Réseaux Avancés

DI 5 / Polytech 'Tours J.Y. RAMEL 2008-2009

Bibliographie

- Cours Réseaux avancés. Polytech'Tours 2006. Alain Delaplace
- Service Informatique DI Polytech'Tours (intranet)
- Analyse structurée des réseaux. J. Kurose, K. Ross. Pearson Education 2003
- Transmission et réseau. Guy Pujolle. Dunod. 2003.
- Cours sur les réseaux sans fil de C. Diou - LICM Metz.
- Cours sur les Réseaux privés virtuels (VPN) de Michel Le Tohic – ENST Bretagne

- Le web
  - http://renater.fr
  - Les RFC
  - Wikipedia
  - Cisco Systems, http://www.cisco.com/…
  - …

Plan du cours ➔ Romain Clair + JY Ramel

- **Le cours de Réseaux de DI3 est considéré comme maitrisé !**
  - Après une séance de rappel (maintenant)
  - Modélisation en couches des réseaux (OSI et autres)
  - Réseaux locaux (Ethernet, adresse MAC, Hub, Switch, VLAN, …)
  - Interconnexion de réseaux (pont, routeur, routage)
  - TCP / IP et internet
- **Réseaux avancés (plan)**
  - Les Réseaux sans fil (wifi, bluetooth …)
  - Sécurisation des échanges (chiffrement, SSL, IPsec, certificats, …)
  - Sécurisation des réseaux (Firewall, VPN, attaques classiques…)
  - IP nouvelle génération (IPv6, VoIP, …)
  - Réseaux de terrain (CAN, …)

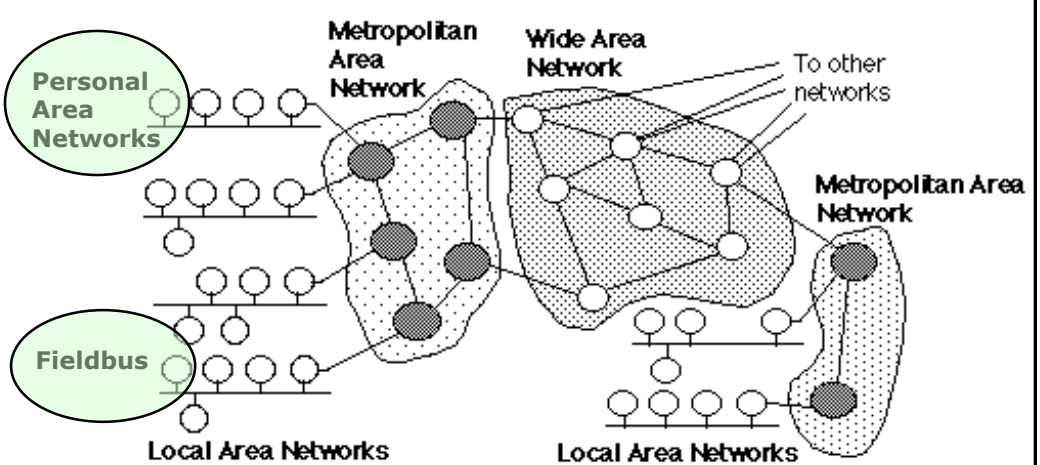
20h de TP

- **Planning ➔ Romain Clair + JY Ramel**
  - 1 Rappel config machine 2h Romain
  - 2 SSH 2h Romain
  - 3 routage 2h Romain
  - 4 5 Iptables firewall 4h Romain
  - 6 7 IPV6 4h JY
  - 8 9 Réseau de terrain 4h JY
  - 10 wifi 2h JY

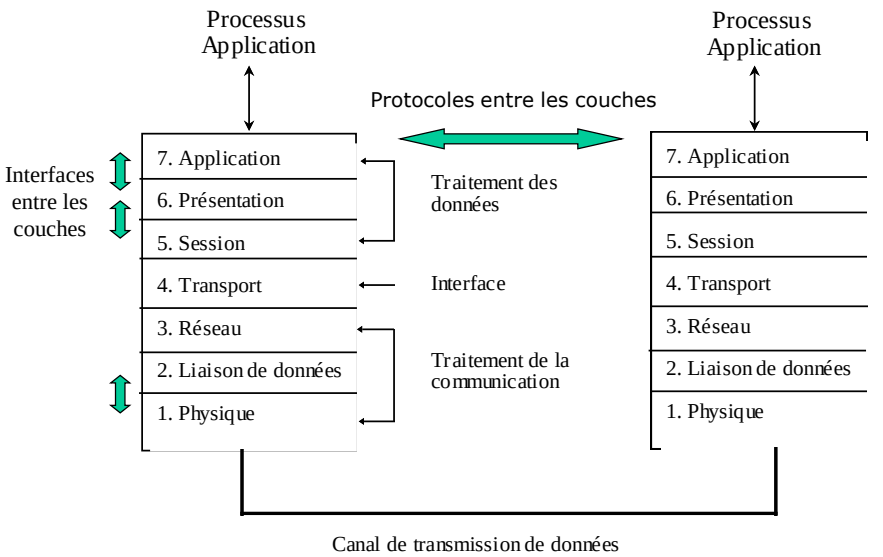
C'est parti …

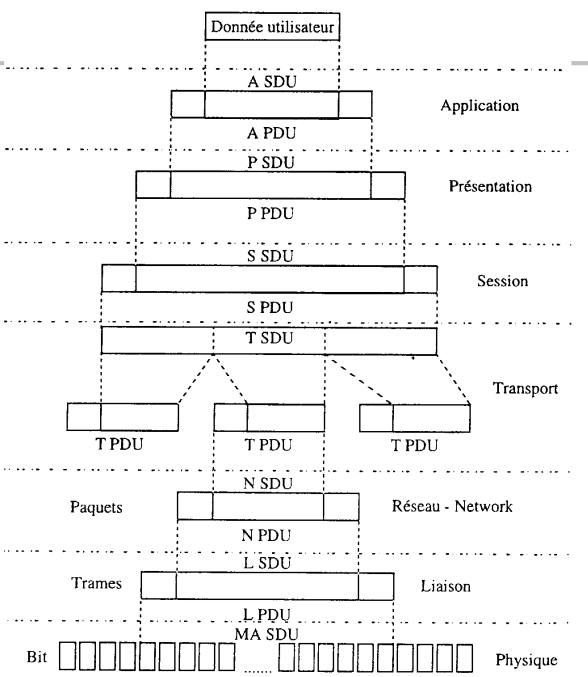
Rappel ➔ A vous de jouer les professeurs…

Types de réseaux et équipements

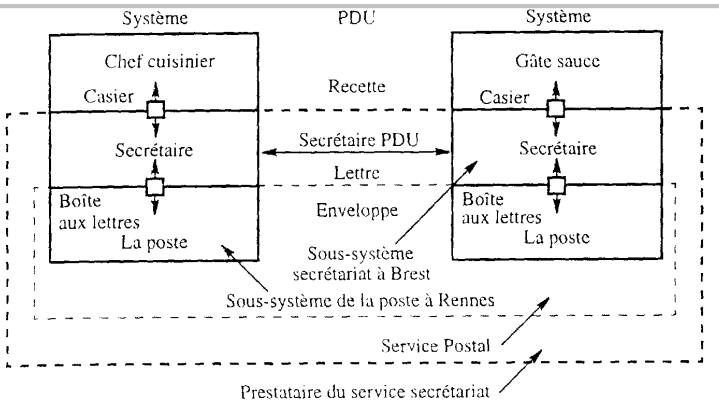


Architectures multi-couches





Objectifs (exemple wifi/IP)



Service	Entités protocolaires homologues	PDU échangées	Points d'accès
Cuisine	Chef cuisinier Gâte-sauce	Recettes	Restaurant
Secrétariat	Secrétaires	Lettres	Casier
Postal	Postiers	Enveloppes	Boîtes à lettres

Synthèse

Les couches OSI	Component physique													
7—Application	Logiciel d'application	Réseau local : logiciel compatible E-mail, diagnostics, traitement de texte, base de données												
	Applications réseau													
6—Présentation	Utilitaires de conversion	Différents types de réseaux et logiciel de poste travail passerelle												
5—Session	Système d'exploitation	SPX		NetBIOS		DECnet™	TCP/IP			AppleTalk®				
4—Transport		Novell® Netware® IPX™		PC LAN	LAN Mgr	DECnet	PC/TCP®	VINES™	NFS	TOPS®	Apple Share®			
3—Réseau														
2—Liaison	Réseau	E	A	TR	P	TR	E	TR	E	E		E	P	E	P
1—Physique		E=Ethernet ; TR=Token Ring ; A=ARCNET® ; P=PhoneNET®												

Ethernet voir applet

- TRAME ETHERNET : identique à la trame 802.3 sauf le champ type indiquant le type de protocole véhiculé dans le trame :
  - Champ Type = 2 octets représenté sous la forme hexadécimale XX-YY ou XXYY.
  - la valeur du champ type est normalement supérieure à 1500 c'est à dire la valeur maximum du champ longueur de données dans la trame IEEE; les valeurs connues sont :
    - **0806 : ARP, 0800 : IP**
    - **6000 à 6009 : protocoles DEC**
    - **...**

Champs	PRE	SFD	DA	SA	Type	LLC DATA	PAD	FCS
Taille en octets	7	1	2 ou 6	2 ou 6	2	< 1519	< 64	4

Ethernet : adressage

Les adresses IEEE 802.3 ou Ethernet sont codées sur 48 bits (6 octets).

- Syntaxe :
  - 08:00:20:09:E3:D8 ou 8:0:20:9:E3:D8
- Adresse Broadcast: FF:FF:FF:FF:FF:FF
- Adresse Multicast: le premier bit d'adresse transmis est égal à 1 (le premier octet de l'adresse est impair) :
  - **09**:00:2B:00:00:0F, **09**:00:2B:01:00:00
- Adresse individuelle : comprend le premier bit transmis à 0 (premier octet d'adresse pair) :
  - **08**:00:20:09:E3:D8 ou **00**:01:23:09:E3:D5

Ethernet : adressage

- **Une adresse de station individuelle est administrée soit localement soit globalement :**
  - localement : adresse significative **que** pour le réseau sur lequel elle est connectée; le second bit d'adresse transmis est égal à 1 : le premier octet de l'adresse est égal à 02, 03, 06, 07, 0A, 0B, 0E, 0F ,12, etc.
  - globalement : cette adresse est dite universelle et est attribuée par l'organisme IEEE; le second bit d'adresse transmis est égal à 0 : le premier octet de l'adresse est égal à : 00, 01, 04, 05, 08, 09, 0C, 0D, 10, etc.

Ethernet : adressage

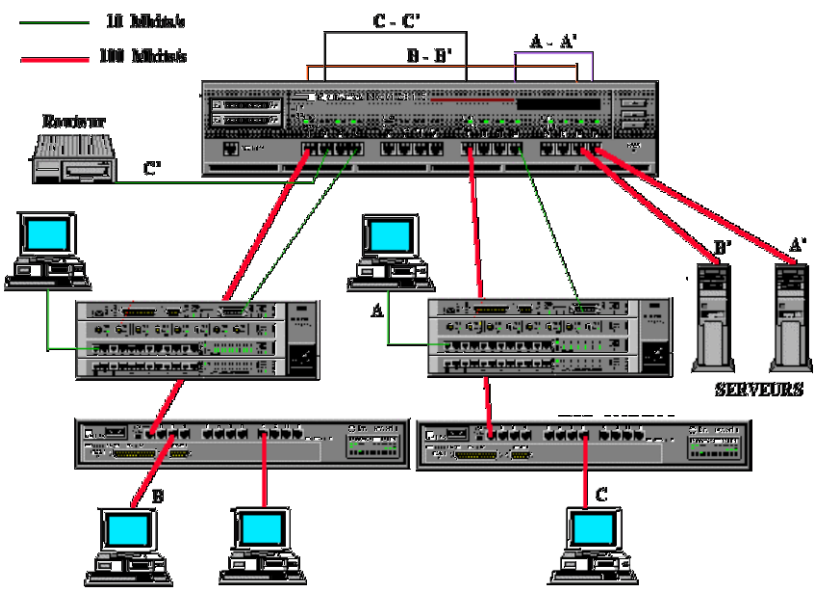
- Le constructeur reçoit une adresse dont :
  - les trois premiers octets sont fixés, code fabricant (Vendor Code) ou OUI (Organizationally Unique Identifier)
  - les trois suivants étant laissés à sa libre utilisation
- Ces adresses Ethernet sont alors unique dans le monde.
  - Les adresses étaient attribuées par le consortium (DEC, INTEL, XEROX)
  - C'est maintenant l'IEEE qui distribue ces adresse (1000 $ pour 2^{24} adresses)

  - 00:00:0C:XX:XX:XX **Cisco**
  - **08**:00:20:XX:XX:XX **Sun**
  - 08:00:09:XX:XX:XX **HP**

Ethernet et commutation

- Démo CSMA

Ethernet et commutation



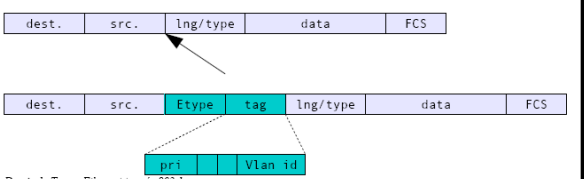
- **Hub vs switch**
- **Adresse MAC**
- **CSMA/CD**
- **VLAN**
- **…**

Ethernet : VLANS

- **Questions**
  - VLAN et domaine de diffusion ?
  - VLAN et trafic Broadcast ?
  - Appartenance d'un PC a plusieurs VLAN ?
  - Appartenance d'un port a plusieurs VLAN ?
  - Appartenance d'une trame a plusieurs VLAN ?
  - Mode de création des VLAN ?

- **Protocoles associés**
  - 802.1q → Gestion des VLAN
    - GVRP - GARP → Dialogue switch-switch ou switch-carte
    - VLAN Aware (informé)
    - Tagging de trames
    - VLAN dynamique
  - 802.1p → Priorité via VLAN

Generic Attribute/VLAN Registration Protocol)



Dessin 1: Trame Ethernet taggée 802.1q

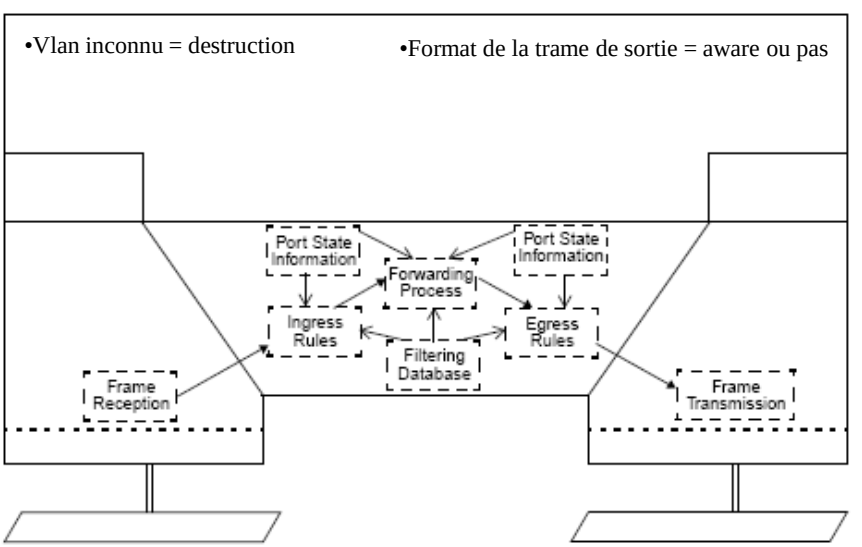
- *Switch IVL (Independant Vlan) et SVL (Shared Vlan)*

Ajout de 4 octets (ProtoID, Priorité, nVLAN)

Ethernet : VLANS

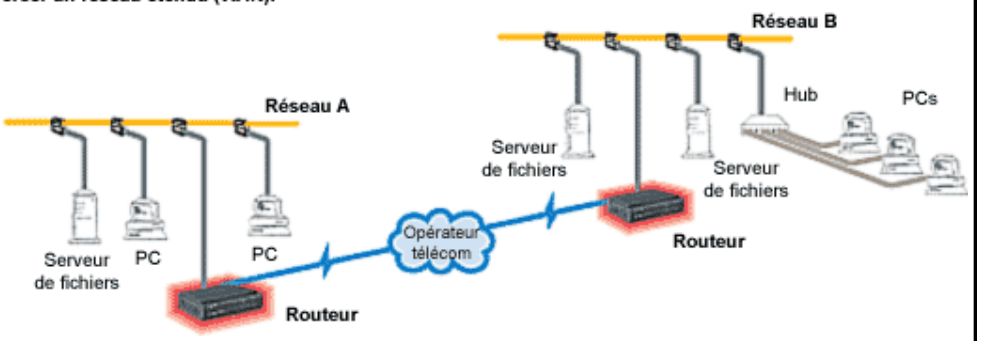
•Vlan inconnu = destruction

•Format de la trame de sortie = aware ou pas



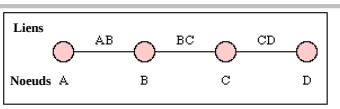
Interconnexion de réseaux

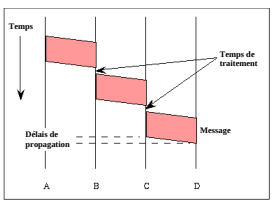
Routeurs et ponts interconnectent plusieurs réseaux locaux (LAN) pour créer un réseau étendu (WAN).



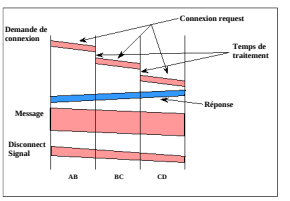
- Niveau 3 VS Niveau 2
- Routeurs (gateway, …)

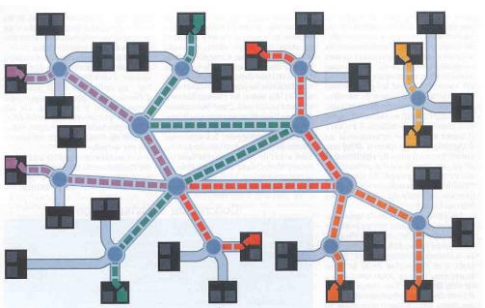
Circuits Virtuels VS Datagrammes

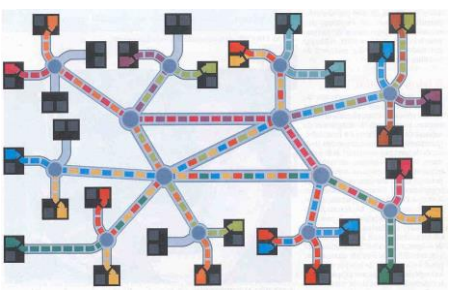




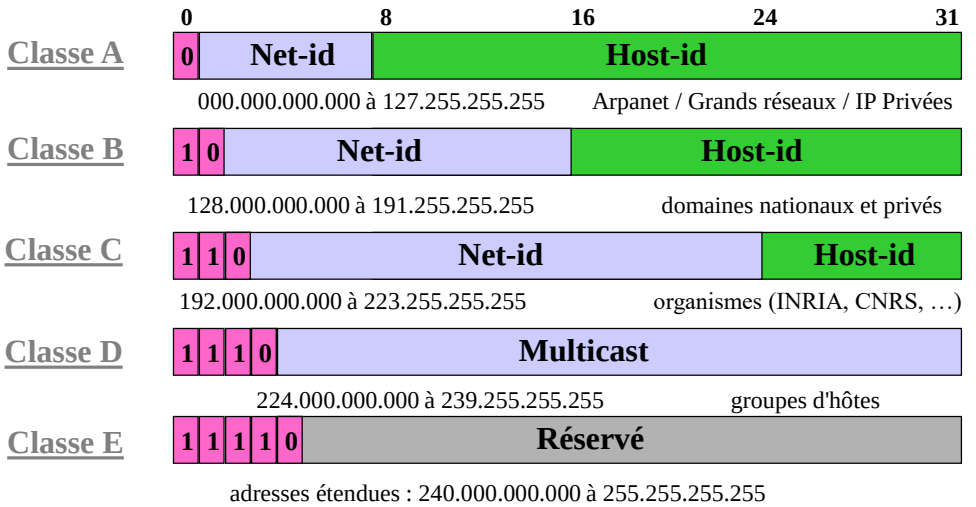
ATM vs IP
Commutation vs routage







L'adressage IPv4



L'adressage IPv4

- Notation décimale

  L'interface utilisateur concernant les adresses IP consiste en la notation de quatre entiers décimaux séparés par un «.», chaque entier représentant un octet de l'adresse :

  10000000 00001010 00000010 00011110 est écrit : 128.10.2.30

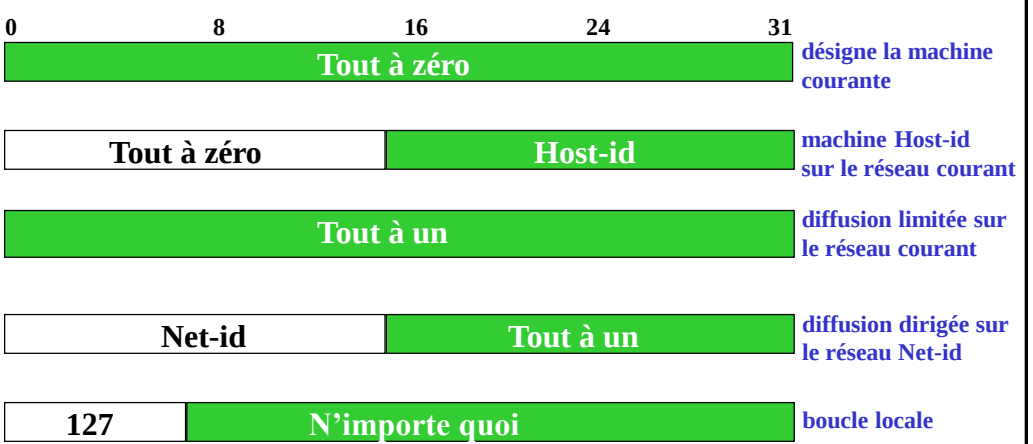
- Adresses particulières
  - Adresses réseau : adresse IP dont la partie hostid ne comprend que des zéros; => la valeur zéro ne peut être attribuée à une machine réelle : 191.20.0.0 désigne le réseau de classe B 191.20.
  - Adresse machine locale : adresse IP dont le champ réseau (netid) ne contient que des zéros;
  - Adresses **IP privées** : RFC 1597/1918
    - Classe A : 10.X.X.X
    - Classe B : 172.[16→31].X.X
    - Classe C : 192.168.X.X

L'adressage IPv4

- Adresses de diffusion : la partie hostid ne contient que des 1
- L'adresse de diffusion dirigée : netid est une adresse réseau spécifique => la diffusion concerne toutes les machines situées sur le réseau spécifié : 191.20.255.255 désigne toutes les machines du réseau 191.20.
- En conséquence, une adresse IP dont la valeur hostid ne comprend que des 1 ne peut être attribuée à une machine réelle.
- Adresse de boucle locale : l'adresse réseau 127.0.0.0 est réservée pour la désignation de la machine locale, c'est à dire la communication intra-machine. Une adresse réseau 127 ne doit, en conséquence, jamais être véhiculée sur un réseau et un routeur ne doit jamais router un datagramme pour le réseau 127.
- Adresse Loopback = 127.0.0.1 "localhost" interne à la machine .

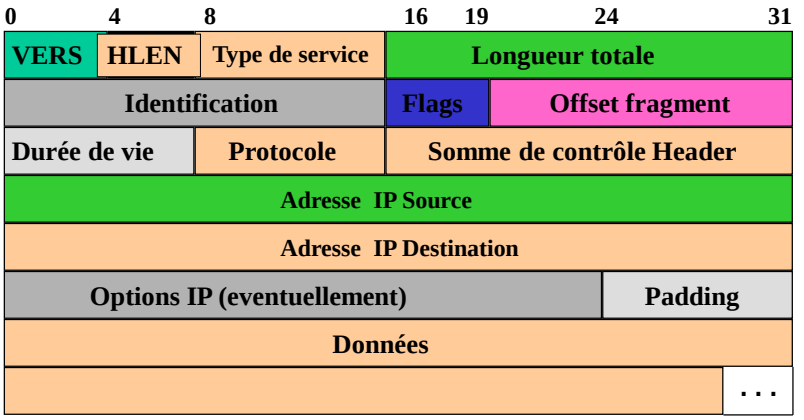
L'adressage IPv4

- Résumé



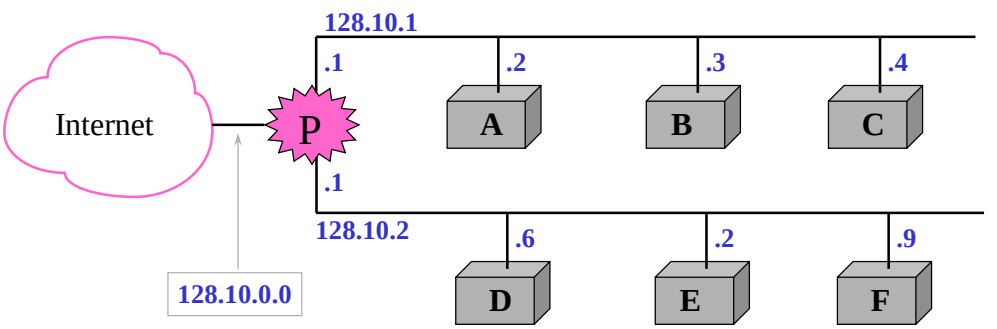
IPv4 : le datagramme

• Le datagramme IP : L'unité de transfert de base dans un réseau internet est le datagramme qui est constituée d'un en-tête et d'un champ de données:



Le sous-adressage

Les sous-réseaux 128.10.**1.**0 et 128.10.**2.**0 sont différenciés via la valeur du 3e octet de l'adresse → **Subdivision de la partie Host**



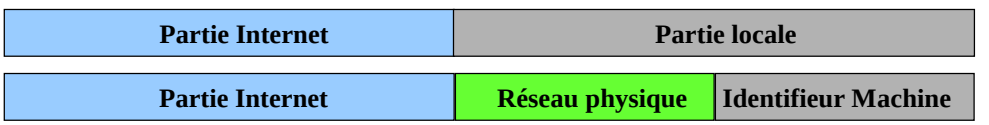
Un site avec deux réseaux physiques doivent utiliser le sous-adressage de manière à ce que ses deux sous-réseaux soient couverts par une seule adresse IP de **classe B (128.10)**.
La passerelle P accepte tout le trafic destiné au réseau 128.10.0.0 et sélectionne le sous-réseau en fonction du troisième octet de l'adresse destination.

Le sous-adressage

- Le site utilise une seule adresse pour les deux réseaux physiques.
- A l'exception de P, toute passerelle de l'internet route comme s'il n'existait qu'un seul réseau.
- La passerelle doit router vers l'un ou l'autre des sous-réseaux ; le découpage du site en sous-réseaux a été effectué sur la base du troisième octet de l'adresse :
  - les adresses des machines du premier sous-réseau sont de la forme 128.10.1.X,
  - les adresses des machines du second sous-réseau sont de la forme 128.10.2.X.
- Pour sélectionner l'un ou l'autre des sous-réseaux, P examine le troisième octet de l'adresse destination : si la valeur est 1, le datagramme est routé vers réseau 128.10.1.0, si la valeur est 2, il est routé vers le réseau 128.10.2.0.

Le sous-adressage

- Conceptuellement, la partie locale dans le plan d'adressage initial est subdivisée en "partie réseau physique" + "identification de machine (hostid) sur ce sous-réseau" :



- «Partie Internet» correspond au NetId (plan d'adressage initial)
- «Partie locale» correspond au hostid (plan d'adressage initial)
- les champs «Réseau physique» et «identifieur Machine» sont de taille variable; la longueur des 2 champs étant toujours égale à la longueur de la «Partie locale».
- **Le découpage [sous-réseau – host] est spécifié par le Masque de sous-réseau**

Le sur-adressage (RFC 1517-1520)

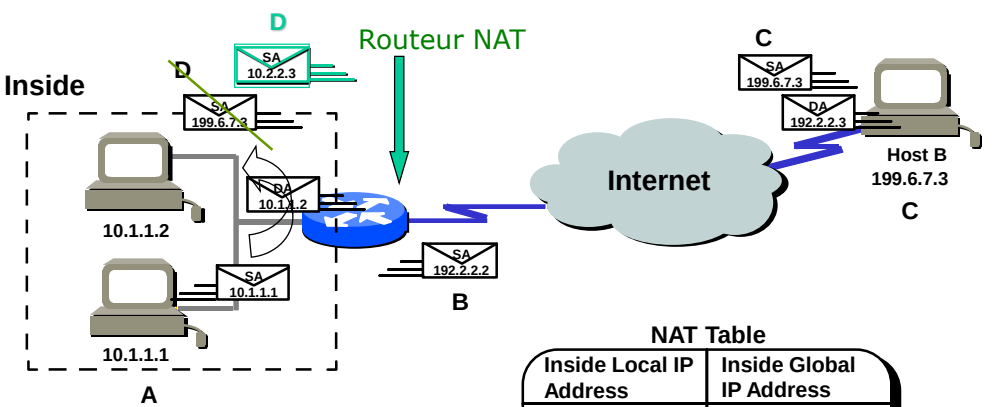
- Idem sous adressage mais sur la partie Net id
  → On concatène des réseaux (de classes C souvent)
- **CIDR = Classless Inter-Domain Routing**
  → Notation : Adresse IP / Prefix → 192.33.11.0/22

Partie Internet	Partie locale

Partie Internet	Sur Réseau	Identifieur Machine

- «Partie Internet» correspond au NetId (plan d'adressage initial)
- «Partie locale» correspond au hostid (plan d'adressage initial)
- les champs «Sur-reseau» est toujours de taille faible. Il permet d'ignorer les derniers bit de la partie Net-Id
- PB pour le routage mais OK pour RIPv2, OSPF, BGPv4

NAT : Inside vs Outside

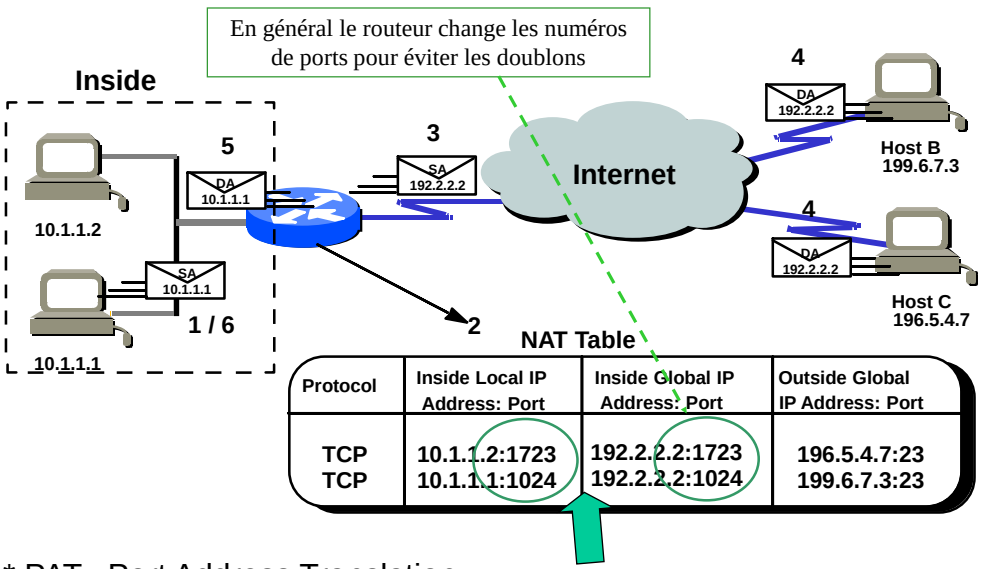


NAT Table

Inside Local IP Address	Inside Global IP Address
10.1.1.2	192.2.2.3
10.1.1.1	192.2.2.2

- Inside Local IP Address A
- Inside Global IP Address B
- Outside Global IP Address C
- Outside Local IP Address D / D

Surcharge des adresses internes globales ou PAT ("overloading")



* PAT : Port Address Translation → **1 IP Globale pour 2 machines internes**

Le routage

- **Les principaux algorithmes :**
  - **Notion de systèmes Autonomes**
  - **Type IGP**
    - Type Vecteur de distance : **RIP** : simple mais quelques risques
      Table Locale = Destinataire, Nœud suivant, Coût
    - Type Etat de liaisons : **OSPF** : robuste mais complexe
      Table Globale = Liaison, Coût
  - **Type EGP**
    - Lien entre systèmes autonomes : **GGP** (gateway gateway Protocol) , **EGP** , **BGP**
  - **Routage et ISO : Dual IS-IS-ES** (Intermediate/End System)
  - Interdomain Routing Protocol (IDRP)

Tables de routage

- Une table de routage est une liste où chaque élément possède 4 entrées
  - Target : une adresse IP
  - Prefix-length : la longueur du préfix réseau applicable
  - Next-hop : une adresse IP
  - Interface : une référence vers une interface physique permettant d'accéder à un lien

TARGET	PREFIX LENGTH	NEXT-HOP	INTERFACE

Le routeur cherche les entrées qui « match » l'adresse destination.

Matching dans une table de routage

- Pour chaque entrée dans une table de routage, il y a un « match » si les PREFIX-LENGTH bits les plus à gauche du champ Destination Address et de la colonne TARGET sont identiques
- Lorsqu'il y a plusieurs match dans une table, le protocole IP spécifie que le match avec le plus long préfixe est utilisé pour router
- Lorsque le routage a été résolu, le paquet IP est envoyé sur l'interface correspondante au nœud dont l'adresse IP est indiqué en NEXT-HOP
- Le champ NEXT-HOP peut être l'adresse d'un routeur plus « proche » de la destination ou une indication signalant que le nœud destination est directement connecté sur le lien correspondant à l'interface.

Exemple de table de routage

- Paquet IP à router : Destination Address = 7.7.7.1

TARGET/PREFIX-LENGTH	NEXT-OP	INTERFACE
7.7.7.99/32	IP Router 1	A
7.7.7.0/24	IP Router 2	B
0.0.0.0/0	IP Router 3	B

- Première entrée : 32 bits de préfix = adresse complète
- Seconde entrée : 24 bits de préfix, c'est-à-dire 7.7.7 Match !
- Troisième entrée : 0 bits de préfix, donc Match à tout le coup !
  - C'est l'entrée 2 qui match avec le plus grand préfixe !

Les trois types d'entrées

- Dans une table de routage, il y a trois types d'entrées
  - Les *host-specific*, avec un préfixe de 32 bits
  - Les *network-prefix*, dont le PREFIX-LENGTH est compris entre 1 et 31
  - La *default* route, qui correspond à un préfixe de longueur nulle et qui accepte donc tout les paquets, tout en étant moins prioritaire que n'importe quel autre « match »
- S'il n'y a aucun « match », et donc aucune route default, le router émet un paquet ICMP Unreachable au nœud source de ce paquet.

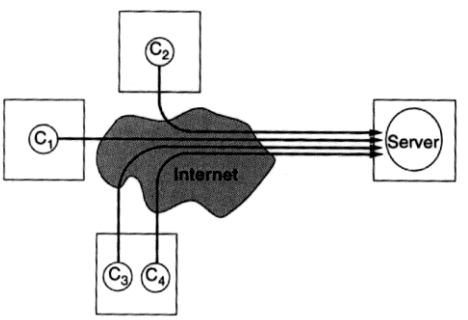
Algorithme simplifié du routage IP

Route_Datagramme_IP(datagramme, table_de_routage)

- Extraire l'adresse IP destination, ID, du datagramme,
- Calculer l'adresse du réseau destination, IN.
- Si IN correspondant à une adresse de réseau directement accessible,
  envoyer le datagramme vers sa destination, sur ce réseau.
- sinon si dans la table de routage, il existe une route vers ID
  router le datagramme selon les informations contenues dans la table de routage.
- sinon si IN apparaît dans la table de routage,
  router le datagramme selon les informations contenues dans la table de routage.
- sinon s'il existe une route par défaut
  router le datagramme vers la passerelle par défaut.
- sinon déclarer une erreur de routage.

UDP et TCP

- Protocole de transport plus ou moins fiable.
  - transferts tamponés : découpage en segments
  - connexions bidirectionnelles et simultanées
- service en mode connecté ou non
- Notion de ports (client - serveur)



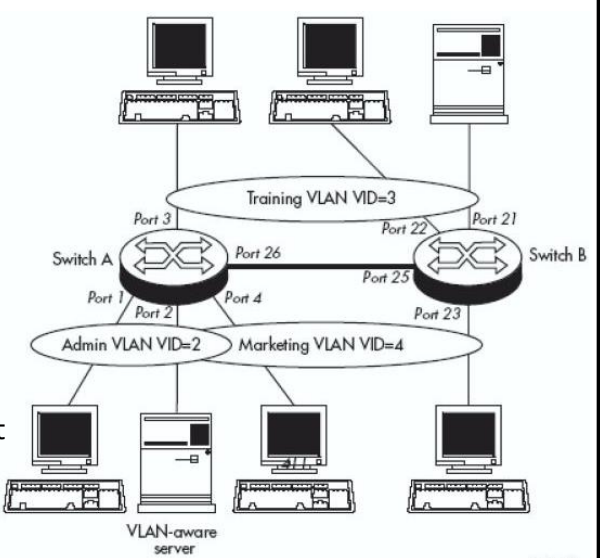
Protocoles : Exemples

Famille	Nom	Client	Serveur	Port
Courrier	SMTP	Sendmail	Sendmail	25
	POP3	Eudora	Popper	110
	IMAP	Eudora	Imapd	143
Transfert de fichiers	FTP	ftp	Ftpd	20/21
Forums	NNTP	Tin	Nntpd	119
Web	HTTP	Netscape	Httpd	80
Conversion IP/Nom	DNS	Resolver	BIND in.named	42/udp

Ports réserves =< 1024 - Ports libres > 1024

Exercice Config IP + VLAN

- Commentez l'architecture réseau décrite. On précisera notamment les différents VLAN mis en place, leur type, l'intérêt de ce découpage, les PC et ports appartenant à chacun des VLAN, …
- Vous discuterez aussi des problèmes de l'appartenance d'une machine à plusieurs VLAN et du cas particulier des ports 25 et 26.
- Donnez IP locales + DHCP + DNS + …



Routage RIP ? OSPF ?

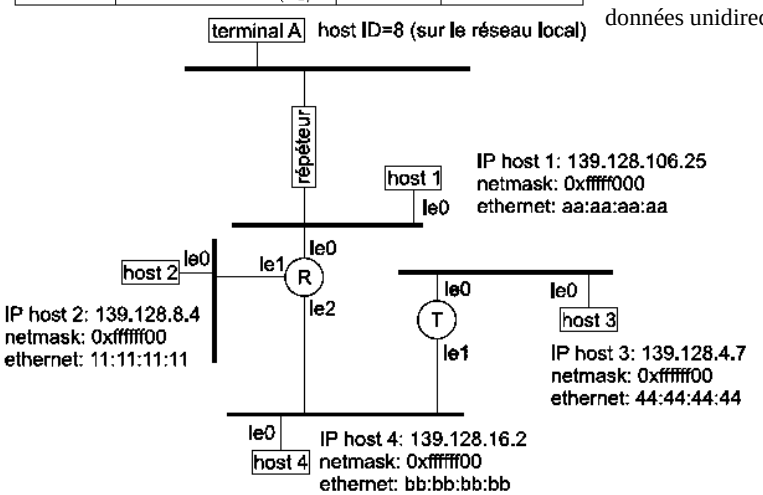
Destination = 10.1.8.66 0100 0010

N°	Destination	Masque	Routeur	Métrique
1	0.0.0.0	/0	10.1.3.65	1
2	10.1.0.0	/16	10.1.3.65	1
3	10.1.3.0	/26	10.1.3.1	0
4	10.1.3.64	/26	10.1.3.126	0
5	10.1.3.128	/26	10.1.3.190	0
6	10.1.3.192	/26	10.1.3.254	0
7	10.1.4.0	/26	10.1.3.4	11
8	10.1.4.64	/26	10.1.3.4	9
9	10.1.4.128	/26	10.1.3.4	10
10	10.1.16.64	/26	10.1.3.65	5
11	10.1.8.0	/24	10.1.3.65	6
12	10.1.8.0	/26	10.1.3.65	9
13	10.1.8.64	/26	10.1.3.65	17
14	10.1.8.64	/26	10.1.3.62	22
15	10.1.8.128	/26	10.1.3.65	25

Interface	IP	Netmask	Ethernet
routeur R			
le0	139.128.106.26 (R_0)	0xffffff000	01:01:01:01
le1	139.128.8.5 (R_1)	0xffffff00	02:02:02:02
le2	139.128.16.3 (R_2)	0xffffff00	03:03:03:03
routeur T			
le0	139.128.4.8 (T_0)	0xffffff00	04:04:04:04
le1	139.128.16.4 (T_1)	0xffffff00	05:05:05:05

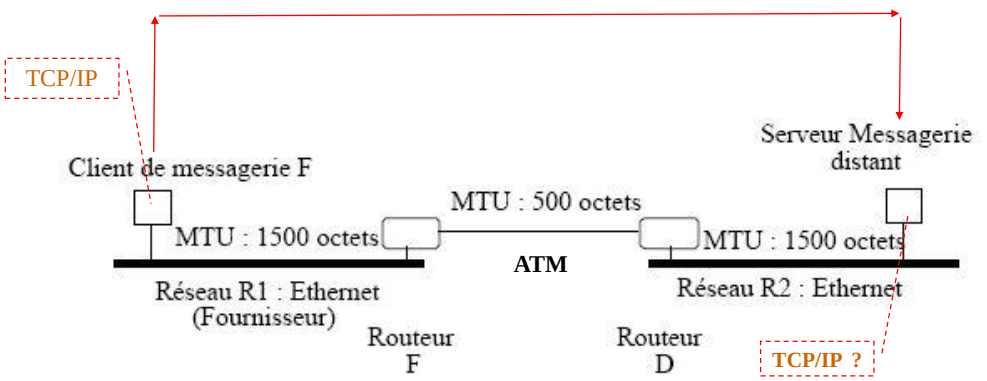
•1. Donnez l'adresse IP du terminal *A*.

•2. Donnez les champs d'adresses source et destination dans les en-têtes Ethernet et IP quand on considère un transfert de données unidirectionnel host 3 → host 1.

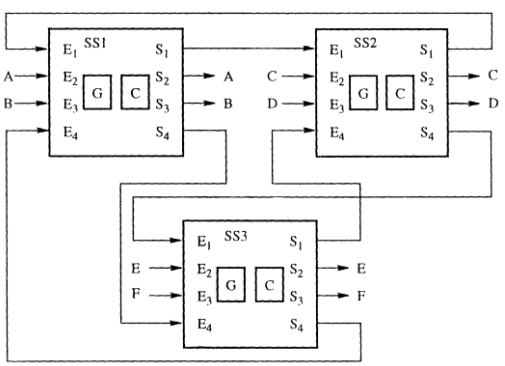


MTU ? IP ? TCP ? ARP ? OSI ?

Envoi d'un 7_PDU de 4000 octets



Commutation de circuit ?



[3,Données] envoyé par A ?

$DLCI_{msg}$ / Voie	1 (S_i,$DLCI_{sortie}$)	2 (S_i,$DLCI_{sortie}$)	3 (S_i,$DLCI_{sortie}$)	4 (S_i,$DLCI_{sortie}$)	5 (S_i,$DLCI_{sortie}$)
E_1	2,1	3,1	4,5	3,3	4,3
E_2	1,1	1,2	4,1	4,2	3,10
E_3	4,4	1,4	4,3	2,47	
E_4	2,2	3,2	1,6	4,6	

$DLCI_{message}$ / Voie	1 (S_i,$DLCI_{sor-tie}$)	2 (S_i,$DLCI_{sor-tie}$)	3 (S_i,$DLCI_{sor-tie}$)	4 (S_i,$DLCI_{sor-tie}$)	5 (S_i,$DLCI_{sor-tie}$)
E_1	2,1	3,1	1,5	4,5	4,2
E_2	1,1	1,2	4,1	3,12	
E_3	1,3	1,4	2,3	4,4	
E_4	2,2	2,8	1,6	2,12	

$DLCI_{message}$ / Voie	1 (S_i,$DLCI_{sor-tie}$)	2 (S_i,$DLCI_{sor-tie}$)	3 (S_i,$DLCI_{sor-tie}$)	4 (S_i,$DLCI_{sor-tie}$)	5 (S_i,$DLCI_{sor-tie}$)
E_1	2,1	3,1	1,5	4,5	3,3
E_2	1,1	2,2	4,1	4,2	
E_3	1,3	1,4	4,3	4,4	
E_4	1,2	3,2	2,18	1,4	

Chapitre 1

Réseaux sans fil :

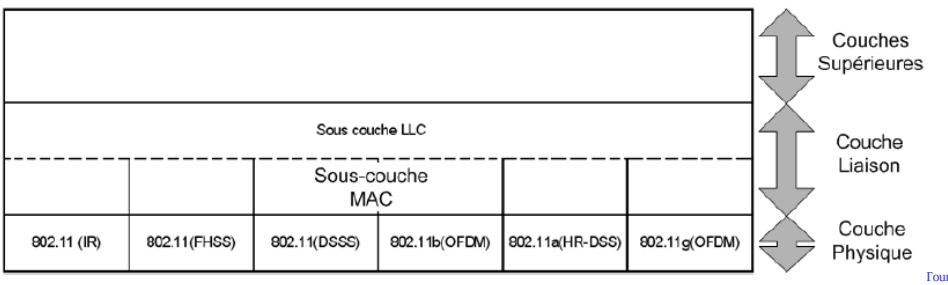
Wifi (802.11), Bluetooth (802.15), …

WiFi = *Wireless Fidelity*

- Ensemble de standards internationaux décrivant les caractéristiques et les modes de fonctionnement d'un réseau local sans fil (*WLAN*)
  - Géré par le groupe IEEE → Normes 802.11xxx
  - Et le WECA (*Wireless Ethernet Compatibility Alliance*) : organisme chargé de maintenir l'interopérabilité entre les matériels
- Principales différences avec les autres réseaux
  - couche 1 (plusieurs normes) et MAC (2 normes)
  - Plus normes d'interopérabilités (wifi et wifi5) et de sécurité
  - Liaison haut débit sur un rayon de plusieurs dizaines de mètres en intérieur (généralement entre une vingtaine et une cinquantaine de mètres). Dans un environnement ouvert la portée peut atteindre plusieurs centaines de mètres.

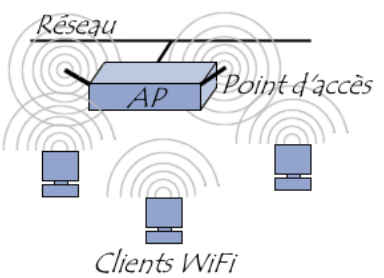
WiFi = *Wireless Fidelity*

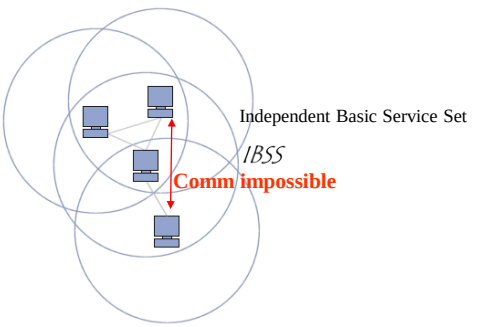
- **Couche Liaison de données (MAC)**
  - 802.2 (CSMA/CA ou *Point Coordination Function - PCF*)
- **Couche Physique(PHY)**
  - DSSS, FHSS, OFDM, …
  - Infrarouge, …
- **Incompatibles mais interopérables (via LLC)**



Modes opératoires

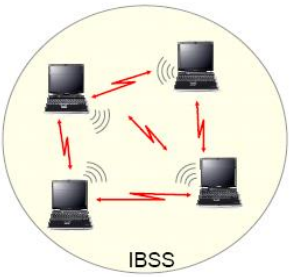
- Le standard 802.11 définit deux modes opératoires :
  - Le mode infrastructure (BSS et ESS) dans lequel les clients sans fil sont connectés à un point d'accès
  - Il s'agit généralement du mode par défaut des cartes 802.11b.
  - Le mode ad hoc (IBSS) dans lequel les clients sont connectés les uns aux autres sans aucun point d'accès

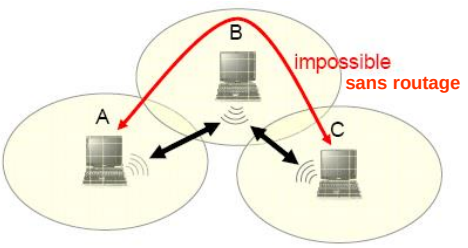


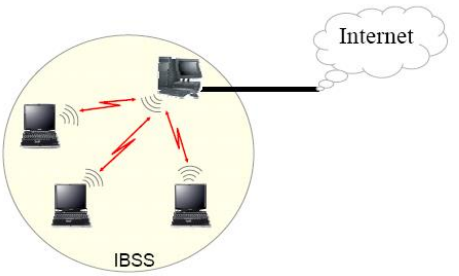


Mode ad-hoc (IBSS)

- Pas de point d'accès
  - Communication point à point entre station
  - Partage de connexion internet possible (fonctionne comme BSS)
  - Possibilité d'ajouter un protocole de routage par inondation (présent dans toutes les stations)





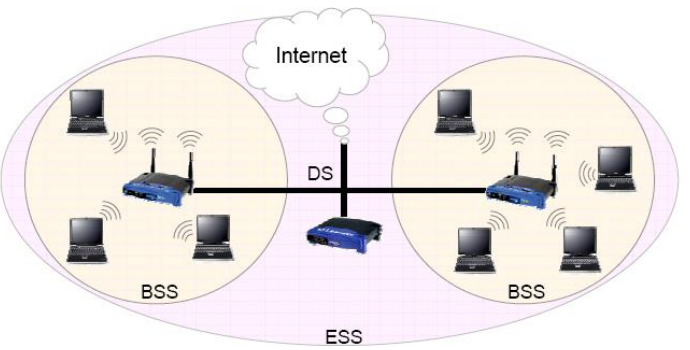


Mode Infrastructure (BSS)

- Un seul point d'accès (PA)
  - 1 cellule = 1 point d'accès = 1 Basic Service Set
  - 100 stations partagent le canal de communication et donc le débit
  - SSID = Adresse MAC du PA

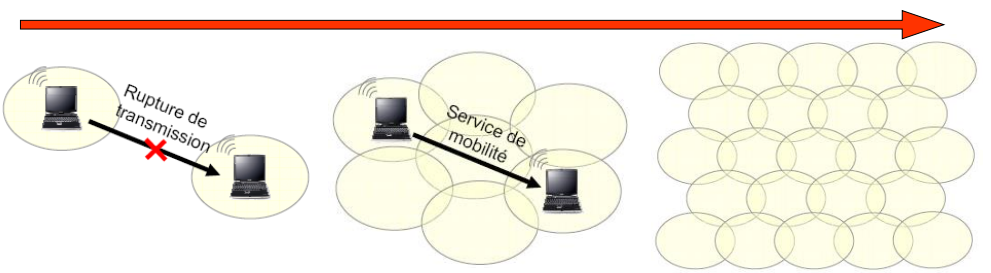
Mode Infrastructure (ESS)

- Plusieurs points d'accès (Extended)
  - Plusieurs Basic Service Set connectés entre eux par un système de distribution (DS)
  - DS : souvent ethernet ou autre WLAN
  - Sortie vers Internet possible
  - SSID = un nom de réseau



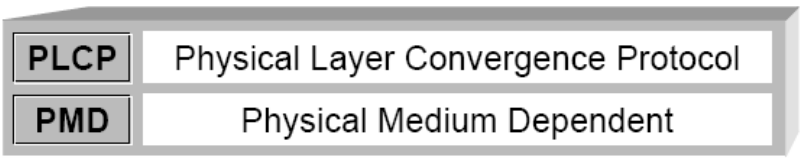
Mode Infrastructure (ESS)

- Plusieurs topologies ESS possibles
  - Cellules non recouvrantes
  - Cellules recouvrantes, Mode « Réseau ambiant »
  - Gestion d'un plus grands nombre de connexions sans perte de performance
  - Gestion de la mobilité (roaming - 802.11f) : échange d'info entre les BS via le DS pour éviter les coupures de comm.



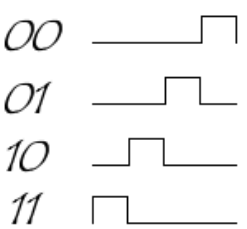
Couche Physique

- **Divisée en deux sous couches :**
  - PMD gére l'encodage des données et la modulation
  - PLCP gère l'écoute du canal et signale à la couche MAC la disponibilité du canal par un CCA (Clear Canal Assessment)



Transmission Infrarouge

- une onde lumineuse en "vue directe" ou par réflexion.
- Le caractère non dispersif des ondes lumineuses offre un niveau de sécurité plus élevé.
- Il est possible grâce à la technologie infrarouge d'obtenir des débits allant de 1 à 2 Mbit/s en utilisant une modulation appelé **PPM** (*pulse position modulation*).
- La modulation *PPM* consiste à coder l'information suivant la position de l'impulsion.
- Le débit de 1 Mbps est obtenu avec une modulation de *4-PPM*, le débit de 2 Mbps est obtenu avec une modulation *16-PPM* :



Peu utilisé pour le WIFI

Transmission radio

- **Gestion des bandes !**

- Les gouvernements sont en général le régulateur de l'utilisation des bandes de fréquences
- ils proposent des bandes de fréquence pour une utilisation libre, c'est-à-dire ne nécessitant pas de licence de radiocommunication.

- Les organismes chargés de réguler l'utilisation des fréquences radio sont :
  - l'ETSI (*European Telecommunications Standards Institute*) en Europe
  - la FCC (*Federal Communications Commission*) aux Etats-Unis
  - le MKK (*Kensa-kentei Kyokai*) au Japon

- Bandes ISM :
  - En 1985 les Etats-Unis ont libéré 3 bandes de fréquence à destination de l'Industrie, de la Science et de la Médecine
  - *902-928 MHz*, *2.400-2.4835 GHz*, *5.725-5.850 GHz*.
- En Europe
  - la bande s'étalant de *890 à 915 MHz* est utilisée pour les communications mobiles (*GSM*)
  - Seules les bandes *2.400 à 2.4835 GHz* et *5.725 à 5.850 GHz* sont disponibles

Transmission radio

- Problèmes et contraintes :
  - Le partage de la bande passante entre les différentes stations présentes dans une même cellule → Création de canaux (multiplexage en fréquences et temps)
  - La propagation par des chemins multiples d'une onde radio (différentes direction, réfléchie ou réfractés réception multiples de mêmes informations ayant emprunté des cheminements différents
  - Chevauchement de cellules (en mode ESS) !

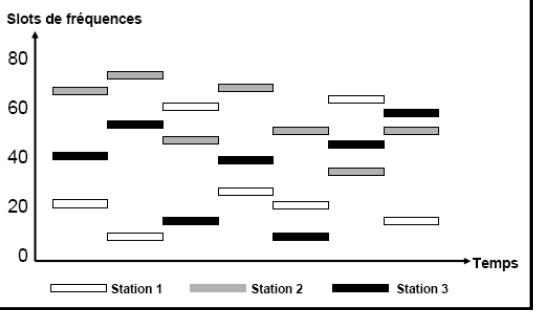
- Plusieurs solutions techniques :
  - La technique de l'étalement de spectre à saut de fréquence
  - La technique de l'étalement de spectre à séquence directe
  - …

FHSS (*Frequency Hopping Spread Spectrum)*

– *Etalement de spectre par sauts de fréquences*

- Dans la norme 802.11, la bande de fréquence *2.4 - 2.4835 GHz* permet de créer 79 canaux de 1 MHz (*hops* = *sauts* de largeur 1MHz)
- Transmission en utilisant une combinaison de canaux connue de toutes les stations de la cellule = Envois sur un canal puis sur un autre pendant une courte période de temps (400 ms)
- originalement conçue dans un but militaire afin d'empêcher l'écoute
- réduire les interférences entre les stations d'1 cellule

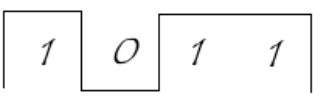
- Débit pas très élevés (1 ou 2Mb/s)
- Résistant aux interférences
- Taux d'erreurs assez important
- Cout faible

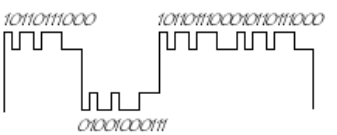


DSSS (*Direct Sequence Spread Spectrum*)

– Etalement de spectre à séquence directe

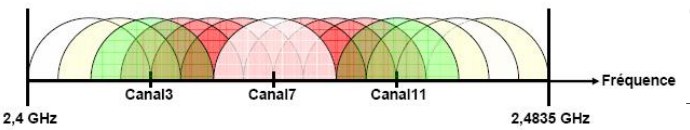
- Technique (appelée *chipping*) de modulation de chaque bit par une séquence appelée *Barker*.
- *Barker* = séquence de bits (*bruit pseudo-aléatoire*)
- Chaque bit valant 1 est remplacé par la séquence et chaque bit valant 0 par son complément.
- La norme 802.11 définit une séquence de 11 bits (*10110111000*) pour représenter un 1 et son complément (*01001000111*) pour coder un 0.
- On appelle *chip* ou *chipping code* (*puce*) chaque bit encodé à l'aide de la séquence (XOR).

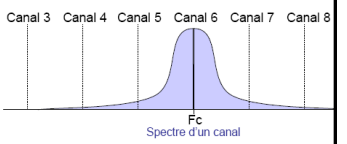




DSSS (*Direct Sequence Spread Spectrum*)

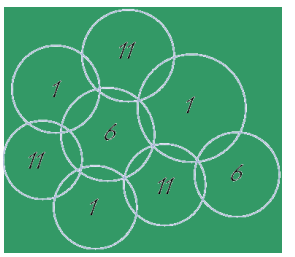
- *Etalement de spectre à séquence directe*
  - 14 canaux de 20MHz espacés de 5MHz





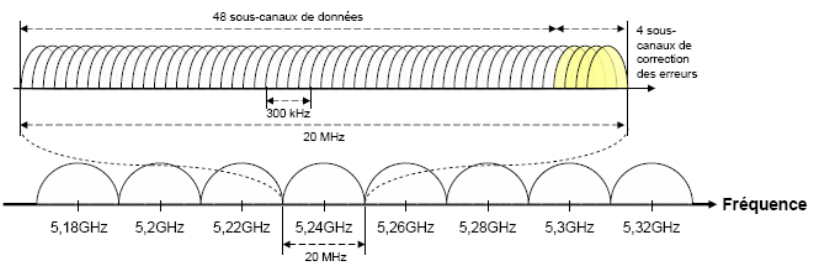
  - Canaux recouvrants inexploitables simultanément **(1 7 13 ou 1 6 11)**
  - Risque de chevauchement → Canaux différents

- Débit correct (jusqu'à 11Mb/s avec chip de 8 bits)
- Pas très résistant aux interférences
- Taux d'erreurs faibles (redondance)
- Cout élevé
- Norme la plus rependue (802.11b)



OFDM (*Orthogonal Frequency Division Mux*)

- Au départ, bande de fréquence différente UNII (5Ghz) → 802.11a
- 802.11g → Utilisation de la bande ISM
- Division de la bande en 8 canaux redécoupés en 52 sous-canaux de 300KHz → une transmission = 52 frequences = 48 data + 4 synchro
- Utilisation de tous les sous-canaux en parallèle lors d'une transmission
- Modulation BPSK à 0,125Mb/s par sous canal → 6Mb/s
- Modulation QAM64 à 1,125Mb/s par sous canal → 54Mb/s

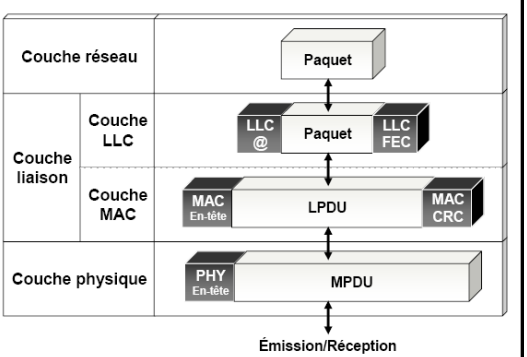


MIMO (Multiple In Multiple Out)

- Pas encore sortie officiellement (802.11n) ?
- Utilisation de plusieurs antennes / canaux simultanément
- Puissance plus élevée → Distance plus importante
- Débit prévu = 108 Mb/s
- Prix MIMO :
  - Routeur = 150 € - carte = 100 €

Couche 2 : MAC + LLC

- **Sous-couche LLC**
  - LSAP : Logical Service Access Point
  - Contrôle de flux
  - Reprise sur erreur
  - Type de LLC (avec/sans ACK, connexion)

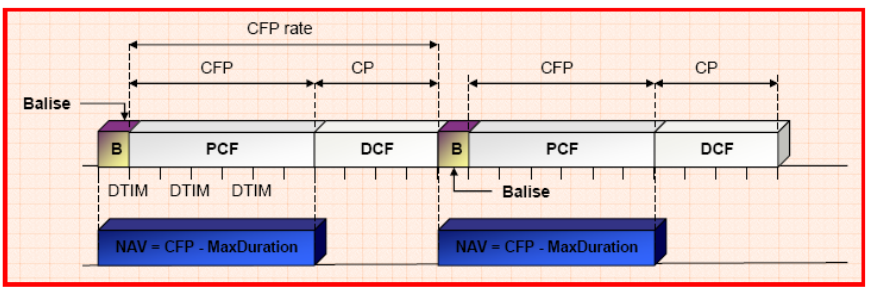


- **Sous-couche MAC**
  - Contrôle d'accès au canal
  - Contrôle d'erreur : CRC
  - Formatage, fragmentation, réassemblage
  - QoS : Sécurité, mobilité, énérgie

  - 2 modes : Point & Distributed Coordination Function

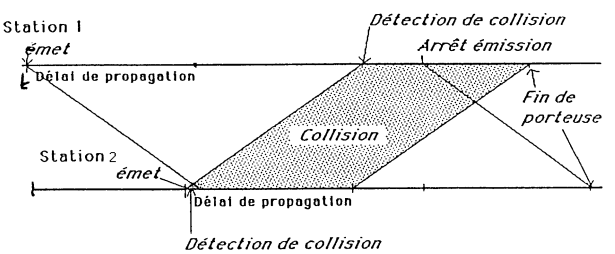
Point & Distributed Coordination Function

- Le point d'accès prend le contrôle du dialogue → Polling
  - Transfert isochrone (temps réel, voix, video, …)
- Mode mixte
  - Balisage et division du temps en 2 périodes :
  - DCF + PCF



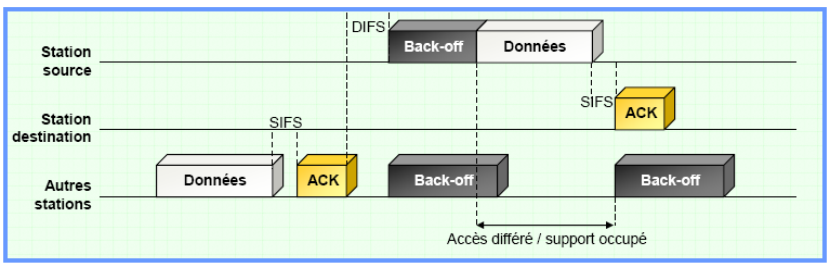
Distributed Coordination Function

- Basé sur CSMA /CA
  - Eviter les collisions en scrutant le canal
  - Accès aléatoire avec algorithme du Backoff → utilisation d'un timer
- Cf CSMA /CD (cours DI3)
  - Tranche canal (time-slot)



Distributed Coordination Function

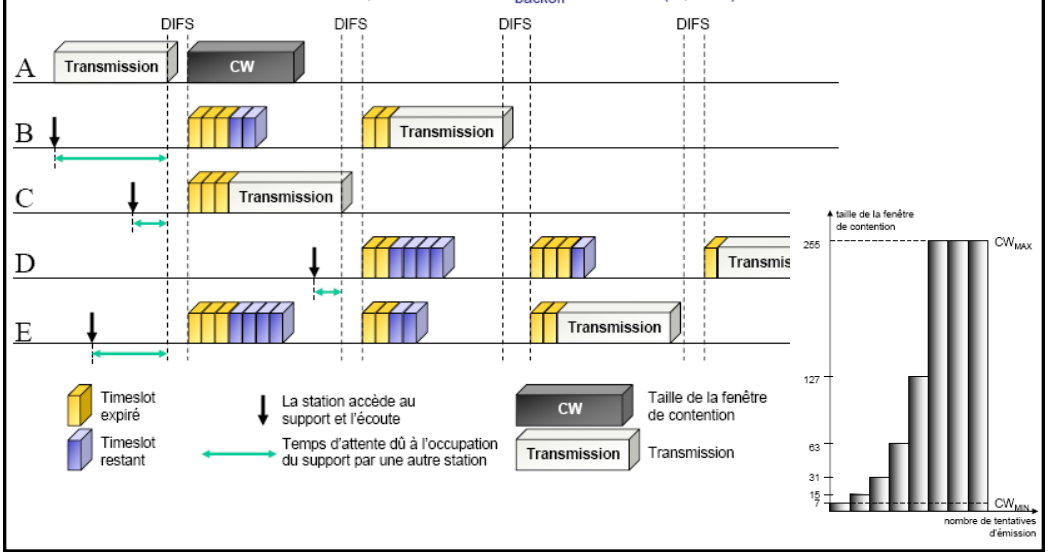
- CSMA /CA
  - Eviter les collisions en scrutant le canal
  - Attente aléatoire avant émission mais après la fin d'une émission
  - Espacement entre les trames (Inter Frame Spacing)
    - Short IFS : durant un dialogue entre 2 machines (entre DATA et ACK)
    - Double IFS : entre 2 dialogues
    - Extented IFS : en cas d'erreurs
  - Dialogue sans réservation



CSMA/CA & Fenêtre de contention

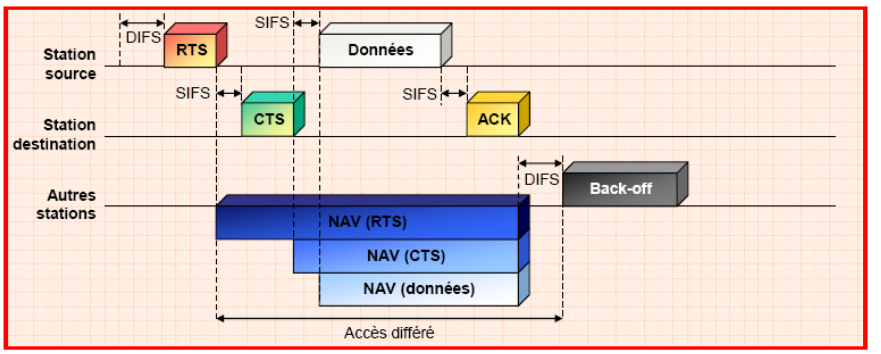
❖ **Algorithme du Backoff → utilisation d'un timer**

❖ fenêtre de contention CW, et un *timer* $T_{backoff}$=random(0,CW)×timeslot



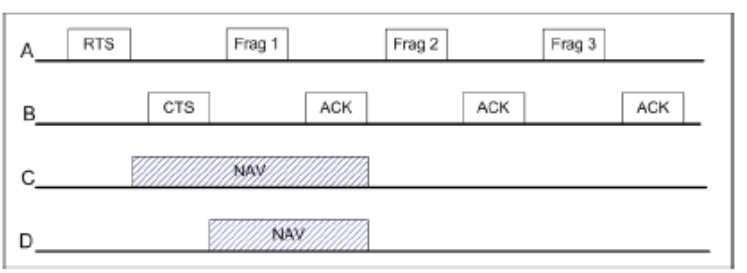
Distributed Coordination Function

- Dialogue avec réservation (optionnelle car chute du débit)
  - Trames RTS : demande d'autorisation avec délais de réservation
  - Trame CTS (autorisation)
  - Utilisation de timers NAV (network vector allocation) calculé par toutes les stations



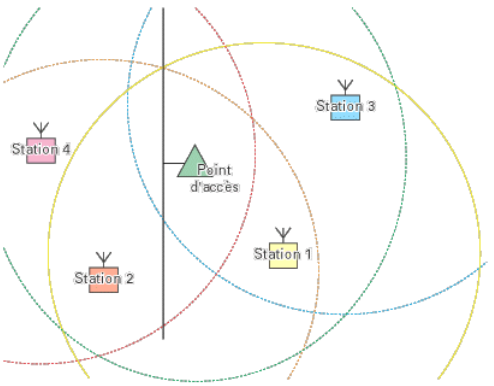
Distributed Coordination Function

- Fragmentation / réassemblage
  - Pour lutter contre le bruit
  - Chaque fragment est acquitté individuellement
  - Champs de contrôle dans la trame (cf IP)

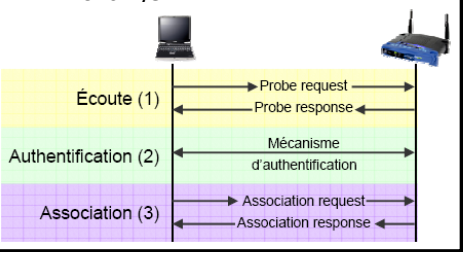


Distributed Coordination Function

- Autres problèmes
  - Chevauchement = Station cachée
  - ACK systématique



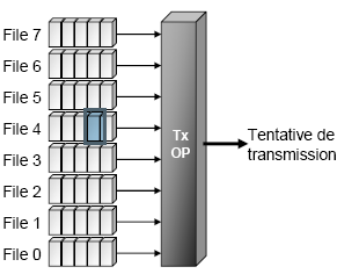
- ***Solution***
  - *Station = trame probe request (arrivée)*
  - PA = trame beacon (horloge)
  - Une station se trouvant à la portée de plusieurs points d'accès peut choisir le point d'accès offrant le meilleur compromis de débit et de charge



Fonctionnalités et services (QoS)

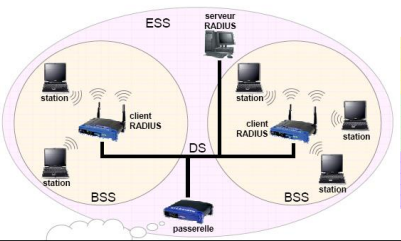
- Autres fonctionnalités
  - Variable rate shifting
  - Economie d'énergie
  - Gestion de priorités
    - Liste de priorités avec IFS spécifiques
  - Sécurité
    - Authentification (WEP)
    - Chiffrement

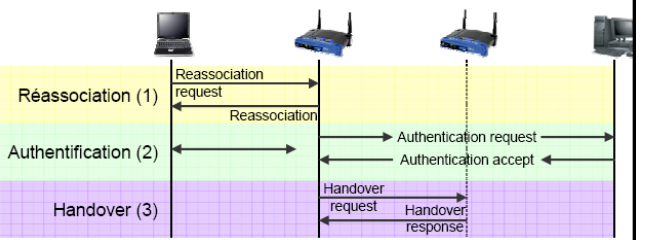
Vitesse (Mbits/s)	Portée à l'intérieur	Portée à l'extérieur
11	50 m	200 m
5,5	75 m	300 m
2	100 m	400 m
1	150 m	500 m



Fonctionnalités et services (QoS)

- Mobilité (Roaming)
  - Changement transparent de PA en fonction de la charge, taux d'erreurs, puissance du signal
  - Via un procédé de Handover possible mais non définit dans les normes de base
  - Protocole IAPP : Inter Access Point Protocol (802.11f)
    - Niveau 4 (au dessus de UDP)
    - Utilise le protocole RADIUS pour l'authentification (Remote Authentification Dial in User Server)





Format des Trames

Version de protocole (2 bits)		Type (2 bits)		Sous-Type (4 bits)			
To DS (1 bit)	From DS (1 bit)	More Frag (1 bit)	Retry (1 bit)	Power Mgt (1 bit)	More Data (1 bit)	WEP (1 bit)	Order (1 bit)

MAC

Octets : 2	2	6	6	6	2	6	0 à 2312	4
Contrôle de trame	Durée/ ID NAV	Adresse 1	Adresse 2	Adresse 3	Contrôle de séquence	Adresse 4	Corps de la trame	FCS

En-tête MAC

Données de synchronisation 128 bits	Indicateur de début de trame 16 bits	Signal 8 bits	Service (réservé) 8 bits	Longueur 16 bits	CRC 16 bits

PLCP Préambule 144 bits	En-tête PLCP 48 bits	MPDU

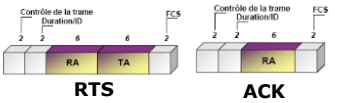
Changement éventuel de modulation

PPDU
PLCP Protocol Data Unit

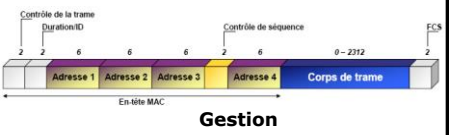
Physical Layer Convergence Protocol (dépend de la modulation, ici DSSS)

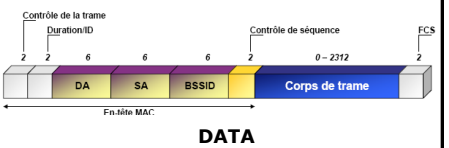
Type de trames & Adresses Wifi

- 3 types de trames
  - Contrôle (RTS,CTS, ACK)
  - Gestion (association, synchro, authentification)
  - Données



- Adresses Unicast, Multicast, Broadcast
- 5 types d'adresses :
  - DA : Destination de la trame
  - SA : Source de la trame
  - TA : Source des données
  - RA : Destination des données
  - BSSID (@MAC ou nom de reseau)

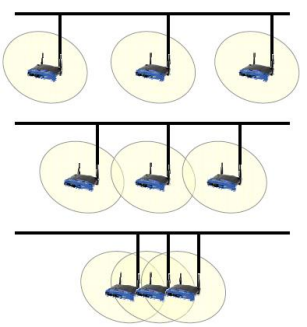




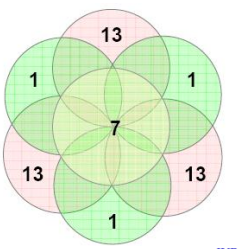
To DS	From DS	Adresse 1	Adresse 2	Adresse 3	Adresse 4
0	0	DA	SA	BSSID	Aucun
0	1	DA	BSSID	SA	Aucun
1	0	BSSID	SA	DA	Aucun
1	1	RA	TA	DA	SA

Mise en place

- **Choix de la topologie et de la position des PA**
  - Zones non recouvrantes
    - Pas d'interférences
    - Pas de mobilité
  - Recouvrement faibles
    - Exploitation de l'espace
    - Mobilité
  - Recouvrement forts
    - Nombre d'utilisateurs importants
    - Configuration plus complexe

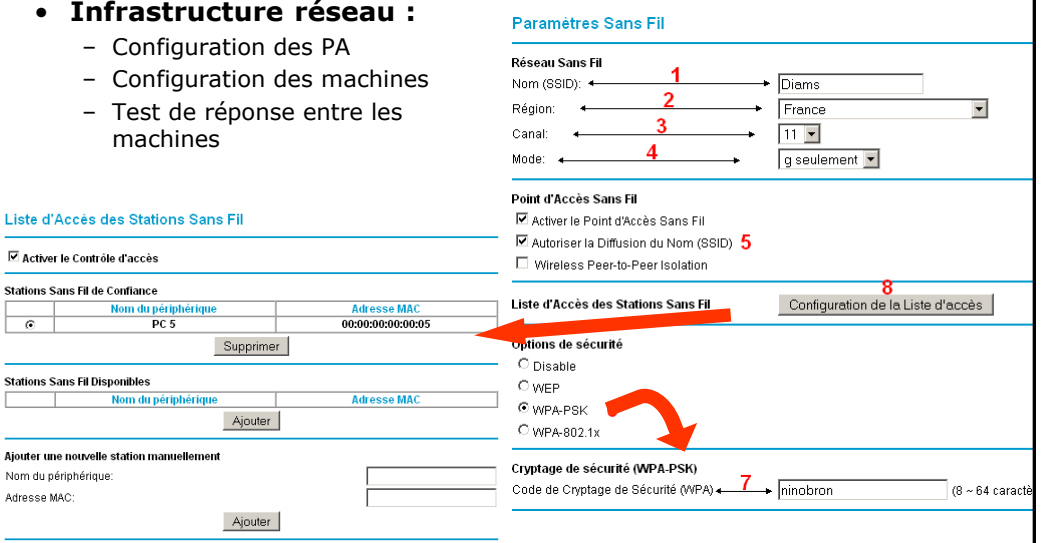


- **Affectation des canaux**
  - Zones recouvrantes → 14 canaux en DSSS mais seuls 3 exploitables simultanément !



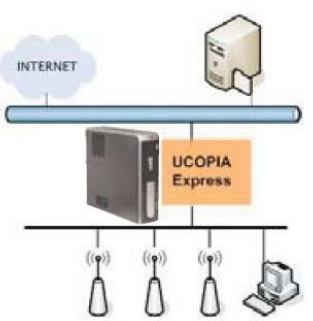
Mise en place

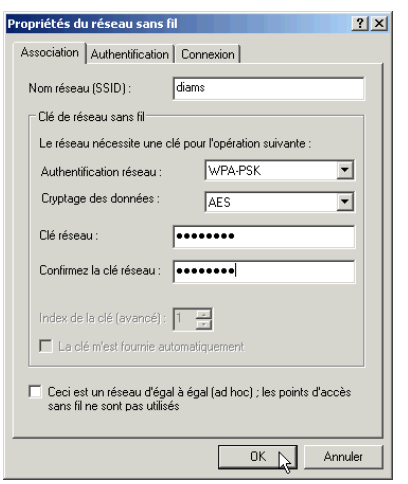
- **Infrastructure réseau :**
  - Configuration des PA
  - Configuration des machines
  - Test de réponse entre les machines



Mise en place

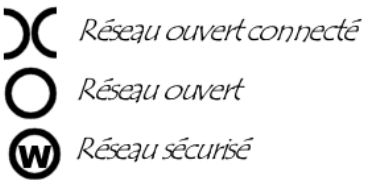
- **Infrastructure réseau :**
  - Configuration des PA
  - Configuration des machines
  - Test de réponse entre les machines
  - Lien avec l'infrastructure réseau (DHCP, DNS, Passerelle, …)
  - Outils d'administration :
    - Serveurs d'authentification :RADIUS, ucopia
    - Filtrage, VPN, VLAN …





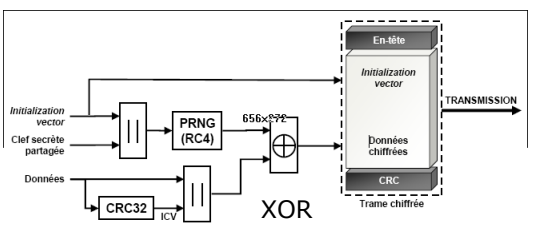
Sécurité … A améliorer…

- Les risques liés à la mauvaise protection d'un réseau sans fil sont multiples :
  - L'interception de données consistant à écouter les transmissions des différents utilisateurs du réseau sans fil
  - Le détournement de connexion dont le but est d'obtenir l'accès à un réseau local ou à internet
  - Le brouillage des transmissions consistant à émettre des signaux radio de telle manière à produire des interférences
  - Les dénis de service rendant le réseau inutilisable en envoyant des commandes factices
- Parades :
  - Pas de valeurs par défaut
  - Filtrage MAC par ACL
  - WEP - Wired Equivalent Privacy
  - VPN

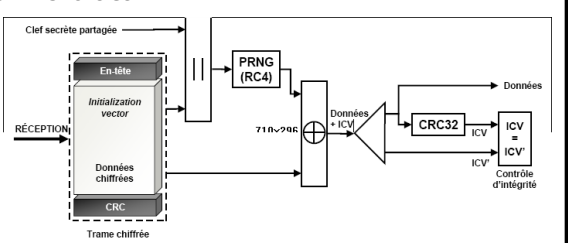


WEP Wired Equivalent Privacy

- Repose sur RC4 :
  - 4 Clés secrètes partagées
  - Vecteur d'initialisation (*IV*)
  - Intégrité vérifiée via CRC !



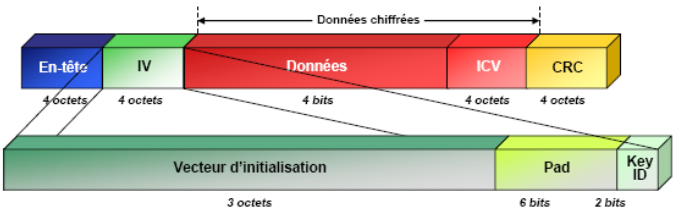
- Failles
  - Taille des clés **(104b = 26 symboles hexa) → Clé WEP cassable en qq secondes (cf Airsnort et Aircrack)** !
  - *IV* transmis (24b)
  - Usurpation d'adresse MAC
  - SSID transmis en clair



- Solutions
  - WEP+, WPA
  - WPA2 = 802.11i = utilisation d'AES

Trames chiffrée (WEP)

- Trame chiffrée partiellement



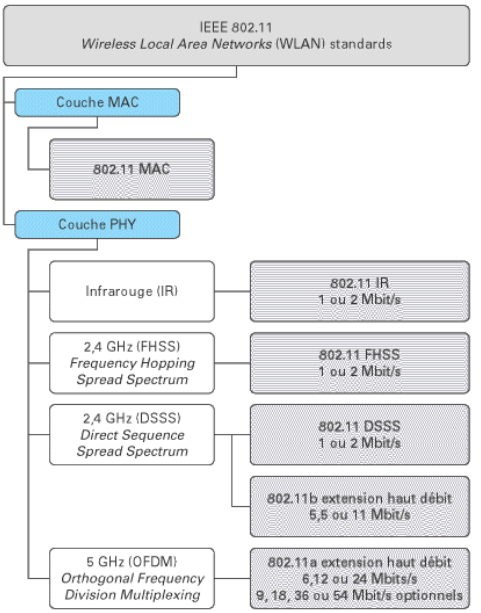
- **IV** : vecteur d'initialisation défini dans le WEP
- **Pad** : ne contient que des 0
- **Key ID** : valeur d'une des 4 clefs permettant de déchiffrer la trame

WPA Wireless Protected Access

- WPA repose sur RC4 aussi mais :
  - Clés de 128 bits secrètes partagées
  - Vecteur d'initialisation de 48 bits
  - Intégrité vérifiée via MIC au lieu de CRC32
  - Temporal Key Integrity Protocol (TKIP) = changement dynamique les clés (génération de sous-clés a partir d'une clé)
    - Avec un serveur de clés (serveur Radius, PKI)
    - Sans serveur → phrase secrète partagée

- WPA2 = 802.11i = repose sur l'utilisation d'AES et de fonction de hachage encore plus évoluée

Résumé des normes WiFi !



Norme *IEEE 802.11* (*ISO/IEC 8802-11*)

- **802.11a -** Wifi5
  - La norme 802.11a (baptisé *WiFi 5*) permet d'obtenir un haut débit (54 Mbps théoriques, 30 Mbps réels). Le norme 802.11a spécifie 8 canaux radio dans la bande de fréquence des 5 GHz.
- **802.11b -** Wifi
  - La norme 802.11b est la norme la plus répandue actuellement. Elle propose un débit théorique de 11 Mbps (6 Mbps réels) avec une portée pouvant aller jusqu'à 300 mètres dans un environnement dégagé. La plage de fréquence utilisée est la bande des 2.4 GHz, avec 3 canaux radio disponibles.
- **802.11c -** Pontage 802.11 vers 802.1d
  - La norme 802.11c n'a pas d'intérêt pour le grand public. Il s'agit uniquement d'une modification de la norme 802.1d afin de pouvoir établir un pont avec les trames 802.11 (niveau *liaison de données*).
- **802.11d -** Internationalisation
  - La norme 802.11d est un supplément à la norme 802.11 dont le but est de permettre une utilisation internationale des réseaux locaux 802.11. Elle consiste à permettre aux différents équipements d'échanger des informations sur les plages de fréquence et les puissances autorisées dans le pays d'origine du matériel.

Norme *IEEE 802.11* (*ISO/IEC 8802-11*)

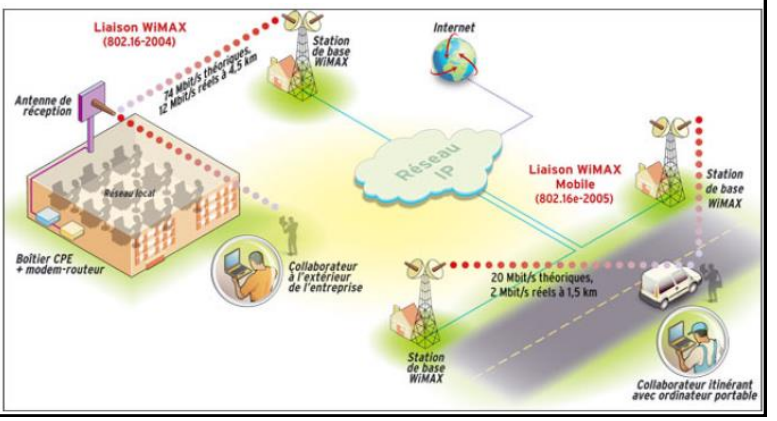
- **802.11e -** Amélioration de la qualité de service
  - La norme 802.11e vise à donner des possibilités en matière de qualité de service au niveau de la couche *liaison de données*. Ainsi cette norme a pour but de définir les besoins des différents paquets en terme de bande passante et de délai de transmission de telle manière à permettre notamment une meilleure transmission de la voix et de la vidéo.
- **802.11f -** Itinérance (roaming)
  - La norme 802.11f est une recommandation à l'intention des vendeurs de point d'accès pour une meilleure interopérabilité des produits. Elle propose le protocole *Inter-Access point roaming protocol* permettant à un utilisateur itinérant de changer de point d'accès de façon transparente lors d'un déplacement, quelles que soient les marques des points d'accès présentes dans l'infrastructure réseau. Cette possibilité est appelée *itinérance* (ou *roaming en anglais*)
- **802.11g**
  - La norme 802.11g offre un haut débit (54 Mbps théoriques, 30 Mbps réels) sur la bande de fréquence des 2.4 GHz. La norme 802.11g a une compatibilité ascendante avec la norme 802.11b, ce qui signifie que des matériels conformes à la norme 802.11g pourront fonctionner en 802.11b

Norme *IEEE 802.11* (*ISO/IEC 8802-11*)

- **802.11h**
  - La norme *802.11h* vise à rapprocher la norme 802.11 du standard Européen (HiperLAN 2, doù le *h* de 802.11h) et être en conformité avec la règlementation européenne en matière de fréquence et d'économie d'énergie.
- **802.11i**
  - La norme *802.11i* a pour but d'améliorer la sécurité des transmissions (gestion et distribution des clés, chiffrement et authentification). Cette norme s'appuie sur l'*AES* (*Advanced Encryption Standard*) et propose un chiffrement des communications pour les transmissions utilisant les technologies 802.11a, 802.11b et 802.11g.
- **802.11IR**
  - La norme *802.11ir* a été élaborée de telle manière à utiliser des signaux infra-rouges. Cette norme est désormais dépassée techniquement.
- **802.11j**
  - La norme *802.11j* est à la règlementation japonaise ce que le 802.11h est à la règlementation européenne.

Le futur ?

– **WiMax → 802.16 → WMAN**
  - Grandes distances
  - Gros débits 540 Mb/s
  - Bcp d'utilisateurs par cellule
  - Large Bande = 10-66 GHz – Modulation OFDM et Scalable-OFDM
  - En cours…



Quelques mots sur

Bluetooth™

Historique de Bluetooth

- Harald Blaatand, roi du Danemark de 940 à 981
  →« Bluetooth » II,
- Toujours les dents bleues car il mangeait des mûres …..
- A toujours souhaité unir le Danemark et la Norvège
- Inspiration pour la technologie : unir des appareils différents
  - ***1994*** : invention du concept par Ericsson
  - ***1998*** : Création du Bluetooth SIG (Special Interest Group). Ericsson est rejoint par IBM, Intel, Nokia & Toshiba
  - ***1999*** : Microsoft les rejoint
  - ***Aujourd 'hui*** : Plus de 4000 entreprises dans le SIG

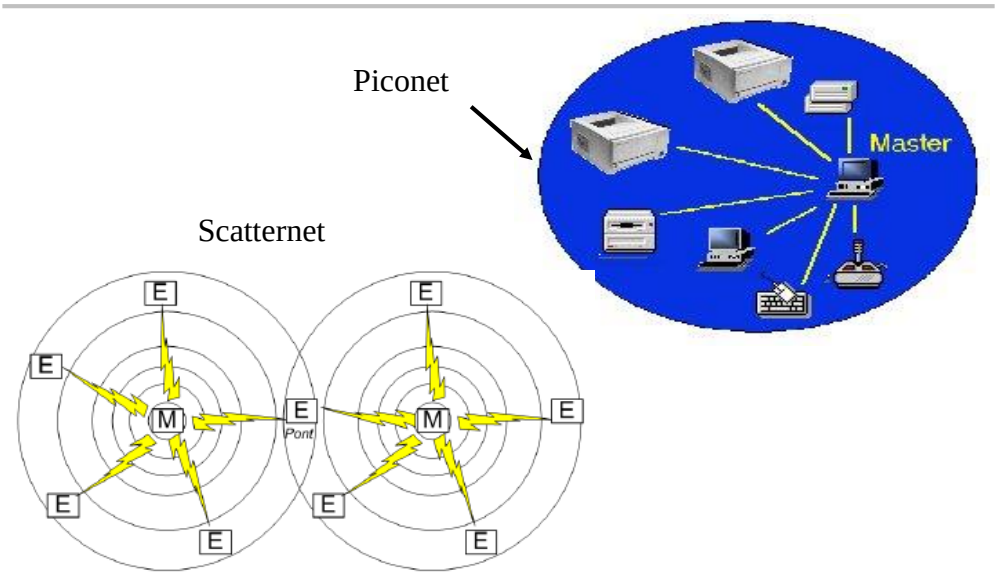
Concepts

- PAN : Personal Area Network (802.15)
- Suppression des câbles
- Faire communiquer tout type d 'appareils
  - PC, ordinateurs portables
  - Téléphones Portables
  - Souris, PDA
  - montres …

Concepts

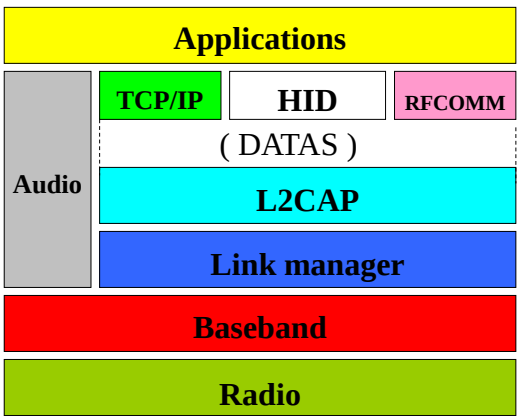
- Constitution de réseaux dans un rayon de 10 à 100 mètres (10 mètres aujourd'hui) par liaisons radio ultracourtes (2,4 GHz)
- On parle alors de picoréseau ou de « **piconet** »
- Jusqu 'à 8 appareils dans un piconet (255 en mode veille)
- 1 seul « maître », les autres sont des esclaves
- Plusieurs piconet forment un **scatternet** via un nœud pont

Concepts



Pile protocolaire simplifiée

- Non conforme au modèle OSI
- Complexe



Couche radio

- Couche la plus basse : assure la radio transmission (couche physique)

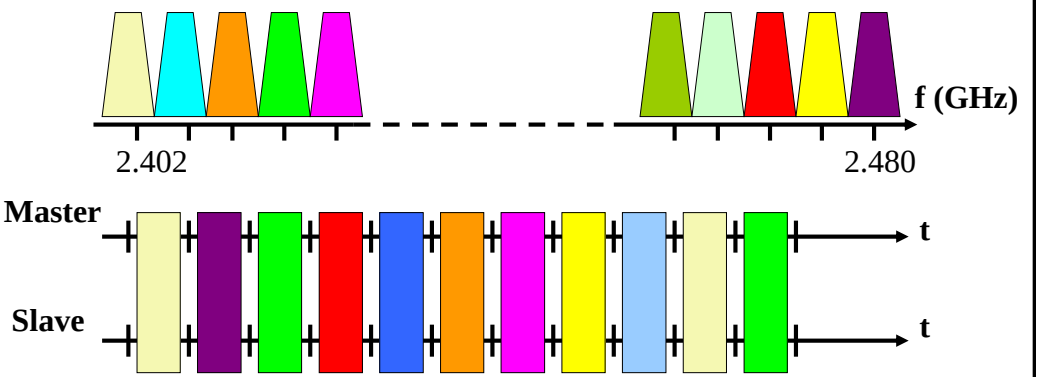
- FHSS : modulation fréquentielle avec 79 canaux de 1 MHz
- Opère dans la bande de fréquence des **2,4 GHz** ISM
- 1600 échanges par seconde
- 3 classes d'émetteurs radio
  - Classe 1 : 100mW → 100 m
  - Classe 2 : 20mW → 15 m
  - Classe 3 : 1mW → 10 m

- Problème d'interférence entre Wifi et Bluetooth

Couche radio

- Couche la plus basse : assure la radio transmission (couche physique)

- FHSS : modulation fréquentielle avec 79 canaux de 1 MHz
- 1canal = 1piconet – 1 esclave = 1 intervalle de temps



Couche Baseband

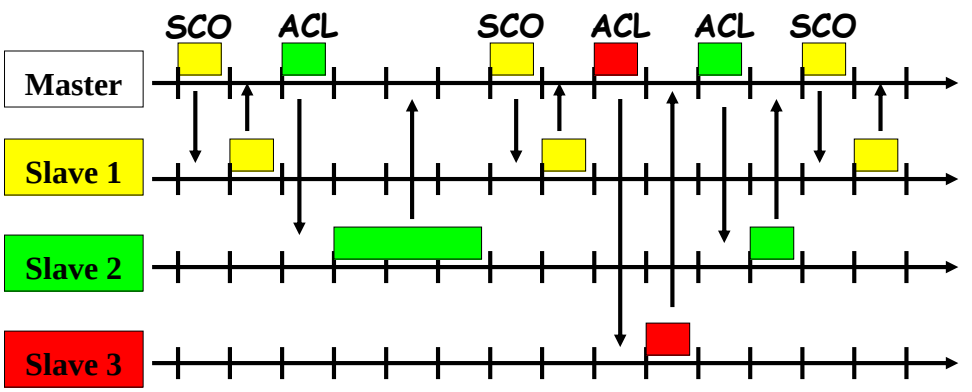
Couche la plus importante de Bluetooth

- Echange de trames
- Contrôle les liens existants : synchrones ou asynchrones
- Gère les canaux physiques (MAC)
  - 1 piconet = 1 canal (de 1MHz)
  - 1 maitre donne la parole aux esclaves
  - Via le mécanisme Time Duplex Division

Types d'échange de données

- Deux modes :
  - ACL : asynchronous connection less link
    - Sans connexion mais avec retransmission
    - Echanges asynchrones, symétrique ou non
    - Accès au canal par polling (pour chaque esclave)
    - Données jusqu'à 196 kbps
  - SCO : synchronous connection oriented link
    - Avec connexion mais sans retransmission (flux)
    - Echanges symétriques et synchrones
    - Accès au canal par réservation de slots à intervalles fixes
    - 3 communications max
    - Voix, vidéo à 64 kbps, 128 kbps ou 196 kbps

Multiplexage des liaisons



Format des trames

- Format

- Access code :
  - DAC : Pour communiquer avec un appareil donné
  - CAC : Lors d 'un ajout d 'appareil
  - IAC : Scanner un espace à la recherche d 'appareils

- Le champs « en-tête » permet de spécifier des adresses, champs de contrôle, le type de connexion (ACL ou SCO) ainsi que les débits associés

Couche Link Manager

Fonctionnalités :

- management de piconet :
  - ajout / libération d 'esclaves
  - changement de maître:
  - établissement de liaisons ACL / SCO

- configuration de liaisons
  - QoS suivant le type de paquets
  - contrôle de puissance

- Options de sécurité
  - authentification
  - cryptage et gestion des clés

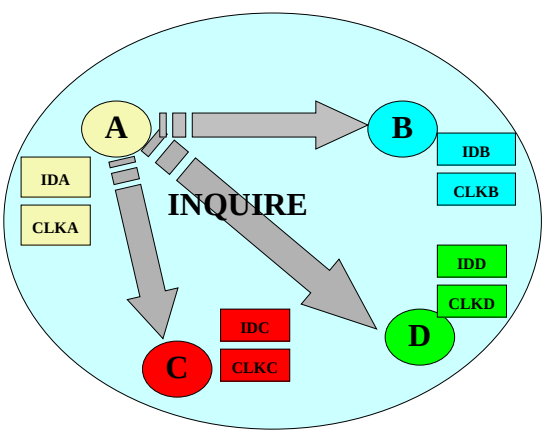
Couche L2CAP

- **Logical Link Control and Adaptation Protocol**
- **4 rôles :**
  - Multiplexage des données
  - Segmentation & réassemblage
  - Veille au respect de la QoS établie entre deux appareils
  - Formation de groupes d 'appareils : équivalent du broadcasting

Exemple d'ajout d'un élément

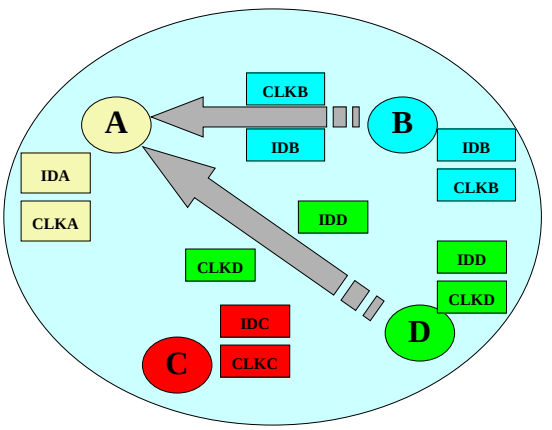
- (1) : Le maître scanne l 'espace :

« inquiring »



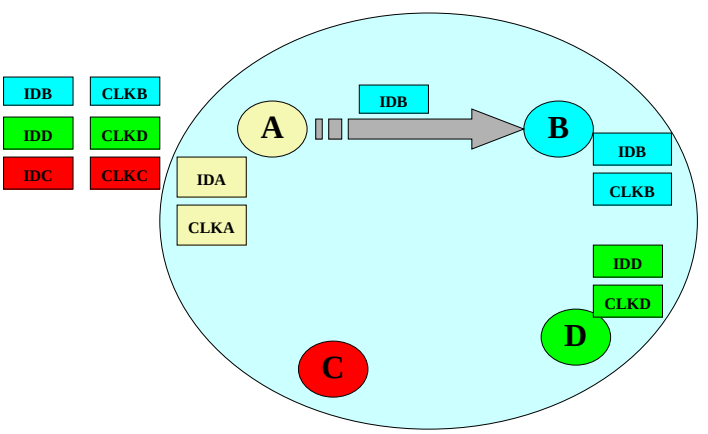
Exemple d'ajout d'un élément

- (2) : Le maître écoute les réponses



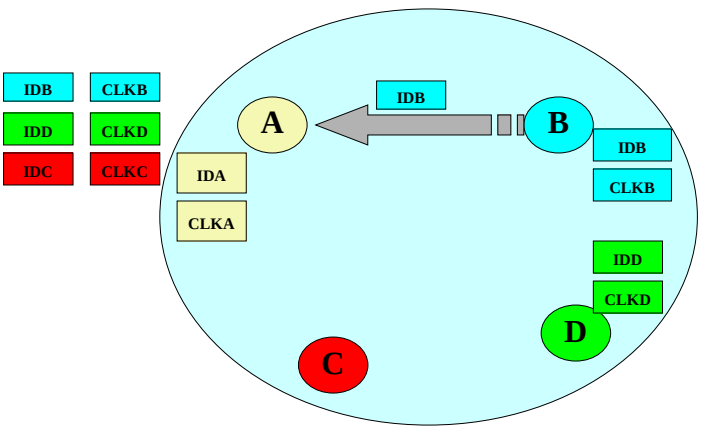
Exemple d'ajout d'un élément

- (3) le maître souhaite établir une liaison avec 1 esclave :



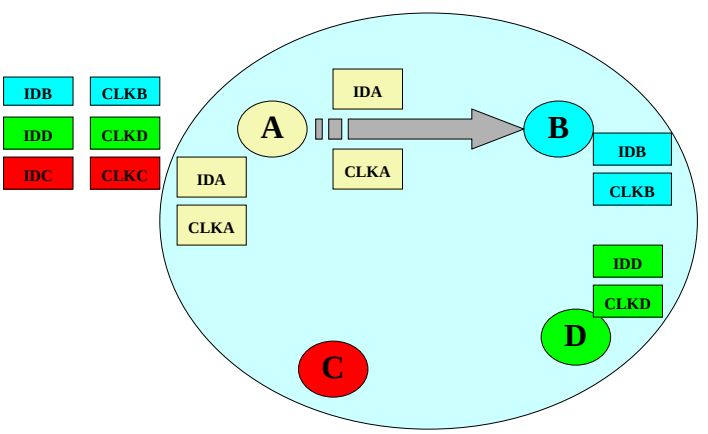
Exemple d’ajout d’un élément

- (3) L ’esclave B est bien joignable



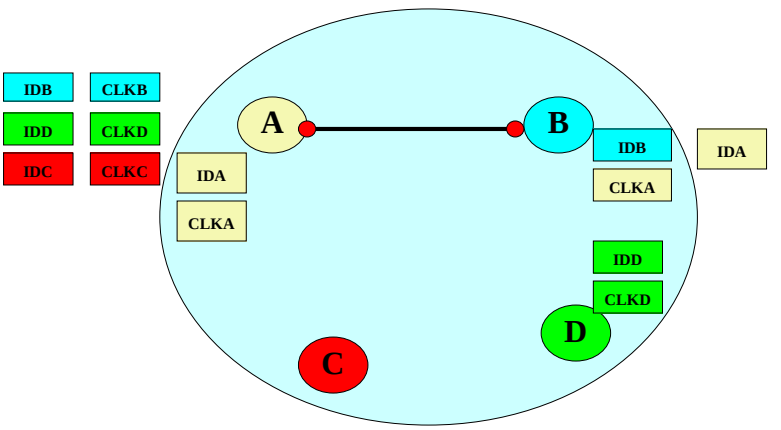
Exemple d’ajout d’un élément

- (3) le maître ajoute l ’esclave B



Exemple d'ajout d'un élément

- (4) Liaison effective entre A et B



Chapitre 2

IP Nouvelle Génération :

IPv6, VOIP, …

De IPv4 à IPv6

- Dans les années 90, manque d'adresses IPv4 →
- L'EITF décide de lancer IPv6

- Objectifs
  - Résoudre le problème du manque d'adresses
  - Réduire la taille des tables de routage
  - Plus d'efficacité
  - Plus de sécurité
  - Améliorer la QoS
  - Permettre la mobilité

- Sortie en décembre 1992
  - Common Architecture for the Internet → RFC 1707
  - Simple Internet Protocol Plus (IPv6) → RFC 1770, 1460 - 1466
  - TCP and UDP with Bigger Adresses

De IPv4 à IPv6

- **Nouveautés**

  - 128 bits au lieu de 32 → 8 fois 16 bits (en Hexa)
  - Entête plus simples (7 champs au lieu de 13)
  - Gestion des options simplifiée
  - Authentification et confidentialité

- **Les adresses IPv6 peuvent être de 3/4 types**

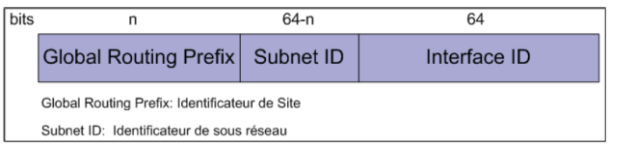
  - Unicast
  - Multicast - Broadcast
  - Anycast
    - Nouveau type d'adressage
    - Comme une adresse multicast, désigne un groupe d'interfaces
    - Ne sera remis qu'à un seul membre du groupe, par exemple le plus proche au sens de la métrique
    - Pour l'instant, une seule adresse anycast est utilisée, elle est réservée au routeur mais dans l'avenir, d'autres pourraient **être définies**

De IPv4 à IPv6

- **Utilisation de la notation CDIR : Blocs/masque**
  - Exemple: 2001:660:3003::/48
- :: → Une suite de zéro
- Plages réservées →
- Nombreux RFC !!!
  - RFC 2374 - 3587
- Adressage global

INTERNET PROTOCOL VERSION 6 ADDRESS SPACE
[last updated 27 February 2006]

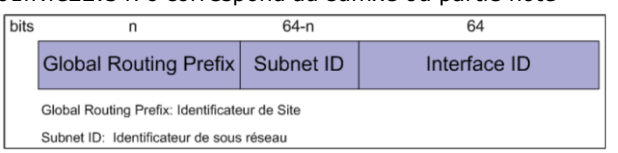
IPv6 Prefix	Allocation	Reference
0000::/8	Reserved by IETF	[RFC3513]
0100::/8	Reserved by IETF	[RFC3513]
0200::/7	Reserved by IETF	[RFC4048]
0400::/6	Reserved by IETF	[RFC3513]
0800::/5	Reserved by IETF	[RFC3513]
1000::/4	Reserved by IETF	[RFC3513]
2000::/3	Global Unicast	[RFC3513]
4000::/3	Reserved by IETF	[RFC3513]
6000::/3	Reserved by IETF	[RFC3513]
8000::/3	Reserved by IETF	[RFC3513]
A000::/3	Reserved by IETF	[RFC3513]
C000::/3	Reserved by IETF	[RFC3513]
E000::/4	Reserved by IETF	[RFC3513]
F000::/5	Reserved by IETF	[RFC3513]
F800::/6	Reserved by IETF	[RFC3513]
FC00::/7	Unique Local Unicast	[RFC4193]
FE00::/9	Reserved by IETF	[RFC3513]
FE80::/10	Link Local Unicast	[RFC3513]
FEC0::/10	Reserved by IETF	[RFC3879]
FF00::/8	Multicast	[RFC3513]



Adressage IPv6

Les adresses unicast

- Elles comportent une partie réseau "préfixe" et une partie hôte "suffixe"
- La partie réseau ou préfixe est codée sur 64 bits
  - 48 bits publics "Global Routing Prefix" **(hiérarchie ISP + IANA + RFC 3177)**
  - 16 bits de site définissant le sous-réseau (Admin « Local »)
- La partie hôte ou suffixe est codée aussi sur 64 bits
  - fabriquée à partir de l´adresse MAC de l'interface (ajout de FFFE)
  - elle permet d'identifier la machine dans un réseau donné.
- Exemple : fe80::20d:61ff:fe22:3476
  - fe80:: en réalité fe80:0000:0000:0000 correspond au préfixe (IP privée)
  - 20d:61ff:fe22:3476 correspond au suffixe ou partie hôte

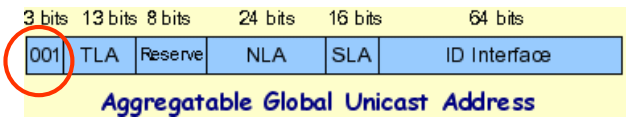


Adressage IPv6

Les adresses unicast

- Adresse de boucle locale (loopback)**::1** remplace l'adresse IPv4 127.0.0.1
- Adresse 0:0:0:0:0:0:0:0 (notée "**::**") est utilisée pendant l'initialisation de l'adresse IPv6 d'une machine (phase transitoire)
- Le préfixe d'une adresse de LAN (Lien Local) est **fe80::/10** (suivi de @carte)
- Le préfixe d'une adresse de **site** (Network) est **fec0::/10** (suivi de @Net@carte)
  - Remplace les adresses IPv4 privées
  - Qu'est ce qu'un **site** ?

- Mappage d'adresses IPv4 (double pile) → ::ffff:147.30.20.10
- OU en 6to4 → 2002::/16 suivi de 147.30.20.10 puis suffixe
- OU en ISATAP → [2001:1:2:3/64]:0:5EFE:[32 bit de l'adresse IPv4]
  (Intra-Site Automatic Tunnel Addressing Protocol)
- Adressage agrégé = hiérarchisé (→ adresses commençant par 2000::/3)



Top Level Aggregator – Next Level Aggregator - Site Level Aggregator – Host
Opérateurs internationaux - Fournisseurs d'accès - Gestionnaires de sites

1 seul ouvert par l'IANA → 2001::/16

Adressage IPv6

Les adresses multicast

- IPv6 généralise l'utilisation des adresses multicast qui remplacent les adresses de type "broadcast".
- un paquet broadcast était très pénalisante pour toutes les machines se trouvant sur un même lien
- Le format des adresses multicast (ff00::/8) est le suivant :
  - ff01 : noeud local, les paquets ne quittent pas l'interface
  - ff02 : lien local, les paquets ne quittent pas le lien (Lan)
  - ff05 : site local, les paquets ne quittent pas le site (Network)

Exemple qui permet de détecter les hôtes actifs (::1) sur le lien local :

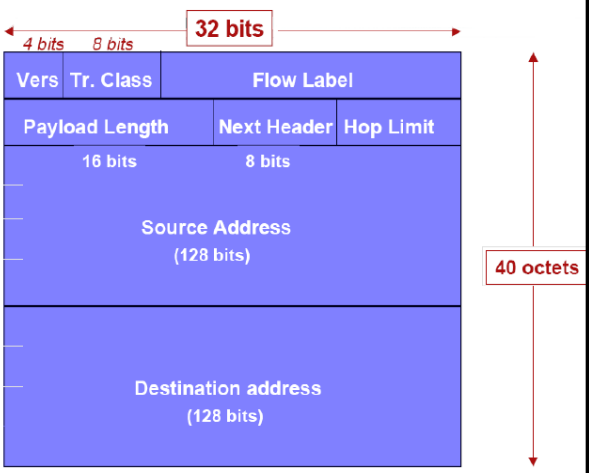
```
# ping6 -I eth0 ff02::1

PING ff02::1(ff02::1) from fe80::20e:35ff:fe8f:6c99 eth2: 56 data bytes
64 bytes from ::1: icmp_seq=1 ttl=64 time=0.048 ms
64 bytes from fe80::20d:61ff:fe22:3476: icmp_seq=1 ttl=64 time=9.05 ms (DUP!)
64 bytes from ::1: icmp_seq=2 ttl=64 time=0.045 ms
64 bytes from fe80::20d:61ff:fe22:3476: icmp_seq=2 ttl=64 time=3.33 ms (DUP!)
64 bytes from ::1: icmp_seq=3 ttl=64 time=0.037 ms
```

2 hôtes actifs fe80::20e:35ff:fe8f:6c99 (celui d'où est passée la commande) et fe80::20d:61ff:fe22:3476 (un autre poste du LAN).

Datagramme IPv6

- Classe de trafic → Distinguer les exigences de QoS (temps réel, …)
- Flow label → Identification / réservation de bande passante pour un trafic contraint (QoS) → IP Switching
- Longueur des données
- Hop Limit = TTL
- Next Header
-
  - **Possibilité de faire se su-**
  -ccéder des entêtes facultatifs
  - **RFC 1883**



RFC 1883 → Entêtes facultatifs

- **Saut par saut**
  - **Infos pour les routeurs traversés**
- **Option de destination et routage**
  - **Pas encore utilisé**
- **Routage**
  - **Liste ordonnée de routeurs à traverser**

Prochain en-tête	Longueur d'en-tête facultatif	Type de routage	Segments restants
Données spécifiques au type			

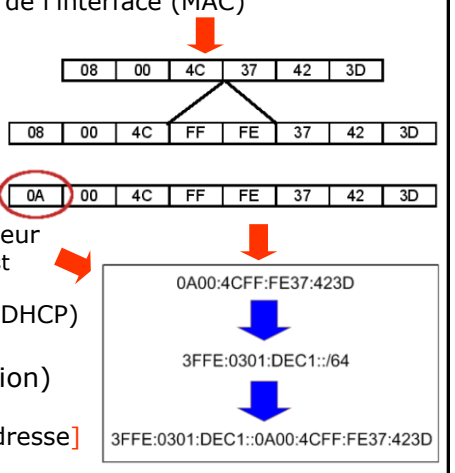
- **Fragmentation**
  - **Cf fragmentation IPv4**
  - **En IPv6 seul la source peut fragmenter !**
- **Authentification puis Chiffrement des données**
  - **Cf IPsec → identité émetteur+intégrité+anti-rejeu+chiffrement → MD5, SHA, DES, 3DES, AES, …**
- **Option de Destination**
- **Couche supérieur = dernier entête = 59 → info sur TCP ou UDP**

Auto-configuration

- Pas pour les routeurs mais pour les nœuds terminaux
- 3 protocoles
  - Neighbour discovery
    - Analyse du réseau → Router Sollicitation (RS)
      - Envoyer en multicast par un hôte pour découvrir les param du réseau
      - Pour un PC, récupération de son adresse et autres paramètres (gateway, …)
    - Pour les routeurs, envoi d'info aux hotes du reseau → Router Advertissment (RA)
      - Envoyé périodiquement ou en réponse à un RS
    - Scruter les hotes vivants → Neighbour Sollicitation (NS) → Réponse = NA
      - Résolution d'adresse (cf ARP)
  - Multicast Listener Discovery
    - Permet aux routeurs de découvrir les membres d'un groupes multicast
    - Intégré a ICMPv6
  - ICMPv6

Processus d'auto-configuration

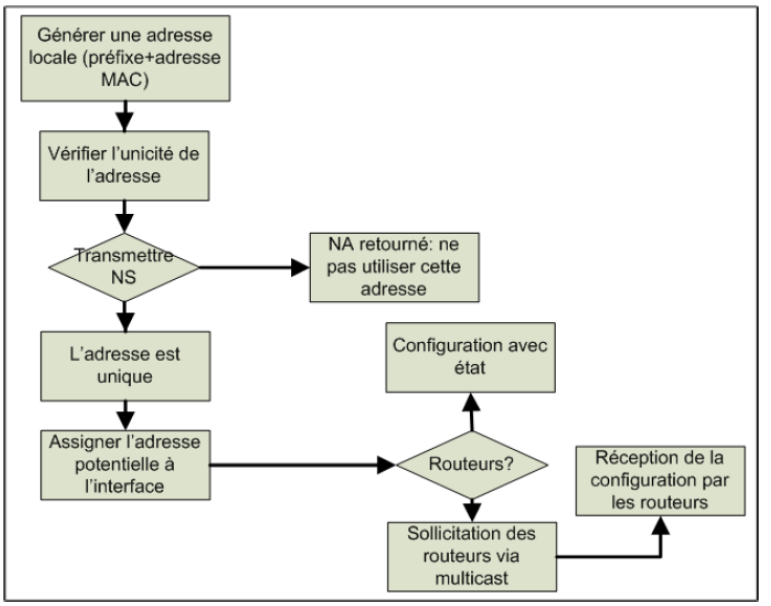
- 1/ Création d'une adresse locale
  - Récupération/transformation de l'adresse de l'interface (MAC)
  - Ajout du préfix par défaut: 0xFE80



RFC 3513 : Inversion du bit universel (le 7e)

- 2/ Récupération d'info sur le Réseau
  - Mode Stateless → Préfix fourni par le routeur
    - Régulièrement et sur demande en multicast
  - Mode Stateful → Utilisation d'un serveur (DHCP)
- 3/ Vérification (Duplicate Address Detection)
  - 2 adresses MAC identiques ?
  - Envoi d'un paquet ICMP [SRC=**::**DEST=Adresse]
  - Pas de réponse = OK

Processus d'auto-configuration



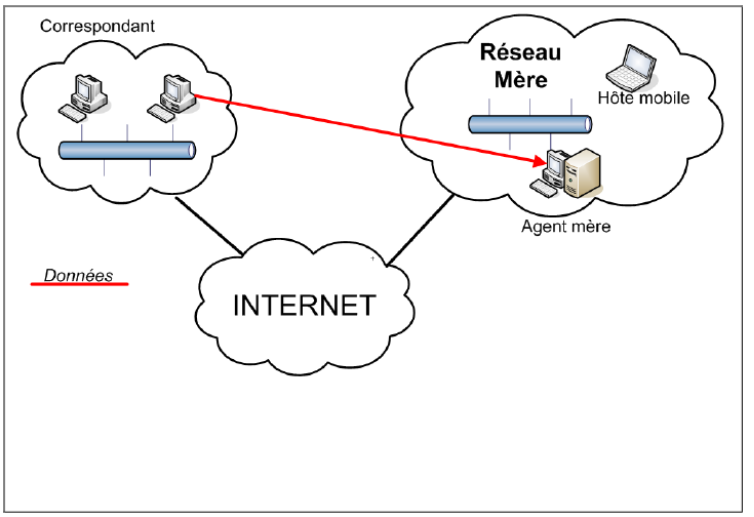
Gestion de la Mobilité

- **Principe**
  - Un Hôte mobile est attaché à un unique Réseau mère
  - Un Hôte mobile peut quitter son Réseau mère pour aller sur un Réseau visité
  - Un Agent mère est chargé de faire suivre les paquet vers l'hôte mobile
  - L'hôte mobile reçoit une Adresse temporaire sur le Réseau visité
  - L'hôte mobile doit informer l'Agent mère de sa position (adresse temporaire) → via des paquets Binding Update

  - Un hôte mobile est apte a s'autoconfigurer partout (cf juste avant)
  - Il communique alors son adresse à l'agent mère → Binding Update
  - L'agent mère intercepte le trafic à destination de l'hôte mobile et lui fait suivre
  - L'hôte mobile prévient alors son correspondant (via un Binding Update) qui peut ensuite lui envoyer directement les paquets suivants
  - Sans passer par l'agent mère

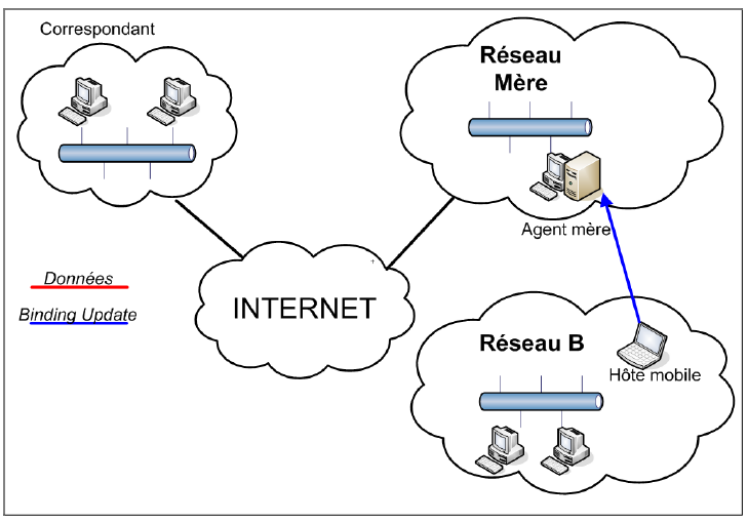
Gestion de la Mobilité

- **Illustration**



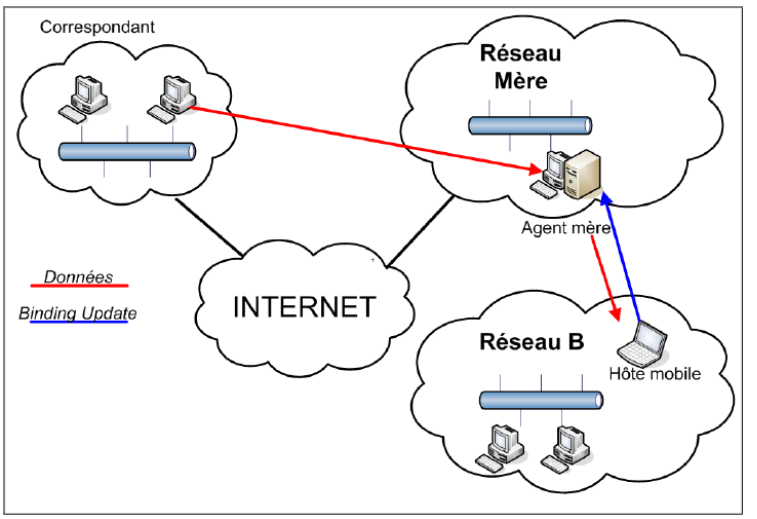
Gestion de la Mobilité

- **Illustration**



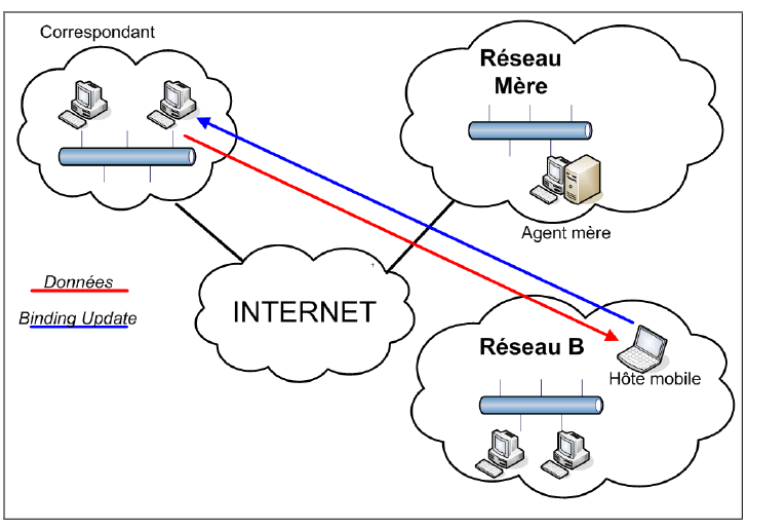
Gestion de la Mobilité

- **Illustration**



Gestion de la Mobilité

- **Illustration**



Gestion de la Mobilité

- **Binding Updates**
  - **Mécanisme complexes et dangereux**
  - **Inclusion d'une durée de vie**
  - **Gestion d'une liste d'hôtes mobiles**
  - **Nécessite des Binding Acknowledge**
  - **Update et Acknowledgement nécessitent un mécanisme d'authentification contre l'usurpation d'identité**

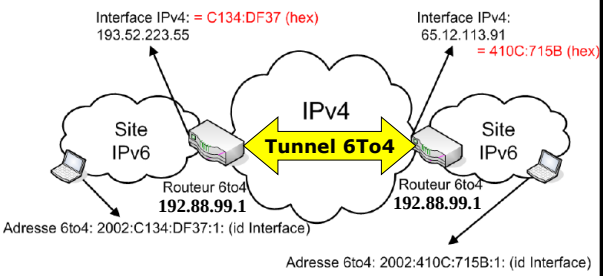
Les + d'IPv6

- **Simplification de la configuration**
  - **Configuration automatique des machines lors du boot (adresses)**
- **Qualité de services**
  - **Contrôle de flux et Classe de trafic : est utilisé pour distinguer les sources qui doivent bénéficier du contrôle de flux**
  - **Cette distinction des flux permet aux routeurs de mieux réagir en cas de congestion**
  - **Des priorités de 0 à 7 sont affectées aux sources capables de ralentir leur débit en cas de congestion. Les valeurs 8 à 15 sont assignées au trafic temps réel (les données audio et vidéo en font partie) dont le débit est constant**
  - **Le champ Identificateur de flux contient un numéro unique choisi par la source qui a pour but de faciliter le travail des routeurs et de permettre la mise en oeuvre les fonctions de qualité de services comme RSVP (*Resource reSerVation setup Protocol*).**
  - **Mobilité**
  - **Sécurité et chiffrement :**
    - **l'informations concernant les numéros de port peuvent être masquées aux routeurs intermédiaires.**
    - **Chiffrement des données**

De IPv4 à IPv6

- 6-Bone
  - Créer en 1996 en Asie, Europe, USA, Australie
  - Fermer en juin 2006 !

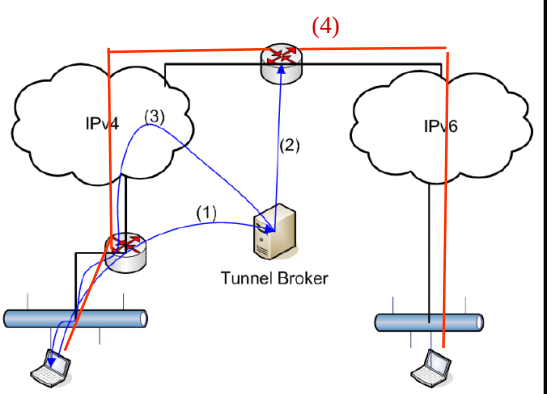
- Transition en douceur ?
  - Interopérabilité IPv4/IPv6
  - Ilot IPv6 dans IPv4
  - Comm. IPv4 → IPv6
  - Comm. IPv6 → IPv4
  - Double couche Réseau ?
  - Tunnels (6To4 via routeur relay 6To4 **(RFC 3056),** TSP, …)
  - Routeurs NAPT **(RFC 2766)** = Translation IPv6-IPv4 = idem NAT
  - DNS IPv6



De IPv4 à IPv6

- **Tunnel Broker (TB) – Tunnel Setup Protocol (TSP)**
  - Tunnel temporaire
  - Encapsulation dans IPv4
  - (protocole 41)
  - Client (web) / Serveur (TB)
  - Authentification

- **TSP**
  - Négociation automatique
  - Port 3653
  - 1. Connexion
  - 2. Broker configure le tunnel
  - 3. Config envoyé au client
  - 4. Communication encapsulée



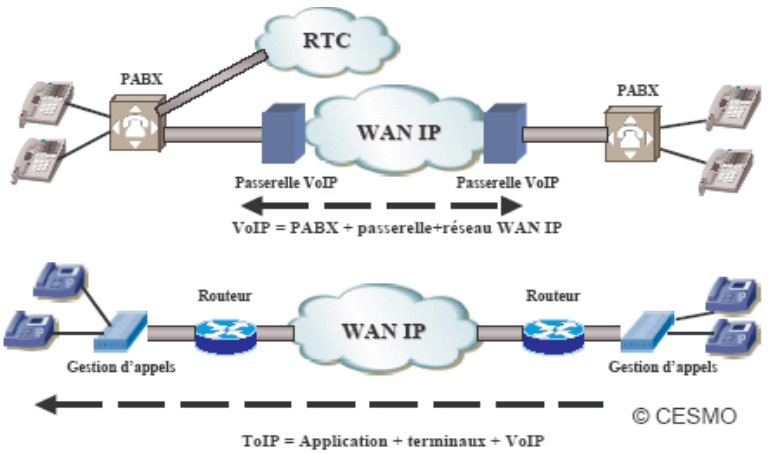
Voice Over IP

- Une communication RTC traditionnelle
  - 64 Kbps: 1 IT en commutation de circuit
  - Circuit activé et maintenu pendant la durée de la communication: coût élevé
  - Sous utilisation du circuit: les 'temps morts' sont facturés!
  - Etc.
- De plus en plus, convergence entre Voix, Données, Vidéo
  - Mutualisation des ressources réseaux
  - Optimisation des ressources réseaux
  - Commutation en mode paquets
  - Etc.

Convergence IP

- IP le protocole 'tout-en-un' ?
- La VoIP = début de convergence mais
  - La VoIP : limitée aux infrastructures de transport de la voix sous forme de paquets, contournant ainsi le réseau téléphonique commuté
  - La ToIP: incluant la VoIP et les terminaux de communication de bout en bout (téléphones IP, ordinateurs, etc.)
  - Autre différence: la ToIP modifie les équipements terminaux (ex. IP Phones) alors que la VoIP ne concerne que les PBX et leur adaptation au réseau IP par des passerelles

ToIP vs VoIP



Les protocoles

- Le transport de la VoIP fait appel à certains protocoles:
  - TCP: transport des données en mode connecté; nécessite des accusés de réception → temps de latence!
  - UDP: transport des données en mode non connecté; donc sans accusé de réception
  - RTP (Real Time Protocol): permet de répondre aux exigences de délais de la VoIP et de corriger les éventuelles pertes dues à la VoIP sur UDP
  - RTCP (Real Time Control Protocol): permet de compléter RTP avec la fonctionnalité QoS
  - CRTP (Compressed RTP): permet d'utiliser RTP en mode compressé (gain de Bande Passante)

Caractéristiques réseaux et délais

- Le temps de latence:
  - Correspond au temps de réponse du réseau VoIP
  - Valeur théorique: ≤ 100ms
  - Valeur admise: ≤ 200ms
- La gigue:
  - Correspond à la variation maximale du temps de latence entre 2 envois consécutifs de paquets par la même source
  - Valeur théorique: ≤ 40ms
  - Valeur admise: ≤ 75ms
- Le taux de perte du réseau
  - Valeur théorique: ≤ 1%
  - Valeur admise: ≤ 3%

La ToIP: Principe

- Un terminal A souhaite appeler un terminal B dans un réseau ToIP:
  - A envoie une requête au Gatekeeper (G) en composant le numéro de B
  - Le Gatekeeper (G) assure la translation entre le numéro tél. de B et son adresse IP et envoie une requête IP sur le réseau pour vérifier la disponibilité de B
    - Si B est disponible, alors G met en relation A et B en fournissant à A l'adresse IP de B
    - Si B n'est pas sur le même LAN que A, alors G route l'appel vers la Gateway (GW) pour localiser B
  - Une fois l'appel terminé, G met à jour ses tables pour la disponibilité des terminaux A et B

ToIP: les protocoles de signalisation

- **H.323 (ITU puis RFC 2543)**
  - Pile la plus mature et utilisée
  - G7xx = (De)codage en num. du son

Speech	Control			
G.7xx	RTCP	H.225	Q.931	H.245
RTP				
UDP			TCP	
IP				

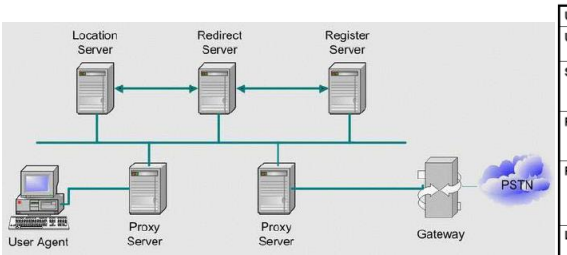
- RTP (Real Time Protocol)
  - Flux multimedia (UDP)
  - Uni/Multicast
  - Réservation - Supervision

- RTCP (Real Time Control Protocol)
  - Envoi régulier de paquets de supervision aux participants
  - Gestion QoS

- H225 : communication avec le Gatekeeper
- H245 : Call Control : négociation des paramètres d'une comm
- Q931 : Call Signalisation

ToIP: les protocoles de signalisation

- **SIP (Session Initiation Protocol, IETF - RFC 3261)**
  - Plus récent et plus souple que H323
  - Niveau 7 - Adapté aux réseaux à très grande échelle
  - Visio conf, audio conf, telephone, multimedia, …
  - Basé Texte (comme HTTP) pour initialiser une session de communication



UAC (user agent client)	Caller application that initiates and sends SIP requests.
UAS (user agent server)	Receives and responds to SIP requests on behalf of clients; accepts, redirects or refuses calls.
SIP Terminal	Supports real-time, 2-way communication with another SIP entity. Supports both signalling and media, similar to H.323 terminal. Contains UAC.
Proxy Server	Contacts one or more clients or next-hop servers and passes the call requests further. Contains UAC and UAS.
Redirect Server	Accepts SIP requests, maps the address into zero or more new addresses and returns those addresses to the client. Does not initiate SIP requests or accept calls.
Location Server	Provides information about a caller's possible locations to redirect and proxy servers. May be co-located with a SIP server.

- MGCP (Media Gateway Control Protocol)
  - Standard commun UIT (MEGACO) et IETF (H.248)
  - Complémentaire à H.323 et SIP
  - Passerelle entre les réseaux IP et Télécoms

ToIP: les protocoles de signalisation

Item	H.323	SIP
Designed by	ITU	IETF
Compatibility with PSTN	Yes	Largely
Compatibility with Internet	No	Yes
Architecture	Monolithic	Modular
Completeness	Full protocol stack	SIP just handles setup
Parameter negotiation	Yes	Yes
Call signaling	Q.931 over TCP	SIP over TCP or UDP
Message format	Binary	ASCII
Media Transport	RTP/RTCP	RTP/RTCP
Multiparty calls	Yes	Yes
Multimedia conferences	Yes	No
Addressing	Host or tel. number	URL
Call termination	Explicit or TCP release	Explicit or timeout
Instant messaging	No	Yes
Encryption	Yes	Yes
Size of standards	1400 pages	250 pages
Implementation	Large and complex	Moderate
Status	Widely deployed	Up and coming

Matériels pour la ToIP

- **Les hardphones**
  - **Disposent d'une connexion LAN**
- **Les softphones**
  - **Logiciels d'émulation de terminaux téléphoniques sur PC**
  - **L'utilisation est tributaire du PC connecté au réseau IP**
- **Le Gatekeeper**
  - **Serveur informatique localisé sur le LAN avec les postes IP**
  - **Réalise les fonctions H.323 ou SIP**
- **La Gateway**
  - **Passerelle avec le réseau téléphonique commuté**
  - **Contient des cartes d'interface T0, T2 ou analogique**

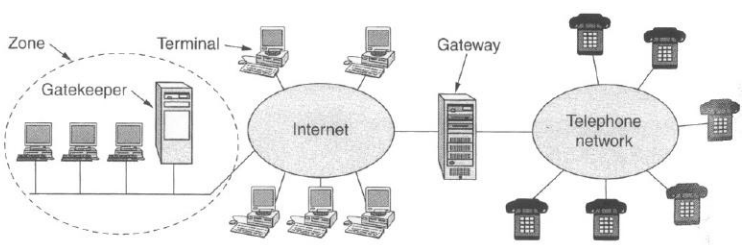
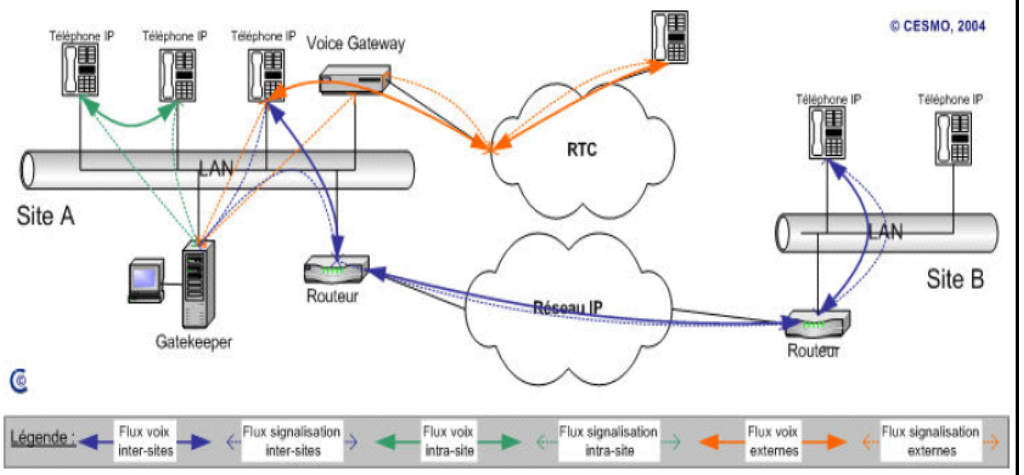


Schéma illustratif



Chapitre 4

VPN & Firewall

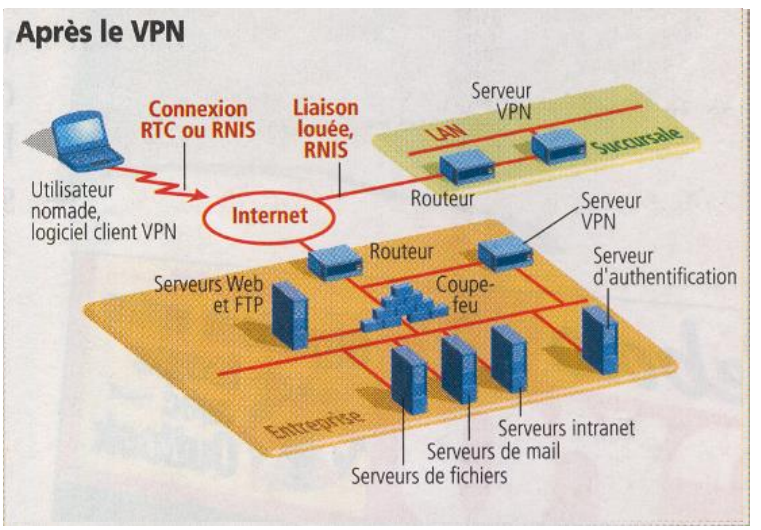
Principes et mise en œuvre

Concept de VPN

VPN : Virtual private Network – Réseau privé virtuel

- Consiste à faire transiter un protocole par l'intermédiaire d 'un autre
- Fournir un accès à distance transparent aux ressources du système d'information
  - Malgré la traversée d'un réseau public (Internet)
  - Avec les risques inhérents (intrusion)
- Utilisation possibles
  - Permettre l'accès à des services internes depuis l'extérieur
  - Connexion de sites distants (eg. succursale)
  - Externalisation (de l'exploitation du SI)
  - Offres commerciales (opérateurs télécoms)
  - Télé-travail

Illustrations



Comment faire ?

Que doit assurer un VPN ?
- Authentification (de préférence forte)
- Intégrité
- Confidentialité
- Protection contre le rejeu
- Eventuellement compression

- VPN = Mode Client / Serveur ?
  - Termes parfois impropres (cf plus loin)
  - Client VPN
    - Équipement (PC) initiant une connexion VPN vers un serveur VPN
  - Serveur VPN
    - Équipement qui accepte des connexions VPN de clients
    - Fournit une connexion VPN (accès distant ou routeur à routeur)

- Généralisation du concept de tunnel
  - Réseau à Réseau ou Machine à Réseau ou Machine à Machine

Types de VPN

- VPN niveau application (couche 7)
  - Créer de nouvelles applications intégrant les fonctions cryptographiques
  - Exemple : SSH

- VPN niveau transport (couche 5)
  - Liaison logique entre des programmes qui chiffrent les communications
  - Exemple (https, pops, imaps …) utilisant SSL

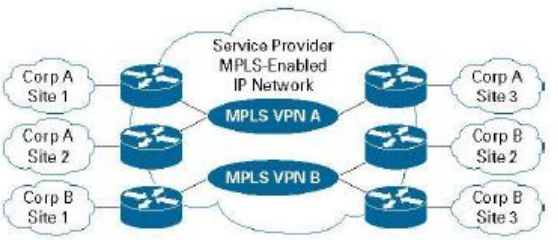
- VPN niveau réseau (couche 3)
  - Le chiffrement est effectué directement au dessus du support réseau
  - Impliquent la configuration des équipements d'interconnexion

- VPN niveau liaison (couche 2)
  - Impliquent la configuration d'équipements au niveau de l'infrastructure réseau (de l'opérateur)

Types de VPN

– VPN Réseau (*Network Based*) – Niveau 2 et 3
- Destinés exclusivement aux VPN site à site
- Fonctions VPN implémentées en cœur de réseau (par l'opérateur)
- Possibilité de garantie de QOS
- Différentes techniques utilisées…
  - Des circuits virtuels basés sur Frame Relay ou ATM
  - Une technologie phare en VPN IP : MPLS
  - Compatible avec IPSec

Site-to-Site MPLS-Based VPN

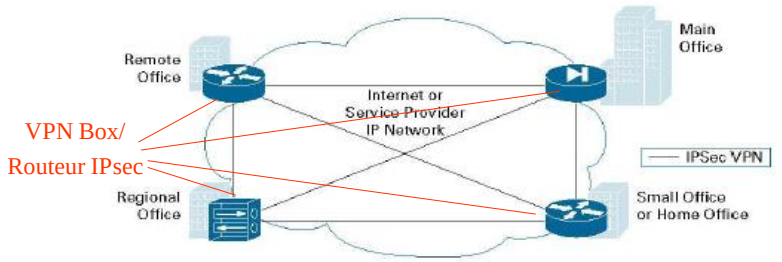


Types de VPN

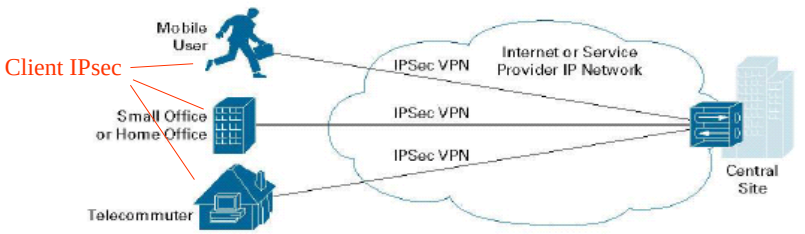
– VPN Client ou CPE (*Customer Premise Equipment Based – Niveau 3*)
- Destinés aux VPN site à site et aux VPN accès distant
- Fonctions VPN implémentées sur des passerelles (routeurs, firewall, …) interconnectant les sites et le réseau public (Internet)
- On parle aussi de VPN Box
- Pas vraiment de gestion de QoS
- Pléthore de solutions !
- Utilisant pour la plupart une technologie standard : IPSec
  - … mais complexe à mettre en œuvre ☹
  - … mais problématique avec NAT
  - … et nécessitant un « client IPSec »

Types de VPN

Site-to-Site IPSec-Based VPN



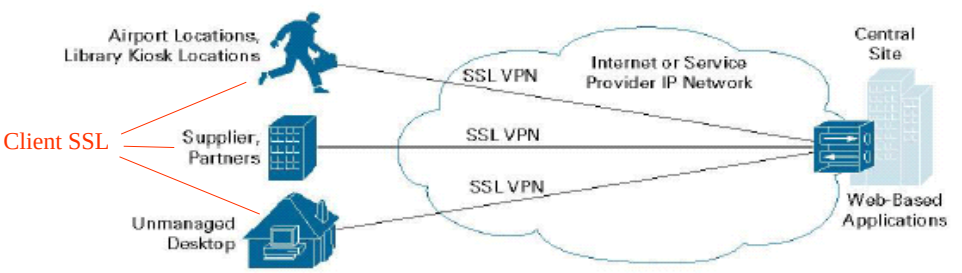
Remote Access IPSec-Based VPN



Types de VPN

- VPN Session (Session Based – Niveau 5) et applicatif (Niveau 7)
  - VPN SSL
  - Convient bien aux accès distant (mais moins fiable)
  - Accès à un portail d'applications et non au réseau interne
  - Un simple navigateur web peut suffire

Remote Access SSL-Based VPN



Protocoles de tunneling

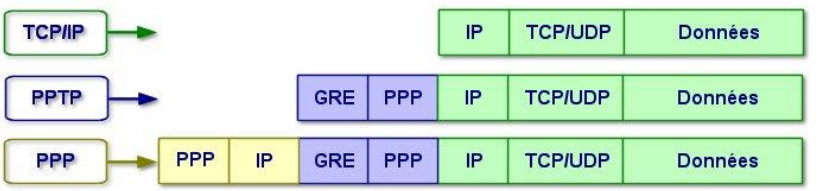
- Plusieurs catégories :
  - Les protocoles de niveau 2
    - PPP (Point to Point Protocol)
    - PPTP (Microsoft)
    - L2TP (Cisco, 3com, microsoft)
  - Les protocoles de niveau 3
    - IPsec
    - MPLS
  - Les protocoles de niveau supérieur
    - SSL

PPP

- Point to Point Protocol - RFC 1331
  - Liaison point à point entre un client et un serveur d'accès (VPN)
  - Encapsulation de paquet IP, IPX, …
  - Full duplex
  - Similaire à HDLC
  - LCP (Link Control Protocol) pour mettre en place la connexion
    - Phase 1 : Ouverture de connexion
    - Phase 2 : Authentification
    - Phase 3 : Fermeture
- Compatible ADSL, Ethernet, Rnis, ATM, relais de trame.

PPTP : Protocole ouvert M$

- RFC 1701, 1702 et 1171
- Utilise PPP
- PPTP ne définit pas comment chiffrer
  - Microsoft authentification MS/CHAP V2 (mot de passe)
  - Microsoft chiffrement MPPE (RC4 / 40 ou 128 bits)
- Utilise deux canaux :
  - Port TCP 1723 pour la supervision
  - Protocol GRE: Generic Routing Encapsulation (IP 47) pour les données
  - Etablissement d 'une connexion PPP à l 'intérieur du canal de donnée éventuellement compressé et crypté



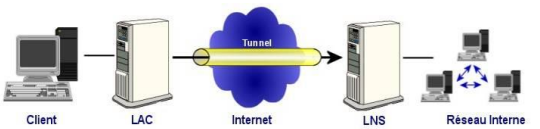
PPTP Protocole ouvert M$

- A n'utiliser que si c'est la seule solution
- Avantages:
  - Facile à installer (Windows depuis Win95 et Linux)

- Inconvénients majeurs:
  - Faiblesse de l'authentification (attaque du mot de passe)
  - Protocole GRE pas toujours traité sur les routeurs de site ce qui nécessite d'ouvrir tout IP vers le serveur VPN

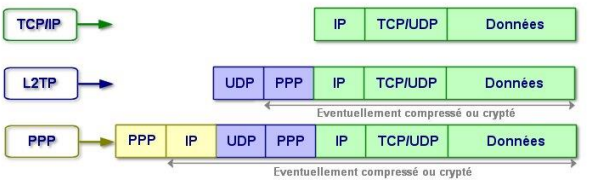
L2TP (Layer Two Tunneling Protocol)

- Encapsulation de paquets PPP au niveau 2 (FrameRelay, ATM) ou 3 (IP)
- L2TP repose sur :
  - les concentrateurs d'accès L2TP (LAC)
  - les serveurs réseau (LNS)



  - L2TP n'intègre pas directement de protocole pour le chiffrement
  - L'IETF préconise l'utilisation conjointe d'IPSec et L2TP.

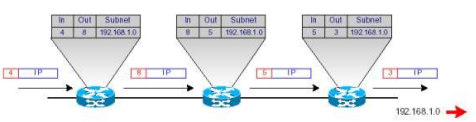
  - L2TP utilise UDP
  - L2TP utilise PPP

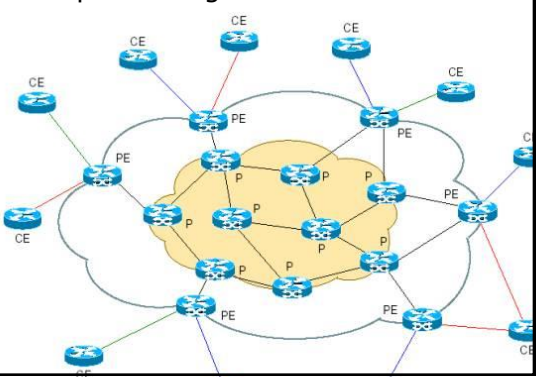


MPLS (Multi Protocol Label Switching)

- Basés sur des routeurs (LSR Label Switch Routers) utilisant la commutation de labels (label swapping)
  - Réseau MPLS : les paquets IP sont classés dans des FEC (Forwarding Equivalent Classes) et sont ensuite label-switchés
  - Les paquets appartenant à une même FEC suivront le même chemin
  - CV = Label Switch Path (LSP) unidirectionnel
  - Les FEC sont des préfixes IP définit par les Ingress LSR de la backbone MPLS

• VPN entre routeurs LSR sur la base des labels (RFC 2547 bis)
  - *P = LSR*
  - *PE = Ingress LSR*
  - *CE = Routeurs classiques*





VPN IPSec ou SSL ?

	IPSec VPN	SSL VPN
Application accessibility	**ALL IP applications (Web applications, enterprise, e-mail, VoIP and multimedia**	**Primarily Web applications**
Software required	**IPSec client software**	**Standard Web browser**
Information exposure	**Only designated people / computers are allowed access**	**Access from everywhere (e.g. internet kiosks). Information can be left behind (intentionnaly or unintentionnaly)**
Level of client security	**Medium-High (depending on client software being used)**	**Low-Medium (Medium can be achieved via dedicated software – non-clientless solution)**

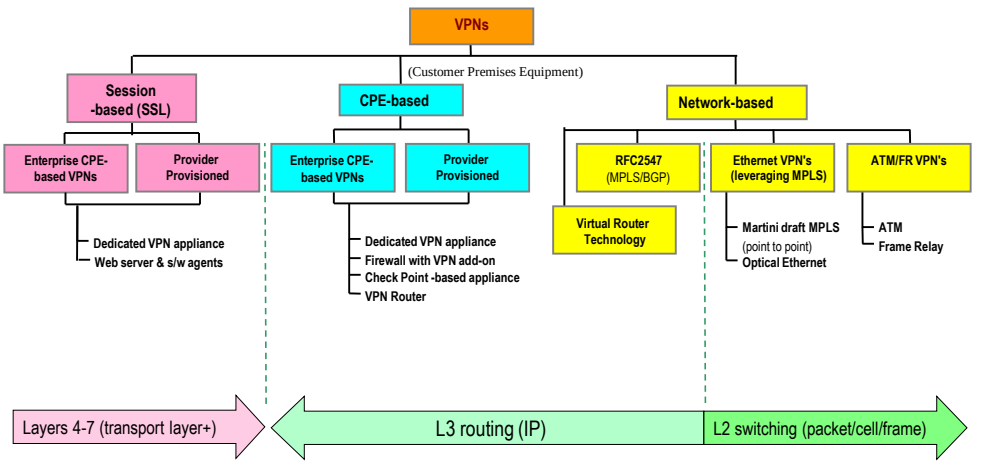
(Source Chek Point Software)

VPN IPSec ou SSL ?

	IPSec VPN	SSL VPN
Scalability	**Highly scaleable, proven in tens of thousands of customer deployments**	**Highly scaleable, easy to deploy**
Authentication methods	**Supports multiple authentication methods; embedded PKI available from some vendors**	**Supports multiple authentication methods; use of strong authentication requires extra cost and limits access devices**
Security implications	**Extends security infrastructure to remote access; enhances end-point security with integrated security (e.g. personal firewall)**	**Limited control over information access and client environment; good for accessing less-sensitive information**
Ideal for	**Secure employee access; site-to-site access**	**External Web customer access**

(Source Chek Point Software)

Synthèse VPN



Exemple 1 : OpenVPN

- OpenVPN est un système VPN ouvert Ciient / Serveur
- Clients et serveur utilisent la librairie OpenSSL
- Config via la notion d'interfaces (dev) virtuelles (tap0; tun1)

- 2 types de tunnels
  - les tunnels IP routés « routed » - mode nomade - Encapsulation d'IP dans IP
    - nécessite une modification du routage
    - Ne transmet pas le broadcast
    - Ne permet pas le partage de fichiers Windows

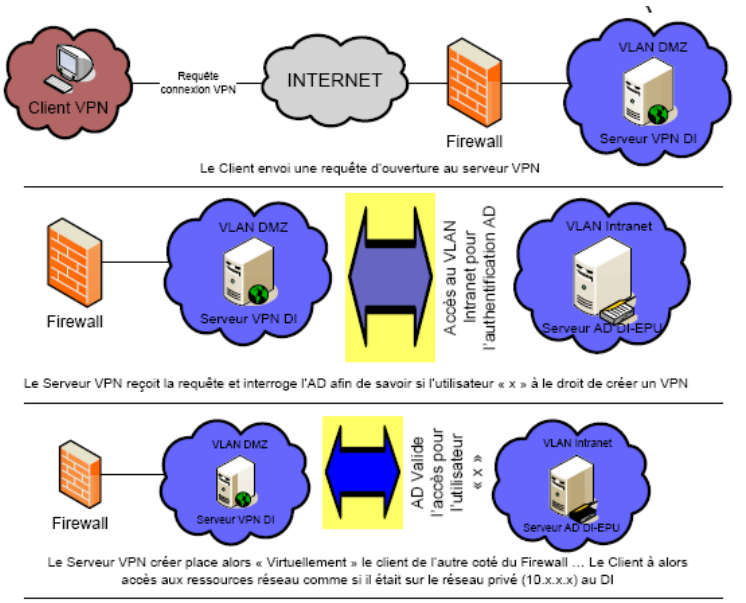
  - les tunnels « bridged » - mode pont entre 2 ethernet → Trame encapsulée dans IP.
    - Les interfaces LAN1 et LAN2 ont alors liées entre elles en une seule entité = VPN

- Le tunnel utilise le port 5000 (ou 1194) par défaut et le protocole UDP (on peut passer en TCP mais ce n'est pas recommandé)

- Authentification forte des extrémités du tunnel
  - supporte les certificats X509 pour authentifier la session
  - protocole TLS pour échanger les clés
  - la possibilité d'utiliser un plugin PAM pour authentifier le client

- Chiffrement par clé partagée, bi-clés RSA ou certificats.
- **DANGER :** si on arrive a obtenir la clé secrète d'un client on a accès a tous !
- → Clients fiables indispensables → antivirus….

Exemple 2 : VPN Microsoft



Exemple 3 : SSL Explorer

- SSL-Explorer est un logiciel libre réalisant un VPN construit sur OpenSSL et développé en JAVA (http://sourceforge.net/projects/sslexplorer)

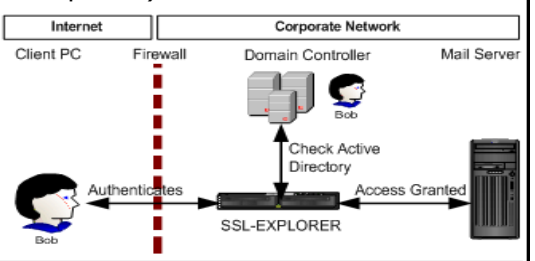


Fig. 3: The SSL-Explorer VPN authenticates the connecting user by querying Active Directory on the Microsoft Windows domain controller.

- Fonctionnalités:
  - Client web
  - Accès aux partages Windows
  - Redirection de ports (Web-forwarding)
  - Authentification des clients sur Active-Directory ou base locale
  - Management par interface Web
  - Possibilité de créer différents profils utilisateurs
  - Supporté sous Windows 2000/2003 et Linux

Conclusion

- VPN = outil extrêmement puissant…
- Mais …
- … aussi une brèche redoutable
- A n'utiliser que dans le cadre d'une architecture déjà sécurisée
- Bien authentifier les extrémités (pas facile et ne suffit pas…)
- Quelques questions :
  - Pour quels services ?
  - Ou mettre le point d'entrée dans l'architecture réseau ?
  - Que faut il comme sécurité sur le poste client ?

Firewall

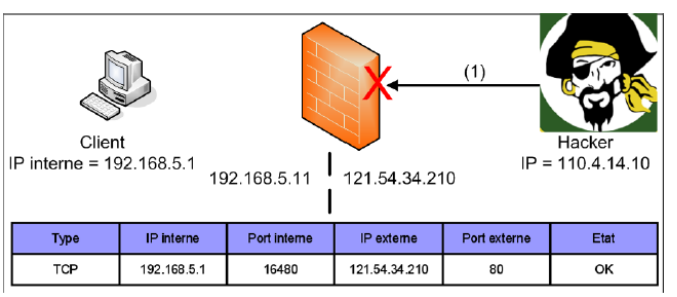
- Pare-feu : Filtrage mais pas blocage
- Services offerts :
  - Filtrage de paquets
  - Inspection avec rapport d'état
  - Proxy applicatif
  - Monitoring (log = preuves)
- Assure souvent :
  - Cache web
  - Restriction par rapport au contenu (url, video, mot clé…)
  - Analyse du trafic → détection d'intrusion, p2p, …
  - Détection → réaction (alertes, ajout de règles)
- N'assure jamais :
  - Attaques internes
  - Usurpation d'identités
  - Chevaux de Troie
- En option :
  - Antivirus, antispam, anti spyware, …
  - VPN et tunnel
  - Authentification – Gestion de plages horaires
  - …

Filtrage simple

- Règles utilisant les informations disponibles dans les entêtes protocolaires de niveau 3 et plus
  - Champs des datagrammes IP (adresses, protocole, fragment, …)
  - Ports TCP, UDP
  - Type de message ICMP
  - Adresse MAC, …
- Simple et rapide
- Efficace
- N'examine pas le contenu des données
- Pas d'authentification (spoofing/usurpation d'adresse)
- Pas de suivi / mémoire (analyse du trafic)
- Problème lié à la fragmentation → Le firewal doit reconstruire ?

Stateful inspection

- Firewall à mémoire
- Terminologie Checkpoint
- Mémorisation des connexions établies pour l'analyse
- Suivi de l'ouverture et fermeture des connexions
  - Pour les ports TCP > 1023
  - Ouverture depuis l'extérieur interdite

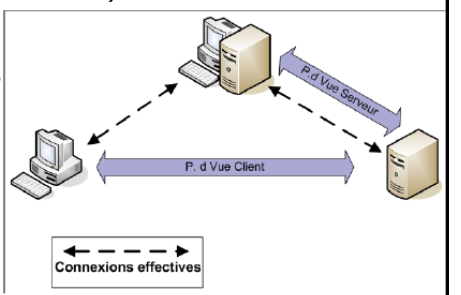


Type	IP interne	Port interne	IP externe	Port externe	Etat
TCP	192.168.5.1	16480	121.54.34.210	80	OK

- Quelques noms : PIXcisco, Kerio, IPcop, …

Filtrage applicatif : Proxy

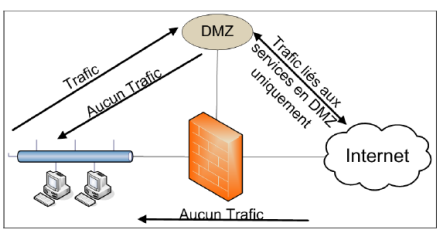
- Serveur mandataire (intermédiaire) qui intervient au niveau 7
  - Analyse des contenus (web, ftp principalement !)
  - Service de cache / répartition
  - Authentification, suivi (log)
  - Analyse & génère de nouveaux paquets
  - Contrôle parental



- Problèmes
  - Configuration et Maintenance
  - Onéreux
  - Goulot
- Proxy vs Reverse-proxy
  - Proxy : Utilisateurs internes → Internet
    - **Fonction de cache**
  - Reverse : Serveurs internes ← Utilisateurs externes
    - **Fonction de Load balancing**
- Le plus connu : Squid

Firewall et DMZ

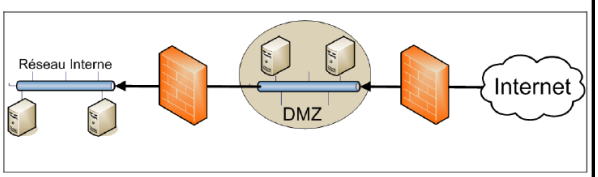
- Lorsque le réseau offre des services accessibles de l'extérieur
- Zone isolée dans le réseau interne → DMZ
  - Ouverte de l'extérieur et de l'intérieur
  - Mais fermée vers l'intérieur
  - Zone à surveiller
  - Contient les serveurs accessibles de l'extérieur



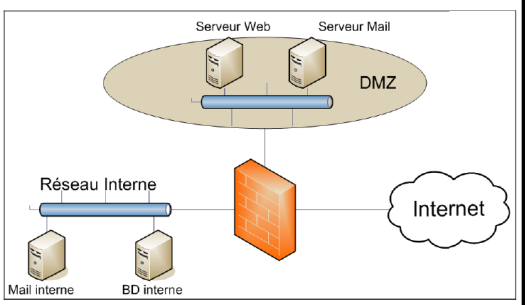
- 2 architectures possibles
  - 1 firewall avec triple interfaces
  - Multiples Firewalls

Firewall et DMZ

- Multiples Firewalls
  - Plus simple
  - Plus flexible (NAT)
  - Sécurité accrue

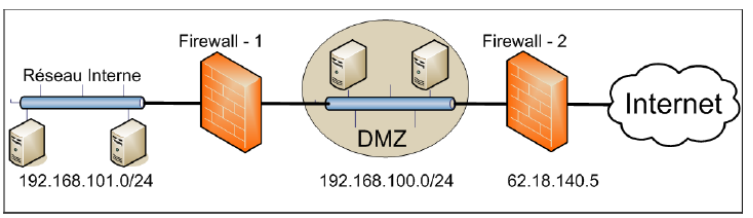


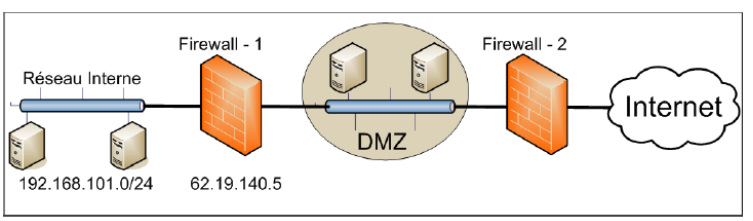
- Triple interfaces
  - Centralisation des difficultés
  - Config et maintenance plus complexe
  - Goulot



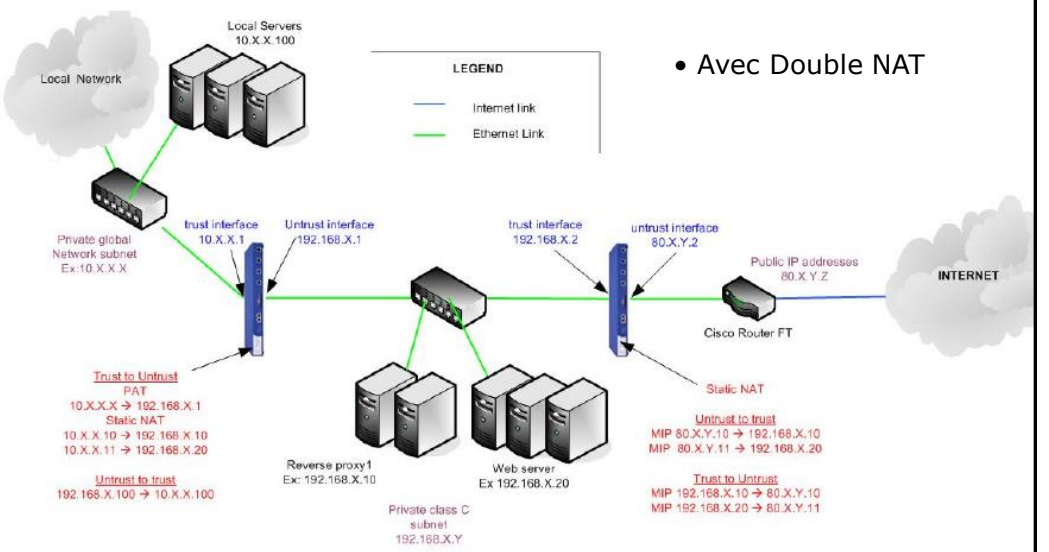
Firewall et DMZ

- DMZ NATée ou pas ?
  - Quel firewall fait le NAT ?





Est ce une bonne config ?

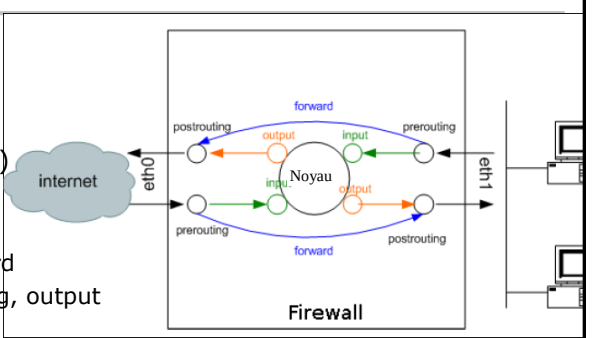


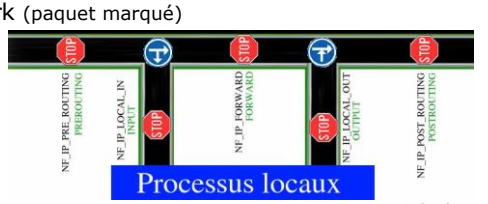
- Avec Double NAT

Firewall : Mise en oeuvre

- Iptables + Netfilter

- Fonctionnement
  - Tables (ensemble de chaines)
    - Filter, nat, mangle
  - Chaînes (listes de règles)
    - Filter = input, output, forward
    - Nat = prerouting, postrouting, output
    - Mangle = idem pour QoS
  - Cîbles (actions)
    - Accept, drop, reject
    - Log, Masquerade (paquet modifié), Mark (paquet marqué)
  - Modules
    - Conntrack : suivi de connexions
      - Etat : New, established, related, Invalid





Firewall : Mise en oeuvre

- Iptables permet de :
  - **Rajouter des règles/chaînes**
  - **Supprimer des règles/chaînes**
  - **Modifier des règles/chaînes**
  - **Afficher les règles/chaînes**

- **Exemple :**

```
#Suppression des régles prédéfinies
iptables -F
iptables -t nat -F
iptables -t mangle -F
#Suppression de toutes les régles de l'utilisateur
iptables -X
#Politique par defaut (tout rejeter)
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP
# la loopback du firewall peut émetre dans tous les sens :
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT
# les connections invalides sont refusées :
iptables -A INPUT -m state --state INVALID -j DROP
iptables -A FORWARD -m state --state INVALID -j DROP
# les connections etablies ou assimilables sont acceptées en entrees :
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Flush = vider Chaines prédéfinies

table

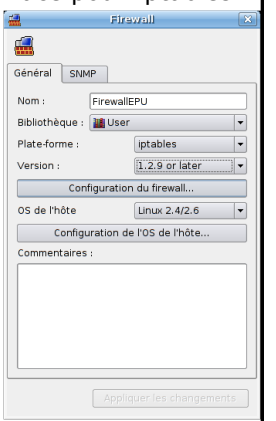
Vider Chaines utilisateurs

Policy = politique par defaut

Action

Ajout

- Plus convivial…
  - FWBuilder = Interface pour Iptables



Attaques classiques

- **Injection SQL**
  - Dans les formulaires

```
SQLQuery = "SELECT Username FROM Users WHERE Username
= '" & strUsername & "' AND Password = '" &strPassword & "'"
strAuthCheck = GetQueryResult(SQLQuery)
If strAuthCheck = "" Then
    boolAuthenticated = False
Else
boolAuthenticated = True
End If
```

692x251

```
SELECT Username FROM Users WHERE Username = '' OR ''=''
AND Password = '' OR ''=''
```

- Man in the middle
  - Interception de trafic

- Détournement de DNS
  - DNS ID Spoofing : on répond avant le vrai DNS à une requête
  - DNS cache poisoning → ajout de fausses info dans le cache d'un DNS en se faisant passer pour un autre DNS

Attaques classiques

- **ICMP**
  - TTL = 1 → Msg ICMP
  - Ping → Msg ICMP
  - Destination injoignable
- **Fragmentation IP** → Analyse difficile
  - Entete des fragments incomplet
- **IP spoofing**
  - Usurpation d'adresse locale
- **DOS et DDOS**
  - Denial Of Service, Distributed DOS
  - **SYN Flood** : surcharge de demande de connexion sans attente de la réponse
- **Port scanning**
  - **NMAP**

ICMP		
Type	Sens	Action
Echo Request	Sortant	Autoriser
Echo Reply	Entrant	Autoriser
TTL dépassé	Entrant	Autoriser
Destination injoignable	Entrant	Autoriser
Echo Request	Entrant	Interdire
Echo Reply	Sortant	Interdire
Redirect	Entrant	Interdire

Préconisation Filtrage ICMP

NMAP (Network Mapper)

- Scanner de ports
  - Aujourd'hui détectable par IDS (Inspection Detection System)
- Types de scans :
  - **ping ICMP normal ou TCP ping sur le port 80**
  - **TCP connect : option -sT**
    - **Principe : une connexion TCP habituelle est tentée sur chaque port**
  - **SYN scan : option -sS**
    - **Principe : Un paquet SYN est envoyé. Si le port est ouvert, un SYN|ACK est renvoyé, sinon un RST est renvoyé.**
  - **IDLE scan : option -sI @zombie:port zombie**
    - **Principe : Une machine "zombie" permet de masquer la source du scan Quasiment impossible à tracer**
  - **FIN, XMAS et NULL scans : options -sF, -sX et -sN**
    - **Principe : envoi de paquet FIN, de paquet FIN|URG|PSH et de paquet sans aucun flag TCP activé**
  - **SCAN UDP : option -sU**
    - **Principe : Envoi d'un paquet UDP vide. Les ports fermés retournent un paquet ICMP port unreachable**

Législation

Loi pour la confiance dans l'économie numerique

Article 30
I. - L'utilisation des moyens de cryptologie est libre.
II. - La fourniture, le transfert depuis ou vers un Etat membre de la Communauté européenne, l'importation et l'exportation des moyens de cryptologie assurant exclusivement des fonctions d'authentification ou de contrôle d'intégrité sont libres.

Article 35
1° Le fait de ne pas satisfaire à l'obligation de déclaration prévue à l'article 30 en cas de fourniture, de transfert, d'importation ou d'exportation d'un moyen de cryptologie ou à l'obligation de communication au Premier ministre prévue par ce même article est puni d'un an d'emprisonnement et de 15 000 EUR d'amende ;
2° Le fait d'exporter un moyen de cryptologie ou de procéder à son transfert vers un Etat membre de la Communauté européenne sans avoir préalablement obtenu l'autorisation mentionnée à l'article 30 ou en dehors des conditions de cette autorisation, lorsqu'une telle autorisation est exigée, est puni de deux ans d'emprisonnement et de 30 000 EUR d'amende.

Législation

Article 226-18 du code pénal
Le fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende.

Article 323-1
Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30000 euros d'amende. Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 45000 euros d'amende.

Législation

Début 2006, un californien a été arrêté après s'être servi d'une armée de 400 000 pcs zombies pour lancer des attaques DDoS, usage de spywares, spamming, etc. Il louait entre autres ses moyens à d'autres pirates. Il aurait ainsi gagné près de 60 000$.
57 mois de prison ferme.

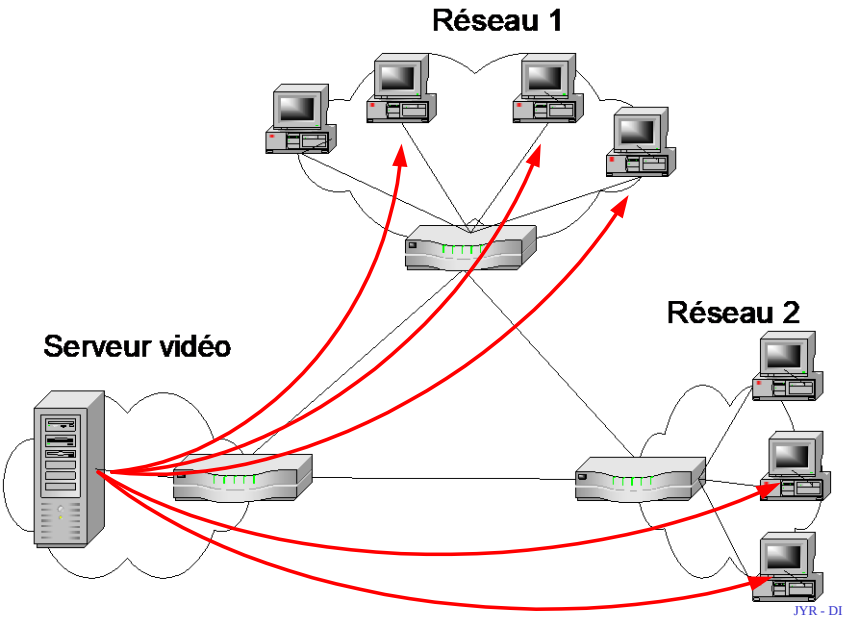
Gary McKinnon :
700 000$ de dégâts sur le réseau du pentagone, de l'armée et de la NASA.
Arrêté en 2002 en GB, s'il est extradé il risque une peine maximum de 70 ans de prison + 1.75 M de $ d'amende.
Extradition autorisée en juillet dernier

Un hacker français a été condamné à 2000 euros d'amende et 5300 euros de dommages et intérêts pour s'être introduit dans le système d'un hébergeur de sites suisse, Net4all.ch.

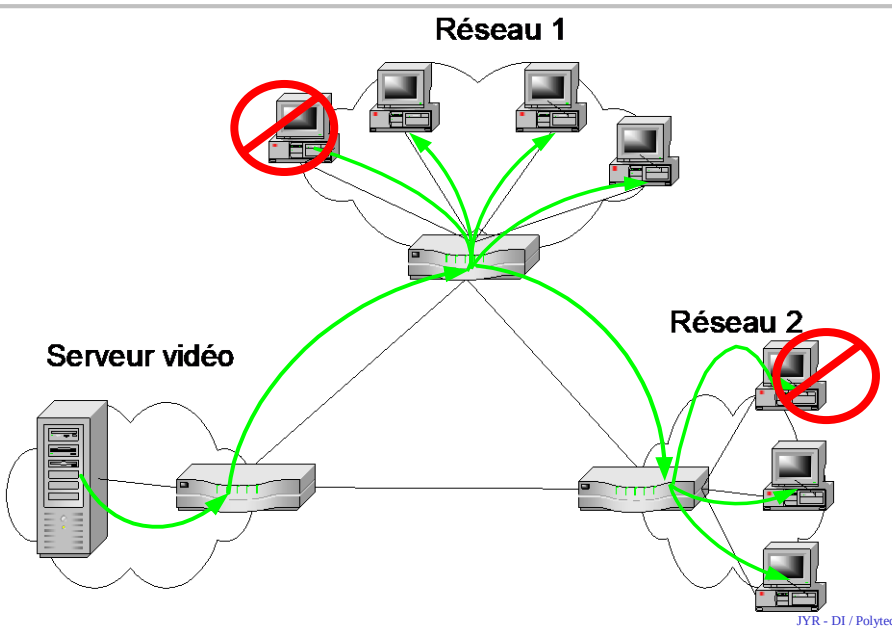
Chapitre 5

Le Multicast sur IP et ses applications

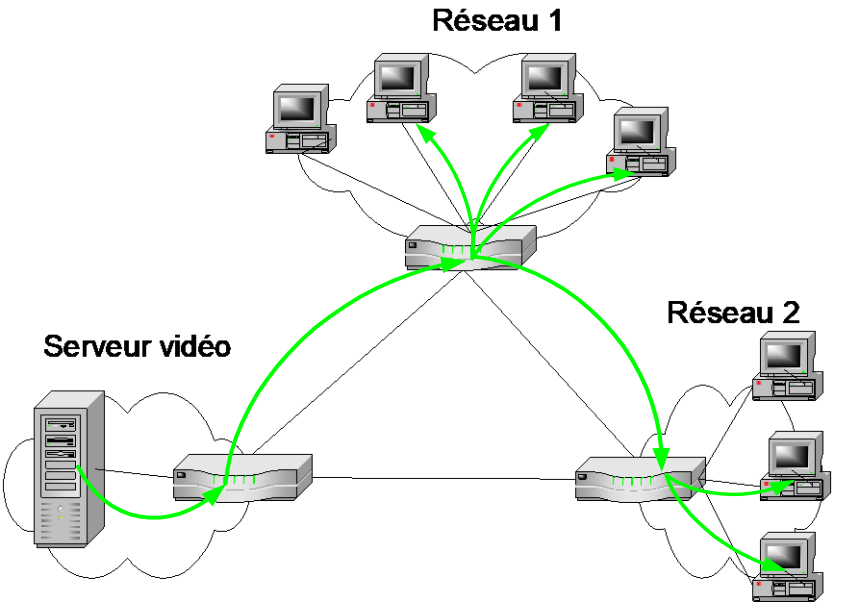
Multicast vs Unicast



Multicast vs Broadcast

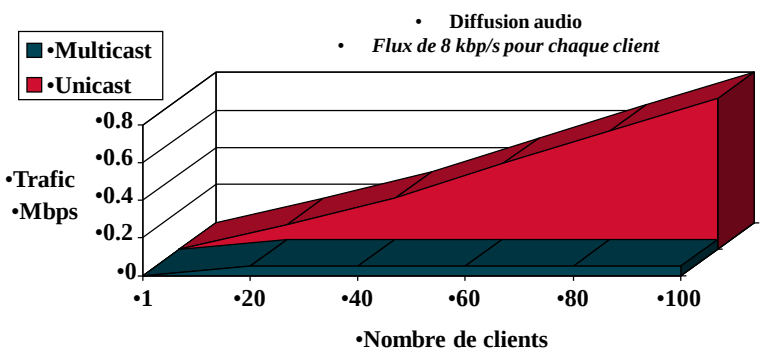


Multicast



Avantages du Multicast

- *Réduction de la charge des éléments actifs*
- *Optimisation de l'utilisation du réseau*



Deux Modes Multicast IP

- ASM = Any Source Multicast
  - Un récepteur s'abonne à un groupe et reçoit les paquets venant de toutes les sources pour le groupe
  - vic/ rat / isabel …
- SSM = Specific Source Multicast
  - Un récepteur s'abonne à un groupe mais n'acceptera que les paquets venant de sources connues
  - WM player …

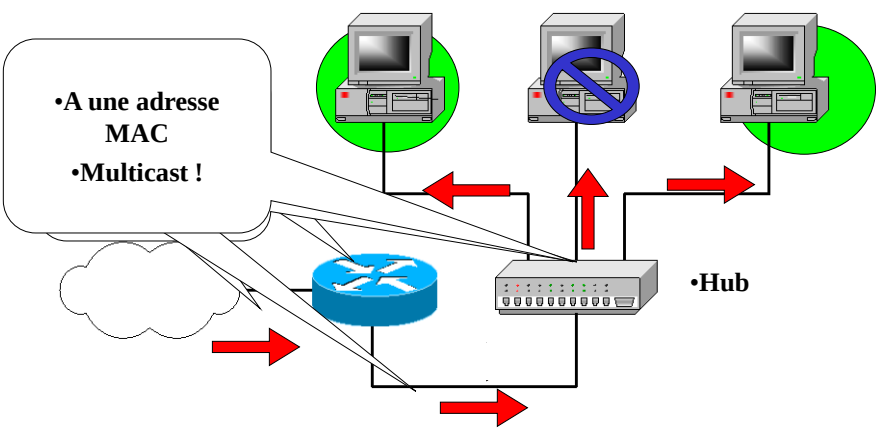
Adressage Multicast

L'adressage IPv4

- *Utilise la classe D*
  - Adresses : 224.0.0.0 à 239.255.255.255
  - Chaque adresse correspond à un groupe
- *Adresses réservées*
  - Pour dialoguer avec les routeurs
  - De 224.0.0.0 à 224.0.0.255
  - Exemples:
    - 224.0.0.1 Tous les postes multicast du réseau
    - 224.0.0.2 Tous les routeurs multicast du réseau
- *Adresses privées*
  - Fonctionnement et rôle identique à celle unicast
  - De 239.0.0.0 à 239.255.255.255

L'adressage

- *Obligation d'un adressage spécifique*

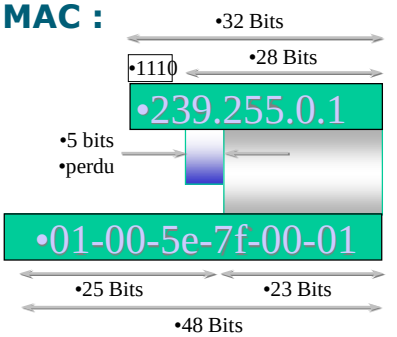


L'adressage

- **Nécessité d'adressage de niveau 2 :**

  Création d'une classe d'adresse MAC spécifique :
  01-00-5E-xx-xx-xx

- **Mappage d'adresse IP / MAC :**



L'adressage IPv6 (RFC 3513)

8 bits		4 bits	4 bits	112 bits
1111	1111	flags	scope	group ID
F	F			

- 8 premiers bits positionnés à 1
- Adresses dérivées du préfixe FF00::/8
  - Champ **flag**(4 bits) : 0RPT
    - T = 0 si adresse permanente (Définies par l'IANA)
    - T = 1 si adresse temporaire
    - Bits P et R : type de groupe
  - Champ **scope**
    - Permet de limiter la portée de la diffusion sur un réseau
      - 0 –Reservé
      - 1-Portée noeud local
      - 2 -Portée lien local
      - 3 -Portée sous-réseau local
      - 4 -Portée Admin-local
      - 5 -Portée site-local
      - 8 -Portée organisation-local
      - E -Portée globale

L'adresse Multicast sollicitée

- Construite à partir de l'adresse unicast
  - Concaténation de FF02::1:FF00:0/104 + les 24 derniers bits de l'adresse unicast
  - Chaque équipement construit une adresse multicast sollicitée
- Les équipement qui connaissent l'adresse v6 d'un équipement mais pas l'adresse MAC peuvent utiliser l'adresse multicast sollicitée
  - Protocole de détection d'adresses dupliquées
  - Découverte des voisins sur le lien-local (NDP)
  - Evite l'utilisation de l'adresse MAC de diffusion générale (FF-FF-FF-FF-FF-FF)
- Exemple:
  - 2001:0660:010a:4002:4421:21FF:FE24:87c1 (unicast)
  - FF02:0000:0000:0000:0000:0001:FF00:0000/104 (concat)
  - FF02:0000:0000:0000:0000:0001:FF24:87c1 (resultat)

La signalisation :

IGMP & MLD

IGMP et MLD

- **Internet Group Management Protocol**
- **Multicast Listerner Discovery** **(pour IPv6 = 1 partie de ICMPv6)**

- **Signalisation entre routeurs et ordinateurs**

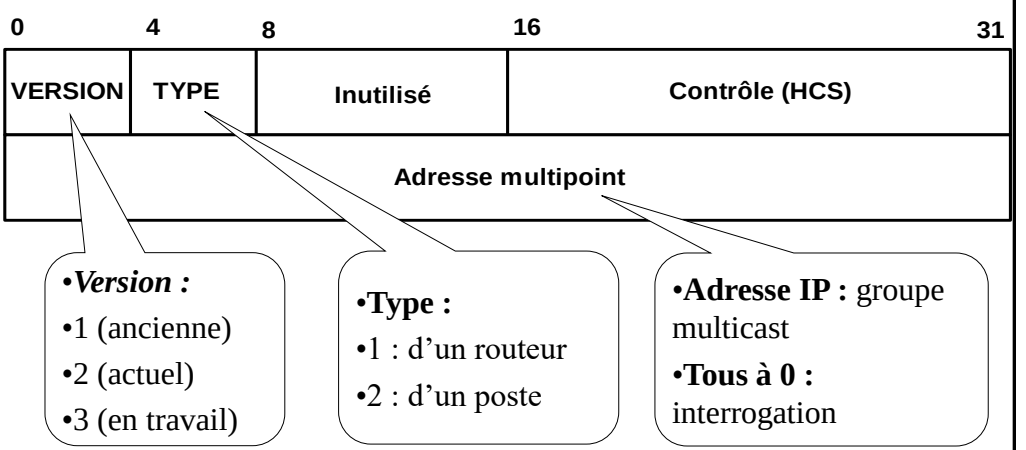
  – Choisir
  – Maintenir
  – et quitter un groupe

- **Trames IGMP**

  – De même niveau qu'ICMP
  – Encapsulée dans des trames IP

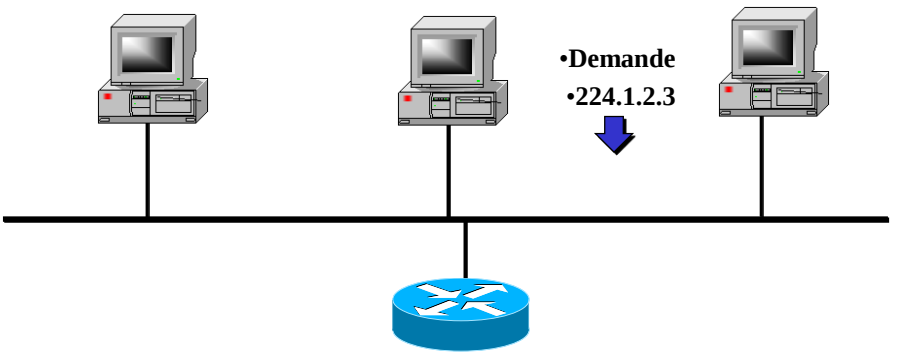
IGMP

- ***Trames IGMP :***



IGMP

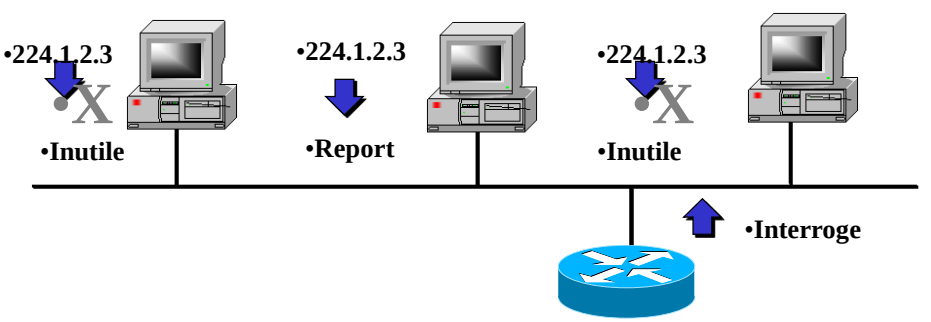
•Rejoindre un groupe



- Le poste envoie une demande au routeur
- Le routeur fait suivre la demande

IGMP

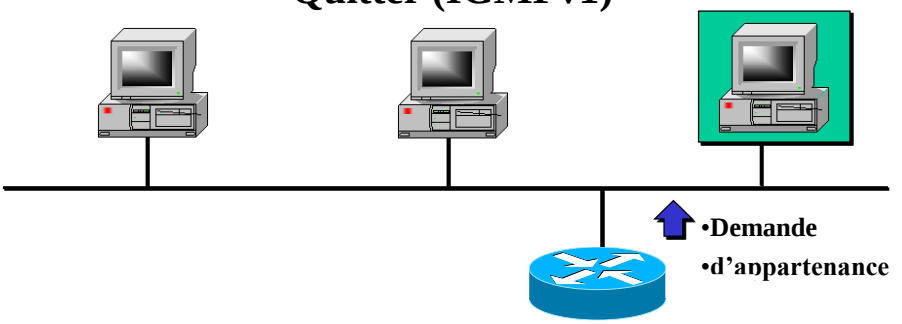
•Maintenir



- Le routeur interroge le 224.0.0.1 périodiquement.
- **Un membre répond (Report).**
- **Les autres voient la réponse et annule la leur.**

IGMP

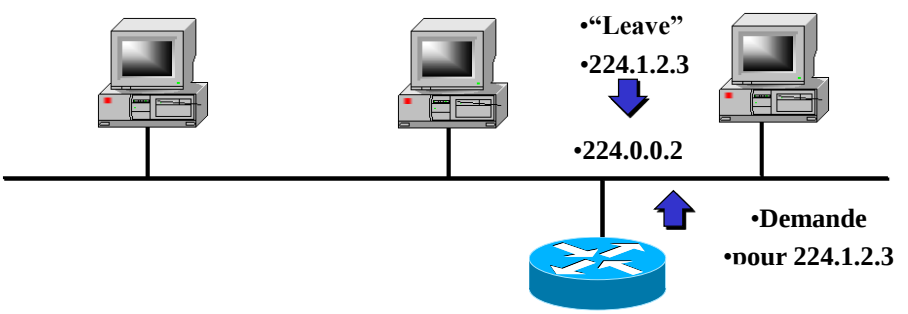
•Quitter (IGMPv1)



- Un poste quitte "silencieusement"
- Le routeur envoie au maximum 3 demandes
- Pas de réponse d'un des postes
- Arrêt de l'émission multicast

IGMP

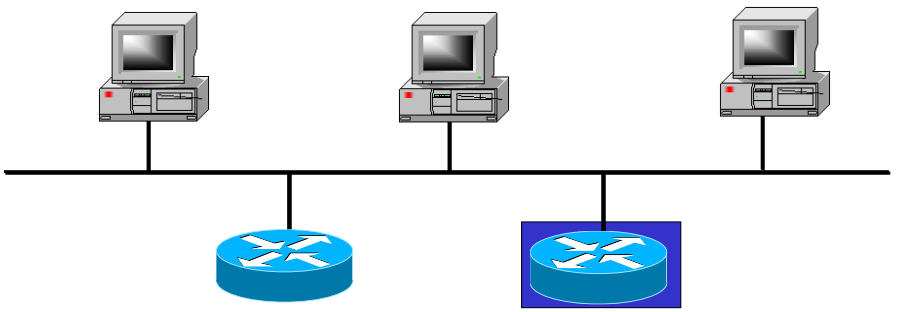
•Quitter (IGMPv2)



- Le poste envoie un message de fin à 224.0.0.2
- Le routeur envoie une demande au groupe
- Si pas de Report dans les 3 secondes
- Arrêt de l'émission multicast

IGMP

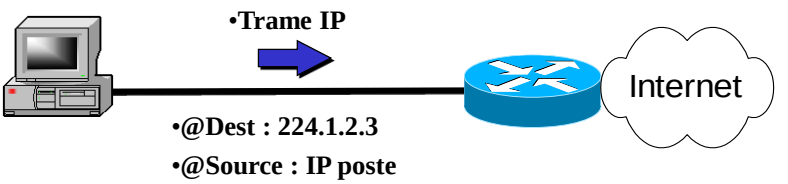
•Cas de plusieurs routeurs



- **Election d'un routeur "dominant" DR**
- **IGMP v1 : en fonction du routage**
- **IGMP v2 : adresse IP la plus petite**
- **Le DR gère l'IGMP**

Emission / Réception

- *Emission*
  - A une adresse multicast = un groupe
  - Appartenance au groupe facultative



- *Réception*
  - Automatique par le routeur qui est abonné au groupe
  - Envoyer grâce à une trame de niveau 2 multicast
  - Abonnement obligatoire

Techniques et Protocoles Multicast

Généralités du routage

- Attention le routage en multicast n'a pas de point commun avec le routage unicast !
- Il s'intéresse plus à la source qu'à la destination d'un message.

Vocabulaires

- Inonder (Flood)
  - Envoyer un message sur la totalité de l'arbre
- Élaguer (Prune)
  - Enlever une branche inutile
- Greffer (Graft)
  - Ajouter une branche à l'arbre

Types de protocoles

- **2 types :**
  - Mode Dense :
    - Inondation du réseau
    - Élagage des branches non-utiles

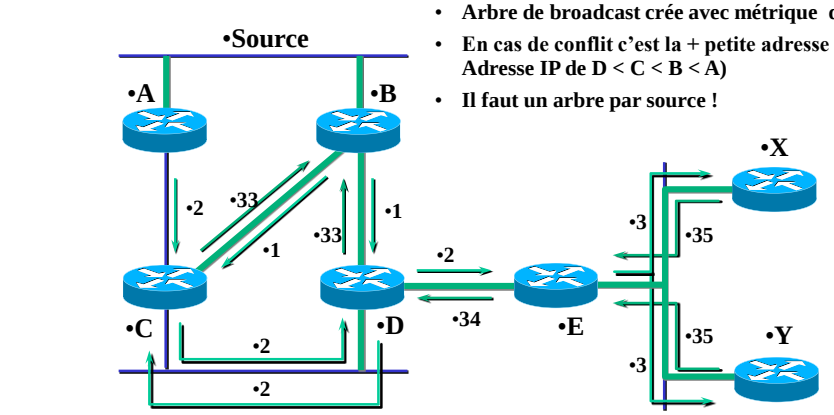
      ⇒ Beaucoup de destinataires
  - Mode Clairsemé (Sparse) :
    - Le trafic est émis à ceux qui le veulent
    - Mécanisme explicite d'attachement

      ⇒ Peu de destinataires

DVMRP : Distance Vector Multicast Routing Protocol

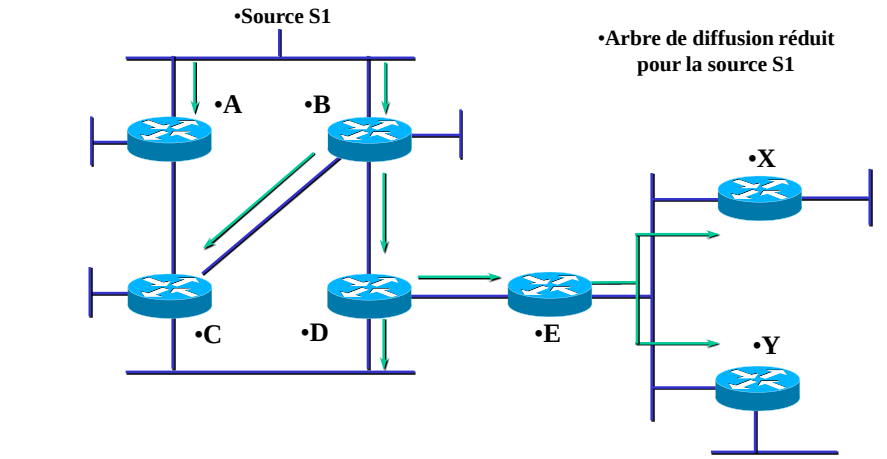
- **Protocole Dense**
  - Algorithme à vecteur de distance
    - Utilise des métriques
    - Proche de RIP
    - Avec un infini à 32 (15 pour RIP)
  - Utilise l'inondation et l'élagage
    - On inonde suivant l'arbre de diffusion réduit
    - Les branches inutiles sont enlevées
    - On re-inonde régulièrement

DVMRP : Création de l'arbre réduit

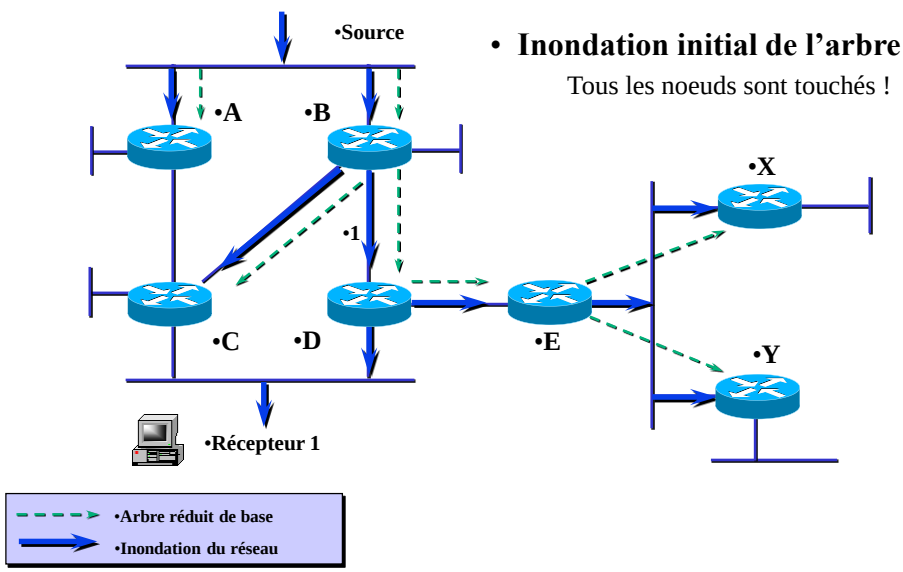


- **Arbre de broadcast crée avec métrique de chaque ligne**
- **En cas de conflit c'est la + petite adresse IP qui gagne. Ici : Adresse IP de D < C < B < A)**
- **Il faut un arbre par source !**

DVMRP : Création de l'arbre réduit

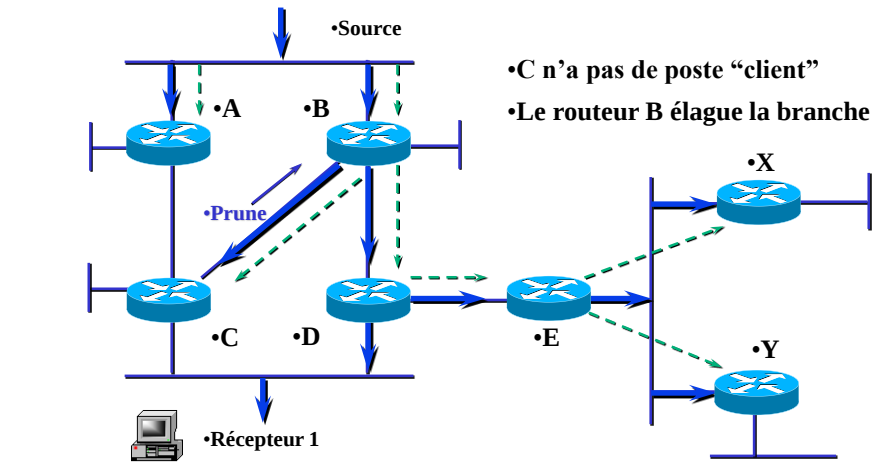


DVMRP : Élagage



- **Inondation initial de l'arbre :**
  Tous les noeuds sont touchés !

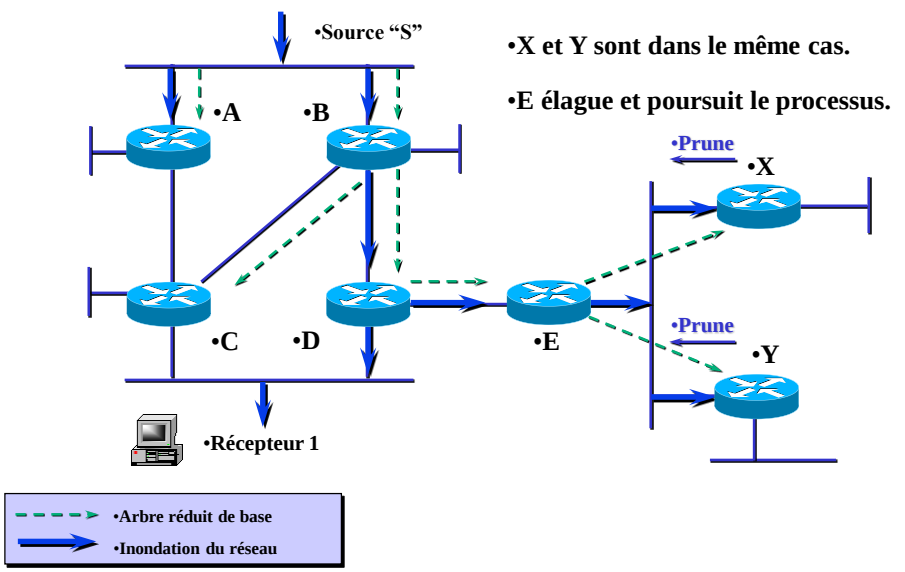
DVMRP : Élagage



•C n'a pas de poste "client"

•Le routeur B élague la branche

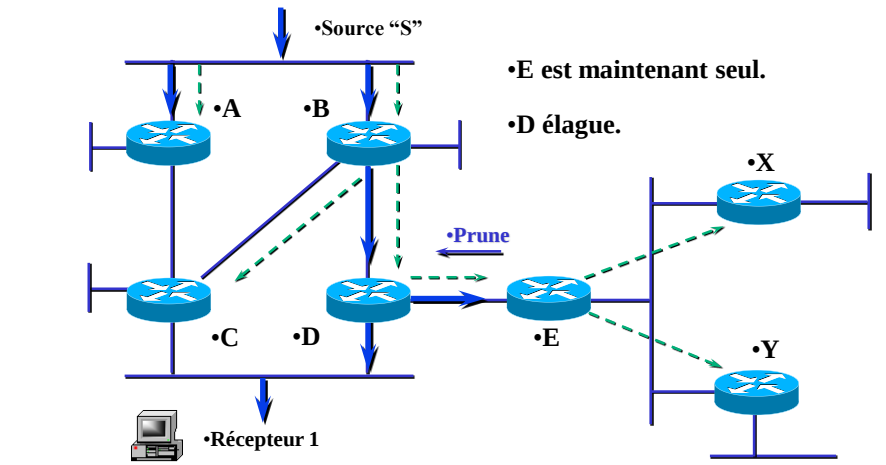
DVMRP : Élagage



•X et Y sont dans le même cas.

•E élague et poursuit le processus.

DVMRP : Élagage



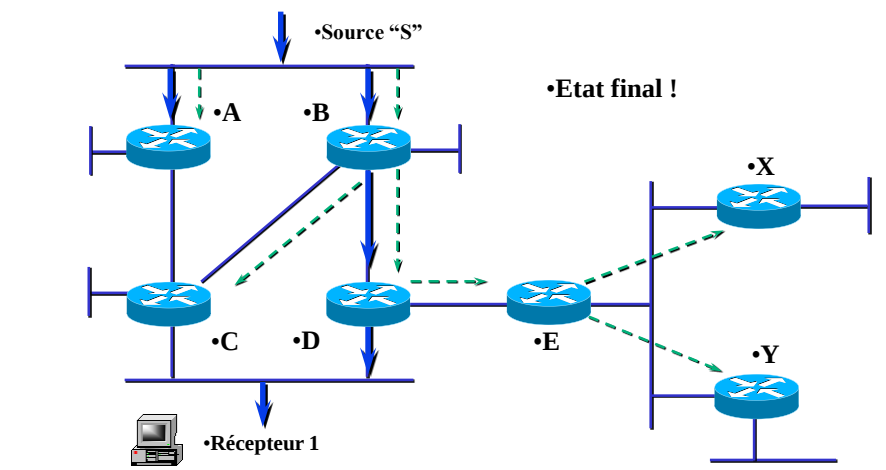
•E est maintenant seul.

•D élague.

•Arbre réduit de base

•Inondation du réseau

DVMRP : Élagage

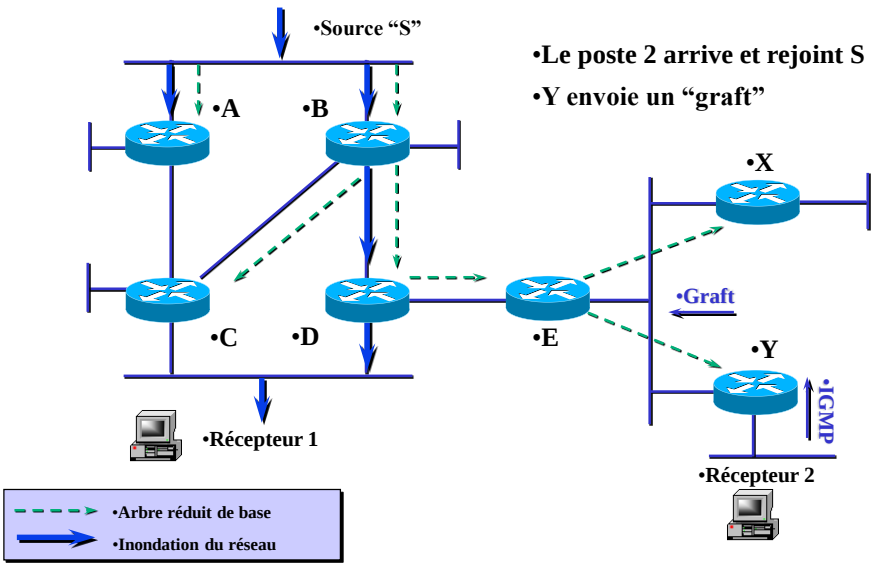


•Etat final !

•Arbre réduit de base

•Inondation du réseau

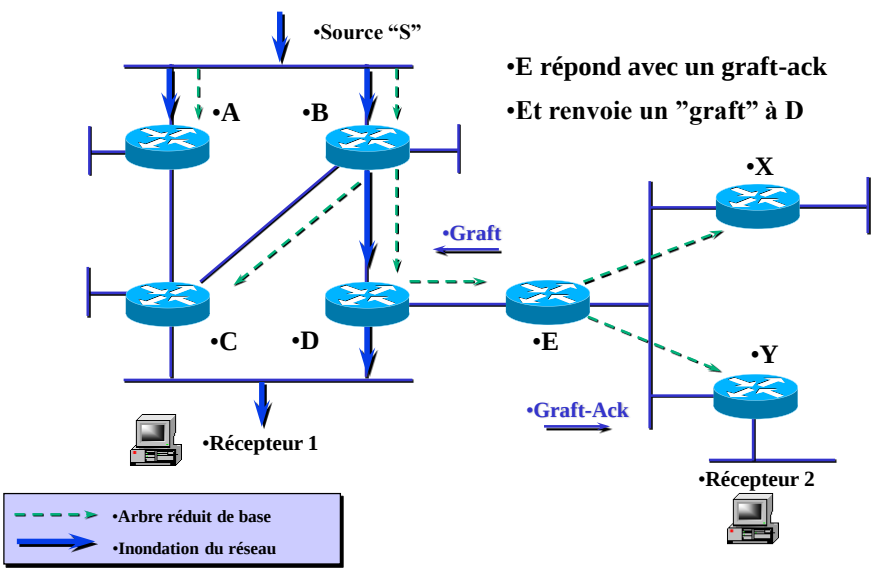
DVMRP : Greffe



•Le poste 2 arrive et rejoint S

•Y envoie un “graft”

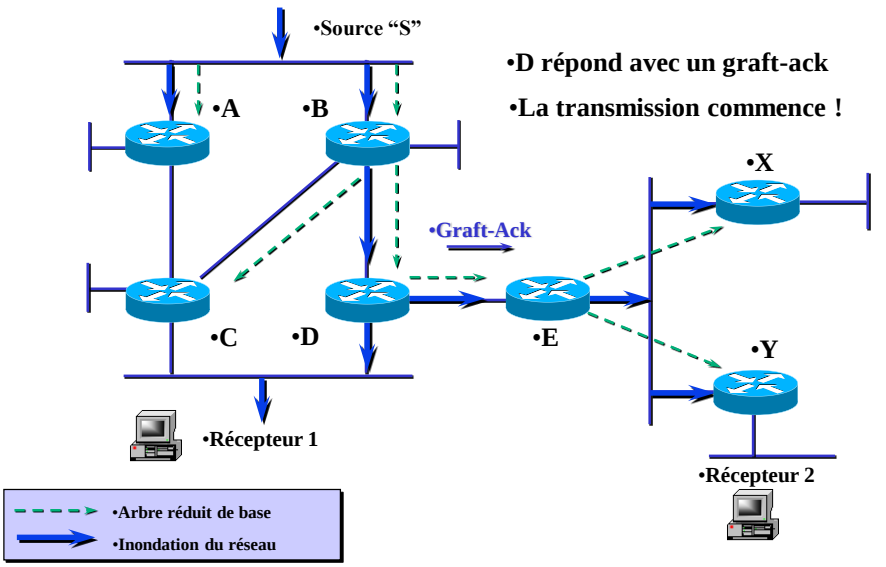
DVMRP : Greffe



•E répond avec un graft-ack

•Et renvoie un ”graft” à D

DVMRP : Greffe



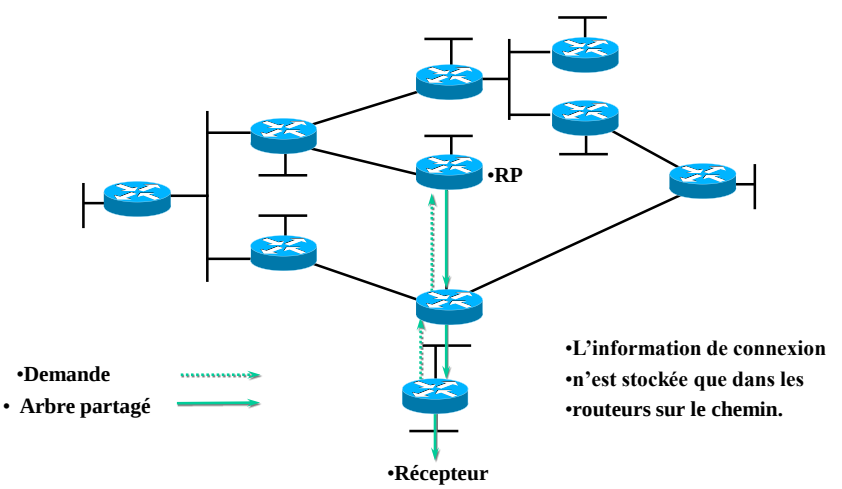
DVMRP

- Très utilisé au début du multicast (solution logiciel mrouted)
- Problème d’augmentation de charge :
  - Convergence lente (comme RIP)
  - Beaucoup d’informations doivent être stockée dans les routeurs
  - Pas de gestion des arbres partagés
- Ne convient pas pour des réseaux de grande taille :
  - Inondation et élagage long et coûteux en ressources
  - Inondation régulièrement répétée pour voir nouveau routeur
    (entre 60 secondes et 3 minutes)

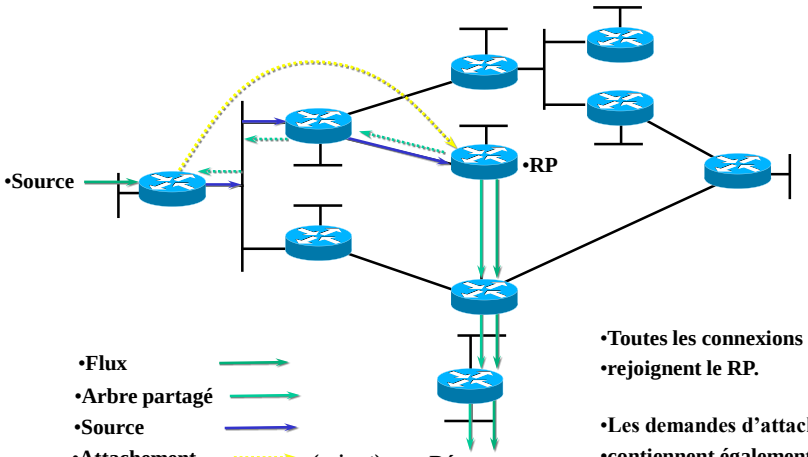
PIM : Protocol Independent Multicast

- **Protocole Sparse Mode :**
  - Peu de densité de récepteurs/émetteurs.
- **Avec point de rendez-vous RP :**
  - Point commun entre tous les postes multicast du réseau pour acquérir et diffuser des données
  - Évite la surcharge des éléments actifs du réseau
  - Fragilisé par la concentration en un point
- **Indépendant du protocole de routage sous-jacent**

PIM : Point de Rendez-Vous



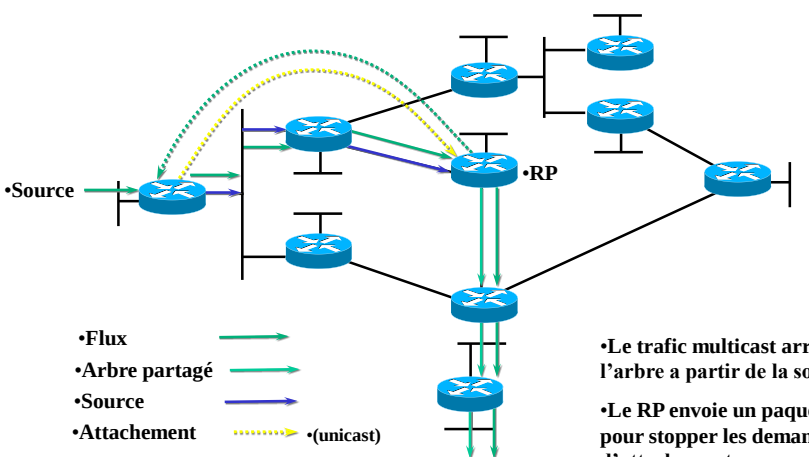
PIM SM : Enregistrement



•Toutes les connexions
•rejoignent le RP.

•Les demandes d'attachement
•contiennent également des
•données.

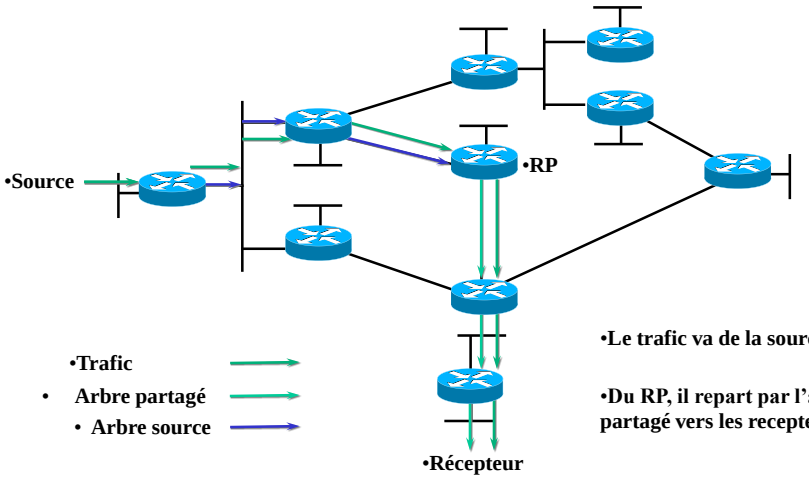
PIM SM : Enregistrement



•Le trafic multicast arrive par l'arbre a partir de la source.

•Le RP envoie un paquet unnicast pour stopper les demandes d'attachement.

PIM SM : Enregistrement

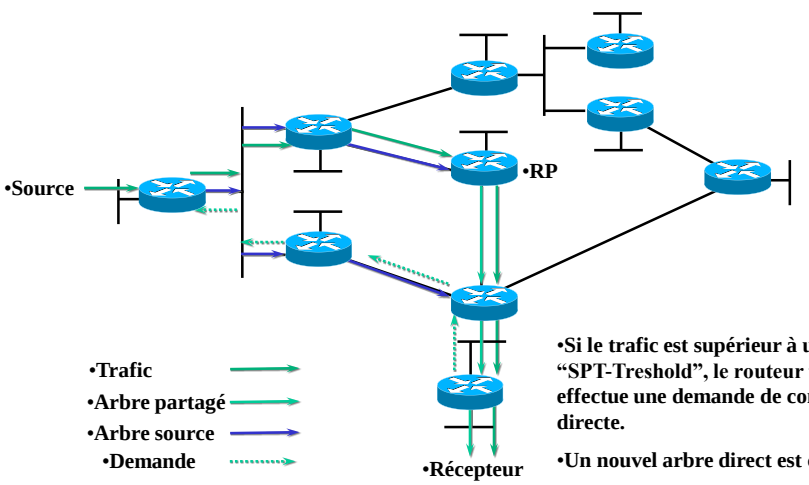


•Trafic
• Arbre partagé
• Arbre source

•Le trafic va de la source au RP.

•Du RP, il repart par l'arbre partagé vers les recepteurs.

PIM SM : Saut du RP

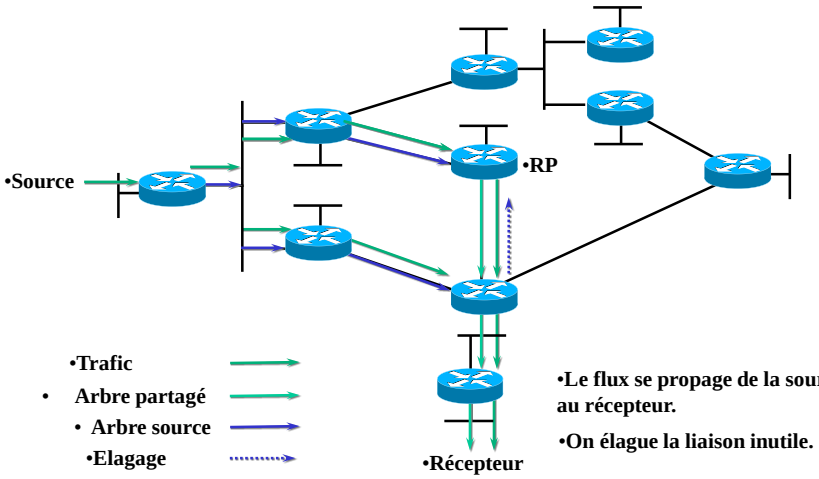


•Trafic
•Arbre partagé
•Arbre source
•Demande

•Si le trafic est supérieur à un seuil "SPT-Treshold", le routeur terminal effectue une demande de connexion directe.

•Un nouvel arbre direct est créé.

PIM SM : Saut du RP

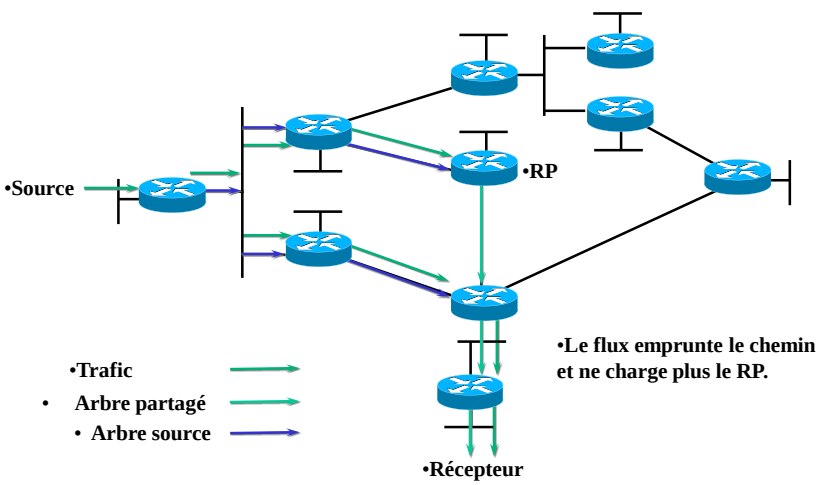


- •Trafic
- Arbre partagé
- Arbre source
- •Elagage

•Le flux se propage de la source au récepteur.

•On élague la liaison inutile.

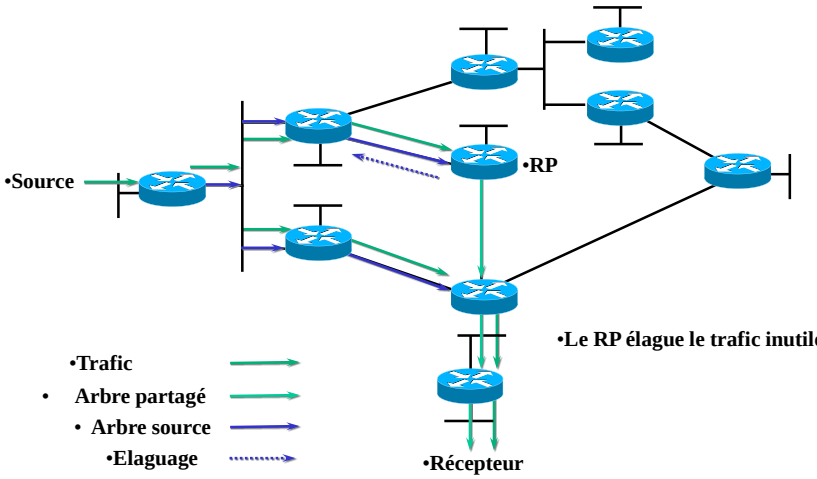
PIM SM : Saut du RP



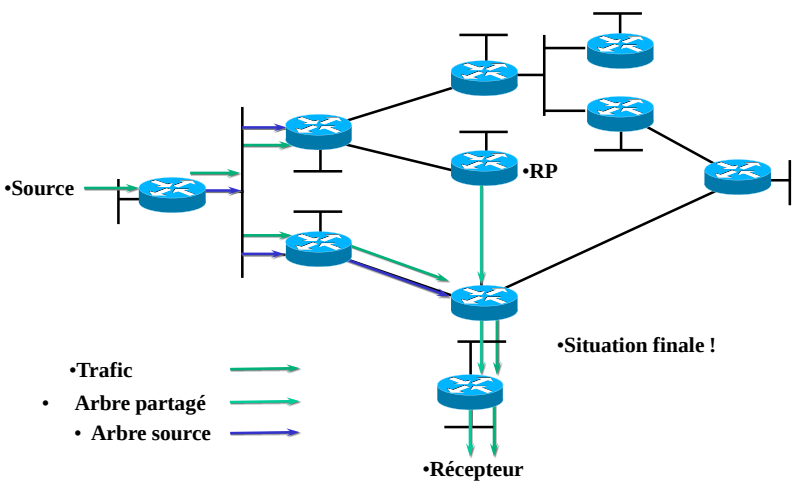
- •Trafic
- Arbre partagé
- Arbre source

•Le flux emprunte le chemin direct et ne charge plus le RP.

PIM SM : Saut du RP



PIM SM : Saut du RP



PIM SM : Conclusion

- Efficace pour tous le types de réseaux
- Avantages:
  - Le trafic ne se répand que lorsqu'on le souhaite
  - Quand le trafic est trop important on repasse en mode direct
- Très utilisé actuellement (inventé et déployé par Cisco)

PIMv2 = PIM SDM pour les grands réseaux

- **PIMv2 adapté à toutes les situations :**
  - Dense **: si pas de RP défini**
  - Sparse **: si un RP est présent**
- **Gestion des grands réseaux :**
  - Découpage en plaque (type OSPF/EGP/BGP)
  - Problème :
    Comment transmettre entre plaque ?
    Où placer le RP ?
  - Des solutions existent...

Applications existantes ?

Applications : Système d'exploitation

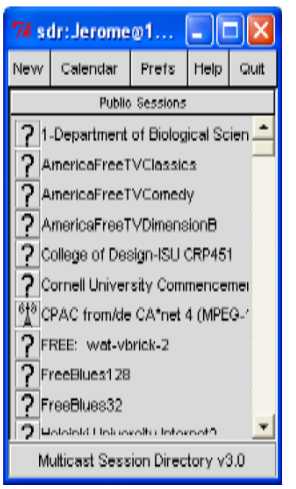
- **Contraintes :**
  - Niveau 2 : Ethernet (carte réseau)
  - Niveau 3 : IGMP, …

- ***Microsoft***
  - **Géré dès Windows 95**
  - **Serveur sous Windows 2000**

- ***Linux / Unix / BSD***
  - **Noyau spécifique**
  - **Pile TCP à mettre à jour**

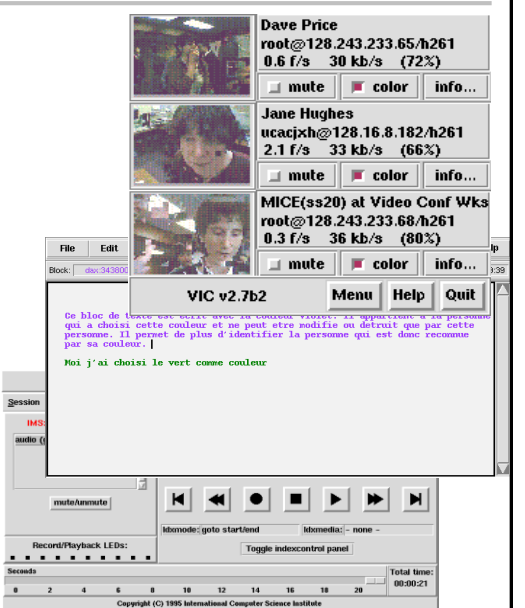
Applications : SDR

- **Connaître et rejoindre un groupe :**
  - Une solution : Session DiRectory (SDR)
  - Utilise une adresse multicast pour diffuser la liste des groupes
- **Créer un groupe :**
  - Spécifie les outils disponibles
  - Et les horaires de présence
  - Publie les infos en multicast sur le groupe SDR
  - Les conflits d'adresses sont résolues à la création de la session
  - Futur : MADCAP (DHCP Multicast)



Applications : travail coopératif

- **Outils usuels :**
  - RAT : Robust Audio Tool
  - VIC : VIdeo Conference
  - NTE : Network Text Editor
  - WB : White Board
  - …
- **Mais outils spécifiques !**
  - Protocoles standards
  - Maintenance dépendant des labos de recherches (University College of London)
  - Pas d'interfaces connues et simples



Applications : Sécurité

- **Problèmes de la diffusion :**
  - Visibilité des données
  - Possibilité d'appartenir à un groupe même si l'on est pas désiré
- **Solution : Chiffrement des annonces :**
  - Grâce à SDR
  - Cryptage DES, PGP
- **Cryptage dans les applications :**
  - Dépend de la confidentialité souhaitée
  - Peut être mis en oeuvre si besoin

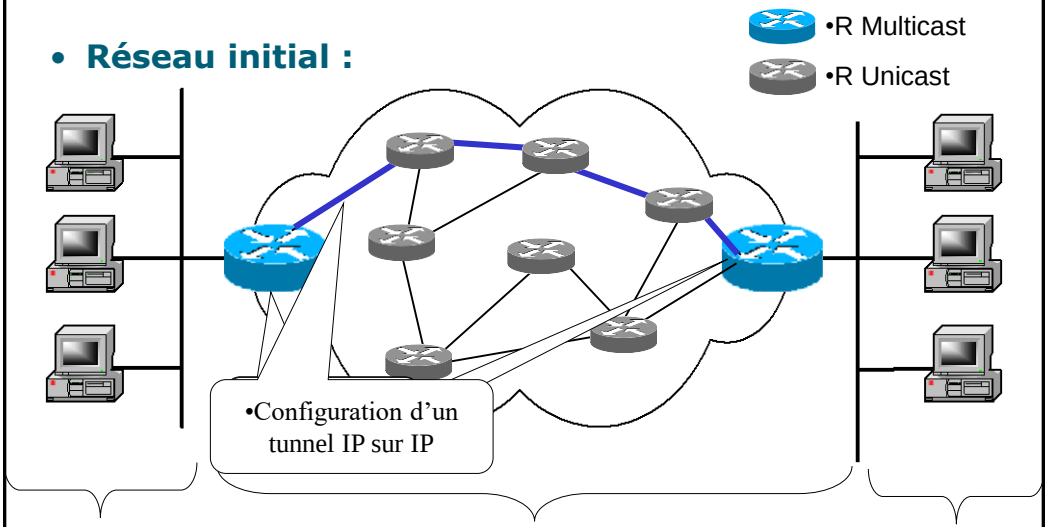
Le MBone

- **Besoin :**
  - Créer un réseau multicast sur Internet
- **Problème :**
  - Sur Internet tous les routeurs ne gèrent pas le multicast
- **Solution :**
  - Créer un sur-réseau au dessus d'Internet
  - Encapsulation des trames multicast dans des trames unicast (IP dans IP)

D'où le Multicast Backbone

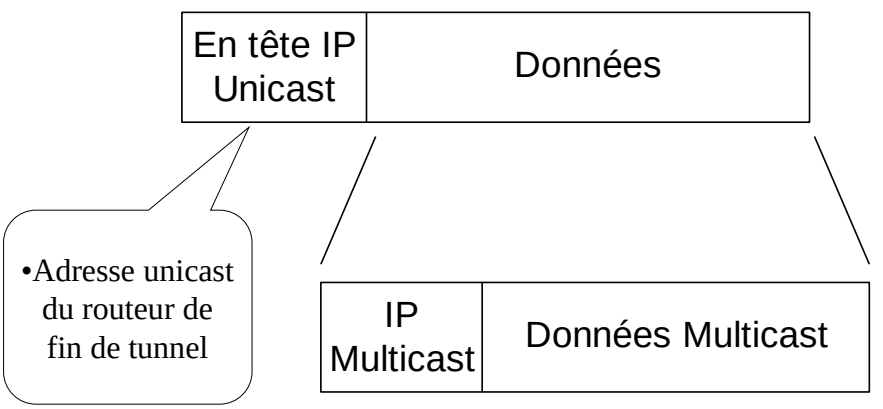
Le Mbone : Architecture

- **Réseau initial :**

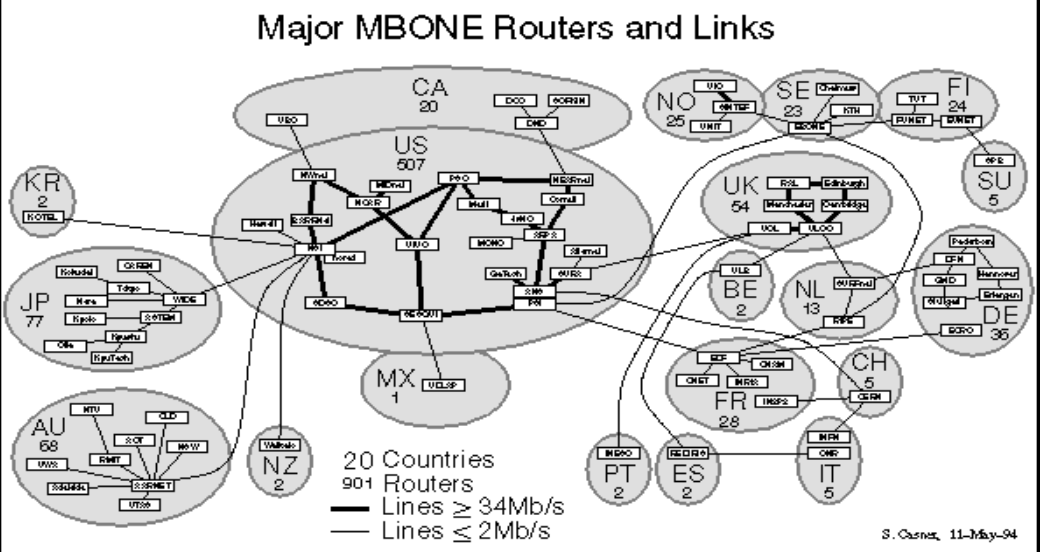


Le Mbone : IP sur IP

- **Encapsulation :**



Le Mbone : cartographie



Le Mbone : Avenir

- **Evolution en cours :**
  - Gérer le multicast de bout en bout
  - Eliminer l'encapsulation
- **Techniques mises en oeuvre :**
  - Internet 2 : Abilene
  - Réseau multicast des fournisseurs d'accès
  - Nouveaux protocoles
  - Déploiement en cours

Le Mbone : en France

- **Le 6bone**
  - Au dessus de Renater
  - Administré dans chaque centre réseau
  - Groupe de diffusion en français
- **En pleine évolution :**
  - Le M6Bone : architecture sur Renater 4
  - Augmentation de débit et de qualité de service par la gestion sur Renater 5 du multicast de bout en bout
  - Test grandeur nature du multicast sur ATM
  - **Déploiement en cours …**

Conclusion

- **Techniques au point :**
  - les défauts de conception ont été contournés
  - Reste des soucis pour les architectures complexes
- **Mise en œuvre principalement universitaire**
- **Gros potentiel d'avenir :**
  - intéressement des acteurs principaux du marché (Cisco, Microsoft, …)
  - Test grandeur nature chez les cablo-opérateurs
- **Manque de développement chez les ISP et d 'applications commerciales**

Domaine d'applications

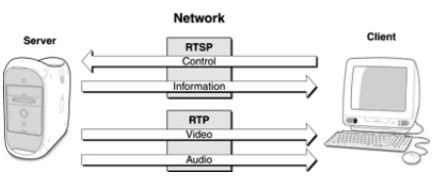
- ***Multimédia :***
  - **Streaming audio/vidéo**
  - **Formation à distance**
  - **Vidéoconférence**

- ***Informatique :***
  - **Distribution d'applications**
  - **Travail coopératif**

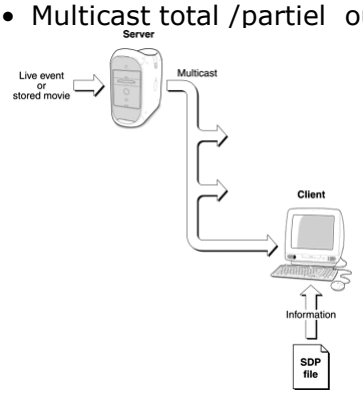
- ***Et n'importe quelle application "un à plusieurs"***

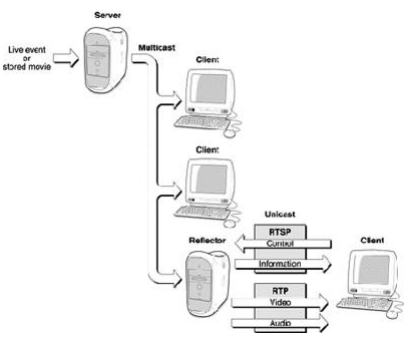
Protocoles pour le streaming

- Streaming
  - Basé sur la pile UDP / RTP / RTSP
  - Real Time Protocol
  - Real Time Streaming Protocol



- Multicast total /partiel ou Unicast





RTP & RTCP : protocole de transport

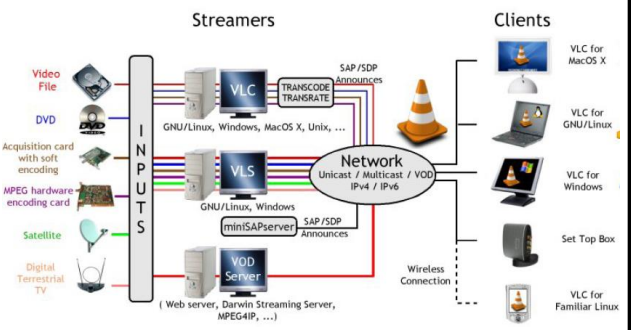
- RFC3550 et RFC3551
- RTP est associé à Real Time Control Protocol
  - **Il existe au moins 55 RFC associés à RTP → 1 pour chaque type de flux de données : H.261, H.264, MPEG4…**
  - **RTP fournit des fonctions de transport de bout en bout pour les applications temps réel**
  - **RTP et RTCP sont faits pour être indépendants de la couche transport**
- RTCP sert à informer :
  - **Qui arrive ou qui quitte la session**
  - **Rapport de réception périodique**
- Pour une session, l'émetteur utilise :
  - **Une adresse de groupe multicast**
  - **Un couple de numéros de ports :**
    - **1 pour le flux de données**
    - **1 pour les paquets de contrôle (RTCP)**
    - **Pour UDP et les protocoles similaires, RTP devrait utiliser un numéro de port pair et le flux RTCP correspondant devrait utiliser le numéro de port impair suivant**

RTSP : protocole de transport

- RFC2326
- Protocole au niveau application
- Ressemble à HTTP (client-serveur / requête/réponse)
- Propose un modèle extensible pour :
- le contrôle et la diffusion à la demande de données en temps réel principalement le multimédia
- Flux pré-enregistrés ou des flux en « direct-live »
- RTSP est fait pour :
  - Le contrôle de la diffusion de sessions
  - choisir le canal entre UDP, TCP, multicast
  - choisir le mécanisme de diffusion tel que RTP

Clients et Serveurs de Streaming

- Serveurs
- Réception flux des producteurs/diffusion multicast via RTP
  - HelixServer
  - Apple Darwin Server
  - Windows Media Server
  - MPEG4IP
  - VideoLan Server (VLS)
  - Conference XP



- Clients
- Lecture fichier SDP + RTP +…
  - VideoLan Client (VLC)
  - Realplayer
  - Windows media player
  - Quicktime

- SAP / SDP : Session Anoncement/Description Protocol

Réseaux Avancés – DI5

Réseaux Industriels :

Can, Profibus, Fip, EtherNet …

CANopen

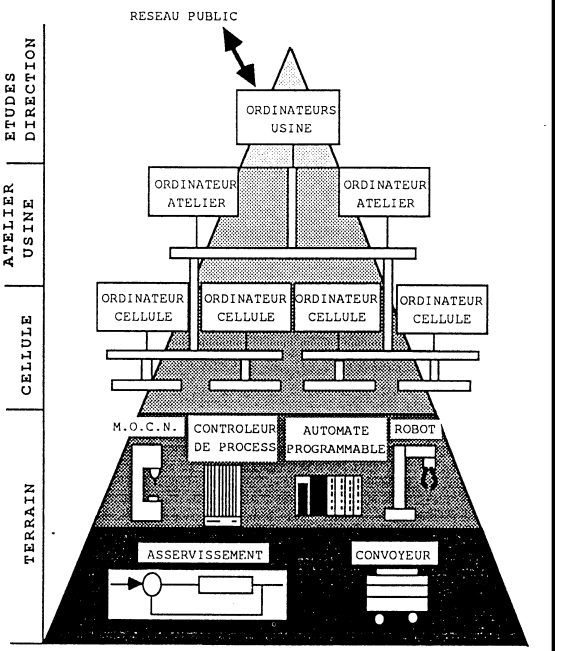
AS-i INTERFACE

WorldFIP THE EFFECTIVE FIELDBUS

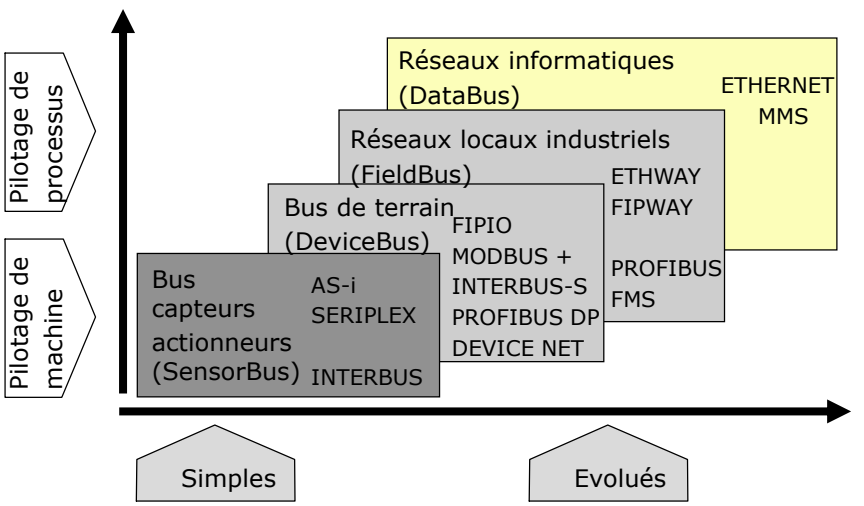
PROFIBUS PROCESS FIELD BUS

EtherNet/IP

Modèle d'usine intégrée



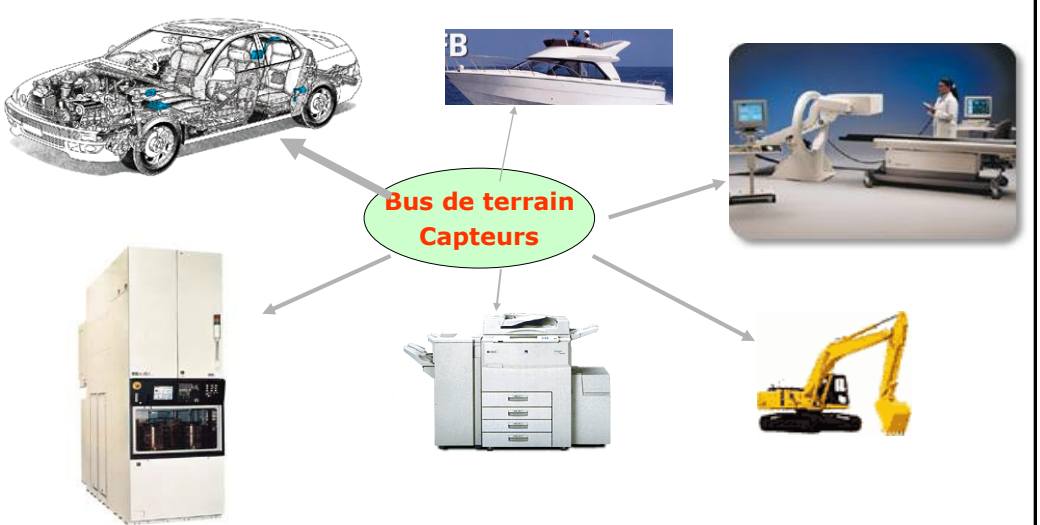
Applications industrielles des réseaux



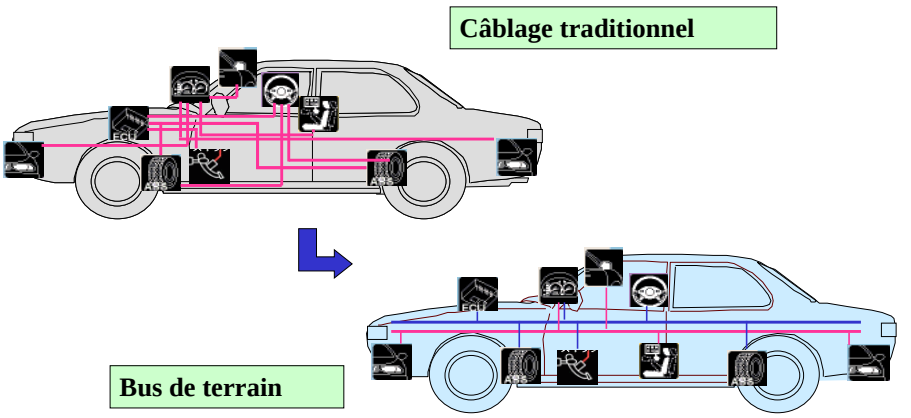
Objectifs et conséquences

- Interconnexion, communication simplifiée entre plusieurs entités d'un même système
- Réduction de la longueur des liaisons entre les différents éléments grâce à un support commun de transmission (simplification du cablage)
- Gain de place (électronique embarquée)
- Sécurisation des liaisons
- Différents modes de transfert d'information (bit par bit, paquet de bits, synchrone/asynchrone, …)
- Simplification de la maintenance
- Plus d'interopérabilité →insertion ou suppression d'éléments au sein d'un même système, normalisation des protocoles

Applications industrielles des réseaux



Applications industrielles des réseaux



Contraintes industrielles

- **Temps Réel**

On dit qu'il y a **traitement temps réel** lorsque le temps de réponse à des interrogations est soumis à des contraintes du système . Il en découle 2 situations:

- Le système transactionnel où l'on tolère le dépassement d'un temps de réponse donné sur quelques échantillons: la contrainte de temps n'entraîne pas de défaillance du système à condition qu'elle se produise avec une probabilité bornée. C'est le temps réel mou.

- La commande de processus où le respect d'un temps de réponse donné doit être garanti dans tous les cas sous peine de voir apparaître une dégradation, voire même un effondrement du système, c'est le temps réel dur.

Contraintes industrielles

- **Déterminisme**

Un système est déterministe quand le comportement des sorties est parfaitement maîtrisé et ce quelles que soient ses entrées
On peut distinguer :

➢ Le déterminisme temporel lorsqu'il y a respect du timing,

➢ Le déterminisme évènementiel lorsque tous les évènements sont traités.

Il découle de cette notion plusieurs autres :

➢ La prévisibilité montre les possibilités que l'on a de prévoir comment le système va se comporter quelles que soient les circonstances.

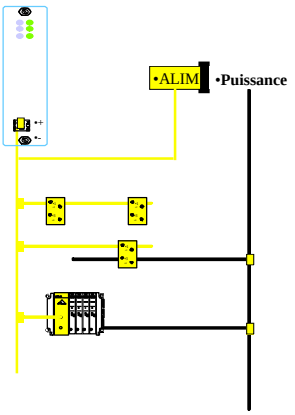
➢ L'urgence : il s'instaure une hiérarchie entre les différents traitements à effectuer ; certains étant plus importants que d'autres.

Caractéristiques des réseaux industriels

- Topologie → Bus
- Méthodes d'accès → Déterministe : M/E, Jeton, Polling
- Débit moyen – longueur des trames faible
- Nombre de nœuds faibles (adressage)
- Modèle OSI simplifié : Couches 1 + 2 + 7

AS-i (Actuator Sensor Interface)

Le Standard International pour le bus de terrain de plus bas niveau



•Réseau de Capteurs / Actionneurs

Caractéristiques de AS-i

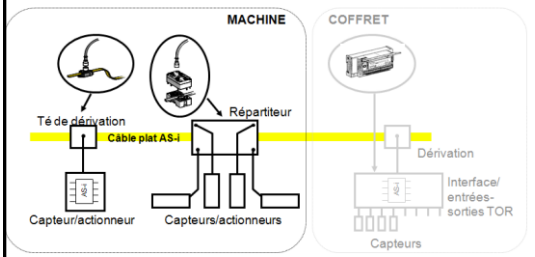
- **PHYSIQUES**
- Topologie: Libre
- Médium: Câble 2 fils non blindés
- Distance: 100m (300 répéteurs)
- Nombre de nœuds: 31 esclaves
- Utilisation du courant porteur
- Données et puissance sur le même câble (jaune)

COMMUNICATION

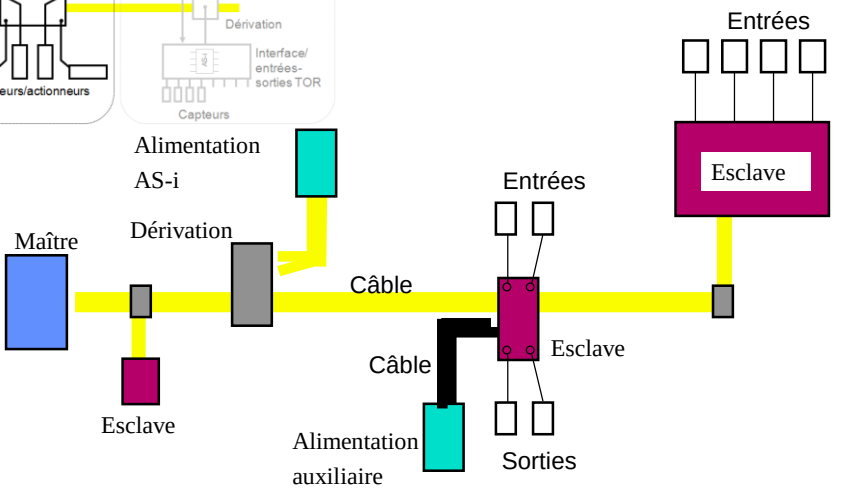
- Principe de communication: Maître/Esclave par polling
- Vitesse: temps de cycle < 5ms
- Taille des données: 4 bits

- **DIVERS**
- Esclave = 4 entrées TOR + 4 sorties TOR + 4 bits de paramétrage
- E/S analogique possible
- Câble auto-cicatrisant

Caractéristiques de AS-i

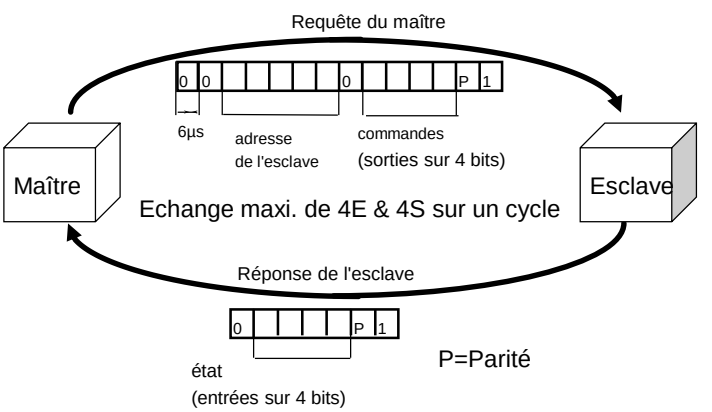


- Dérivation
- Alim auxiliaire possible
- Prises vampires ou boitiers



Caractéristiques de AS-i

- Trame courte, efficace et de longueur constante
- Le temps de cycle AS-i est court et répétitif



FIP (Flux d'Informations Processus)

Projet français lancé par le ministère de l'industrie dans les années 1990

→ cible = réseaux de terrain

Objectif

1) Normalisation des connexions entre capteurs, actionneurs, automates, …

2) Très faible coût => circuit intégré.

Utiliser par Schneider – Télémécanique

En forte perte de vitesse actuellement → cf Ethernet industriel

FIP (Flux d'Informations Processus)

- Caractéristiques d'un réseau de terrain :
  - les échanges sont toujours parfaitement identifiés, répertoriés au moment de la conception du système.
  - Chaque échange peut donc avoir un identificateur.
  - L'ensemble de ces identificateurs (ou objets) constitue ce que l'on nomme la nomenclature.
- Principe du fonctionnement
  - Un protocole à scrutation périodique et diffusion : une station scrutée diffuse l'information précise qui lui a été demandée, les stations réceptrices copient ou ignorent cet objet selon sa nomenclature.

→ Il faut une station maître ou arbitre du bus qui gère l'accès au médium en fonction de la nomenclature.

FIP (Flux d'Informations Processus)

- **Couche physique**
  - médium : paire torsadée pour la version la plus lente
  - topologie en BUS avec prise passive
  - transmission en bande de base, codage Manchester
  - Débit : 50 Kb/s avec une portée de 2km, 250 Kb/s, et 1 Mb/s sur 500m.
- **Couche liaison de données (couche "gonflée")**
  - Gestion centralisée (station maître).
  - Scrutation périodique des éléments du réseau
  - Adressage des actionneurs ou transferts de messages vers les autres équipements à la demande.
  - Bus transporte des messages de la forme : Nom objet - Valeur
  - Nomenclature sur 16 bits : trames d'information comportant de 1 à 16 données codées sur 16 bits.
  - Protection de toutes les trames par code cyclique : erreurs détectées mais non récupérées.

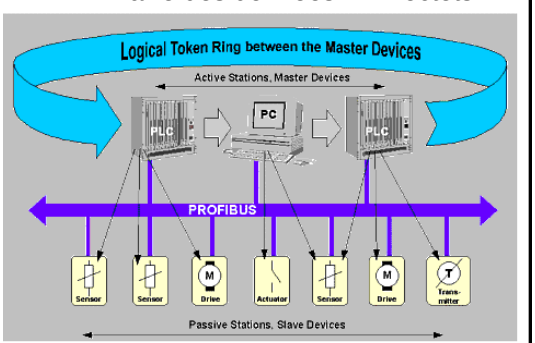
PROFIBUS DP (Distributed Peripherals)

- **PHYSIQUES**
- Topologie: Libre
- Médium: Paire torsadée, fibre
- Distance:
  - 100m à 12 Mbps
  - 1200m à 9.6 Kbps
- Nombre de nœuds: 127

- **Variantes**
- Profibus PA
  - Plusieurs maîtres possibles
  - Jeton sur bus entre les maitres
  - Données et puissance sur le même câble

COMMUNICATION

- Principe de communication: Maître/Esclave
- Vitesse: 9.6 Kbps à 12 Mbps
- Taille des données: 244 octets



- PROFInet bus de terrain sous TCP/IP devrait remplacer Profibus

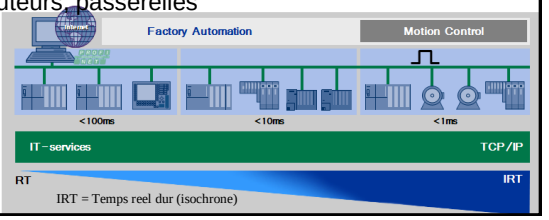
Ethernet + TCP/IP Industriel ?

Contre TCP/IP

- Protectionnisme commerciale et politique
- Chaque Bus de Terrain a ses propres caractéristiques et avantages
- TCP/IP n 'est pas temps réel
- Capacité mémoire importante et processeur puissant
- Mauvaise protection (sûreté de l 'information)

Pour TCP/IP

- Le PC Industriel est présent dans le secteur industriel
- Faible coût des cartes Ethernet pour PC
- Protocole TCP/IP bas niveau = Sockets BSD
- Interconnexion existante : ponts, routeurs, passerelles
- Services Internet (IT)
  - Télémaintenance
  - Supervision



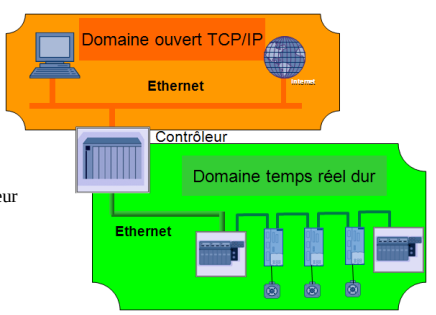
Ethernet + TCP/IP Industriel ?

Ethernet et Temps réel

Real-time class	1	2	3	4
Real-time requirement	low	mean	high	extremely high
User data length	to 500 Kbytes	to 500 byte	32 byte to 200 byte	to 10 byte
Delay time	to 5,000 ms	to 500 ms	to 5 ms	to 0.5 ms
max. jitter of delay time (according to IAONA)	> 1 ms	100 µs to 3 ms	10 µs to 400 µs	0.5 µs to 15 µs

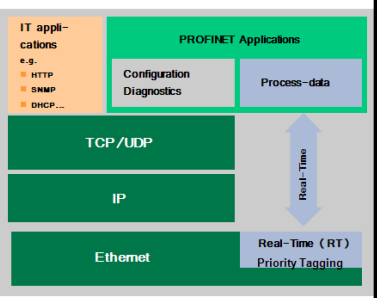
Les solutions existantes

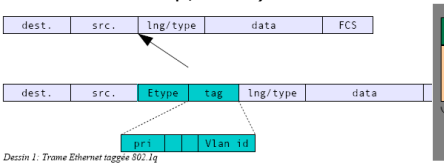
- Temps réel dur non garantie
- Réseau Ethernet fermé
  - Point faible en disponibilité (contrôleur)
  - Pas d'accès ouvert localement
  - L'ouverture extérieure dépend du fournisseur du contrôleur



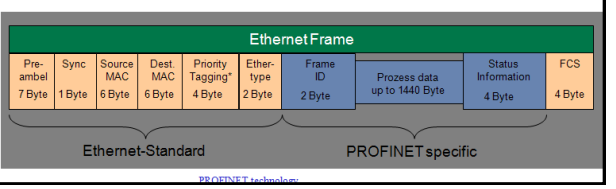
Profinet de Siemens

- Ethernet Standard
  - Tag de Priorité (802.1Q): 6 classes de priorité pour les trames Ethernet
  - Ether type selon IEEE pour les trames PROFINET temps-réel
    - 0x0800: trame IP
    - 0x8892: trame PROFINET temps-réel
- Spécifique Profinet:
  - Allocation des données reçues via le Frame-ID
    - Transmission Cyclique de données (de process)
    - Transmission événementielle (alarmes et événements)
  - Informations
    - Status de l'appareil et des données (e.g. Run, Stop, Error)





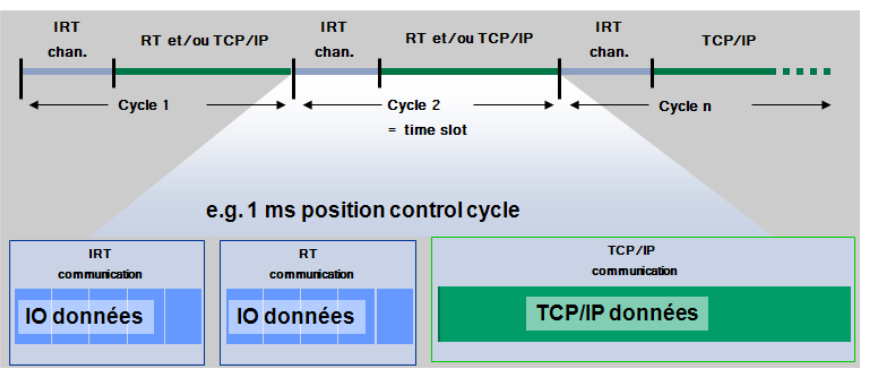
Dessin 1: Trame Ethernet taggée 802.1q



PROFINET technology

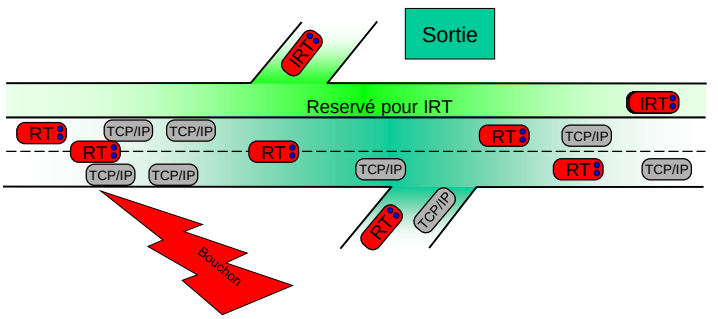
Profinet de Siemens

- Nécessite un support matériel pour l'allocation de créneaux horaires pour les messages temps-réel
  - Aucune influence des échanges TCP/IP ou broadcast/multicast sur les caractéristiques de la communication temps-réel
  - Niveau élevé de performance, même dans le cas de switches cascadés
  - Précision élevée des données horodatées
- Technologie de Base pour les applications isochrones



Profinet de Siemens

- Organisation de l'autoroute des données
  - 1 voie réservée pour IRT
  - RT via priorisation
  - Propriétés Real-time garanties, indépendamment de la charge réseau
  - Communication standard ouverte (TCP/IP, IT, etc.)



PROFINET technology

Ethernet Industriel : le matériel existe

- E/S déportées sur ETHERNET TCP/IP (WAGO Contacts)
- Automates

Un exemple type : CAN en détails

Historique

Depuis les années 1960 la **longueur** de câble utilisée dans l'automobile ne cesse de croître pour dépasser 2000 m en 1995. Le **nombre des connexions** atteint 1800 à cette même date. La fiabilité et la sécurité sont menacés.

Les normes en matière de **pollution** et de consommation d'énergie obligent les constructeurs à multiplier les capteurs et actionneurs intelligents dans leur véhicules accélérant ce processus de multiplication des câbles et connexion depuis une vingtaine d 'années.

Le besoin de sécurité accrue (ABS, ESP, AIR-BAG…) et la demande de confort (mémorisation des réglages de conduite, climatisation régulée par passager, système de navigation…) ne font que renforcer cette tendance.

La société BOSCH développe dès le début des années 1980 une solution de multiplexage des informations circulant à bord de la voiture. Le bus **CAN** apparaîtra et sera normalisé dans les années qui suivent (dès 1983).

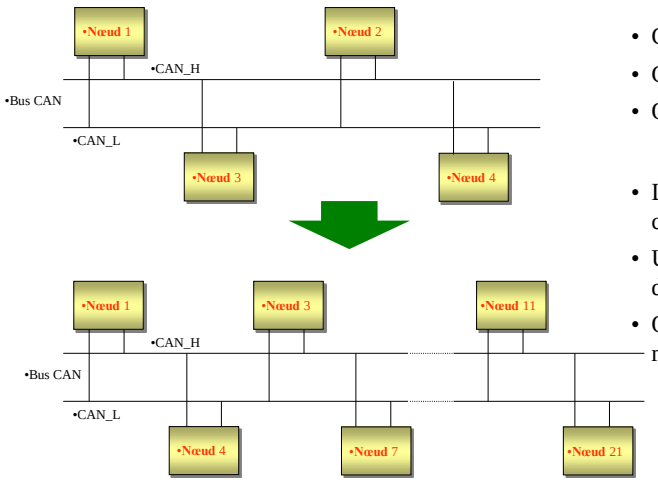
Les composants CAN se démocratisent et investissent d'autres secteurs de l'industrie (moissonneuses, pelleteuse, médical, produits numériques, systèmes électrotechnique…).

Bus CAN et modèle OSI

OSI	OSI	TCP/IP	Bus CAN
Couche application	Niveau application	-	Spécifié par l'utilisateur
Couche présentation	Niveau présentation	-	-
Couche session	Niveau session	-	-
Couche transport	Niveau message	TCP	CanOpen protocol
Couche réseau	Niveau paquet	IP	Network / presentation layer
Couche liaison données	Niveau trame	Acces reseau	MAC /LLC
Couche physique	Niveau physique	Acces reseau	PLS/PMA/MDI

La couche Physique

- Topologie du bus



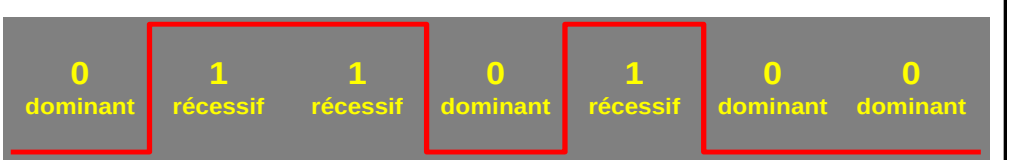
- **Avantages**
- Configuration simple
- Câblage réduit
- Ordre des nœuds indifférent

- **Désavantages**
- L'ensemble des nœuds est affecté en cas de défaut
- Une défaillance est plus délicate à diagnostiquer
- Outils de diagnostique et de maintenance spécialisés

La couche Physique

Codage NRZ : bits dominants et récessifs

- Utilisation de la méthode du NRZ (Non Return To Zero).
- Pendant la durée totale du bit, le niveau de tension de la ligne est maintenu
- Le niveau 0 est dominant – le niveau 1 est recessif

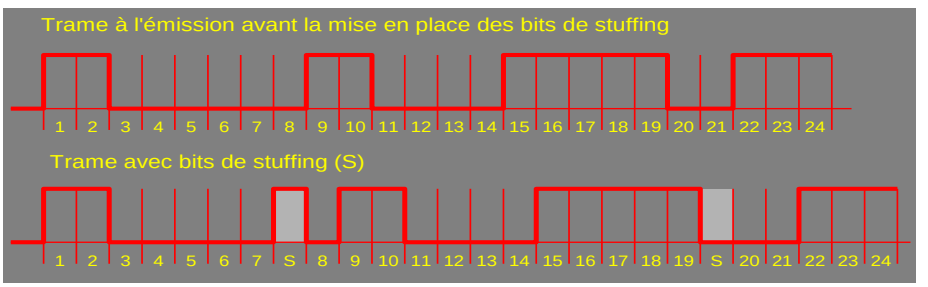


La couche Physique

Le bit stuffing

•Problème de fiabilité si un grand nombre de bits identiques se succèdent

•Le Bit Stuffing impose au transmetteur d'ajouter automatiquement un bit de valeur opposée lorsqu'il détecte 5 bits consécutifs dans les valeurs à transmettre (bit ignoré par le recepteur).

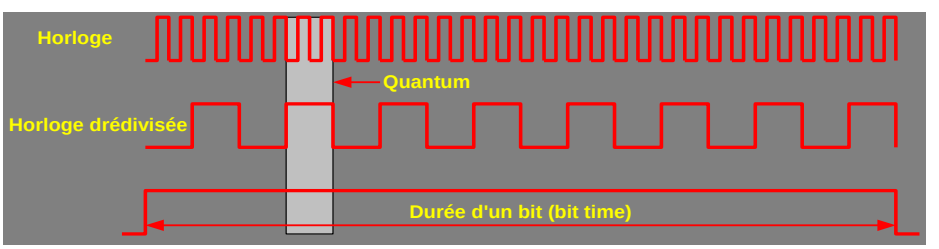


La couche Physique

Le bit timing

• On définit la plus petite base de temps reconnue sur un bus CAN comme étant le *Time Quantum*.

• Cette base de temps est une fraction de l'horloge de l'oscillateur du bus. Un bit dure entre 8 et 25 quantum

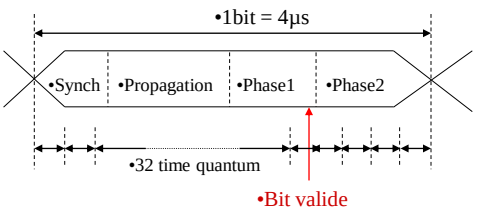


La couche Physique

Bit timing : lecture d'un bit

• 1 bit correspond à 32 coup d'horloge

• La lecture du bit devra être faite au 20^{éme} coup d'horloge



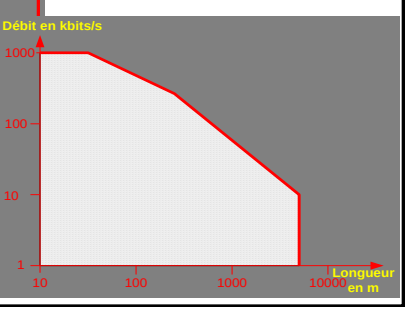
•ISO11898 : High Speed CAN

•250 Kbps

La couche Physique

Longueur du bus et débit

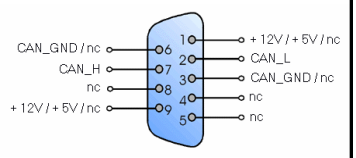
Débit	Longueur	Longueur d'un bit
1 Mbit/s	30 m	1 µs
800 kbit/s	50 m	1,25 µs
500 kbit/s	100 m	2 µs
250 kbit/s	250 m	4 µs
125 kbit/s	500 m	8 µs
62,5 kbit/s	1000 m	16 µs
20 kbit/s	2500 m	50 µs
10 kbit/s	5000 m	100 µs

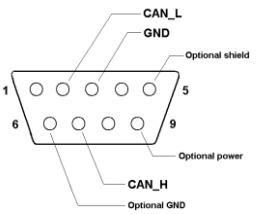


La couche Physique

Support CAN → norme ISO 11898-2

- CAN High Speed.
- Une paire par émission différentielle → On mesure la différence de tension entre les deux lignes (CAN H et CAN L)
- Terminaison par des résistances de 120 Ohm à chacun des bouts
- Différentes connectiques (RS485, usb, …)



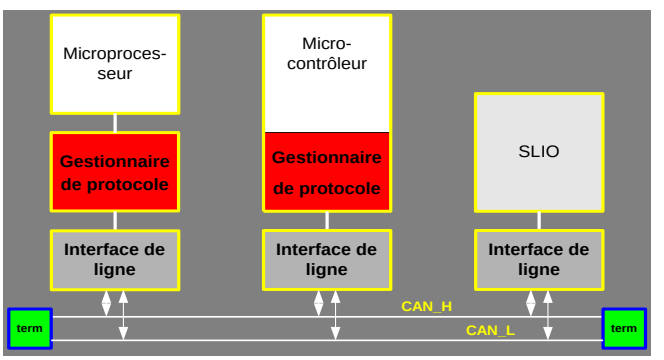


- Fibre optique ou transmission hertzienne possible

La couche Physique

Types de nœuds CAN

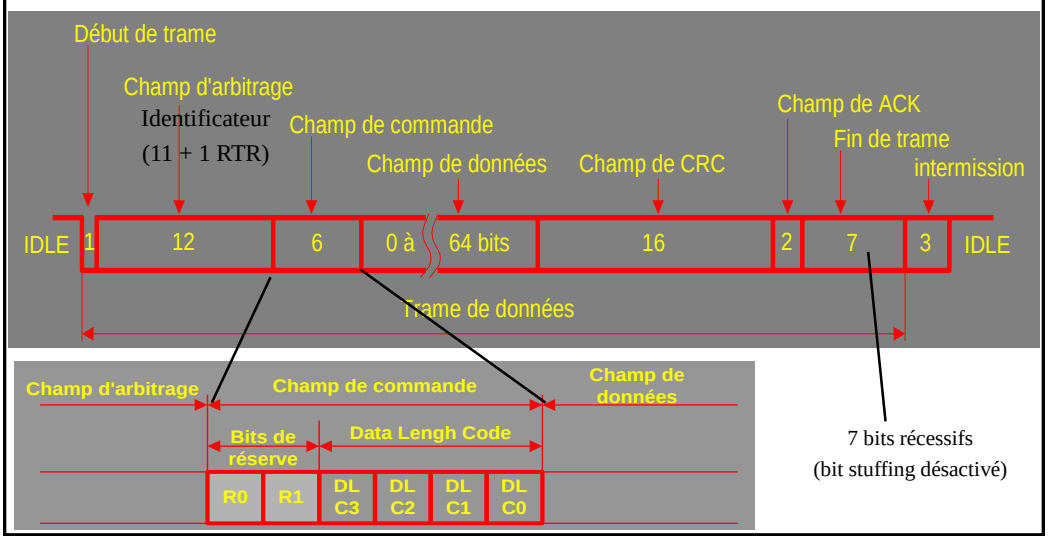
- les gestionnaires de protocole
- les microcontrôleurs à gestionnaire CAN intégré
- les interfaces (*transceivers* - ou encore *drivers*) de lignes
- les *Serial Linked Input Output* - SLIO



Trames CAN

Trame de données (data frame)

- Standard CAN 2.0A le plus utilisé (CAN2.0B possible via les bits R0 - R1)



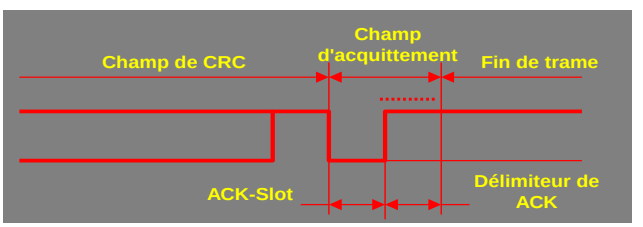
Trames CAN

Le champ de CRC : est composé de la séquence de CRC sur 15 bits suivi du CRC Delimiter (1 bit récessif)

- $P(X) = X^{15}+X^{14}+X^{10}+X^{8}+X^{7}+X^{4}+X^{3}+1$

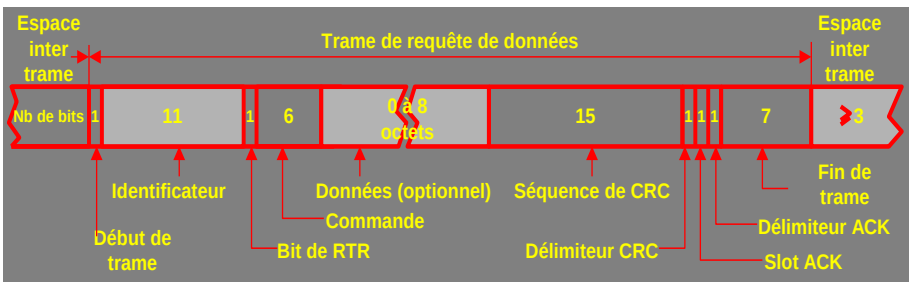
Le champ ACK

- 2 bits = ACK Slot + ACK Delimiter (1 bit récessif)
- le nœud en train d'emettre envoie un bit récessif pour le ACK Slot
- le nœud ayant reçu correctement le message en informe le transmetteur en envoyant un bit dominant pendant le ACK



Trames CAN

Trame de requête



Contrairement au cas précédent, le bit RTR est récessif. C'est donc ce bit qui différencie une *data frame* d'une *remote frame*

Pour mise en place d'un fonctionnement Requête-Reponse

Cette trame est moins prioritaire que la trame de données

Les Remote Frame sont peu utilisées en pratique

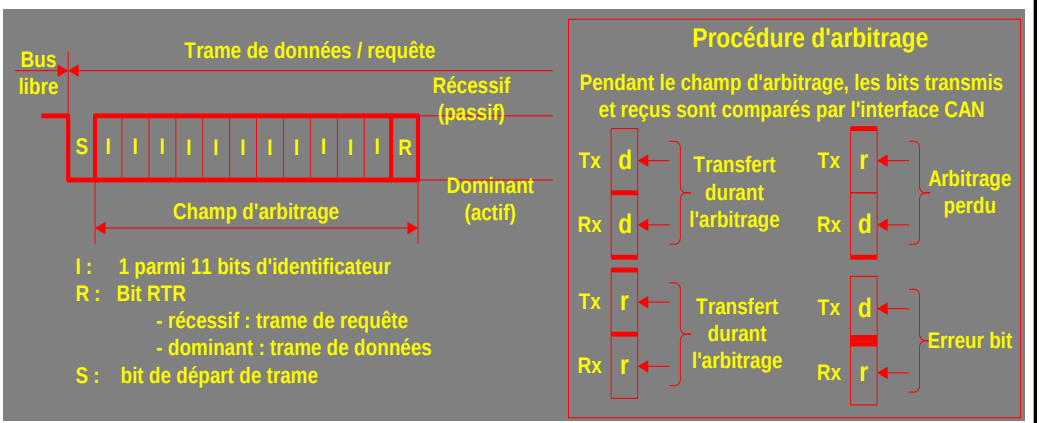
Methode d'acces MAC

- Basée sur la diffusion broadcast → proche ethernet

- Chaque station connectée au réseau écoute les trames transmises par les stations émettrices.
- Chaque nœud décide quoi faire du message, s'il doit y répondre ou non, s'il doit agir ou non, etc…
- Le protocole CAN autorise différents nœuds à accéder simultanément au bus
- Arbitrage par priorité → CSMA CD/AMP (*Carrier Sense Multiple Acces with Collision Detection and Arbitration Message Priority*).

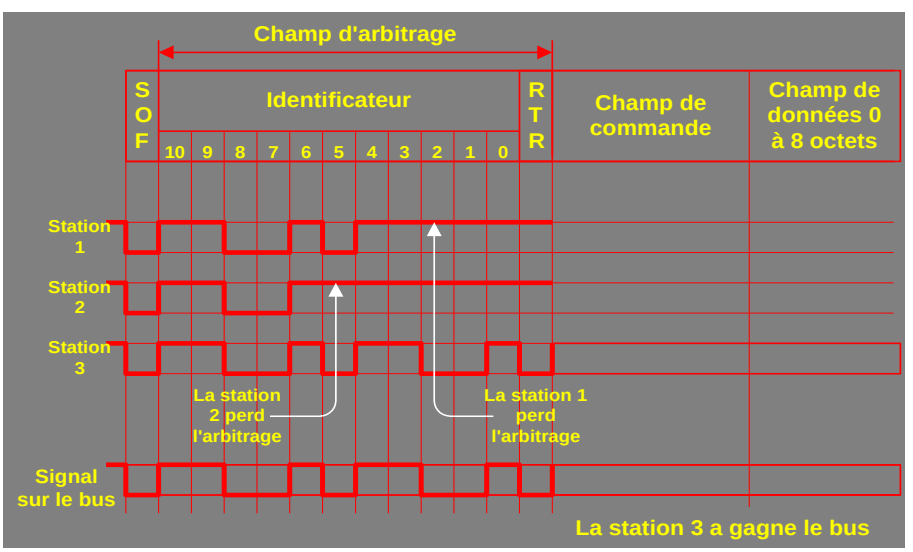
CSMA/CD AMP

La méthode d'arbitrage



CSMA/CD AMP

Exemple d'arbitrage



CSMA/CD AMP

Champs d'arbitrage

•Le bit SOF (début de trame de données) est dominant, il signale à toutes les stations le début d'un échange.

•Toutes les stations doivent se synchroniser sur la transition du bit de départ.

•Identificateur : La longueur de l'identificateur est de 11 bits

•Les 7 bits les plus significatifs (de ID_10 à ID_4) ne doivent pas être tous récessifs.

•Le bit RTR : Lors d'une *dataframe*, le bit de remote *transmission request* (RTR) doit être dominant.

La gestion des erreurs

•Mécanisme de confinement → pour déterminer si le bus :

- n'est pas perturbé du tout
- est peu perturbé
- est un peu plus gravement perturbé
- est tellement perturbé qu'il doit passer en bus off

• Le contrôleur du bus passe dans le mode *bus off* lorsque trop d'erreurs se sont produites

• Il se place dans l'état de sommeil (*sleep mode*)

• Il peut reprendre son activité si le taux d'erreur diminue

• Tous les (micro)contrôleurs conformes CAN possèdent deux compteurs internes bien distincts :

- le *transmit error counter*
- le *receive error counter*

La gestion des erreurs

De 0 à 127 inclus : état error active

- Le nœud continue de recevoir et d'émettre normalement
- Erreur détectée→ envoi de *active error*

De 128 à 255 inclus : état error passive

- Le nœud continue de recevoir et d'émettre normalement
- Erreur détectée→ envoi de passive error flag

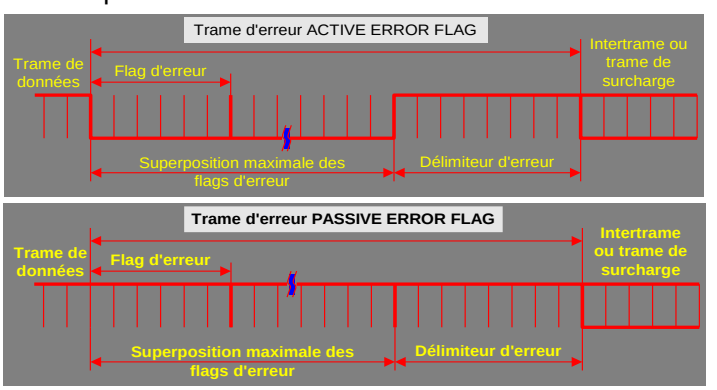
Au-delà de la valeur de 255 : état de bus off

- Le nœud en question cesse de recevoir et d'émettre normalement
- Le protocole autorise un nœud *bus off* à redevenir *error active* (en ayant remis tous ses compteurs d'erreurs à zéro) après que celui-ci ait observé, sans erreur sur le bus, 128 occurrences de 11 bits récessifs

Trames CAN

Trames d'erreurs

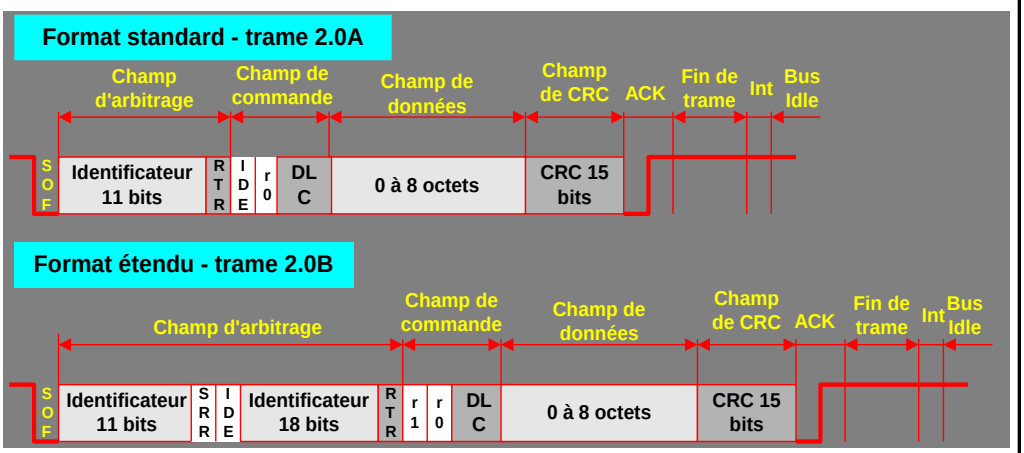
- Les 8 bits de l'Error Délimiter donnent l'autorisation aux nœuds du réseau de reprendre leurs communications.



- Des recherches ont montré que le taux d'erreurs non détectées par le protocole CAN est très faible : 1 erreur non détectée pour 1000 années de fonctionnement

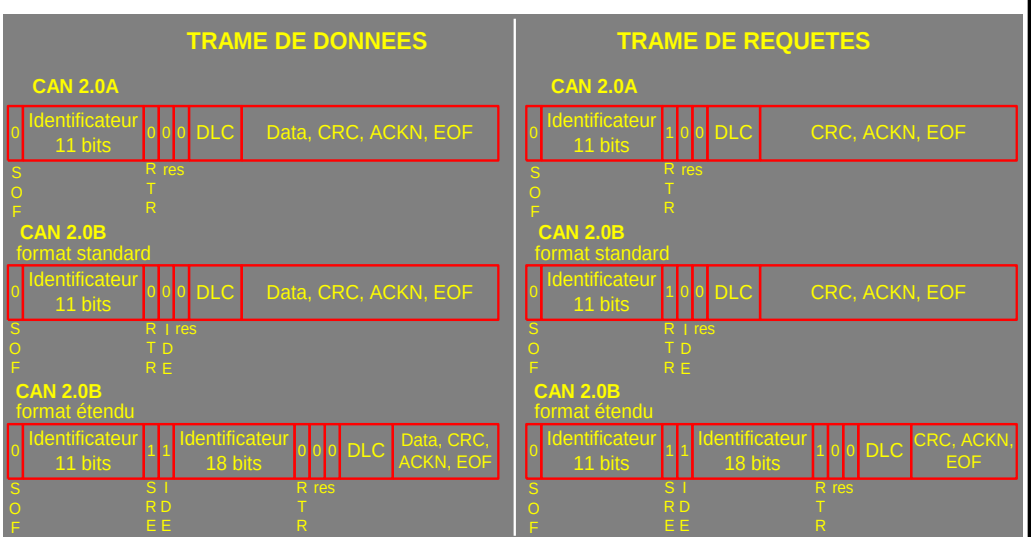
Le bus CAN 2.0B

Format des trames



Le bus CAN 2.0B

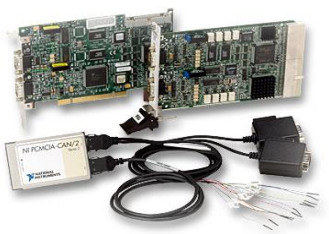
Le bus CAN2.0B est compatible avec le CAN2.0A

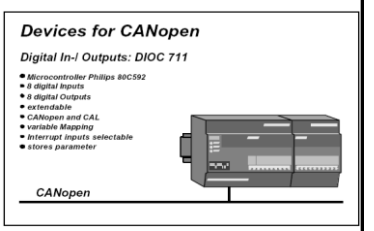


Les composants

Types de composants existants

- les gestionnaires de protocole
- les microcontrôleurs avec gestionnaires de protocole
- les interfaces de ligne
- les circuits d'entrées/sorties de type SLIO (série)





Exemple de mise en œuvre

Programmation via environnement spécialisé

Lecture de Variables mise à jour périodiquement via le bus

API : Programme et librairie fournis

• Les fonctions suivantes fournies par le constructeur de la carte contrôleuse du bus permettent de dialoguer sur le bus et de gérer le process (La carte utilise un contrôleur de bus 82527).

• INIT :
  - **CAN_Open**
  - **CAN_Close**
  - **CAN_SetObjectConfig**
  - **CAN_InitBoard**

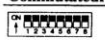
• Message operation:
  - **CAN_GetMessage**
  - **CAN_SendMessage**
  - **CAN_RequestRemoteFrame**

Exemple de mise en œuvre

Réglage du débit numérique

Le débit numérique se règle avec les commutateurs DIP 6 et 7. Il doit être réglé à une valeur identique sur tous les modules-noeuds.

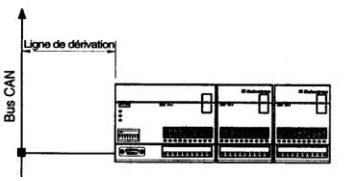
Remarque: La vitesse de transmission (débit numérique) influence la longueur de bus maximale possible.

Commutateur DIP S1	Commutateur:	Fonction:
	1 ... 5	Adresse CAN
	6 ... 7	Débit numérique
	8	Réserve

Commutateur DIP S1

6	7	Débit numérique	Long. max de bus	Ligne dérivation max.
off	off	20kBit/s	1000m	7,5m
ON	off	100kBit/s (*)	500m	3,75m
off	ON	500kBit/s	100m	0,75m
ON	ON	1MBit/s	40m	0,3m

*: Le remplacement de ce débit numérique par 125kBit/s est en préparation.



Exemple de mise en œuvre

Choix des identificateurs pour les noeuds

CAN identifier setup

The following CAN identifier setup ensures logical communications as shown:

CAN identifier

Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
ID 10 (Prio 2) Channel selection	ID 9 (Prio 1) Direction	ID 8 (Prio 0) Broadcast	ID 7 (Addr 4)	ID 6 (Addr 3)	ID 5 (Addr 2)	ID 4 (Addr 1)	ID 3 (Addr 0)
ID 2 (Spec 2)	ID 1 (Spec 1)	ID 0 (Spec 0)	RTR-Bit	DLC 3	DLC 2	DLC 1	DLC 0

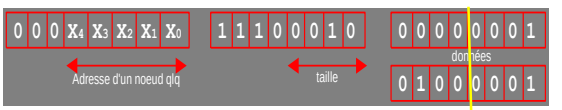
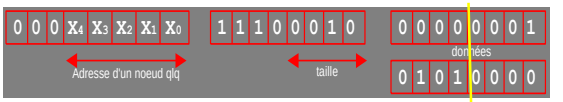
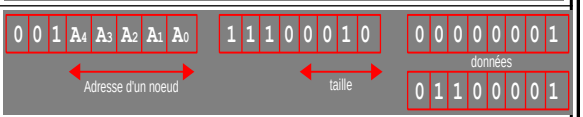
Prio 2 ... Prio 0: Priorities of messages on CAN bus

Addr 4 ... Addr 0: Node addresses

Spec 2 ... Spec 0: Assigned with special functions (mainly for motion communications)

Exemple de mise en œuvre

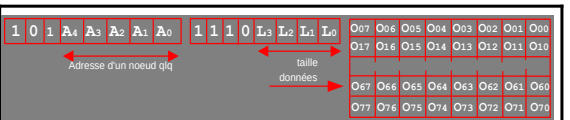
Mise en place des Messages de commande

Broadcast-Switch-Poll-Mode-Telegram : tous les nœud commutent dans le mode "poll" ils envoient les données à la suite d'une demande ; (0141h)	
Broadcast-Start-Communication-Telegram : tous les nœuds peuvent démarrer la communication de données (0150h)	
Broadcast-Stop-Communication-Telegram : tous les nœuds arrêtent la communication de données (0151h)	
Start-Input-Update-Telegram : le nœud actif adressé transmet l'état courant de ses entrées (0161h)	

Exemple de mise en œuvre

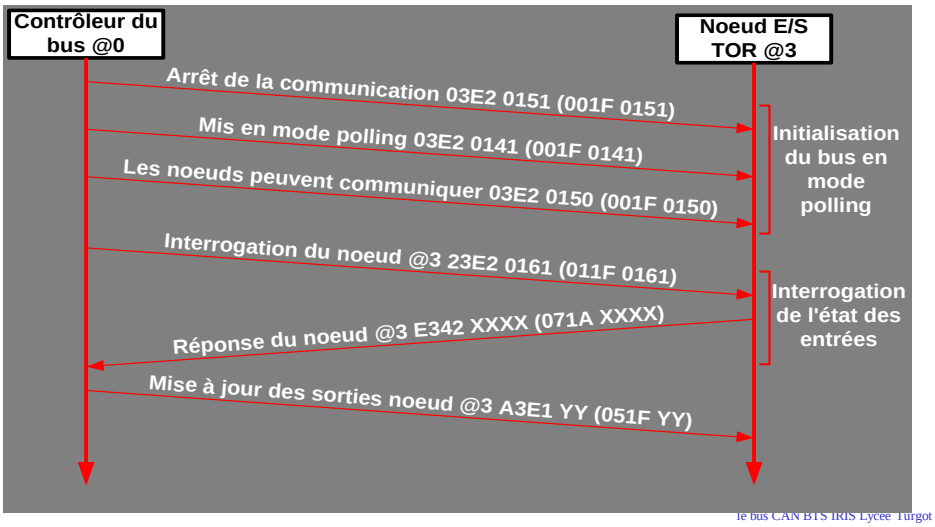
Messages de données :

ces messages permettent de configurer les sorties (du maître vers les modules) ou de connaître l'état des entrées (des modules vers le maître)

Output-Update-Telegram for digital I/O modules : Les données sont appliquées aux sorties du nœud et à ses extensions. La taille dépend du nombre d'extension, 8 octets maximum (1 nœud + 7 extensions maximum).	
Output-Update-Telegram for analog I/O modules : Les données sont appliquées aux 4 sorties analogiques du nœud	
Input-Update-Telegram for digital I/O modules : l'état des entrées du nœud et de ses extensions est transmis vers le maître du bus. La taille dépend du nombre d'extension, 8 octets maximum (1 nœud + 7 extensions maximum).	
Input-Update-Telegram for analog I/O modules : La valeur des 4 entrées analogiques du nœud est envoyée vers le maître du bus.	

Exemple de mise en œuvre

Echanges sur le bus



Références

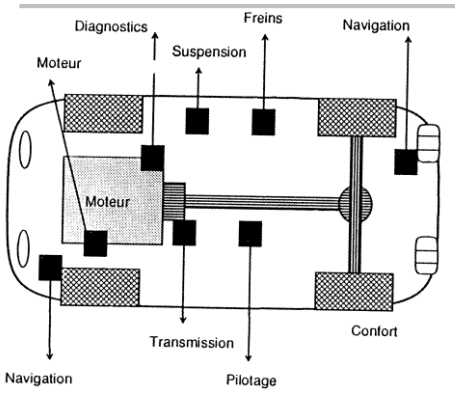
•Le bus CAN de Dominique PARET éditions DUNOD

•Cours de Michel Gaillard sur le bus CAN du BTS IRIS Lycée Turgot Limoges

•Sites internet:

- http://www.hitex.co.uk/softing/cananalysers.html
- http://www.ime-actia.de/web_can/index_can.htm
- http://www.cananalyser.com/
- http://www.vector-cantech.com/index.html

Exercice



Application	Point de raccordement au réseau	Besoins
confort	sièges, verrouillage des portes vitres électriques lampes, climatisation distractions	fréquence 10 msg/s délai acceptable 20 à 50 ms 25 à 50 points d'accès
gestion des inform- ations	groupes d'instruments tableau de bord (vitesse, compte-tours, ...), navigation (clignotants, klaxon, ...) diagnostics feux de route état du moteur, ... sécurités	fréquence 100msg/s délai acceptable 1 à 10 ms grande fiabilité 10 à 25 noeuds
commande temps réel	puissance (allumage électronique injection puissance électrique, tenue de route : suspension anti-blocage de roues direction assistée	fréquence 1000 msg/s délai tolérable ~ 1ms très haute fiabilité 5 à 10 noeuds tolérance aux fautes
mainten- ance	collecte des données chargement de programmes de test mesures	fiabilité du transfert des données

- Environnement ?
- Avantage d'un LAN ?
- Support (lg) ? Topologie ? Protocoles ?
- Format des trames (couche 2) ? Rendement ?
- Débit moyen / classe de fonction ?
- Ethernet industriel ? Tranche canal ?
- Quelles propriétés doivent avoir les services du réseau pour chacune des 4 classes de trafic ?
- Quelles sont les couches du modèle ISO et protocoles associés que vous proposez d'implémenter ?