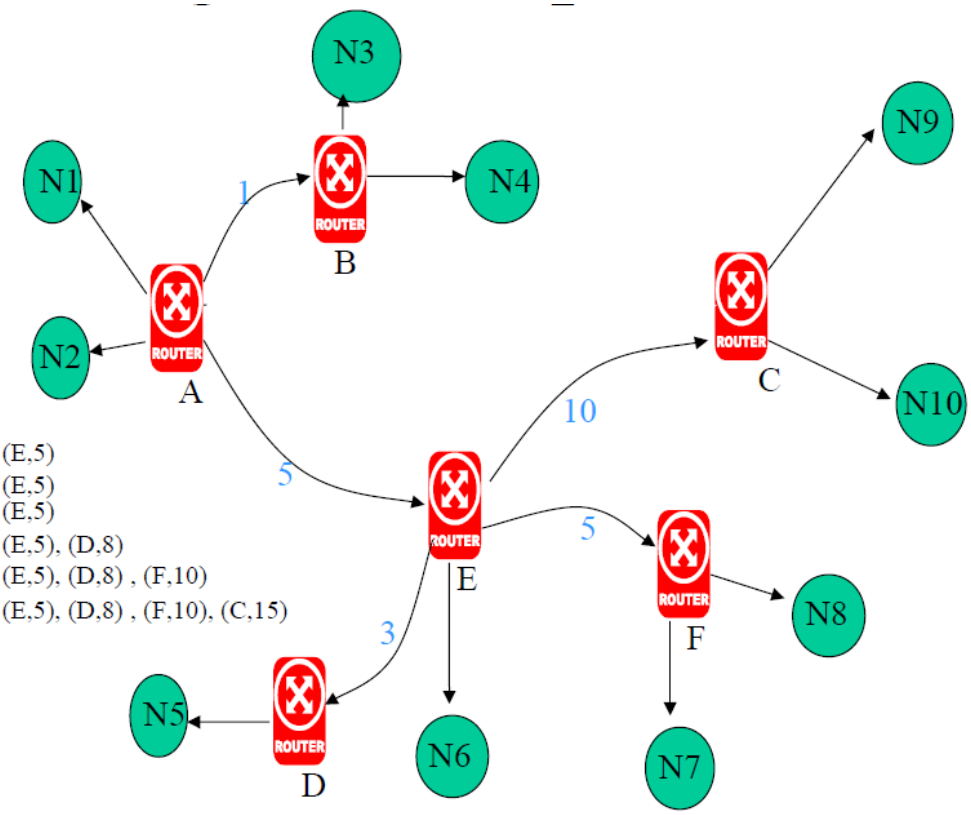
- Converge plus vite
- Utilise moins de bande passante
- Areas
- Métriques (16 bits)
- Supporte Classless
- Supporte plusieurs chemins de même poids
- Extensions TE

Algorithme

1. Démarrer avec soi-même comme root
2. Ajouter tous les voisins (s'ils existent) dans la liste des candidats (s'ils ne sont pas encore dans la liste SPF), en recalculant la distance entre le root et les nouveaux candidats
3. Eliminer les chemins redondants les plus longs (s'il y en a)
4. Sélectionner un des noeuds les plus proches
5. Ajouter ce noeud au SPF (!)
6. Aller à l'étape 2 tant que la liste des candidats n'est pas vide

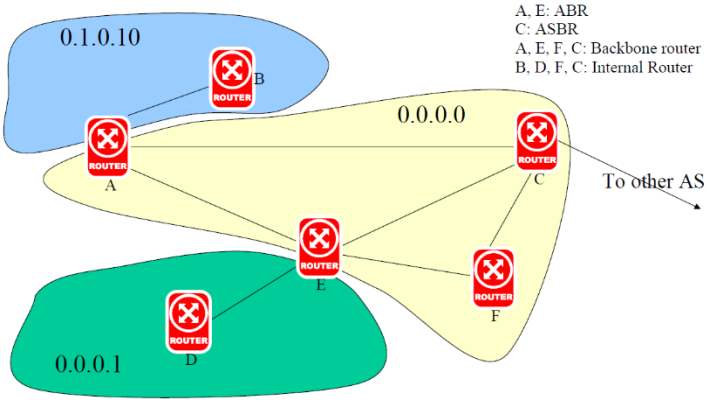
Router A

Candidate list	SPF
1 - (B,1), (C,100), (E,5)	
2 - (C,100), (E,5)	(B,1)
3 - (C,100)	(B,1), (E,5)
4 - (C,100), (D,8), (F,10), (C,15)	(B,1), (E,5)
5 - (D,8), (F,10), (C,15)	(B,1), (E,5)
6 - (F,10), (C,15)	(B,1), (E,5), (D,8)
7 - (C,15)	(B,1), (E,5), (D,8) , (F,10)
8 -	(B,1), (E,5), (D,8) , (F,10), (C,15)



Les Areas

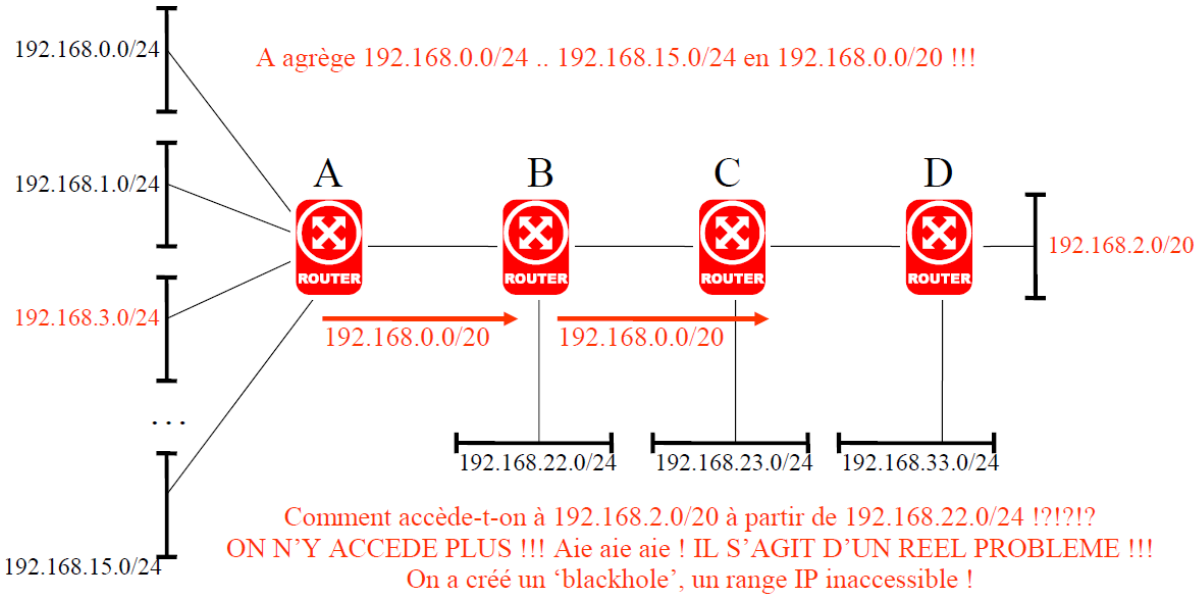
- Flexibilité
- Area ID sur 4 bytes (Pas d'adresse IP)
- Backbone area (ID : 0.0.0.0 ou 0)
- Toutes les areas doivent être connectées à la backbone area
- Virtual link
- Topologie en étoile
- Différents types de routeurs
  - Backbone router
  - Internal router
  - Area Border Router (ABR)
  - AS Boundary Router (ASBR)
- Tous les routeurs n'ont pas la même vue topologique du réseau



(Routing slide 44)

Agrégation

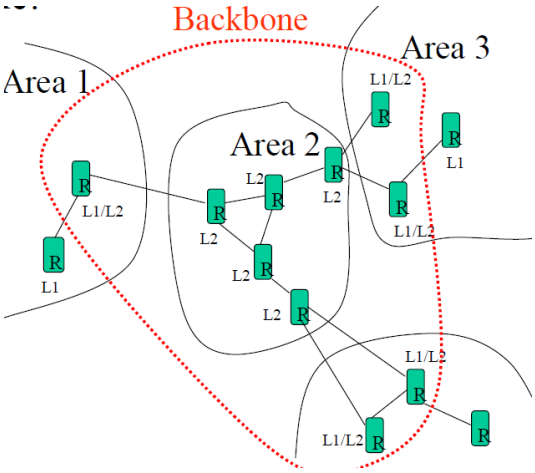
Un design intelligent du réseau peut permettre de diminuer la taille des tables de routages.



Poids

- Sauf configuration contraire, le poids par défaut d'un lien OSPF est lié à la bande passante de l'interface
    - Poids = 10^8 / Bande passante (en bps)
- C'est toujours un entier (codé sur 16 bits)
- La plus petite valeur est 1

ISIS – Intermediate System to Intermediate System



- OSI – Non IP d'origine
- IGP – Link State
- Niveau 1 et 2
- Agrégation d'adresses
- DR
- Authentification
- Supporte Classless
- Extensions TE

EGP – Exterior Gateway Protocol

BGP – Border Gateway Protocol

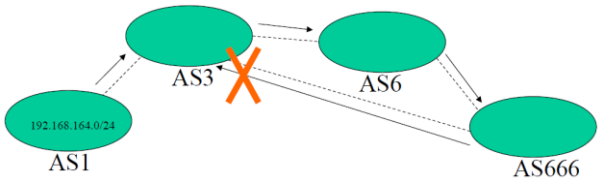
- RFC 1771 et des extensions
- EGP – Distance vector
- iBGP / eBGP
- Peering agreement (config manuelle)
- AS – AS Path – AS Privé (64512 – 65535)
- Supporte Classless

- TCP port 179
- Basé sur des updates formées d'attributs associés à un préfixe

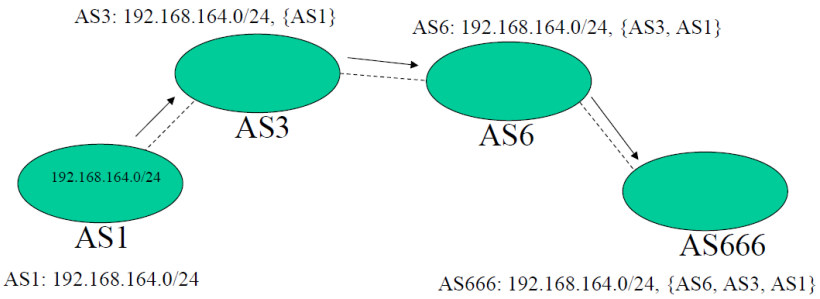
Extensions

- Route reflector
- Confédérations
- Route Flap Dampening
- Attributs
- MPLS – VPN

Fonctionnement de BGP4

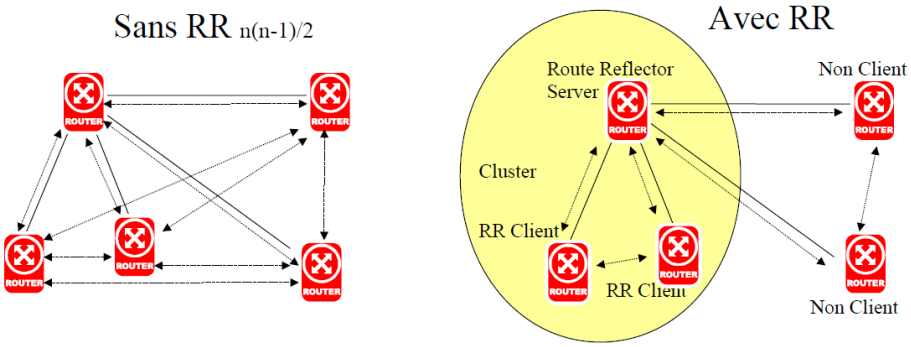
- Le but est de parvenir à créer des chemins les plus courts possibles sans boucle
- Un routeur ajoute son propre numéro d'AS avant d'envoyer une route
- Cela permet de choisir un des chemins s'il en existe plusieurs
- Si le numéro de l'AS est déjà dans le path, on rejette la route (loop avoidance)
  - 

- Un routeur BGP appartient à un AS
- Seuls les changements topologiques sont propagés
- Utilisation de « keepalives » pour vérifier la connection TCP (30 secs)
- Voisin avec Loopback pour éviter les problèmes d'interfaces et augmenter la stabilité.
- Un routeur **iBGP ne propage pas les routes apprises par un voisin iBGP**
- Full iBGP mesh, potentiellement basé sur un IGP
- Voisins eBGP physiquement connectés
- Recommandation : max 4000 voisins BGP



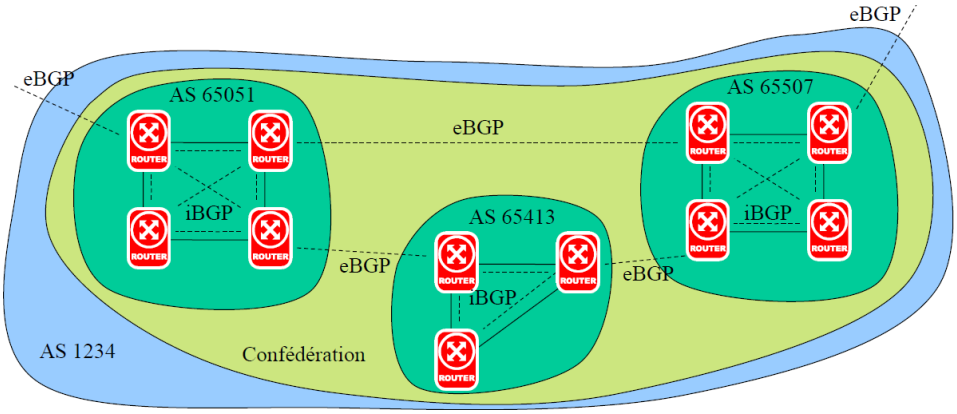
Route reflector

Le but est de minimiser le nombre de peers avec pour limite le fait que les clients du RR ne peuvent pas être voisins de routeurs qui ne sont pas dans le cluster



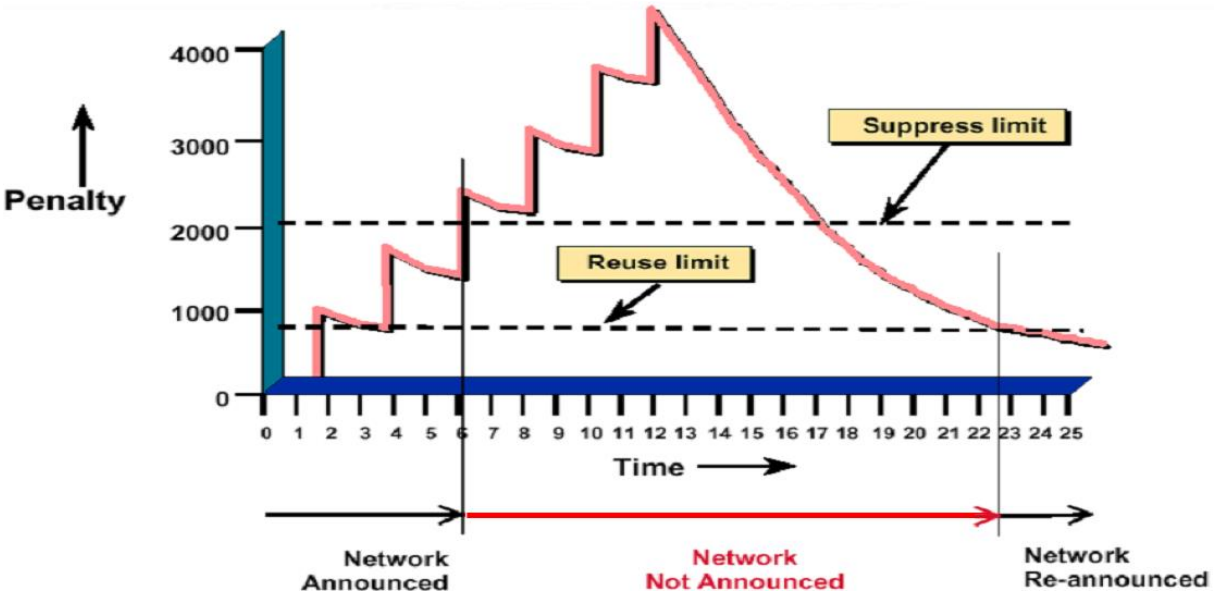
Confédérations

- Un AS est dormé de plusieurs sub-AS
- Transparent pour les autres AS
- Utilisation de numéros d'AS privés



Route Flap Dampening

- Augmenter la stabilité du réseau
- Une route peut être supprimée une fois qu'elle a atteint un certain niveau d'instabilité
- Elle est ré-annoncée une fois qu'elle est redevenue stable



Attributs

1.	Origine	Well known mandatory
2.	AS path	Well known mandatory
3.	Next hop	Well known mandatory
4.	Multi Exit Disc	Optional non transitive
5.	Local pref	Well known discretionary
6.	Atomic aggregate	Well known discretionary
7.	Aggregator	Optional transitive
8.	Community	Optional transitive
9.	Originator ID	Optional non transitive
10.	Cluster list	Optional non transitive

+ Other: Weight (Cisco)…

Well known mandatory: doit être implémenté. Doit exister dans les updates BGP

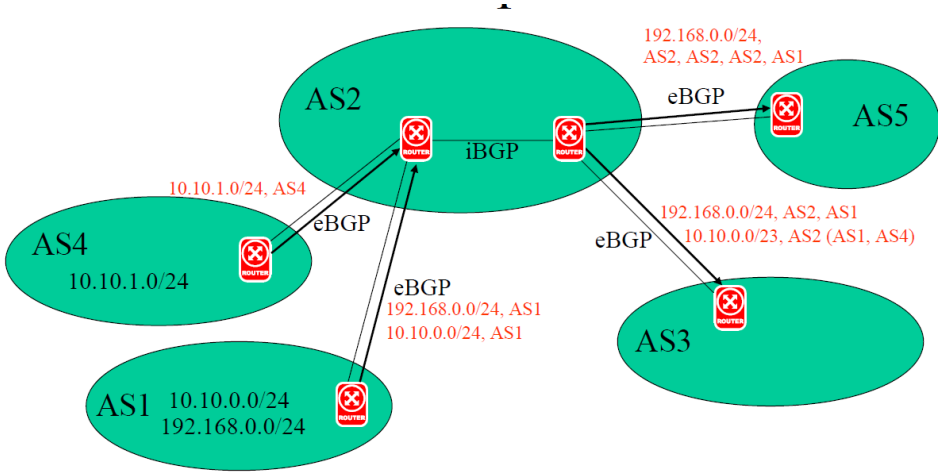
Well known discretionary: doit être implémenté. Peut exister dans les updates BGP

Optional transitive: peut être implémenté. Si oui, doit être transmis dans les updates.

Optional non transitive: peut être implémenté. Doit être ignoré si pas implémenté.

AS Path

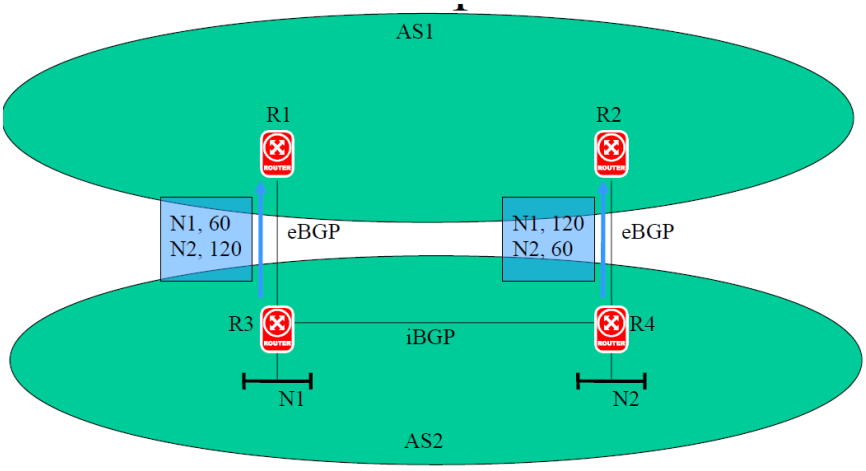
- Well known mandatory
- Séquence de numéros d'AS
- Un eBGP peer ajoute son propre numéro d'AS avant d'envoyer ses informations à ses voisins
- Un path plus court est préféré
- Un autre attribut, AS Set, est utilisé en cas d'aggrégation pour éviter les routings loop !
- Peut être utilisé pour alonger artificiellement un chemin (insertions multiples)



Multiple Exit Discriminator

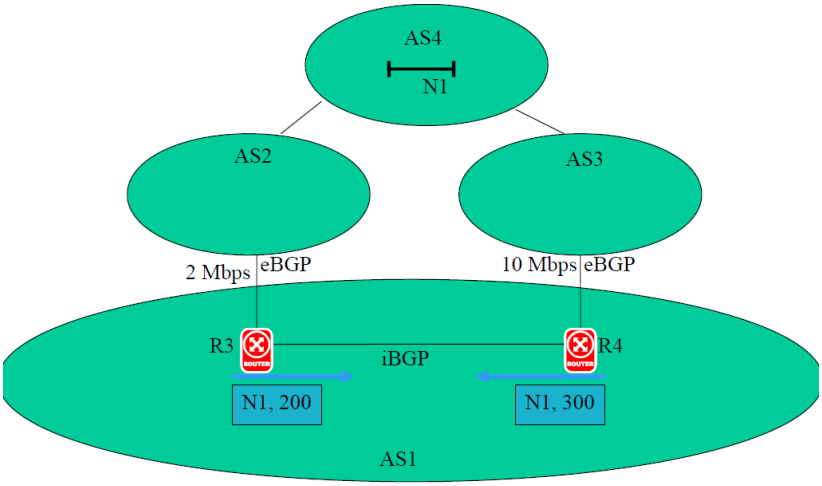
- Optional non transitive
- Utilisé pour tenter de controôler le traffic entrant quand il y a 2 (ou plus) connections au même AS

- Parfois appelé « External metric »
- Possibilité d'injecter le métrique IGP dans le MED pour avoir un comportement symétrique
- Priorité importane => petite métrique



Local Pref

- Well known discretionary
- Utilisé pour contrôler le trafic sortant
- Priorité importante => grande valeur
- Ne sort pas de l'AS



Path selection

1. Si le Next Hop est inaccessible, drop !
2. Choisir la route avec la plus grande Local Pref
3. Si les Local Pref sont identiques, choisir la route générée par le BGP de ce routeur
4. Si la route n'est pas générée par ce routeur, choisir la route avec l'AS Path le plus court
5. Si toutes les routes ont la même longueur d'AS Path, choisir dans l'ordre ceux qui viennent d'abord de l'IGP, puis de l'EGP, puis incomplète pour l'origine
6. Si les origines sont les mêmes, choisir la route avec le MED le moins élevé
7. Si les MED sont identiques, préférer la route externe à la route interne
8. Si les routes sont toujours identiques, préférer le voisin IGP le plus proche
9. Enfin, choisir la route allant vers le router ID BGP le plus petit (l'adresse IP la plus petite)

Route redistribution

On peut, moyennant configuration du routeur, redistribuer les routes d'un protocole dans un autre.

- RIP => BGP
- OSPF => BGP
- RIP => OSPF
- …

Quality of Service (QoS) et Class of Service (CoS)

Flux : Ensemble de paquets définis par :

- Adresse IP destination
- Adresse IP source
- Port TCP/UDP destination
- Port TCP/UDP source
- Protocole de transport (UDP/TCP)

Delais introduit par un device : temps mis par un paquet entre le moment où le premier bit entre dans le device et le moment où le dernier bit sort du device.

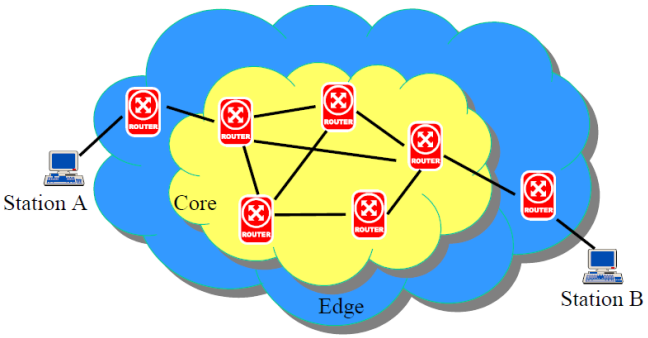
Jitter introduit par un device : différence de temps entre l'intervalle séparant deux paquets avant et après leur passage dans le device.

PHB (Per Hop Behaviour) : Définition du traitement que vont subir les paquets qui transitent par un device. Un PHB peut inclure :

- Policing / Shaping
- (Re)Marking
- Queue Drop criteria
- Queue Scheduling
- Dropping
- (Re)Directing

Edge : endroit où l'utilisateur arrive dans le réseau

Core : endroit du réseau où les utilisateurs n'arrivent pas, leurs paquets ne font qu'y transiter



Quality of Service

- Capacité d'un élément du réseau à assurer un certain niveau de qualité en termes de délai, de débit, de bande passante, …
- Peut être au niveau 2 ou au niveau 3
- Limité par :
  - Le point le moins performant du chemin emprunté par le flux
  - L'état du réseau à ce moment-là
- Deux possibilités, éventuellement combinées

- Réservation de ressources (Intserv, RSVP)
- Priorisation (Diffserv)

- Configuration manuelle
- **Policy management** : COPS (Common Open Policy Service) est un protocole de gestion de police distribuée. Il s'agit de traiter certains paquets différemment en fonction de certaines de leurs caractéristiques, et de centraliser cette gestion sur une machine qui joue le rôle de centre de décision.
- **Authentification :** basé sur des certificats gérés par une autorité centralisée conférant des droits
- **Accounting / Billing :** indispensable pour la facturation

Class of Service

- Le trafic est réparti en classes afin de le traiter en fonction de différentes priorités, décidées par :
  - Le router manager (config manuelle, Diffserv)
  - Le COPS server (COPS)

Conditionnement du flux

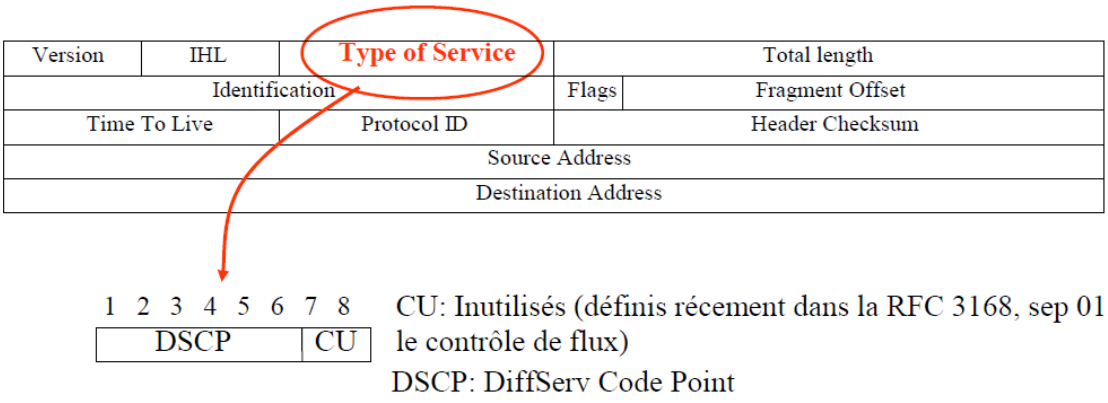
- **Classifier :** décision de la classe à laquelle le trafic appartient et donc un PHB
- **Marker :** marquage des paquets
- **Meter :** mesure, à intervalles réguliers, de la quantité de trafic
- **Conditioner :** mise en forme du trafic

IntServ (Integrated Services)

- Etablir des flux de bout en bout et leur réserver, le long du chemin sélectionné, des ressources (bande passante, priorité, …)
- **Problème :** nombre de flux traversant un routeur peut être très (trop) important
- **Deux types de services :**
  - Contrôlé
  - Garanti

DiffServ (Differentiated Services)

- **Marquage en classes** (fait à l'edge) :
  - Expedited Forwarding (EF)
  - Assured Forwarding (AF)
  - Default behaviour ; best effort (DE)



Selon la RFC 2474 (sep 98), les bits 4, 5 et 6 doivent être à 0, les trois premiers indiquant le 'class selector' (pour correspondre à la RFC 1349, voir le champ ToS).

Les classe DiffServ

- Pour la classe **AF**, il y a **4 classes** prédéfinies, chacune ayant 3 niveaux de « drop precedence »

Précédence	Class 1	Class 2	Class 3	Class 4
Low drop	001 010	010 010	011 010	100 010
Medium drop	001 100	010 100	011 100	100 100
High drop	001 110	010 110	011 110	100 110

- La classe **EF** garantit une latence faible, un jitter faible, une bande passante et des pertes faibles. Elle apparaît comme une ligne louée et utilise le DSCP « 101 100 ». C'est le service premium, le plus cher.

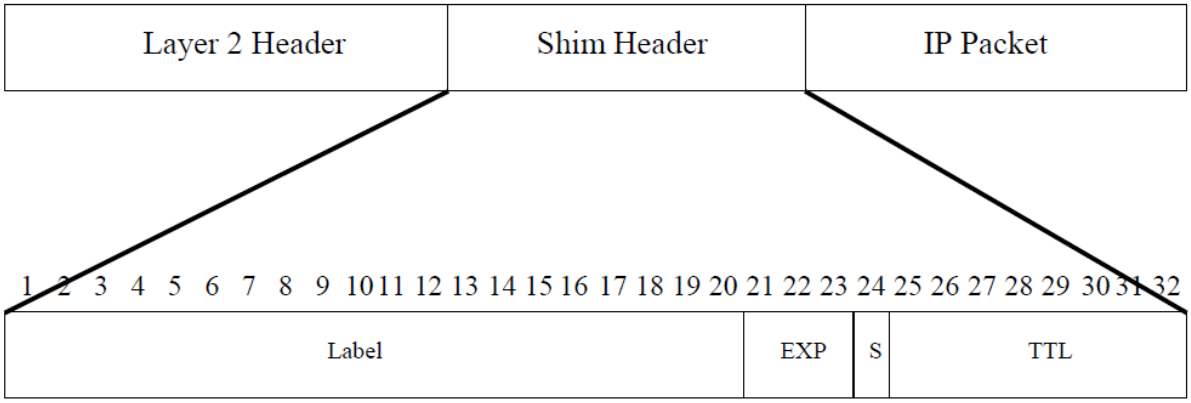
RSVP (Resource reSerVation Protocol)

- Protocol à état (nécessite un keepalive régulier)
- Peut définir une QoS
- Sert à réserver des ressources au sein du réseau
- Reprend l'idée de IntServ

MPLS (Multi Protocol Label Switching)

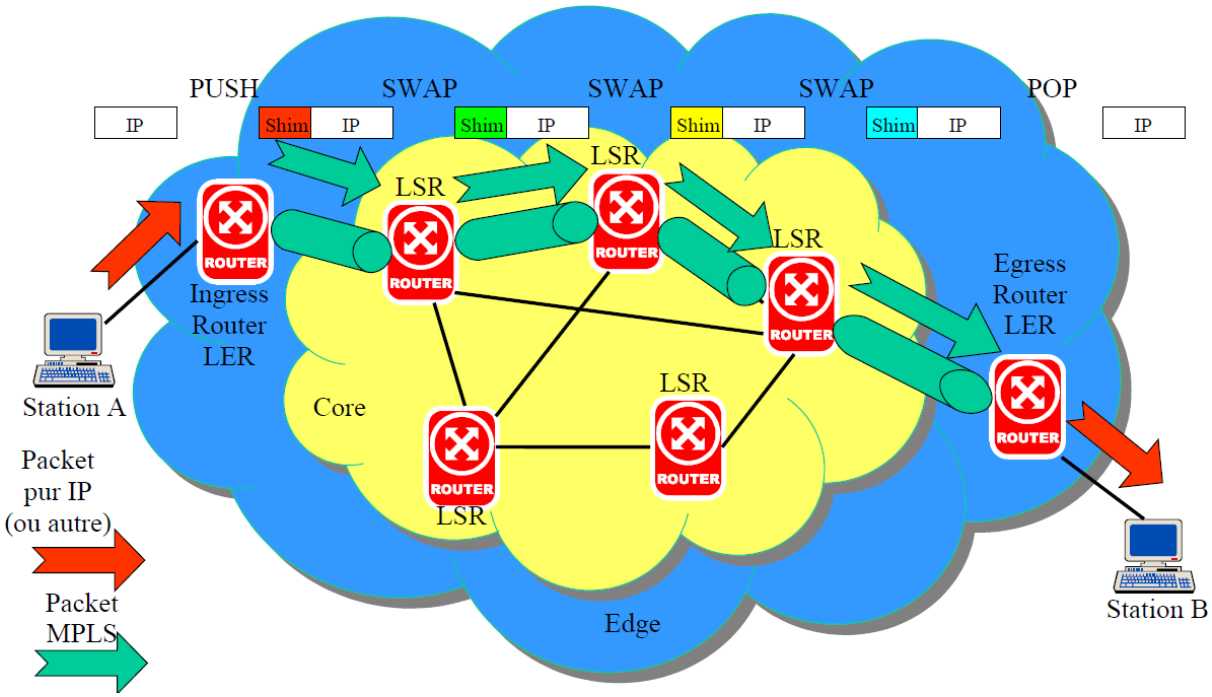
- Switcher plutôt que router (vitesse)
- Shim header, MPLS label de 20 bits
- Création de LSP (donc il y a un état dans le réseau, pas comme en IP) Création – utilisation – fin d'utilisation
- LSR (Label Switch Router) vs LER (Label Edge Router)
- Pas lié à IP (MultiProtocol)
- Possibilités de TE
- Marquage à l'Ingerss et démarquage à l'Egress par paquet

Shim header



- **Label :** 20 bits : identifiant pour le switching
- **EXP :** 3 bits : experimental bits, utilisé pour QoS
- **S :** 1 bit : Stack (MPLS dans MPLS, ou VPN)
- **TTL :** 8 bits : Time to Live

- Trois opérations possibles:
  - PUSH: ajoute un label
  - SWAP: échange un label
  - POP: retire un label
- LSP établis soit manuellement soit par signaling
- LSP unidirectionnels !
- LSP peut être vu comme un tunnel
- LSP peut être point à point ou faire du 'merging' (gain de labels)



LDP (Label Distribution Protocol)

- Label Distribution Protocol (générique ou protocole particulier) (RFC 3036)
- Sert à distribuer automatiquement les labels dans le réseau (et donc créer des LSP)
- Permet de simplifier considérablement la configuration
- Permet de faire du Merging de LSP
- Pas de spécifications de bande passante ou d'autres paramètres de trafic
- Utile dans le cas de:
    - Réduction de la taille des tables de routage
    - VPN tunnels !
- TCP port 646

Fonctionnement

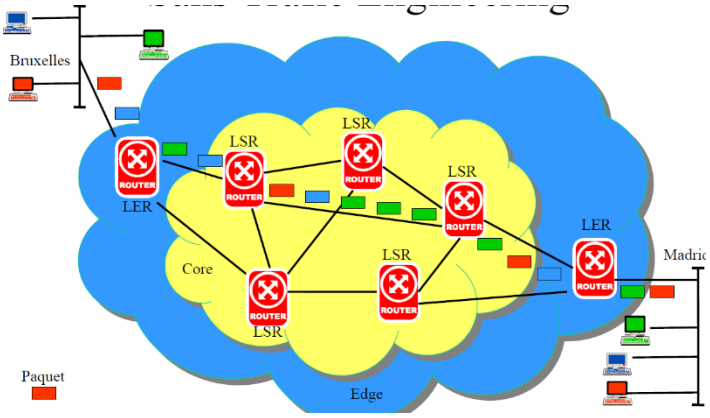
- Le mode de distribution des labels:
    - Downstream on demand
    - Downstream unsolicited
- Le mode de gestion des labels:
    - Libéral (permet de conserver des informations dont on n'a pas directement besoin, mais plus rapide en cas de ré-établissement de LSP)
    - Conservatif (plus économe en mémoire et en processing, mais nécessite plus de temps en cas de problème sur le LSP)
- Le mode de contrôle:
    - Ordonné
    - Indépendant

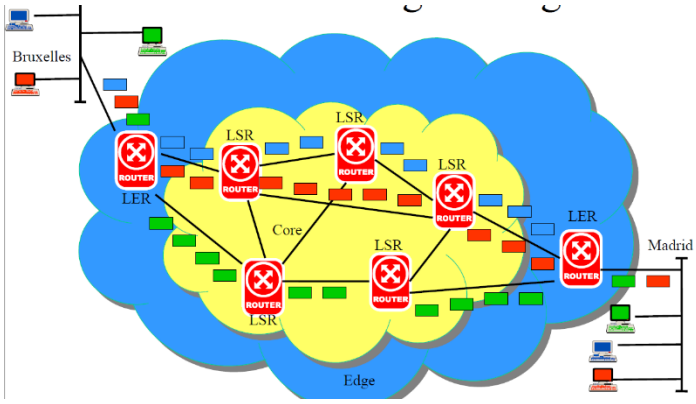
FEC (Forwarding Equivalent Class)

Une FEC est un ensemble de paquets qui seront forwardés de la même manière par le routeur. Cela peut être vu comme l'ensemble des paquets ayant la même adresse de destination (point de vue routage). C'est l'adresse du routeur où le LSP s'arrête.

Traffic Engineering

- Extensions des IGP (OSPF, IS-IS) et de l'EGP (BGP) pour supporter des fonctionnalités de TE
- But: mieux contrôler le trafic (moins se baser sur les protocoles de routage classiques)
- CR – LDP : Constraint-based Routing – LDP
- RSVP – TE : RSVP – Traffic Engineering





VPN (Virtual Private Network)

- Offre une sécurité et une privacité, bien que basé sur des réseaux publics ! C'est le concept même des VLANs !
    - Le VLAN est le principe de séparer un réseau physique en plusieurs réseaux virtuels
        - Rajout d'une série d'information dans la trame
- Mode et finance (amorti en 2 mois…)
- Protocoles de tunneling peuvent être impliqués (PPTP, L2TP (L2F !), IPSec…)
- Il existe des VPN de niveau 2 et de niveau 3

- Sécurité
    - se passe généralement dans un réseau public… Internet.
    - encryption
- Performance
    - L'edge peut faire du trafic shaping ou du policing
- Gestion et administration
    - Indispensable et compliqué par les demandes de plus en plus strictes en termes de souplesse et de sécurité

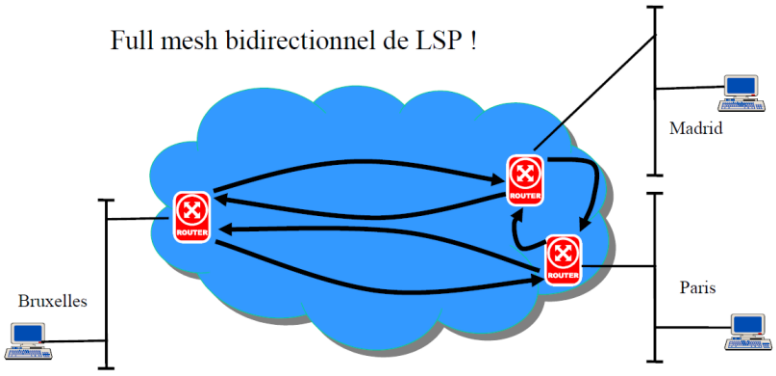
2 types de VPN

- Level 2 VPN
    - Fournis par l'ISP
    - Le routage est fait par l'ISP
    - Identique à un ensemble de lignes louées (donc niveau 2)
    - Peut être basé sur des ATM ou des FR PVCs
- Level 3 VPN
    - ISP pas concerné
    - Basés sur des tunnels
    - L'encryptage et le routage sont faits par le client (!) (donc niveau 3)
    - Protocoles de tunneling (PPTP, L2TP, IPSec, GRE…), encapsulation d'IP dans IP, récemment BGP / MPLS LSP

RFC 2547 bis

- Implémente un VPN sur base d'un full mesh (bidirectionnel) de LSP entre les différents PoPs (donc basé sur MPLS)

- L2 VPN
- Obligation de supporter LDP
- Aussi appelé BGP/MPLS VPN
- Notion de VRF (Virtual Routing and Forwarding instance)



Niveau 7 – Application

- Basé sur la notion de porte (TCP / UDP)
- Processus dans le serveur (daemon / process)
- Plusieurs processus en parallèle sur un serveur
- Chacun sa porte (éventuellement configurable) !!!
- Grande différence entre les standards (de juro) et les applications (de facto)

Telnet

- Utilisé pour se connecter à une machine à partir d'une autre.
- TCP port 23
- Aucune sécurité
- Basé sur la notion de Virtual Terminal
- Une des premières applications (avec FTP) !!!
- Protocoles similaires: rlogin, rsh, rcp

- RFC 854
- Options négociées (RFC 2400, en évolution)
- Négociation des commandes:
    - **DO** L'émetteur veut que le récepteur fasse quelque chose
    - **DON'T** L'émetteur ne veut pas que le récepteur fasse quelque chose
    - **WILL** L'émetteur veut faire quelque chose
    - **WON'T** L'émetteur ne veut pas faire quelque chose

Commandes utilisateur

Pour avoir le prompt Telnet à partir d'une session en cours : **'^]'**

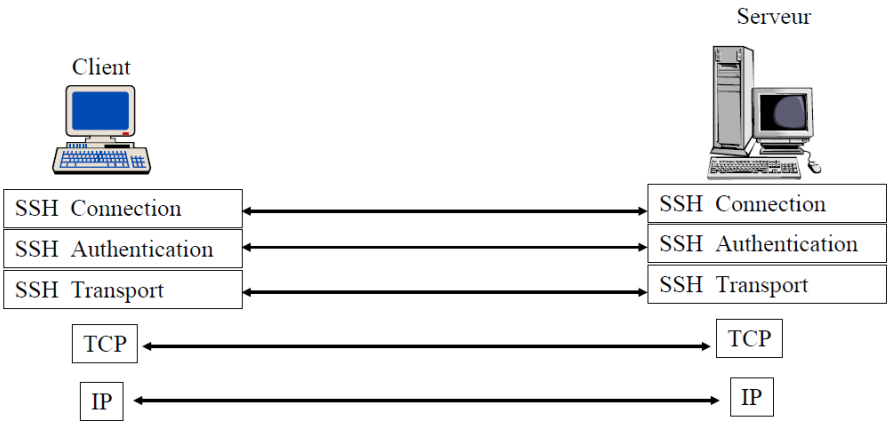
```
telnet> ?
Commands may be abbreviated.  Commands are:

close          close current connection
logout         forcibly logout remote user and close the connection
display        display operating parameters
mode           try to enter line or character mode ('mode ?' for more)
open           connect to a site
quit           exit telnet
send           transmit special characters ('send ?' for more)
set            set operating parameters ('set ?' for more)
unset          unset operating parameters ('unset ?' for more)
status         print status information
toggle         toggle operating parameters ('toggle ?' for more)
slc            change state of special charaters ('slc ?' for more)
z              suspend telnet
!              invoke a subshell
environ        change environment variables ('environ ?' for more)
?              print help information
```

SSH (Secure Shell)

- Utilisé pour se connecter à une machine à partir d'une autre
- TCP port 22
- Accès sécurisé (encryptions)
- V2
- Vient de Unix

- Divers algorithmes d'encryption : Propriétaire (v1), RSA, DES, 3DES, blowfish …
- v2 plus riche et plus sécurisé que v1
- v3 en préparation
- Protège du 'sniffing' du réseau et des attaques 'man in the middle (MIM ou MITM)'
- Basé sur trois sous-protocoles :
    - **SSH Authentication protocol** (authentification du serveur, négociation des paramètres, échange de clés si nécessaire)
    - **SSH Connection protocol** (authentification de l'utilisateur, confidentialité)
    - **SSH Transport Layer protocol** (login interactifs, exécution à distance, mux de plusieurs sessions sur un canal)

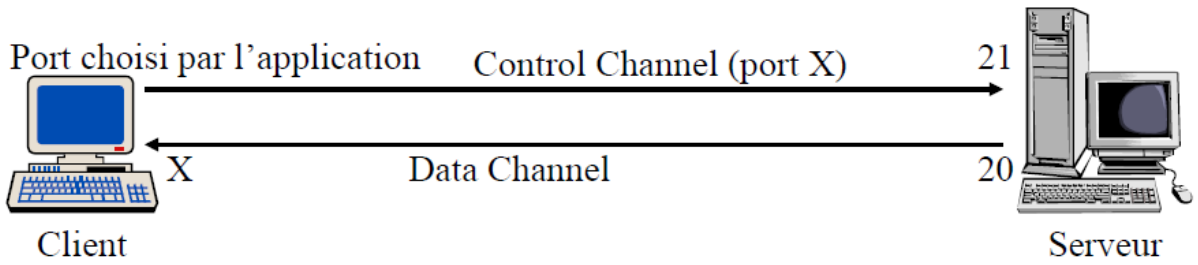


FTP (File Transfer Protocol)

- Utilisé pour transférer un ou plusieurs fichiers d'une machine à l'autre
- TCP port 21
- Aucune sécurité
- Une des premières applications avec Telnet
- RFC 959
- Notion de **login anonyme**. Pas besoin d'être un utilisateur connu du serveur

Fonctionnement

- Le client contacte le serveur pour établir une connexion. Il utilise le port 21 sur le serveur. C'est le « **Control Channel** »
- Om envoie une commande, **PORT**, au serveur, pour l'informer du port sur lequel le client s'attend à envoyer/recevoir des données
- Le serveur crée une deuxième connexion (« **Data Channel** »), avec comme source port le 20 et comme destination port le numéro du port spécifié dans la commande PORT
- C'est sur cette deuxième connexion, établie par le serveur, que le client enverra/recevra les données



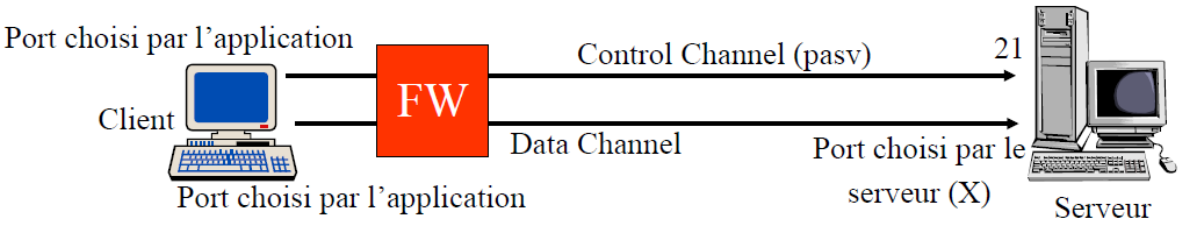
Commandes

- ascii – bin
- cd – lcd
- dir – ls

- hash
- pwd – lpwd
- get – mget
- put – mput
- open – close – quit – bye
- help – ?

Mode passif

- En mode Passif, le client ne spécifie pas de commande « PORT » qui engendre une session initiée par le serveur (Data Channel)
- A la place, le client envoie une commande « **PASV** » qui demande un numéro de port au serveur.
- Le serveur répond par un numéro de port qui pourra être utilisé pour que le client initie la connexion sur le Data Channel. Le serveur écoute donc sur ce nouveau port.
- C'est donc toujours le client qui initie les sessions



TFTP (Trivial File Transfer Protocol)

- Utilisé pour transférer un fichier d'une machine à l'autre
- **UDP** port 69
  - Sur port UDP, donc **pas fiable**
- Aucune sécurité
- Simple et facile
- RFC 1350
- Développé pour avoir une possibilité de transfert de fichier facile à implémenter
  - Parfois utilisé pour le bootstrap

HTTP (Hyper Text Transfer Protocol)

- Utilisé pour afficher des informations d'une machine sur une autre
- TCP port 80
- Pas de sécurité à la base
- En pleine évolution
- V1.1 standardisée dans RFC 2616

- Basé sur deux concepts:
  - **URL** (Uniform Resource Locator) – Hyperliens
    - Définis dans RFC 1738
  - **HTML** (Hyper Text Markup Language)
- Sans connexion et sans état (**connectionless** and **stateless**)

- Différentes méthodes sont utilisées:
  - **GET**: demande d'un document
  - **HEAD**: demande de l'entête d'un document (caching)
  - **RESPONSE**: réponse à une demande (contient généralement de l'HTML)
  - …

URL

- But : avoir un nom unique pour chaque document. A la base, vient du partage des documents scientifiques
- Structure : <Protocole>:// < username>: < password>@< nom_de_machine>< :port>/<répertoire>/ < nom_de_fichier>
- Protocole : ftp, http, mailto, news, nntp, telnet, …

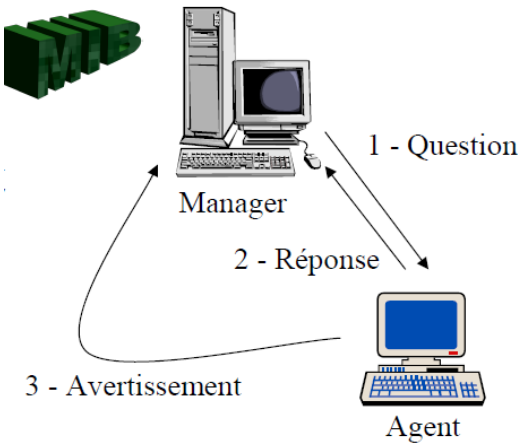
HTML

Language structure, sous-produit de SGML, permettant l'indépendance entre le formatage du document et la machine sur laquelle il est lu.

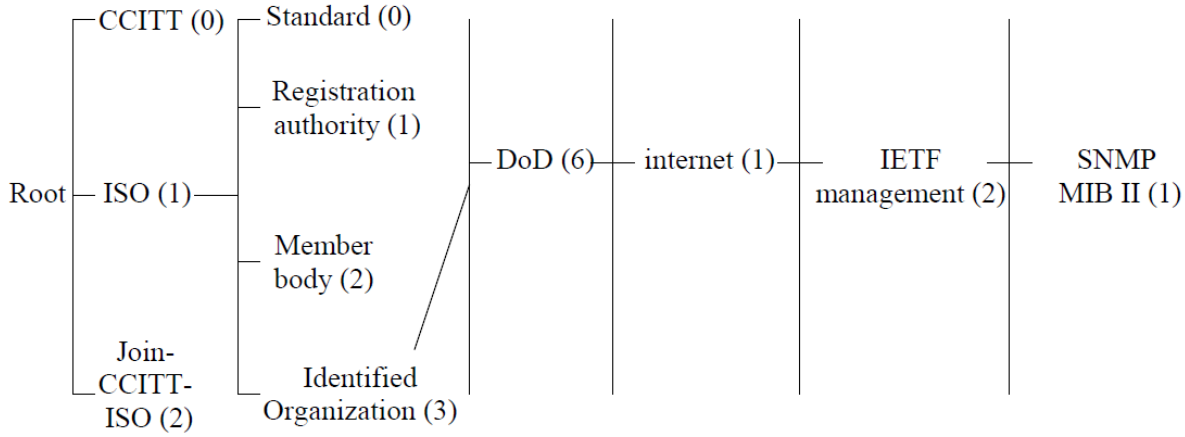
Basé sur la notion de requête – réponse

SNMP (Simple Network Management Protocol)

- Utilisé pour gérer les machines (routeurs, switches, repeters, PCs, imprimantes, machines à café, …) d'un réseau
- UDP port 161
- V1 (pas de sécu), v2 (peu de sécu), v3 (sécu mais quasiment pas implémenté)
- Basé sur la notion de **MIB** (publiques – privées) qui donne un ID aux objets
- MIB écrites en ASN.1
- Deux possibilités :
  - Le manager interroge l'agent
  - L'agent avertit le manager
- Possibilité de proxy



Arbre des MIBs



- 1.3.6.1.2.1.1: System
  - •1.3.6.1.2.1.1.1: System Description
  - •1.3.6.1.2.1.1.2: System Object ID
  - •1.3.6.1.2.1.1.3: System Up Time
  - •1.3.6.1.2.1.1.4: System Contact
  - •1.3.6.1.2.1.1.5: System Name
  - •1.3.6.1.2.1.1.6: System Location
  - •1.3.6.1.2.1.1.7: System Services
- 1.3.6.1.2.1.2: Interfaces
- 1.3.6.1.2.1.3: at
- 1.3.6.1.2.1.4: IP
- 1.3.6.1.2.1.5: ICMP
- 1.3.6.1.2.1.6: TCP
- 1.3.6.1.2.1.7: UDP
- 1.3.6.1.2.1.11:SNMP
- 1.3.6.1.2.1.14: OSPF v2
- 1.3.6.1.2.1.15: BGP v4
- …

Opérations

V1

- Get
- Get next
- Get response
- Set
- Trap

V2

- Get*
- Get next*
- Get bulk
- Response
- Set*
- Inform
- Trap v2
-

IPFIX (IP Flow Information Export)

- Similaire à SNMP, mais avec la notion de flux, basé sur
  - Port source et dest (niveau 4)
  - IP source et dest (niveau 3)
  - Protocol Type (niveau 3)
  - TOS (niveau 2)

    - Incoming interface (niveau 1)
- Il faut que les devices et la console de management soient « IPFIX compliant »...

Mail

- **Adresse :** username@domainname
- Alias, liste de distribution
- Les machines peuvent ne pas être connectées au même moment, donc **spooling** (gestion de queues et essais à intervalles réguliers)

Structure d'un message

- **Enveloppe**
    - Utilisée par les MTAs pour la livraison
    - Emetteur, Récepteurs(s)
- **En-tête**
    - Utilisé par les MUAs
    - Message ID, Date/Heure, Mailer System, …
- **Corps**
    - Contenu du message

Les trois paradigmes du client

- Définis dans la RFC 1733

- **Off-line:** les messages sont downloadés sur la machine du client puis effacé du serveur. Le client se connecte régulièrement au serveur pour voir si de nouveaux messages sont arrivés. C'est donc un modèle de type 'store and forward'. La machine client est souvent unique, même si plusieurs mailbox (pour différents clients) coexistent sur le serveur.

- **On-line:** les messages sont gérés directement sur le serveur. Les messages ne sont pas stockés sur la machine du client. Cela permet une indépendance du lecteur par rapport à la machine : on peut lire sa mailbox de n'importe où ! Plus évolué que le modèle off-line.

- **Déconnecté:** hybride des deux précédents, le mode déconnecté downloade les messages sur la machine client, les manipule localement puis resynchronise lors d'une nouvelle connexion. Attention aux problèmes lors d'accès depuis plusieurs clients.

SMTP (Simple Mail Transfert Protocol)

- Utilisé pour envoyer un mail d'un serveur mail à l'autre
- TCP port 25
- Pas de sécurité
- RFC 821
- Extended SMTP (ESMTP), RFC 1869

Commandes

- HELO <domain>
- MAIL FROM:<reverse-path >
- RCPT TO:<forward-path>
- DATA
- QUIT
- RSET
- VRFY <string>
- SEND FROM:<reverse-path>
- SOML FROM: <reverse-path>
- SAML FROM: <reverse-path>
- EXPN <string>
- HELP [<string>]
- NOOP
- TURN

Connection manuelle

- Telnet smtp.mycompany.com 25
- Commandes :
  - Mail from: <adresse source>
  - Rcpt to: <adresse destination>
  - Data <contenu du message>
  - Quit
  - …

MTA (Message Transfer Agent)

- Utilisé pour recevoir les mails et les fournir aux utilisateurs
- Responsable du routage des messages.
- Partie serveur (ex: Unix sendmail et MS Exchange Server)
- Implémente SMTP

MUA (Message User Agent)

- Utilisé pour recevoir, présenter, préparer et envoyer les mails
- Partie client (ex: Thunderbird, Eudora, Outlook)
- Implémente POP ou / et IMAP

POP (Post Office Protocol)

- Sert à aller **chercher les messages sur le serveur**
- N'implémente que le paradigme « **off-line** »
- Permet aussi d'utiliser un mode « pseudo on-line », où les messages sont laissés sur le serveur
- V3
- RFC 1725
- Pas de sécurité
- TCP port 110
- Le plus ancien et le plus utilisé, et de loin !

Connection manuelle

- Telnet pop.mycompany.com 110

- Commandes :

- User <username>
- Pass <password> (!)
- List
- Quit
- …

DMSP (Distributed Mail System Protocol)

- Implémente le paradigme « déconnecté »
- Une seule application: PCMAIL.
- Quasiment pas utilisé

IMAP (Internet Message Acces Protocol)

- **Implémente les trois paradigmes** (« on-line », « off-line » et « déconnecté ») !!!
- Sert à **consulter les messages sur le serveur**
- Plus complet que POP3 (Superset de POP et de DMSP) puisqu'il implémente les trois paradigmes
- V4
- RFC 2060
- TPC port 143
- Offre plus de possibilités au niveau des **flags** associés à un message (lu, supprimé, répondu…)
- Permet également de ne **demander qu'une partie du message** (entête, corps, correspondance à certains critères…)
- Possibilité de manipulation de **plusieurs mailbox en même temps**, ou par plusieurs utilisateurs en même temps.

Infos supplémentaires sur les Mails

- Généralement, les ISP refusent de faire du 'SMTP relay' vers un autre ISP.
- Pourquoi ? Contre les spammeurs !
- Donc, le serveur POP et le serveur SMTP peuvent être différents.
- En changeant d'ISP, on risque de devoir changer de serveur SMTP.

NTP (Network Time Protocol)

- Sert à synchroniser les horloges de différentes machines à travers le réseau.
- UDP port 123.
- V3 standardisé dans la RFC 1305.
- V4 (transformé en SNTP) dans la RFC
- 2030.
- 10 à 20 millions de clients...
- Précis à quelques millisecondes près...

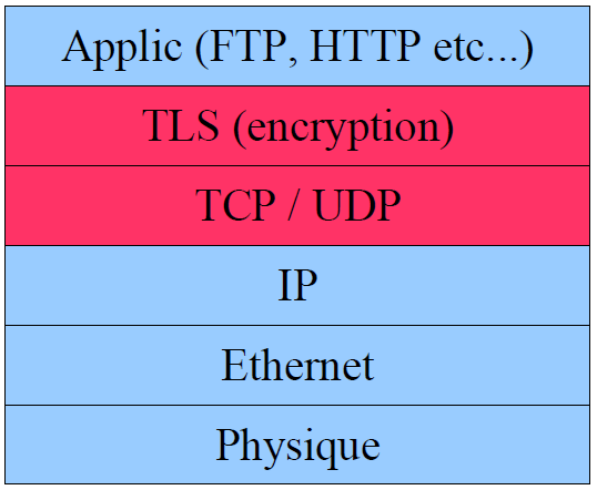
Peer To Peer

- Partage en ligne de musique, de films, de fichiers en général
- Pas de port standard
- Engouement des jeunes
- Problèmes légaux (le programme ou le site est légal, mais pas l'utilisation qu'on en fait)
- Exemples: (Napster), Kazaa, Emule - Edonkey, BitTorrent...

Sécuriser des applications non sécurisées

- Il y a un ensemble d'applications (FTP, HTTP, RTP (voir plus loin), POP etc...) qui ne sont pas sécurisées.
- Une manière de les sécuriser est de rajouter une couche d'encryption avant de transmettre les données à la couche transport
- Cette couche, appelée SSL ou TLS, a été initialement développée par Netscape

TLS (Transport Layer Security)



VoIP

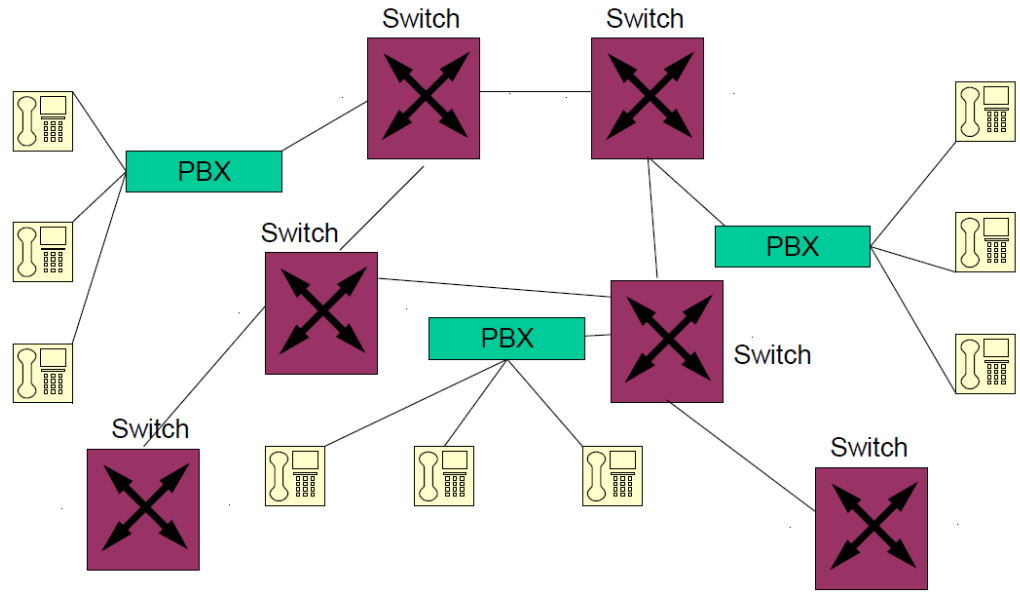
- En mettant la voix sur IP, on fait un meilleur usage de la bande passante (on transmet que quand il y a vraiment quelque chose à transmettre, **en théorie**)
- **En pratique**, on transmet en permanence le flux voix (petits paquets à intervalle régulier)
- **Problème :** Le jitter introduit par les réseaux IP est insupportable pour les flux voix
- Nécessite **QoS** en théorie

Architecture

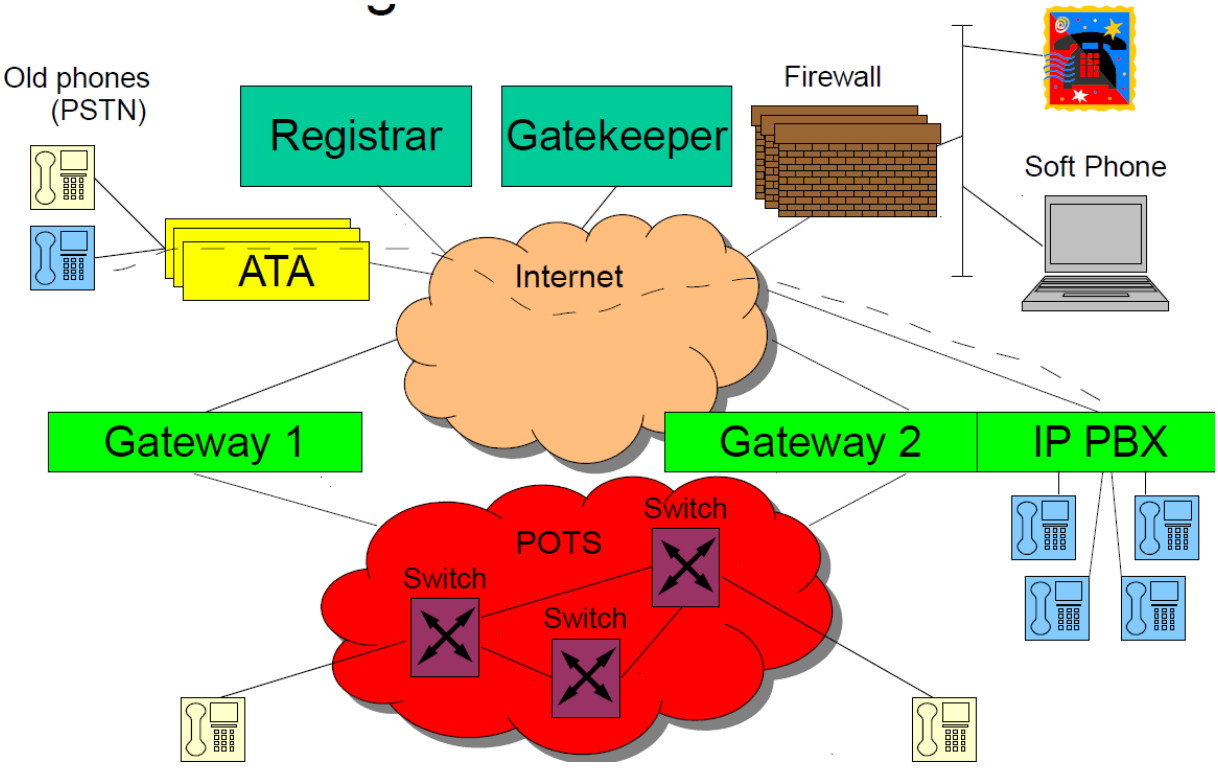
- Gateway
- Gatekeeper (optionnel)
- POTS (PSTN)
- IP Phones ou ATA ou « Soft Phone » ou téléphones (PSTN) ou terminaux
- Accès à l'Internet côté serveur (cloud)

- Accès à l'Internet côté client (centrale virtuelle)
- Deux composantes essentielles :
  - Les protocoles de signaling (H323, SIP, MGCP,…) à comparer avec SS7
  - Le flux voix (RTP/RTCP) à comparer avec la transmission de la voix (maintenant digitalisée)
- Ne pas oublier les aspects de facturation
- Interconnexion obligatoire avec le PSTN (au moins en production)

PSTN



VoIP



Gatekeeper

Les rôles essentiels du gatekeeper sont :

- Accepter ou refuser les appels (admission control)
- Router les appels (les flux voix) vers les bons gateways (LCR)
- Gestion de la bande passante
- Facturer les appels aux utilisateurs (prepaid / postpaid / forfaits / par minute / par seconde / pas de facturation / prix de setup / heures pleines / heures creuses ...)

- Traces des appels : les **CDRs** (Call Detail Record)

Codec

- Pour coder et décoder efficacement les flux voix et vidéos.
- Déterminent la compression et la performance utilisée

Codec	Bit rate (kbps)	Remark
T38		Fax (!!! implémentation!!!)
G.711 µ Law	64	USA - Japan
G.711 A Law	64	Europe
G.721	32	
G.729	8	Pas libre de droits - Fréquent
G.723.1	6.3 / 5.3	

DTMF (Dual Tone Multi Frequency)

- Sert quand on doit guider un automate (IVR: banque, voice mail, carte prépayée, …)
- 3 possibilités :
  - In audio
  - RFC 2833
  - SIP Info

Les principaux protocoles

- Session Description Protocol, Real time Transport Protocol & Real Time Control Protocol
- RFC 1889 & 1890
- Définis pour supporter la voix ET la vidéo !
- SDP pour négocier les capacités des participants (codecs, nombres, portes etc...)
- RTP sert à offrir le transport des paquets de données en temps réel. Paquets de taille fixe.

- RTCP sert à contrôler la QoS offert au sessions RTP.
- Tournent tous les trois sur UDP !

Les numéros de téléphone

- +883 est le code international pour la VoIP
- On peut rerouter (moyennant paiement) vers un numéro géographique. On devient alors indépendant de la situation géographique (cf GSM). C'est le portage. Les clients peuvent garder leur numéro s'ils le désirent.
- Attention aux numéros d'urgence ! Pas supporté en IP

SIP (Session Initiation Protocol)

- Sert à établir, à géter et à terminer des sessions voix et vidéos sur des réseaux à commutation de paquets (comme l'internet)
- RFC 3261 (la plus grosse)
- Fonctionne comme http
  - Mode requête – réponse
  - Basé sur une notion d'adresse appelée **SIP-URL**
- Port 5060 sur UDP
- Utilise le record DNS SRV
- S'appuie sur SDP (Session Description Protocol) pour établir les sessions. Les ports utilisés par SDP sont négociés lors de l'établissement de la session (donc problème de FW)
- SDP permet d'établir des sessions entre 2 **ou plusieurs** points

Les paquets

Requêtes

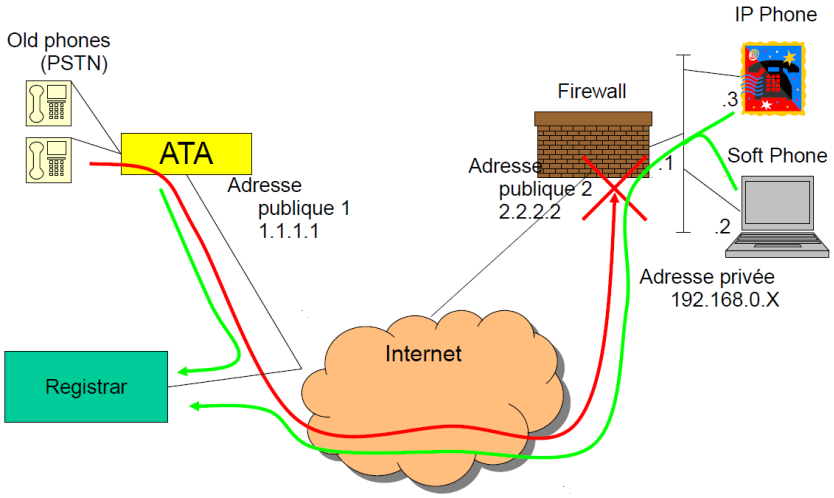
- INVITE
- ACK
- CANCEL
- BYE
- OPTIONS
- REGISTER
- – INFO

Réponses

- 1XX : Provisionning
  - 100 – Trying
  - 180 – Ringing
- 2XX : Succes
  - 200 – OK
- 3XX : Redirection
- 4XX : Erreur Client
  - 404 – Not Found
  - 486 – Busy
- 5XX : Erreur Serveur
- 6XX : Erreur Globale

Problèmes

- Les appels entrants ne savent pas passer un FW / NAT
- Les appels sortant risquent de ne passer que dans un seul sens (depuis l'intérieur vers l'extérieur du FW)



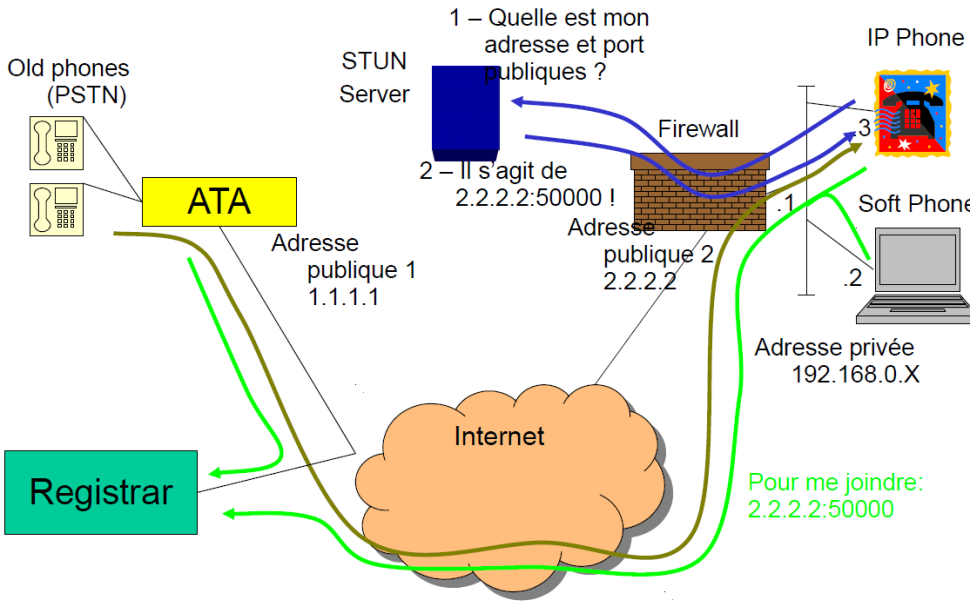
Solutions

Solution 1 :

- Entrée statique dans le FW/NAT
- Diminution de la sécurité
- Oblige à utiliser une adresse fixe (Plus de DHCP ou alors avec réservation)

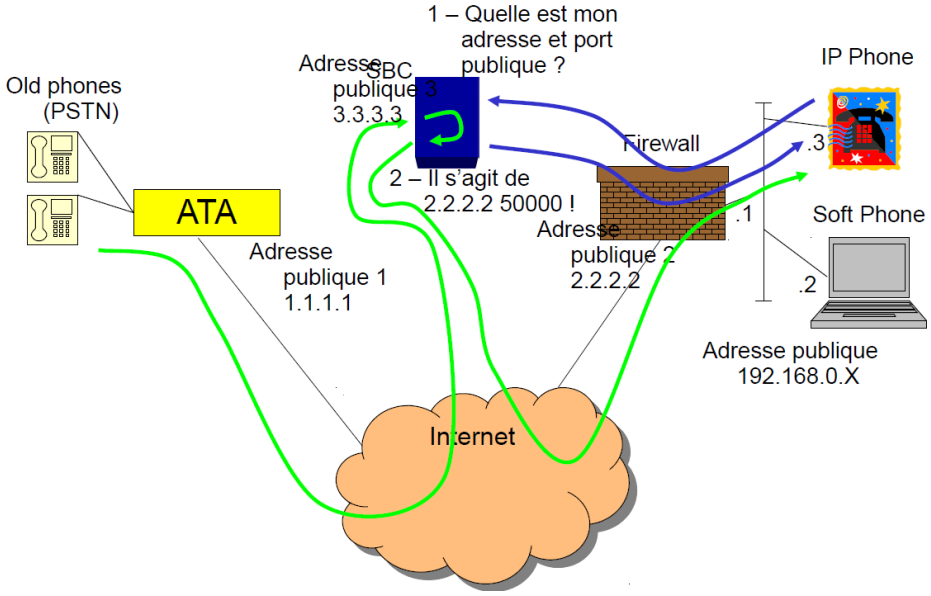
Solution 2 - **STUN**:

- Notion de STUN serveur
- Le téléphone demande au STUN serveur avec quelle adresse il est vu de l'extérieur
- Le STUN serveur répond au client (IP tel) l'adresse et le port public utilisé
- Le client s'enregistre avec cette IP et ce port public
- Attention : ne fonctionne qu'avec des NAT symétriques (dont l'adresse et la porte publique ne dépendent pas de l'adresse et de la porte de destination)



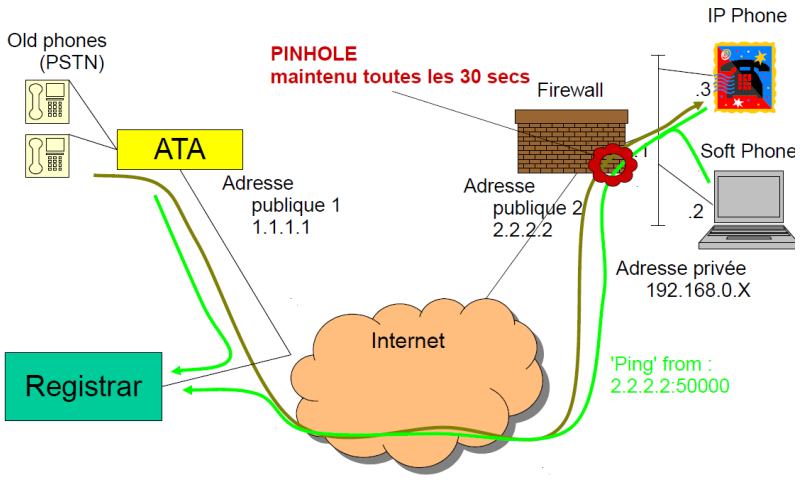
Solution 3 - **SBC (Session Border Controller)** :

- Tout le trafic (signaling plus voix) passe par le SBC, qui a une adresse publique.
- Le client demande au SBC quel est son adresse et port publique (cf STUN).
- Tout le trafic passe par le SBC, qui maintient la session avec le client. Donc, le client est vu comme s'il était le SBC (adresse publique)...
- Le SBC agit comme s'il était un switch téléphonique.
- Performance améliorée, contrôle renforcé (par et dans le SBC).



Solution 4 - **Pinhole** :

- La solution la plus naturelle, pour contourner les FW, est que le téléphone, de l'intérieur du réseau (depuis le LAN) envoie régulièrement des paquets vers le GK ou vers le Registrar ; afin de maintenir un Pinhole ouvert dans le FW.
- C'est mieux, mais risque de timeout
- Le téléphone doit communiquer régulièrement avec le GK (ou Registrar) en fonction du timeout du FW.



Sécurité

Les mots de passe

Les types d'attaques

- Deviner
- Voler / Analyser le trafic
- Force brute
- Attention au nombre de possibilités

	1 sb	2 sb	5 sb	7 sb	10 sb
26	26	676	11881376	8031810176	141167095653376
36	36	1296	60466176	78364164096	3656158440062976
50	50	2500	312500000	781250000000	97656250000000000 (97 millions de milliards)

Sécuriser un mot de passe

- A au moins 14 caractères.
- Contient des majuscules.
- Contient des minuscules.
- Contient des chiffres.
- Contient des symboles, tels que ` ! " ? $? % ^ & * ( ) _ - + = { [}] : ; @ ' ~ # | \ < , > . ? /
- Ne ressemble pas à vos mots de passe précédents.
- Ne contient pas votre nom et / ou prénom.
- N'est pas votre login.
- N'est pas le nom d'un ami(e).
- N'est pas le nom d'un membre de votre famille.
- N'est pas un mot du dictionnaire.
- N'est pas un nom 'classique'.

Routeurs

Les attaques les plus classique sur des routeurs sont :

- Accès non autorisé (mot de passe)
- Reroutage
- DoS
- Renvoi d'une session (éventiellement modifiée)
- Modification de configuration via SNMP
- Sécurité physique (accès à la console)

Les filtres dans les routeurs

- Permettent de filtrer le trafic
- Basé sur les X (60) premiers bytes du paquet IP (par exemple)
- Permet d'assigner des priorités ou de jeter des paquets

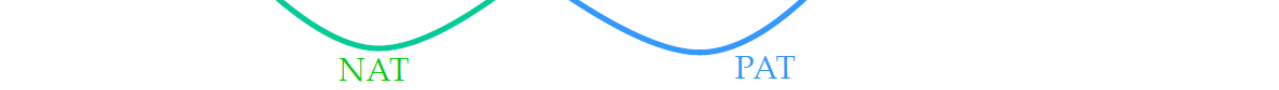
NAT (Network Address Translation)

- Avantage :
  - Permet d'utiliser une seule (ou plusieurs) adresse(s) publique(s) pour plusieurs machines
  - Offre plus de sécurité
- Désavantage :
  - Casse l'idée de bout en bout
- Peut influencer la couche application, si elle ne respecte pas le modèle ISO – OSI

Les différents types de NATing

- **Statique** – N to N
- **Dynamique –** M to N
- **Single** – N to 1 (masquerading/overloading/PAT/NAPT)
- **Sans PAT**, le nombre de machines accédant à l'extérieur simultanément limité par le nombre d'adresses IP publiques disponibles

Adresse source	Adresse destination	Porte source	Porte destination	Nouvelle adresse source	Nouvelle adresse destination	Nouvelle porte source	Nouvelle porte destination
192.168.0.1	94.84.74.64	1282	80	194.78.198.10	94.84.74.64	2000	80
192.168.0.2	94.84.74.64	1282	80	194.78.198.10	94.84.74.64	2001	80
94.84.74.64	192.168.0.1	80	1282	94.84.74.64	194.78.198.10	80	2000
94.84.74.64	192.168.0.2	80	1282	94.84.74.64	194.78.198.10	80	2001



Firewall

- Contrairement aux filtres d'un routeur, le firewall met en relation différents paquets du trafic
- Configurable, mais bloque le trafic entrant par défaut
- Possibilité de DMZ
- Possibilité de NAT
- FTP : 2 canaux
  - Un des canaux peut être bloqué
- Effets indésirables
- **Statefull** – Examen des paquets et mise en relation entre le niveau 3 et 4 (et parfois 7)

Proxy

- Permet de n'accepter le trafic entrant que vers une machine particulière
- Permet à l'entreprise de contrôler les sites vers lesquels sont envoyées les requêtes
- Peut également permettre de s'anonymiser

Cryptographie

Pour crypter un texte clair, il faut une clé pour transformer ce texte en texte cypté.

- La sécurité dépend donc de l'algorithme d'encryption **et** de la clé

Les type de cryptographie

- Algorithmes **symétriques**
  - Introduit par Jules César
  - Une seule clé
    - Si on trouve cette clé, on peut donc déchiffrer ce message
  - DES, 3DES

- Algorithmes **asymétriques**
  - Introduit par Diffie et Hellman
  - La clé est publique
  - RSA
  - Complexe

PGP (Pretty Good Privacy)

- Standard de facto pour l'encryption des mails
- **Etapes**
  - Création et échange des clés
  - Ecriture du mail (sous forme d'un texte)
  - Encryption du texte – production du fichier crypté
  - Envoi du texte en attachement
  - Réception du mail
  - Décryption du fichier attaché et crypté
  - Lecture
- **Système hybride**
  - Compression pour éviter les patterns
  - Clé publique

Les clés publiques

Principe mathématique

- Idée de base : avoir une paire de clé (fonction mathématique); une **publique** (**F**) et une **privée** (**P**), qui sont complémentaires.
- Soit **X** un **message** quelconque
- On veut que P(F(X)) = X
- Dans ce cas, on peut prendre un message X, l'**encoder à l'aide de la fonction F** du destinataire (que tout le monde connaît) et lui envoyer

- Le **destinataire est le seul à** connaître P et à pouvoir retrouver le message original puisque P(F(X)) = X
- Donc, plus de **problème de distribution de clés** !

Principe de signature

- En plus, on peut **signer** ses messages si F(P(X)) = X
- En effet, on peut prendre la clé **privée de l'émetteur** (**Pe**), et la clé **publique du récepteur** (**Fr**)
- Comme précédemment, on calcule Fr(X)
- Avant de l'envoyer, on la **crypte encore une fois avec Pe**. On envoie donc Pe(Fr(X))
- Le récepteur reçoit le message **doublement crypté.**
- Il **applique la fonction Fe** (clé publique de l'émetteur) à ce qu'il a reçu. Il calcule donc Fe(Pe(Fr(X))). Il trouve donc Fr(X).
- Il ne lui reste qu'à appliquer, comme précédemment, sa **propre clé privée (PR)**. Il calcule donc Pr(Fr(X)) et il obtient… X !

Encryption

- RSA
- IKE
- MD5
- DES (Data encryption Standard)
- 3DES (Triple DES)

RSA (Rivest – Shamir -Adelman)

- Clé publique (en théorie)
- En utilisant **2 grands nombres premiers**, et en se basant sur le fait qu'un nombre n'est pas facilement factorisable, **pq=m**, **m** est la **première partie de la clé publique**

- On choisit un nombre **e, premier avec (p-1) (q-1)**. On publie m et e (qui forment l'ensemble de la clé publique). C'est la **deuxième partie de la clé publique.**

- On publie (**e mod m**). C'est la **clé publique**.

- Il faut maintenant calculer la clé de déchiffrement **d** : **d*e= 1(mod(p-1) * (q-1))**. C'est la **clé privée**.

- Pour **encrypter** le message, l'émetteur calcule **C = M ^ (e mod m)**

- Pour **décrypter** le message crypté, le récepteur calcule **M = C ^ (d mod m)**

IKE (Internet Key Exchange)

- Permet de :
    - Négocier un protocole, algorithme et clés (dynamiquement)
    - Authentifier les correspondants
    - Echanger les clés de manière sécurisée
    - Gérer les clés, une fois échangées

MD5 (Message Digest 5)

- Développer par Rivest (RSA)
- RFC 1321
- **Signature digitale :** L'algorithme part d'un message d'une longueur quelconque et produit une « empreinte digitale » de 128 bits
- Utilisé par exemple pour confirmer qu'un fichier a été bien transmis

- Il existe des sites qui collectionnent plusieurs millions de mots de passe encryptés
    - Ne pas utiliser ces sites pour encrypter
    - Rajouter un salt dans les algo d'encryption

IP/Mac Spoofing

- Envoyer des paquets à partir d'une machine, en utilisant l'adresse IP/MAC d'une autre machine (qui a plus de droits,…).
- On peut en effet vouloir permettre ou protéger les utilisateurs d'accéder ou pas à certains services
- Portection : **VPN**

Phishing

- But : Soutirer des informations confidentielles à une victime consentante.
- Méthode : L'attaquant envoie un mail à la victime, en se faisant passer pour une organisation avec laquelle la victime est liée. Le mail renvoie la victime vers un site web, soi-disant mis à la disposition de l'utilisateur par l'organisation. Là, l'utilisateur est averti qu'un problème informatique est à l'origine d'une perte de données et que l'utilisateur doit introduire ces informations confidentielles.
- Protection : Education des utilisateurs, utilisation de son cerveau et méfiance

Phishing bancaire

- Site non sécurisé
- Informations confidentielles demandées par téléphone
- Contact téléphonique anonyme

DoS attacks

- Donner suffisamment de travail au device pour qu'il ne puisse plus fonctionner correctement (ICMP en rafale, Smurf attack, …)
- Surtout sur des mails server, web servers

Exploits

- Caractéristiques imprévues de certains programmes voire bugs
- Utilisés par les hackers pour réaliser des opérations que le programme peut faire mais pas l'utilisateur
- Généralement résolus par des fixes

Les backdoors

- Il s'agit d'une porte d'entrée dans le code qui permet de faire des choses non documentées

Les Virus

- Programmes exécutables
- Pas de virus dans les mails mais bien dans un fichier attaché
- Antivirus gratuit sur le web

Spywares

- Pas vraiment des virus mais en possèdent certaines caractéristiques
- Collectent des données sur votre machine et les envoie à un serveur
- Nécessitent généralement un « Antispyware »

Les ISPs

Le géant américain Google scanne le contenu des courriels sur son service de messagerie, « pour protéger les consommateurs des spams, des virus », mais aussi « pour cibler les publicités en se basant sur le contenu des mails », reconnaît un de ses juristes, Peter Fleischer. Les informations collectées permettent en effet des publicités « sur-mesure ». Le Soir, 22 Janvier 2008 !

IPv6

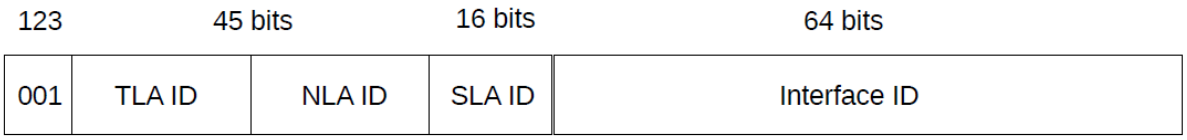
- Parfois appelé IPng (new generation)
- Adresses v6 codées sur **128 bits** (16 bytes) au lieu de 32 en v4

Implémentation native

- Idée générale : intégrer nativement dans le protocole certains points manquants à IPv4
    - Point à point
    - Support pour QoS

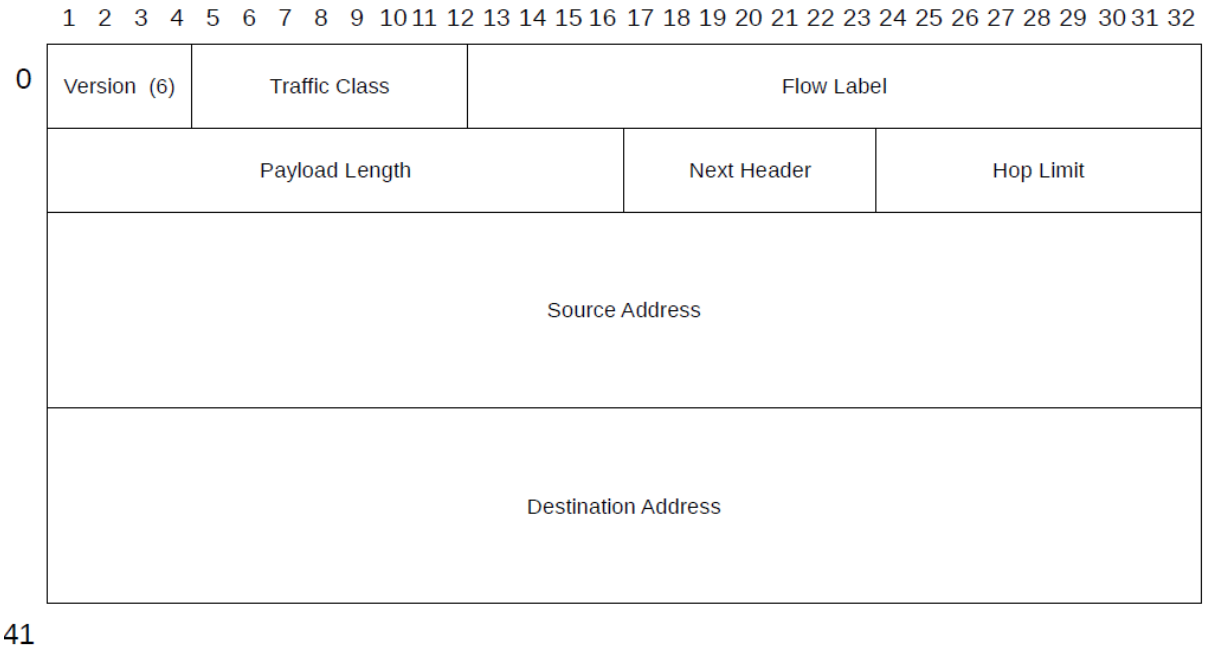
- Support pour Multicast
- Simplification des processus de routage (plus de fragmentation)

- Migration de v4 à v6



- **TLA** : Top Level Aggregator
- **NLA**: Next Level Aggregator (TLA + NLA = Public Topology)
- **SLA**: Site Level Aggregator (Site Topology)
- **Interface** : Identifiant de l'interface – Host ID ou dérivé

Les paquets IPv6



- **Version** : 6
- **Traffic Class** : QoS (équivalent v4 : DSCP)
- **Flow Label:** Flux (équivalent v4: Label MPLS)
- **Next Header** : permet de savoir quel est le protocole de niveau 4 (equivalent v4: Protocol ID)
- **Hop Limit :** équivalent du TTL
- **Adresses source et destination**

En IPv6, **plus de fragmentation**

- Il renvoie un « **ICMPv6 Packet Too Big** » et jette le paquet

Multicasting

- Envoyer **UN paquet** à **PLUSIEURS machines** (un groupe), pas toutes !
- Les machines peuvent, à tout moment, se **joindre** ou **quitter** un **groupe**
- Pas de limitation quant à la localisation des machines
- Adresse IP : **224**.X.X.X – **239**.X.X.X (**cf classe D**)
- Utilisé surtout pour certaines applications :
    - Audio (Radio)
    - Video (TV)

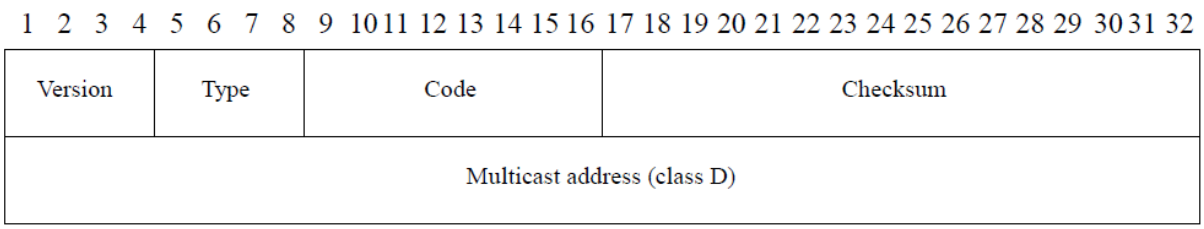
- Toutes les adresses multicast sont dans le range 224.0.0.0 – 239.255.255.255
- Les adresses **224.0.0.0 – 224.0.0.255** sont **réservées** (RIP, OSPF…) par l'IANA
- Les adresses réservées sont décrites dans la RFC 1700
- Problèmes des routeurs : potentiellement plusieurs interfaces de sortie (ou plusieurs fois sur la même interface…)

Les protocoles

- Il existe plusieurs protocoles multicast:
    - IGMP
    - PIM dense mode (Protocol Independent Multicast)
    - PIM sparse mode
    - DVMRP (Distance Vector Multicast Routing Protocol)
    - MOSPF (Multicast OSPF)
    - MBGP (Multicast extensions for BGP)

IGMP (Internet Group Management Protocol)

- RFC 2236
- Les routeurs IGMP envoient régulièrement des requêtes (host membership query) sur leurs interfaces auxquelles répondent (host membership report) les hôtes qui sont dans un groupe particulier
- Quand un hôte veut se connecter à un groupe, il envoie directement un « host membership report »
- IP protocol 2
- TTL : 1



Code :

- **0X11:** Membership query (sent by routers)
- **0X16:** Version 2 membership report
- **0x17:** Leave group
- **0X12:** Versioin 1 membership report

GSM

On trouve de plus en plus de GSM et les utilisateurs veulent pouvoir transmettre des données.

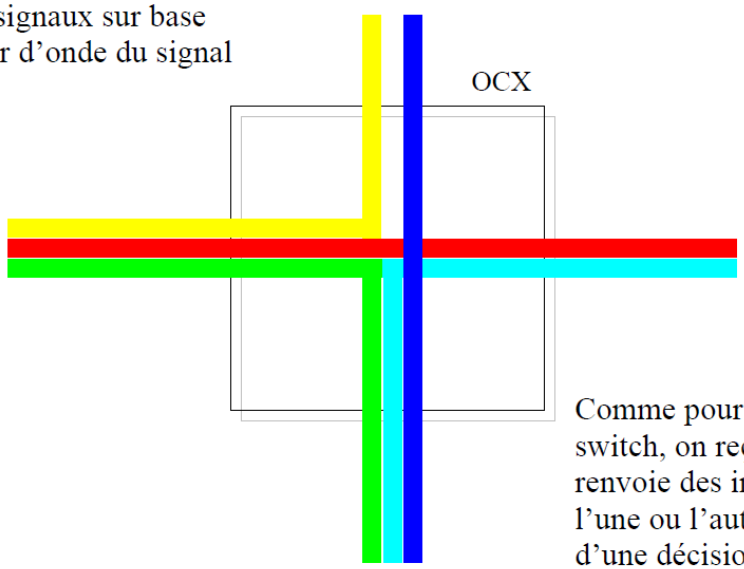
- GSM de base (première génération): circuit based
- GSM extensions: WAP et SMS (deuxième génération)
- **GPRS**:
  - GSM (General) Packet Radio Service
  - Plus de bande passante, partiellement packet based
- **UMTS**:
  - Universal Mobile Telecomunication System
  - Plus de bande passante, entièrement packet based
- WAP
  - Wireless Application Protocol
- EDGE
  - Enhanced Data rates for GSM Evolution
- SMS
  - Short Message Service

- **1G**: Première génération. Téléphone analogique. Basé sur FDMA (Frequency Division Multiple Access)
- **2G**: Deuxième génération. Téléphone digital. GSM. Débit max: 14.4 Kbps
- **2,5G**: Interim avant la 3eme génération. Partiellement basé sur l'IP mobile. GPRS - EDGE. Débit max: 171.2 Kbps
- **3G**: Troisième génération. Entièrement basé sur l'IP mobile (jusqu'aux devices). UMTS. Débit max: 2 Mbps
- **4G**: Quatrième génération. Débit max: 100 Mbps. Basé sur OFDM (Orthogonal Frequency Division Multiplexing). Récemment attribué en Belgique ! Jusqu'à 57 Mbps en Belgique.

DWDM (Wavelength Division Multiplexing)

- **Idée :** Utiliser des émetteurs/récepteurs laser plus précis et plus récents que précédemment et jouer sur la longueur d'onde (λ)
- Puis faire du switching sur base du λ
- **Amélioration :** La longueur d'onde utilisée comme label MPLS

L'Optical Cross Connect forwarde les signaux sur base de la longueur d'onde du signal reçu !



Comme pour un 'simple' switch, on reçoit puis on renvoie des informations sur l'une ou l'autre porte, sur base d'une décision de switching...

Troubleshooting

En cas de problème

- On s'arrête, on se calme, on réfléchit !
- Bien connaître la topologie du réseau (bridge / routeur) et les protocoles qui sont utilisés…

- Les 7 couches, dans l'ordre, en commençant par la couche physique
- Le niveau 2 (arp cache)
- Les outils de base (ICMP (ping, traceroute), telnet)
- Vérifier les ports
- Firewalls, Proxy, Access Lists etc…
- Les outils avancés (TCPDump, Wireshark, Sniffer)
- Regarder les fichiers de logs