Normes et Principes des Réseaux

Polytech 'Tours **J.Y. RAMEL** **2013-2014**

Organisation du cours . . .

- 11 séances de 2 heures + 3 séances de TD + 6 séances de TP
- Examen (2 heures) → la dernière séance + 1 autre note TP
- Plusieurs intervenants :

	Chapitre
JY Ramel	Introduction aux réseaux
	Modèle OSI
	Couche 2 : CSMA, wifi, token-ring, HDLC (rappels)
	Couche 2 : Ethernet non commuté
	Couche 2 : Ethernet avancé (commutation, VLAN, spanning-tree)
	Couche 2/3 : Datagramme vs ATM/MPLS
P Bourquin	Couche 3 : IPv4 (adressage, routage, ARP, etc.)
	Couche 3 : IPv4 (Firewalling, NAT)
	Couche 3 : IPv6
	Couche 3 : protocoles pour le routage IP (RIP, OSPF)
	Couche 4 : UDP, TCP
	Couche 5 à 7 : HTTP, FTP, SMTP, POP, IMAP
	Couche 5 à 7 : DHCP, DNS, LDAP, SNMP, Domaine Microsoft, etc.

P Bourquin ⟹ les TP

Organisation du cours . . .

En se basant sur le Modèle ISO en 7 couches :

- Les principaux composants matériels (couche 1)
- Protocoles et architectures (couche 2)
- Interconnexion de réseaux & routage (couche 3 et 4)
- Couches hautes (5 à 7) : applications, sécurité, administration

- 11 séances de 2 heures + 3 séances de TD + 6 séances de TP
- Examen (2 heures) → la dernière séance + 1 autre note CC/TP

Introduction

Qu'est-ce qu'un réseau ? ? ?

Qu'est-ce qu'un réseau ? ? ?

- **Logiciels :**
  - système d'exploitation
  - protocoles
  - pilotes
  - logiciels réseaux
- **Utilité :**
  - communication
  - partage de ressources
  - travail en groupe
- **Matériel :**
  - câbles
  - cartes réseau
  - Nœuds
  - Terminaux
- **Exemples :**
  - téléphone
  - Ethernet
  - Internet

Définition : groupe d'ordinateurs (ou périphériques) reliés les uns aux autres afin de permettre aux utilisateurs d'échanger des informations et de partager du matériel

Introduction

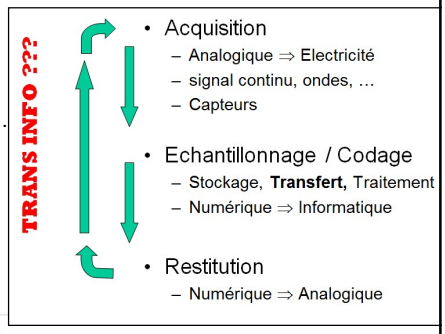
Les réseaux, pourquoi ?

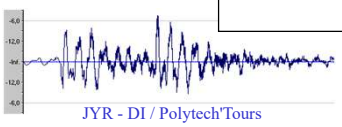
Notion de communication

- La communication définit l'action d'échanger des informations. Cela induit un mécanisme de transmission (aspect physique) et la capacité du récepteur à recevoir et à réagir (aspect logique)

  → Il faut un (des) langage(s) commun(s) = Protocoles

- **Des protocoles, pour quoi** ?
  - composants hétérogènes (avec ou sans fil)
  - composants intelligents ou non intelligents
  - Gérer l'évolutivité très rapide (IP6, wifi,…)…
- **Les besoins :**
  - Un monde numérique
    - Entreprise : Production, gestion, marketing
    - Individus : PC, Iphone, Ipad, voiture, TV, …
  - Bande passante énorme !!!

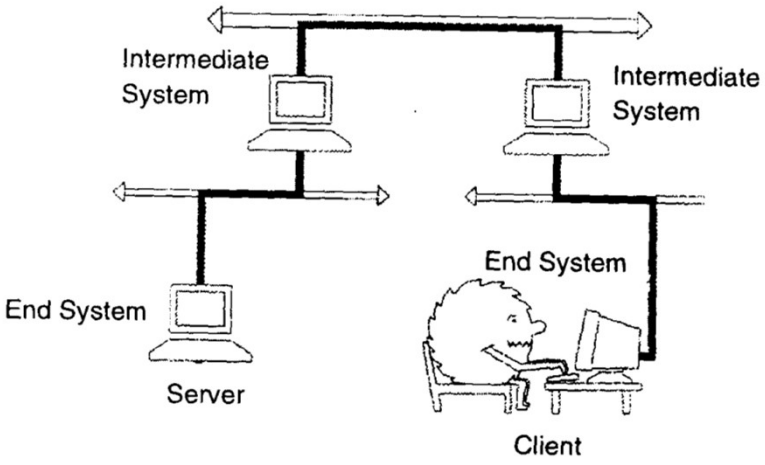




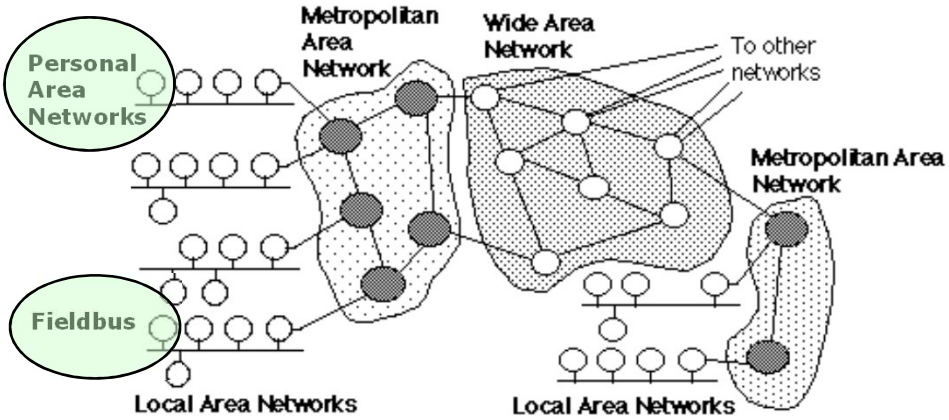
Les contraintes

- **Objectif :** "Un système de communication complet doit permettre un transfert d'information transparent et fiable, en temps utile, d'une source vers un ou plusieurs collecteurs."
- **Engendre des contraintes :**
  - Opérationnelles
    - Transparence : vis à vis du récepteur, vis à vis de la nature de l'information.
    - Fiabilité : taux d'erreur toléré. Dépend de la nature de l'information
    - Reconfiguration : Taux de reconfiguration ? Hétérogénéité des entités communicantes.
    - Sûreté / protection : au niveau logique contre les intrus.
    - Utilisation : facilité d'accès / connexion sur le réseau.
    - Temps de réponse : Temps réel ? Ou plutôt contraintes de délai d'acheminement.
  - Technologiques
    - Parasitage le plus souvent électromagnétique, Attaques /agressions physico-chimiques
    - Disposition géographique dimensionnement, accès en cas de problème, …
    - Contraintes psychologiques liées à l'insertion d'une technologie nouvelle
  - Economiques
    - Le coût du matériel (les câbles, les commutateurs, …).
    - Le coût des logiciels : Attention aux passerelles entre matériels hétérogènes
    - Le coût de l'installation : induit souvent des adaptations du site.
    - Le coût de formation : Tous les futurs utilisateurs doivent être formés au nouveau système Le coût de gestion et de maintenance.

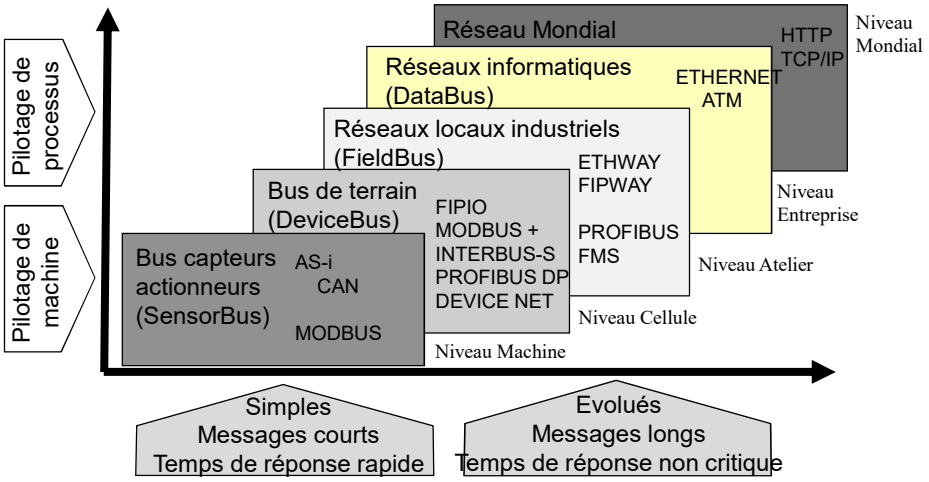
Equipement Intermédiaire / Terminal



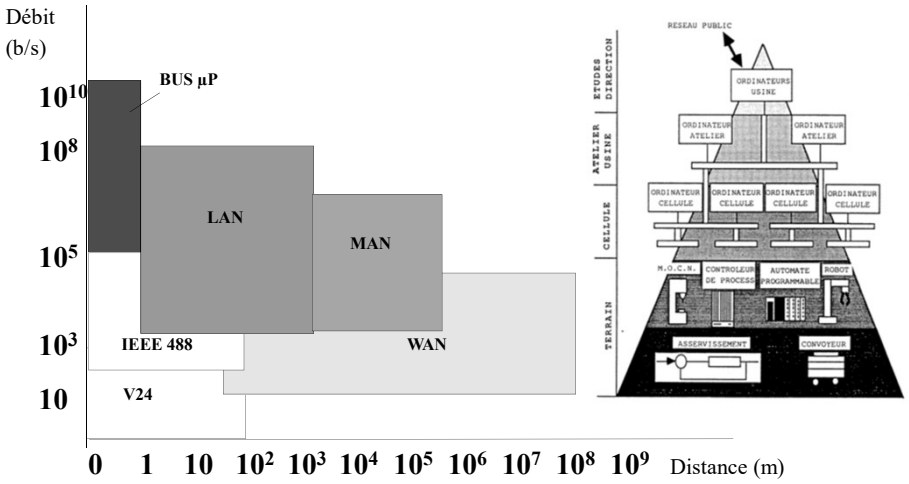
Fieldbus - PAN - LAN - MAN - WAN



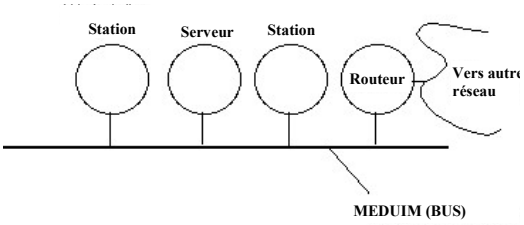
Modèle de l'usine intégré (CIM)

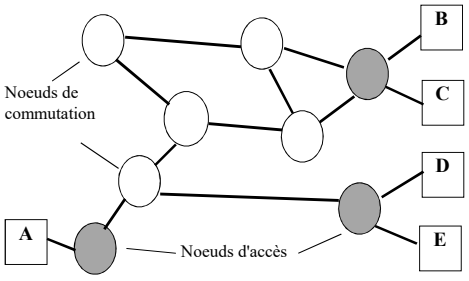


LAN, MAN, WAN et Débit utile



Réseau local VS WAN





Architecture

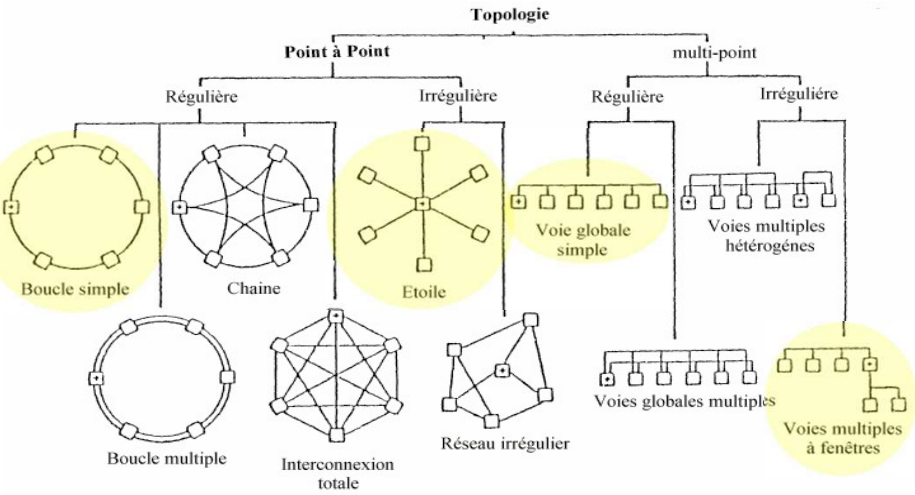
- **Définitions et caractéristiques**
  - **Connectivité** : liaisons pouvant s'établir depuis une station. Elle est totale ou partielle
  - **Diffusion** : capacité à émettre vers l'ensemble des points du réseau
  - **Reconfiguration** : capacité d'ajouter et/ou de supprimer une station
  - **Sûreté de fonctionnement** : conséquence de la défaillance d'une ou plusieurs stations

    → **Structure Physique / Structure logique**

Architecture

- **La topologie** : Arrangement logique des voies de transmission
- **Les topologies point à point :**
  - Chaque support physique est lié à un couple de stations uniquement. La topologie se caractérise par une structure de graphe.
  - Architecture → structure de graphe
- **Les topologies multipoint :**
  - Le modèle quasi-unique de cette catégorie est le bus.

Topologie et Architecture



Chapitre 1

Modélisation des réseaux : Le modèle OSI et ses dérivés

Le modèle OSI de l'ISO

- Le modèle d'Interconnexion des Systèmes Ouverts (*Open Systems Interconnection*) a été proposé par l'ISO (*International Standards Organization*) en 1977.
- Il s'agit d'une norme internationale pour une architecture multi-couches qui permet l'interconnexion de matériels hétérogènes.
- Pourquoi un modèle en couches ?

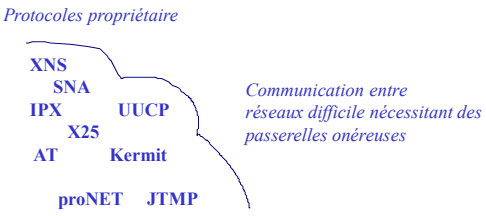
  1° Facilité de développement et de modification : une couche (un protocole) peut être modifiée de façon indépendante tant que l'interface avec les deux couches adjacentes reste inchangée.

  2° Intéropérabilité : une même couche de niveau *n+1* peut utiliser les services de couches de niveau *n* très différentes à condition que l'interface *n/n+1* soit la même.

  → Un modèle commun pour pouvoir communiquer

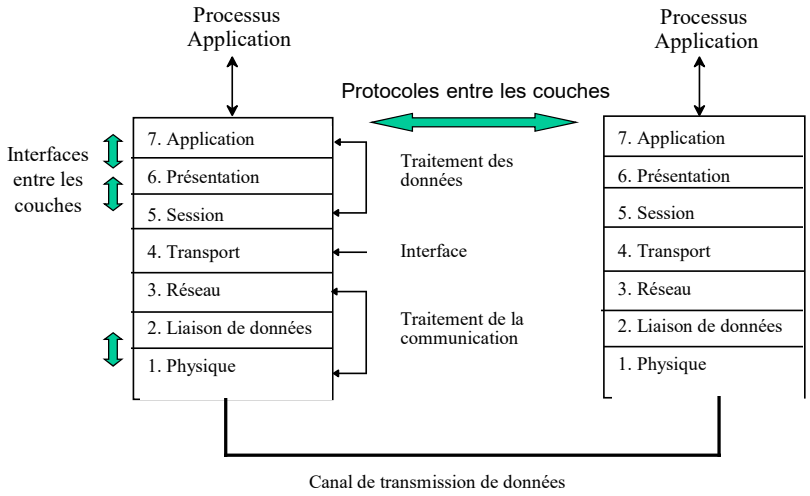
Le modèle OSI de l'ISO

- **Avant l'OSI**



- **Après l'OSI**
  - Un petit nombre de protocoles standards (IP, ATM, ...)
  - Interfaces de communication connues → Interconnexions simplifiées

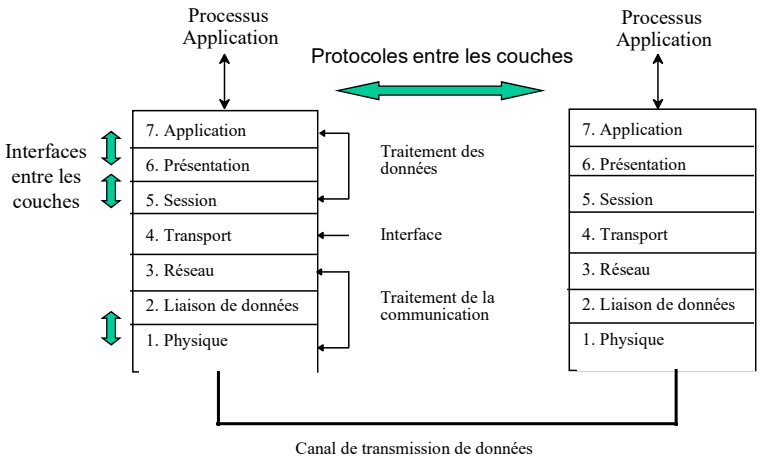
ARCHITECTURE MULTI-COUCHES



Le modèle OSI de l'ISO

- Les principes du modèle OSI :
  1° Une couche doit être créée lorsqu'un nouveau niveau d'abstraction est nécessaire.
  2° Chaque couche exerce une fonction bien définie.
  3° Les fonctions de chaque couche doivent être choisies en pensant à la définition de protocoles normalisés internationaux.
  4° Le choix des frontières entre couches doit minimiser le flux d'informations aux interfaces.
  5° Le nombre de couches doit être assez grand pour que des fonctions très différentes ne cohabitent pas dans une même couche et suffisamment réduit pour que l'architecture soit maîtrisable.

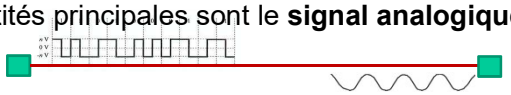
Architecture multi-couches



Architecture multi-couches

Couche Physique ou niveau 1

- “Elle décrit les interfaces mécaniques, électriques, fonctionnels et procédurales nécessaires à l'activation, au maintien et à la désactivation des **connexions physiques** destinées à la transmission de bits entre deux entités de liaison de données”
- Ce niveau est chargé de piloter le **matériel de transmission**
- C'est donc dans cette couche que sont définis le **support physique** ou médium, les signaux, les voies de transmission ou canaux, le raccordement des communicateurs, les débits, …
- Les entités principales sont le **signal analogique et le bit**



Architecture multi-couches

Couche liaison de données ou niveau 2

• Elle permet le transfert **fiable** d'informations entre des systèmes **directement connectés**. Elle fournit les moyens **procéduraux** nécessaires à l'établissement, au maintien et à la libération des connections de liaison de données **point à point**

• Deux sous-couches :

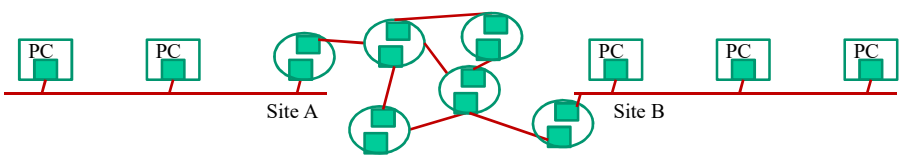
  • Sous-couche MAC (*Medium Access Control*) qui gère l'accès à la voie de transmission. Parfois, liée aux choix du niveau 1(une exception à l'indépendance entre les couches)

  • Sous-couche LLC (*Logical Link Control*) qui regroupe l'aspect logique de la transmission entre systèmes physiquement connectés. C'est à ce niveau que se situent la détection des erreurs et la gestion **de trames**

Architecture multi-couches

Couche réseau ou niveau 3

- Ce niveau est chargé de **l'acheminement et de la communication en paquets** d'information ainsi que de la gestion des connexions réseaux entre sites distants
- Fonctions principales : **le routage**, la recherche du chemin, la gestion de l'adressage global



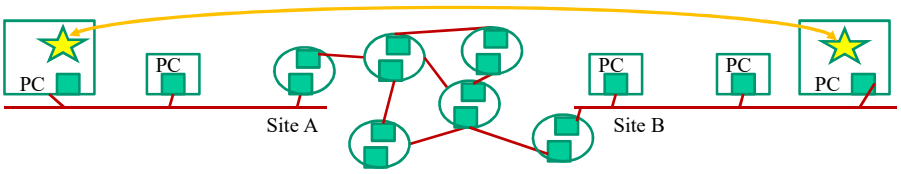
Architecture multi-couches

Couche transport ou niveau 4

Assure un transport de données transparent entre entités de session en les déchargeant complètement des détails d'exécution d'un transfert de données **fiable** et d'un bon rapport qualité/prix **de bout en bout**

Fonctions : contrôle de flux, fragmentation et réassemblage des messages, contrôle d'erreur (perte, duplicata de paquets, modifications), séquencement des messages

Au dessus de la couche transport, le message doit avoir été expurgé de sa connotation communication.



Architecture multi-couches

Couche session ou niveau 5

- Elle fournit des outils de synchronisation et de gestion du dialogue entre entités communicantes
- Fonctions principales : gestion des interruptions, des reprises, checkpoints,…

Couche présentation ou niveau 6

- Elle se charge de la **représentation des informations** que des entités s'échangent, ou auxquelles elles se réfèrent au cours de leur dialogue
- Elle est chargée de décrire de manière cohérente les données et de les coder sous une forme universelle dans le réseau
- Gère une partie des problèmes de sécurité, en particulier ceux relatifs à la sûreté du contenu des messages. Le **cryptage/décryptage** est donc un des services présents dans cette couche

Architecture multi-couches

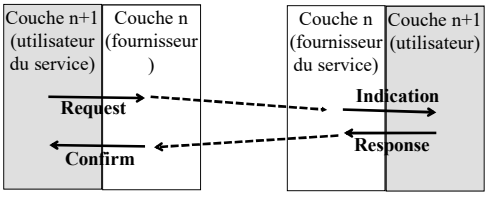
Couche application ou niveau 7

- C'est la couche chargée de la communication entre les processus application et le modèle OSI.
- Elle définit les formats de données spécifiques à une application (mail, ftp, web, …)
- C'est la seule couche ouverte vers l'extérieur. Toute normalisation est donc très difficile.

Modèle OSI : Les Services

- La couche N+1 peut accéder aux services de la couche N via des **points d'accès** au service (**SAP** : *Service Access Point*). Chaque SAP est identifié par une « adresse » unique
- 4 types de primitives de service :

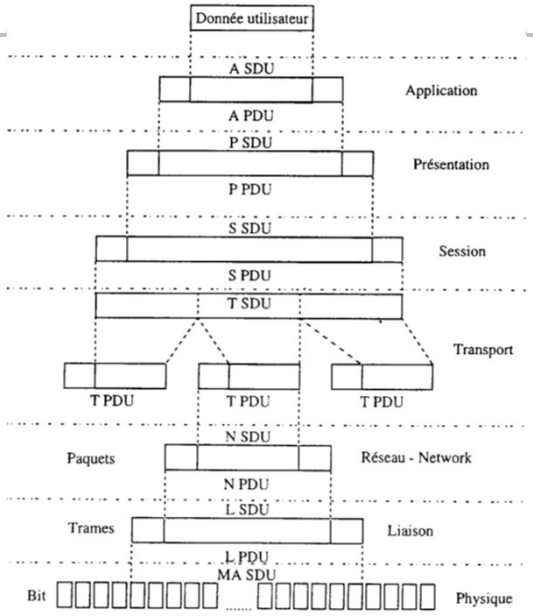
Request	requête (1 entité sollicite un service)
Indication	indication (1 entité est informée d'un événement)
Response	réponse (une entité répond à un événement)
Confirm	confirmation (demande de service bien reçue)



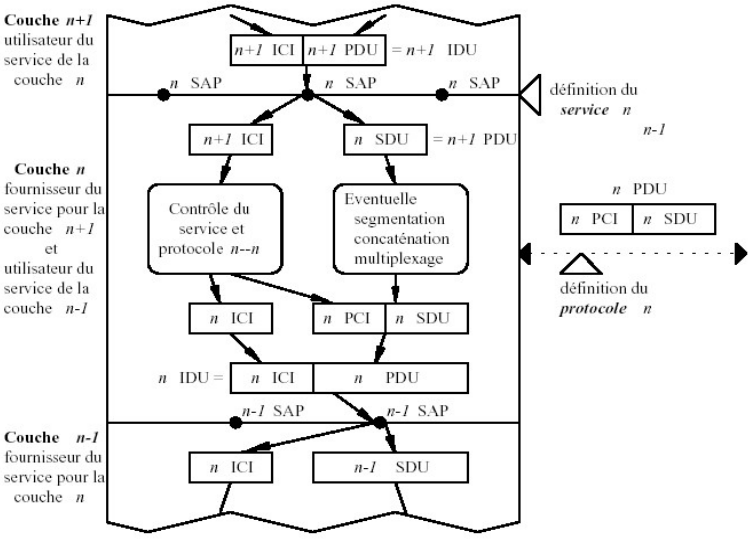
La syntaxe générale est :
Niveau.Fonction.Primitive

Fonction = Connexion, Libération (ou Données.

Services confirmés ou non



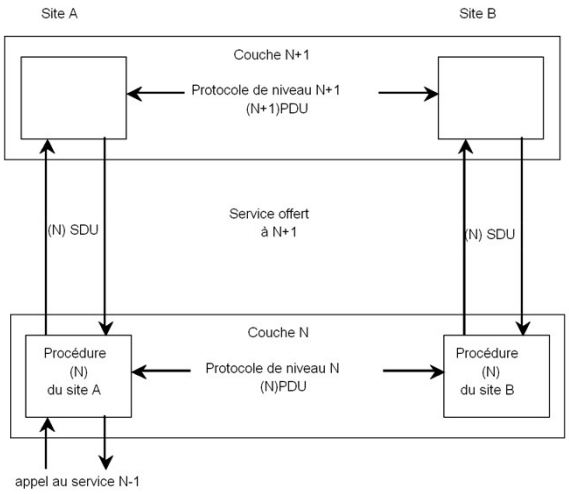
FONCTIONNEMENT DU MODELE



FONCTIONNEMENT DU MODELE

- Les procédures du niveau N+1 s'échangent des unités d'informations appelées **(N+1)PDU** en accord avec le protocole du niveau N+1.
- Chaque échange est réalisé grâce aux services fournis par la couche N (sauf si N+1 = 1 bien sûr!). Les procédures de niveaux N et N+1 d'un même site échangent des **SDU**.
- Plus précisément, entre les couches N+1 et N circulent des **IDU** (*Interface Data Unit*). Une **IDU** est composée de la manière suivante : **IDU = ICI + SDU**
- N-SDU = information passée par N au niveau N-1 ou N+1.
- ICI (*Information Control Interface*) est l'information propre à l'interface N+1/N pour aider les services du niveau N. Elle n'est bien sûr pas transmise sur le réseau.
- De même, dans un protocole, l'entité d'information communiquée devient **PCI + PDU** où PCI (*Protocol Control Interface*) est l'information propre au protocole entre deux entités de même niveau.

FONCTIONNEMENT DU MODELE



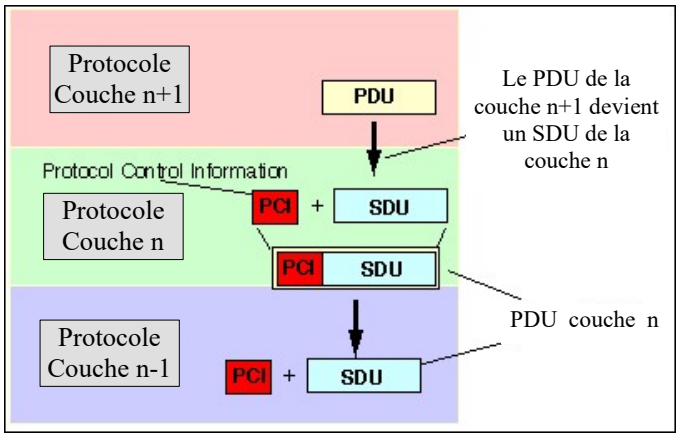
- le protocole : règles de dialogue entre les entités communicantes, pour les préoccupations affectées à 1 couche uniquement. L'entité de base est le PDU (*Protocol Data Unit*).
- le service : règles de dialogue internes à une entité entre la couche courante et la couche immédiatement supérieure (N et N+1). L'entité de base est le SDU (*Service Data Unit*).

FONCTIONNEMENT DU MODELE

- **Activités possibles dans chaque couche *n* :**
  1° Identifier l'interlocuteur : au même niveau, aux niveaux adjacents.
  2° Etablir/relâcher la connexion.
  3° Définir le mode simplex/semi-duplex/duplex. Définir le nombre de canaux par connexion.
  4° Effectuer éventuellement :
    - La segmentation/le regroupement des messages : la taille des messages reçus de la couche *n+1* est supérieure à la taille utilisable par la couche *n*.
    - Le multiplexage/l'éclatement des messages : la capacité d'une liaison de niveau *n* est un multiple du débit des liaisons de niveau *n+1*.
  5° Détecter et corriger des erreurs.
  6° Assurer le respect de l'ordre des messages.
  7° Assurer l'asservissement émetteur-récepteur.
  8° Effectuer le routage des messages.

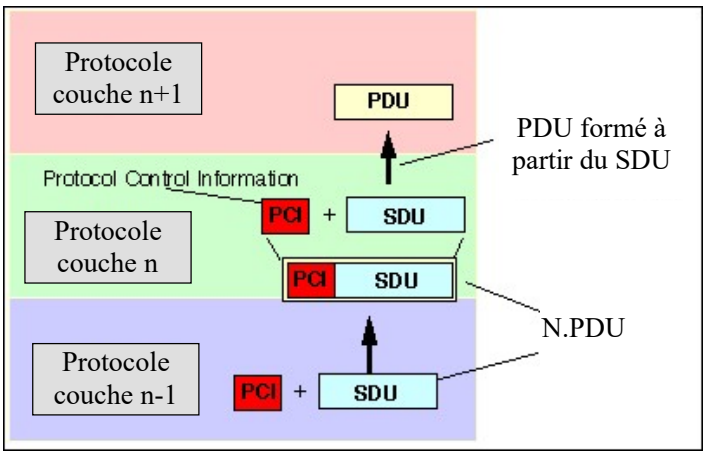
FONCTIONNEMENT DU MODELE

Encapsulation des PDU



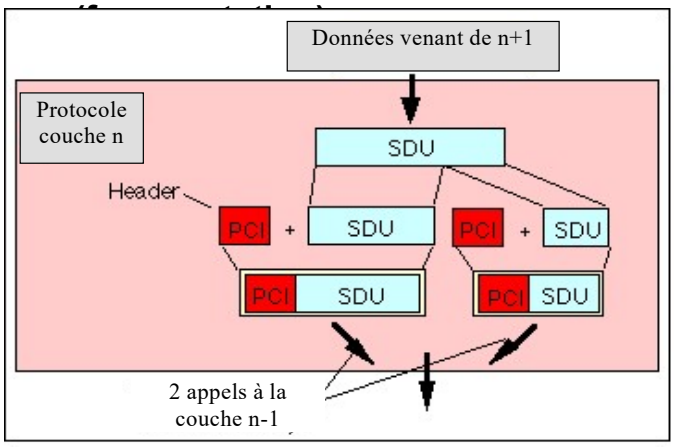
FONCTIONNEMENT DU MODELE

Dé-encapsulation



FONCTIONNEMENT DU MODELE

Segmentation des PDU



Les Services : Mode de transmission

1° **Avec connexion** : création d'une connexion avant le transfert des données.

Avantages : permet de s'assurer que le destinataire peut accepter les messages ;

Désavantage : durée élevée d'établissement de la connexion. Mode intéressant uniquement pour le transfert de volumes importants de données (nombre élevé de messages ordonnés).

2° **Sans connexion** : les données sont envoyées sans qu'une connexion soit préalablement établie.

L'ordre des messages n'est pas nécessairement respecté. Mode utilisable sur des réseaux à voie unique (l'ordre des messages est maintenu grâce à la structure du réseau) ou pour des messages individuels (l'ordre n'a aucune importance).

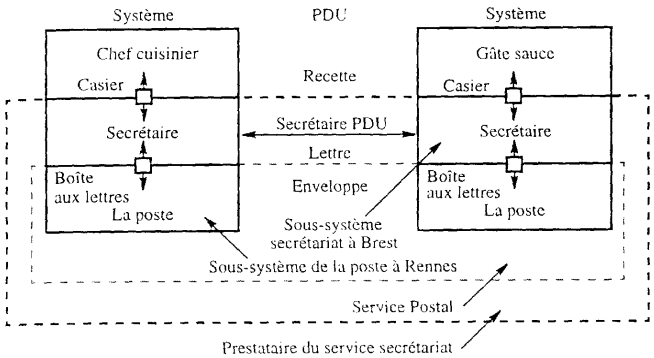
Qualité de service :

1° Service fiable : aucune perte de données grâce au contrôle des erreurs et à l'acquittement de chaque message (exemple : transfert de fichiers).

2° Service non fiable : les erreurs ne sont pas détectées, il n'y a pas d'acquittement pour les messages (exemple : téléphone).

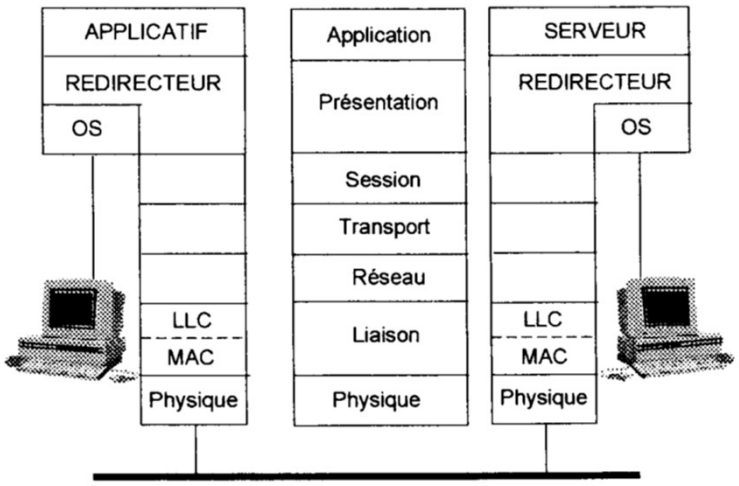
Le mode connecté et le service fiable ne sont en général pas utilisés dans toutes les couches ; si le support est très fiable, le contrôle des erreurs peut être

Les Services



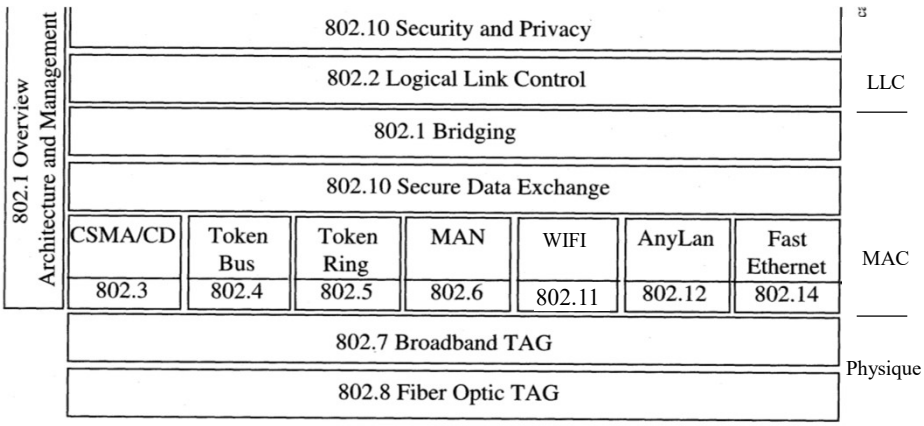
Service	Entités protocolaires homologues	PDU échangées	Points d'accès
Cuisine	Chef cuisinier Gâte-sauce	Recettes	Restaurant
Secrétariat	Secrétaires	Lettres	Casier
Postal	Postiers	Enveloppes	Boîtes à lettres

Les modèles dérivés d'OSI : pour les LAN

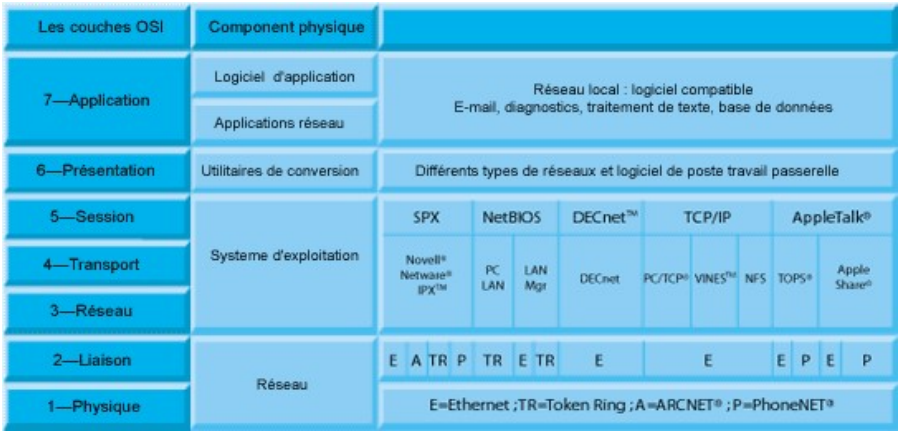


Pour les LAN

→ LES STANDARDS IEEE : conforme aux spécifications ISO, ils détaillent les couches 1, 2 et 7



Evolutions ...



Chapitre 2

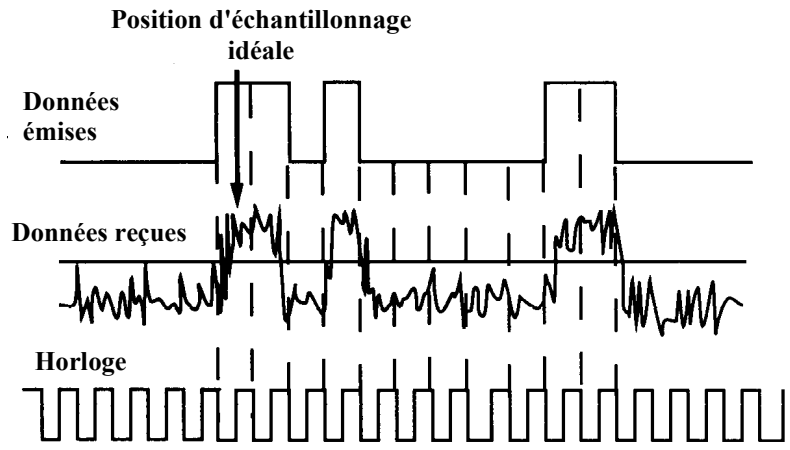
Couche Physique

Signal / Codage / Matériels niveau 1

Couche Physique

Voir cours
Transmission de l'information

Rappel : Voie de transmission

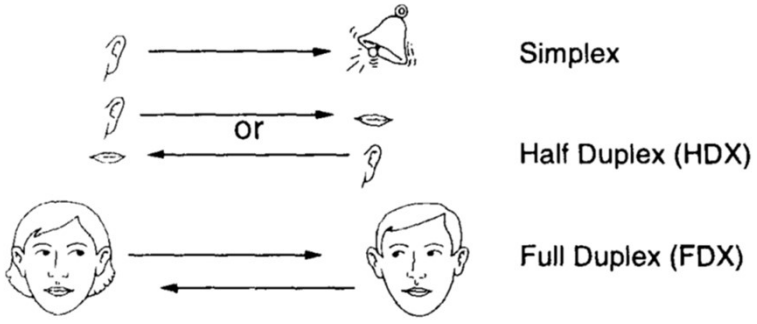


Rappel : Caractéristiques de transmission

- **Instant significatif :** instant choisi pour évaluer l'état du signal transmis (instant d'échantillonnage)
- **Intervalle significatif** Δ : intervalle entre 2 instants significatifs
- **Valence V** : nombre d'états significatifs distincts pour caractériser les états du signal à transmettre
- **Rapidité de modulation R: R = 1 / Δ Bauds** (Δ en s)
- **Débit binaire :** quantité d'information émise. $D = R.\log_2 V$ (bit/s)
- **Le temps de transmission (emission)** est fonction du débit du canal. Il s'exprime donc par : $\mathbf{T_t = N/D}$ où N est le nombre de bits à transmettre et D le **débit binaire** exprimé en bits/s.
- **Temps de transfert** = Temission + Tpropagation + Ttraitement

Rappel : Caractéristiques de transmission

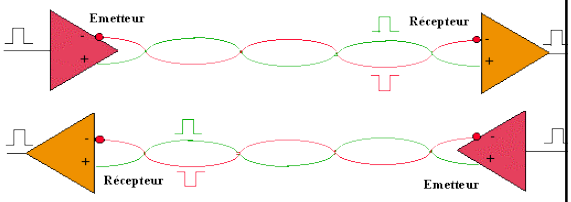
- **Sens de transmission**



half duplex = bi-directionnelle à alternat
full duplex = bi-directionnelle intégrale

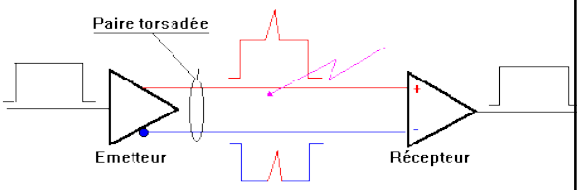
Mode de transmission classique

- **On envoie un signal différentiel de 2V sur une paire torsadée. Le récepteur mesurera la différence entre les deux signaux.**



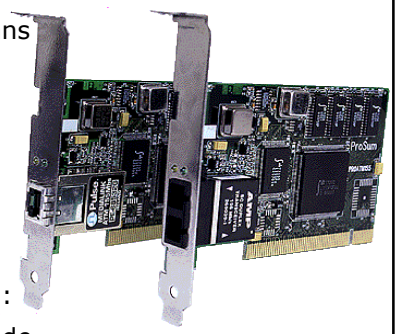
- **Un parasite externe → une perturbation de même signe sur les deux conducteurs de la paire**

→ **ce qui sera annulé par le récepteur**



Raccordement au support : Cartes réseaux

- **Cartes réseaux /coupleurs :**
  - La principale technique de raccordement d'un PC au support physique est le **coupleur réseau**
  - Il s'agit d'une carte que l'on insère dans l'ordinateur.



- **Ancienne terminologie : Transceiver** :
  - Dans le cas d'Ethernet, l'élément de base du raccordement était le ***transceiver*** (*transmitter-receiver*).

Raccordement au support

A l'autre bout du câble, on trouve bien souvent un concentrateurs passifs ou actifs (HUB, Switch, MAU, …)

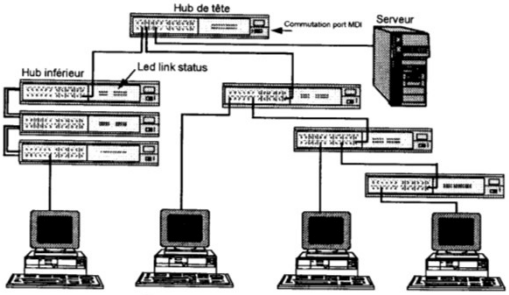
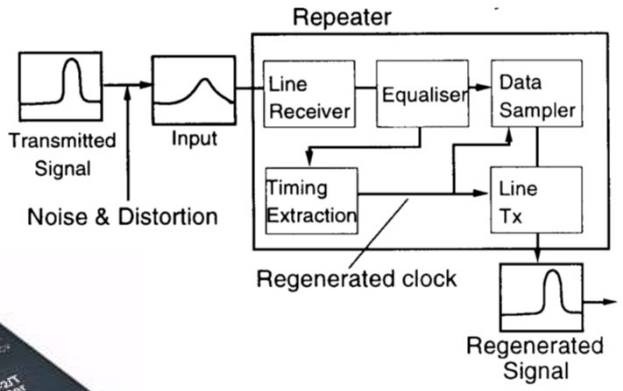


Figure 7.3 – Réseau IEEE 802.3 10 baseT

- Ou un autre coupleur/équipement (selon topologie)

Prolongement du médium

- **Le répéteur :**



Le support physique ou Médium

- Paires torsadées
- Coaxial
- Fibre optique
- Ondes (Laser, satellites, radio)
- . . .

La fibre optique semble l'avenir mais cette technique a aussi des inconvénients majeurs.

- Critère de choix :
  - Coût
  - Extensibilité
  - Fiabilité :
    - Immunité électromagnétique
    - Résistance mécanique
    - Souplesse
    - Résistance thermique
    - Corrosion
    - Facilité de localisation des coupures

Eléments de comparaison ➔ Voir Trans Info

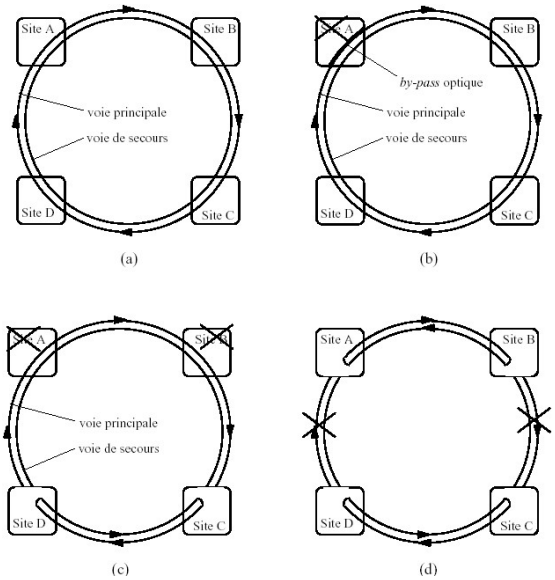
Codage des informations

La couche physique doit réaliser le codage des informations :

- convertir les données (la trame) en une succession de bits afin de l'envoyer au destinataire par l'intermédiaire d'un médium (câble)
- Le destinataire doit récupérer la succession de bits afin de reconstruire la trame.
- Un signal d'horloge est nécessaire afin d'identifier le centre de chaque bit reçu. Il existe 2 méthodes pour fournir ce signal :
  - communication asynchrone (horloges émetteur et récepteur indépendantes)
  - communication synchrone (horloges émetteur et récepteur synchronisées)
- Cf Transmission de l'info (NRZ, Manchester, modulation, …)

Exemple : couche physique de FDDI

- Double Fibres optiques multi-modes 62,5/125µm à gradient d'indice (1300nm)
- Longueur max = 200 km
- Distance max = 2km
- By-pass optique (miroir)
- Voie de secours



Exemple : couche physique de FDDI

- Codage bande de base NRZI (4B/5B) :

Code signalisation	Code 5B	Donnée	Code 5B	Donnée	Code 5B
Idle	11111	0000	11110	1000	10010
J (début)	11000	0001	01001	1001	10011
K (début)	10001	0010	10100	1010	10110
R (*reset*)	00111	0011	10101	1011	10111
S (*set*)	11001	0100	01010	1100	11010
Quiet	00000	0101	01011	1101	11011
Halt	00100	0110	01110	1110	11100
T (fin)	01101	0111	01111	1111	11101

Exemple : couche physique de FDDI

- **Encodage des PDU physiques FDDI :**

Signification des symboles de signalisation (voir la trame FDDI plus bas) :

Idle = symboles émis en continu (en l'absence de trames à envoyer) sur la liaison, doivent maintenir la synchronisation entre les horloges

J = premier délimiteur de début de trame

K = second délimiteur de début de trame

Reset = indique une condition logique "off" ou "faux"

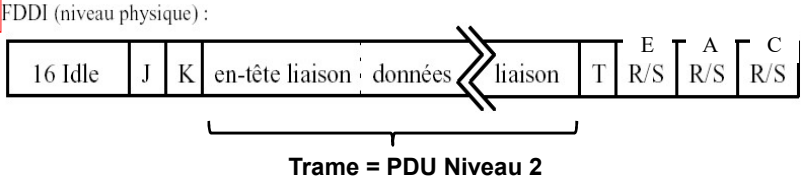
Set = indique une condition logique "on" ou "vrai"

Quiet = indique l'absence de transitions sur la fibre (situation anormale)

Halt = séquence de contrôle couche physique

T = délimiteur de fin

PDU FDDI (niveau physique) :



Trame = PDU Niveau 2

Chapitre 3

PROTOCOLES D'ACCES AU MEDIUM

GESTION DES COMMUNICATIONS

Couche 2 : Liaison de Données

- Quelque soit la **topologie choisie**, il est nécessaire de respecter un **protocole de gestion des communication** pour permettre :
  - le transfert fiable entre des systèmes **directement connectés**
  - l'établissement, le maintien et la libération des connexions
  - Service avec ou sans connexion, avec ou sans acquittement
- **Trame** : succession de bits envoyée entre des systèmes directement connectés

Couche 2 : Liaison de Données

- Pour les réseaux locaux, cette couche est décomposée en **deux sous-couches** :
  - **Sous-couche MAC (*Medium Access Control*)** qui gère l'accès à la voie de transmission.
  - **Sous-couche LLC (*Logical Link Control*)** qui gère la **détection des erreurs** et la gestion de trames. C'est également cette sous-couche qui gère le mode des **liaisons logiques**.

Accès au médium (sous-couche MAC)

- Allocation statique des canaux :
  - Multiplexage en fréquence
  - Multiplexage temporelle

    → Voir Transmission de l'info.

- Allocation dynamique des canaux :

Support = Ressource partagée → Méthode d'accès

Accès au médium (sous-couche MAC)

- Trois catégories de méthodes d'accès :
  - déterministe
  - à compétition
  - mixte (compétition puis déterministe si le nombre de conflits devient trop grand)

- 2 remarques sur la conception d'un réseau :
  - L'**accès au médium** est un élément crucial
  - Etant donné une topologie particulière, le concepteur/architecte du réseau devra déterminer la méthode optimale en termes de minimisation des collisions et du temps d'accès au réseau depuis un nœud quelconque

MAC : Méthodes à compétition

Aloha (Université Hawai – Radio)

- Les stations émettent quand bon leur semble et si aucun acquittement ne revient on reémet après un délais aléatoire.
- Si un seuil est dépassé → Abandon

CSMA/CD (802.3 - Ethernet)

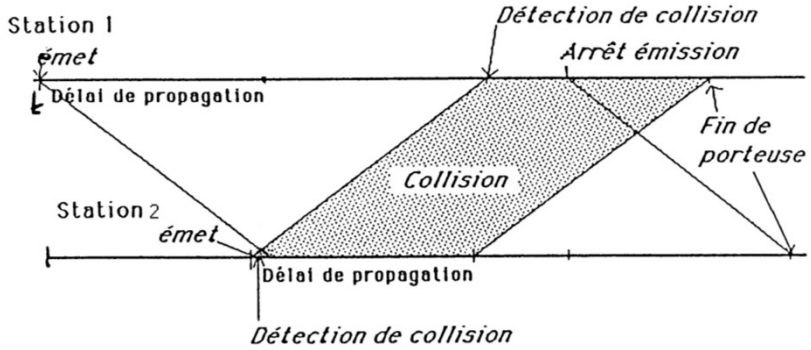
(*Carrier Sens Method Access / Collision Detection*)

- Principe :
  - Toutes les stations “écoutent” en permanence le réseau dans l'attente d'un silence pour pouvoir émettre (détection porteuse).
  - Si plusieurs stations émettent simultanément, alors il y aura mélange des signaux et le message reçu sera différent de celui émis → Collision
  - Gestion des collisions par des temps d’attente.

CSMA/CD (Ethernet)

- Bus → collisions !!!
- Résoudre ce problème : CSMA/CD
- Multiple Access, Carrier Sense (écoute)
  - Une station n’émet sa trame que si le support est libre
  - « J'envoie sur le réseau et j'espère que ça passe »
  - Ce système n’évite pas totalement les collisions…
  - … car le support physique possède un temps de propagation !
  - Exemple
    - Paire torsadée temps de propagation = 5 ns/m, longueur du bus = 100 m
    - Stations A et B situées aux extrémités du bus
    - T0 : A commence à émettre sa trame
    - T0 + 400 ns : B commence à émettre sa trame
    - → Collision !

MAC : Méthodes à compétition



- **Tranche canal** : durée qui s'écoule entre l'émission du premier bit et l'instant où l'émetteur est sur qu'il n'y a pas collision (= 2xTp).

CSMA/CD : explications du schéma précédent

- **COLLISION** : ***le problème***
  - une station regarde si le câble est libre avant d'émettre
  - le délai de propagation n'est pas nul => une station peut émettre alors qu'une autre a déjà commencé son émission
  - les 2 trames se percutent : c'est la collision
  - plus le réseau est grand (nombre de stations), plus la probabilité d'apparition de collisions est grande
- **COLLISION** : ***la solution***
  - limiter le temps pendant lequel la collision peut arriver
  - temps de propagation aller-retour d'une trame (Round Trip Delay) limité à 50 µs
  - ce délai passé, aucune collision ne peut plus arriver
  - la norme 802.3 définit un « Slot Time » d'acquisition du canal égal à 51.2 µs ce qui correspond à une longueur de trame minimum de 512 bits
  - une station doit donc écouter le signal « Collision Detection » pendant 51.2 µs à partir du début d'émission (**valeurs valables pour Ethernet BaseT**)

CSMA/CD

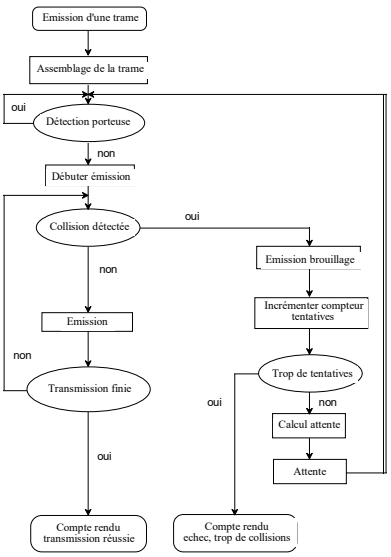
- **COLLISION : *la détection***
  - si une station en train d'émettre détecte une collision, elle arrête son émission
  - si une station en réception reçoit une trame inférieure à 72 octets, elle en déduit l'existence d'une collision
- **COLLISION : *la gestion***
  - en émission, la station aprés avoir détecté la collision (signal CD) la renforce en émettant 32 bits supplémentaires (jam)
  - en réception, la station n'a pas besoin de tester le signal CD car une trame accidentée a une longueur inférieure à 72 octets
- **COLLISION : *la réémission***
  - Après une collision, la station attend R * 51.2s tel que

    $0 <= R < (2^i) - 1$
  - R étant un entier « Random » et i = min(n, 10)
  - n = nombre de retransmissions déjà effectuées
  - le nombre de réémissions est limité à 15

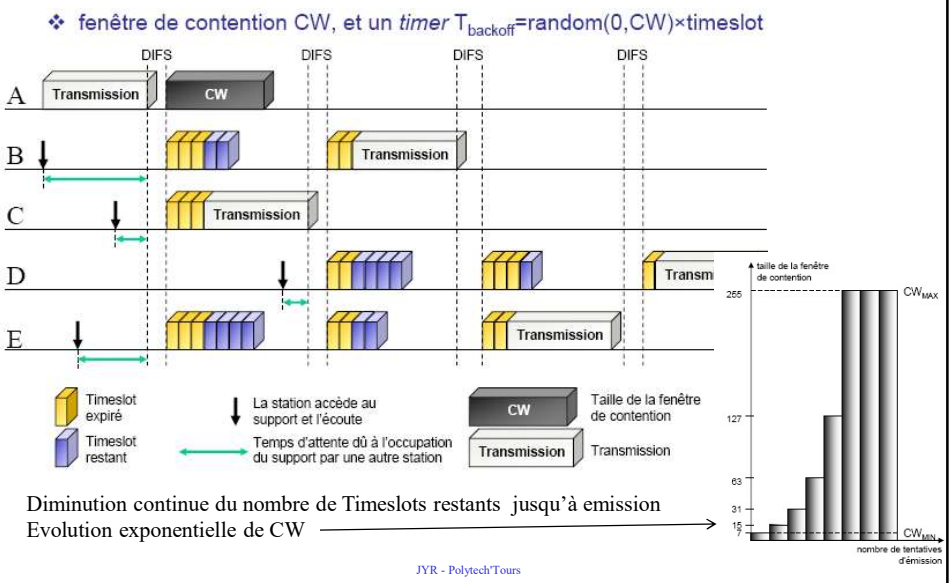
CSMA/CD : Résumé de l'algorithme

Hypothèse :

- Les conflits disparaissent par l'utilisation de temps d'attente de durées aléatoires. Le temps d'attente est calculé par l'algorithme **BEB** (*Binary Exponential Backoff*) :
- Après la $n^{ème}$ collision, le temps d'attente est choisit aléatoirement dans l'intervalle $[0,2^{i-1}]$ / i = min(n,limite BEB).

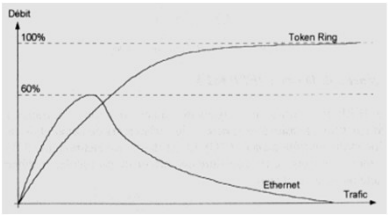


Timeslot & fenêtre de contention



Diminution continue du nombre de Timeslots restants jusqu'à emission
Evolution exponentielle de CW

Conclusion CSMA/CD (Ethernet)



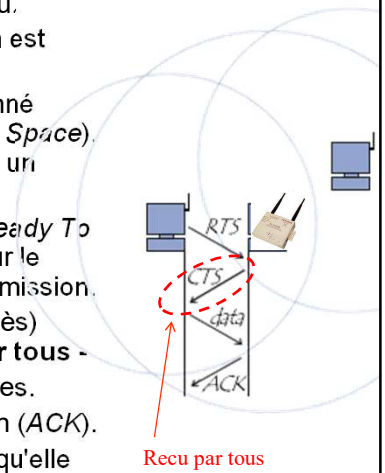
- Performances CSMA/CD
  - Se dégradent très vite si le nombre de stations augmente
- Avantages
  - Algorithme simple à implémenter
  - Accès équitable au support
- Inconvénients
  - Non déterministe
- Aujourd'hui : commutateurs Ethernet = zéro collision
  - Bufferisation des trames (toujours non déterministe)
  - Point à point full duplex

CSMA/CA DCF (WiFi)

- Radio = modulation d'une porteuse
  - mais multiplexage (FDMA, TDMA, CDMA) impossible car tout le monde doit pouvoir entendre tout le monde
- DCF = Distributed Coordination Function
  - La plus utilisée, adaptée pour les données asynchrones
  - Les utilisateurs ont une chance égale d'accéder au support
- Carrier Sense
  - Écoute du support avant émission
- Collision Avoidance
  - En radio il n'est pas pertinent d'écouter ce qu'on émet pour détecter une collision
  - Problème de la « station cachée »
- Acquittements
  - Récepteur envoie un acquittement
  - Emetteur attend acquittement
  - Si émetteur ne reçoit pas d'acquittement alors ***collision probable***

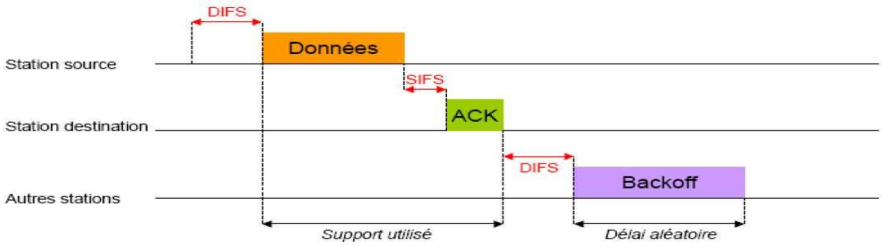
CSMA/CA DCF (wifi)

- La station voulant émettre écoute le réseau.
- Si le réseau est encombré, la transmission est différée.
- Si le média est libre pendant un temps donné (appelé *DIFS* pour *Distributed Inter Frame Space*), alors la station peut tenter d'émettre après un temps d'attente.
- La station transmet un message appelé *Ready To Send* (*RTS*) contenant des informations sur le volume des données et la vitesse de transmission.
- Le récepteur (généralement un point d'accès) répond un *Clear To Send* (*CTS*) **- reçu par tous -**
- la station commence l'émission des données.
- le récepteur envoie un accusé de réception (*ACK*).
- Les stations patientent pendant un temps qu'elle considère être celui nécessaire à la transmission du volume d'information à émettre à la vitesse annoncée.



CSMA/CA DCF (WiFi)

- Constantes temporelles
  - Timeslot = 10µs, SIFS = 10µs, DIFS = 30 µs
- Pour chaque tentative de retransmission i, le temporisateur de backoff croît de la façon suivante
  - $[2^{2+i}$ x randf()] x Timeslot
- Echange type :



CSMA/CA PCF (WiFi)

- PCF = Point Coordination Function
  - Accès géré par un « chef d'orchestre »
    - Point d'accès WiFi
  - Interrogation à tour de rôle des stations
    - « Polling »
    - Schéma « Maître – Esclave »
  - Données synchrones (voix, vidéo)
  - Déterministe !
  - Rarement implémenté dans les points d'accès et les cartes WiFi…

MAC : Méthodes à compétition

⊕ les performances moyennes sont plus intéressantes que les autres méthodes. C'est pourquoi cette approche est très utilisée surtout sur Ethernet.

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

Trame 802.3 (voir HDLC)

Θ Danger si les stations effectuent des tâches similaires avec une périodicité synchronisée → "*dead-lock*"

Θ Le temps d'accès maximal n'est pas garanti

Applet & démo : http://www.rfai.li.univ-tours.fr/PagesPerso/jyramel/applet_lan/appletlan.htm

Applets Reseau

- http://www.rfai.li.univ-tours.fr/fr/applet_lan/csma1/Csma.htm
- http://www.rfai.li.univ-tours.fr/fr/applet_lan/appletlan.htm
- http://mcs.uwsuper.edu/sb/470/Applets/

MAC : Méthodes Déterministes

Polling

- Un maître donne la parole aux esclaves

MLMA (Multi level Multiple Access)

- Inspiré du protocole BipMap (réseau radio)
- Période de contention = Emission de flag de demande d'émission à un moment déterminé
- Envoi de données par les stations élues selon leur numéro d'ordre

BRAP (Broadcast Recognition with Altenating Priorities)

- Idem mais **avec** Permutation circulaire des numéro d'ordre

MAC : Méthodes Déterministes

Jeton : Normes IEEE 802.4 (sur bus) et 802.5 (sur anneau)

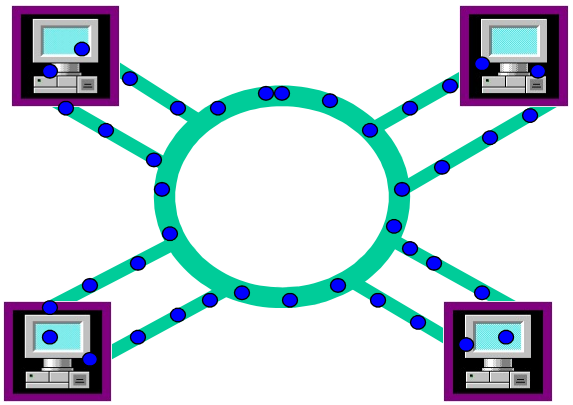
Jeton = droit d'accès unique → une seule station émettrice.

⊕ Un temps d'accès borné
⊕ Meilleur rendement que la méthode AMRT = MLMA
→ utilisée dans FDDI, Token-Ring, Profibus, DQDB, ...

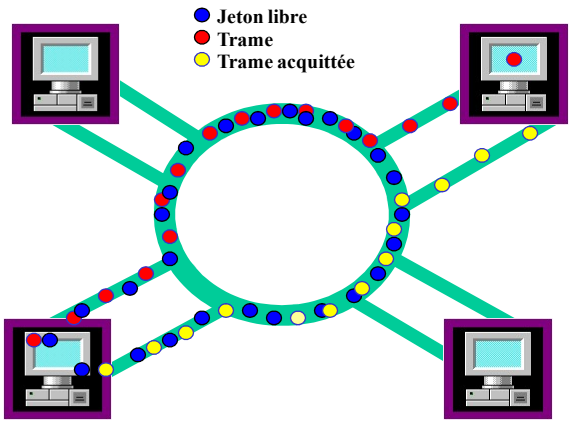
802.4 : Jeton adressé sur bus (anneau virtuel)

- Chaque station est numérotée (1 successeur/1 prédécesseur)
- Bus → tous le monde écoute
- Emission → Passage du jeton

Principes : circulation du jeton



Principes : capture du jeton et trames



MAC : Méthodes Déterministes

Champs	PRE	SFD	FC	DA	SA	LLC DATA	CRC	ED
Taille en octets	1 ou +	1	1	2 ou 6	2 ou 6	0 à 8191	4	1

Format d'une Trame 802.4

Θ Il faut être sûr que le jeton est réellement perdu et pas seulement retardé d'où l'importance de la détermination des délais avant réémission.

Θ borne supérieure du temps d'attente proportionnelle au nombre de stations

Θ Problème si la station qui a le jeton tombe en panne.

Il faut donc que toutes les stations surveillent le réseau pour éventuellement réémettre le jeton.

→ Il faut alors une méthode de compétition pour éviter les duplicatas.

MAC : Méthodes Déterministes

Jeton adressé avec différentes classes de priorités (802.4)

• Principe :
  – priorité dynamique contenue dans le message
  – 4 niveaux de priorités

La station ayant le jeton émet (si les timers de priorité l'y autorisent) dans l'ordre décroissant de priorité jusqu'à expiration de son temps d'accès au médium. Le jeton est alors passé à la station suivante.

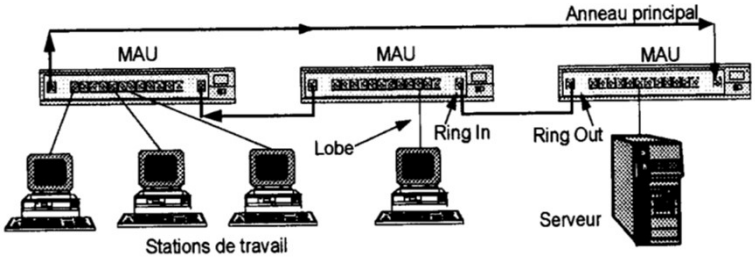
⊕ Accès plus rapide au médium.

MAC : Méthodes Déterministes

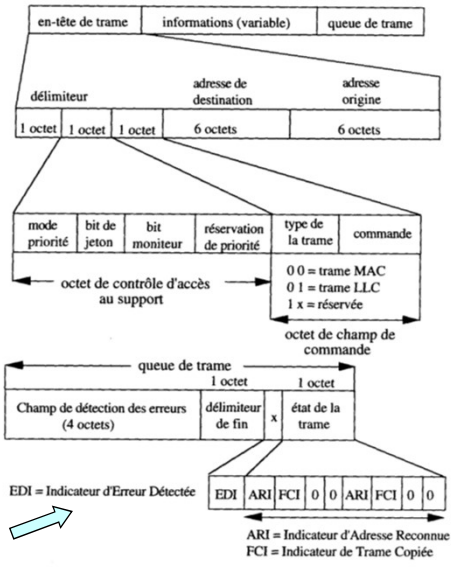
Jeton priorisé sur anneau (802.5)

- Norme soutenue par IBM pour les réseaux *Token-ring*.
  - 1 moniteur / des stations
  - Protocole assez complexe (le jeton indique une priorité)

- **High Speed Token Ring :** 100Mb:s voir 1Gb/s - Basée sur la commutation. Prix du MAU 1000F/port.



MAC : Méthodes Déterministes



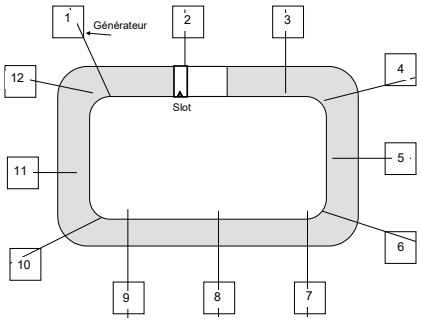
Format d'une trame (de données) 802.5

MAC : Méthodes Déterministes

Slot ou conteneur (802.6)

- Une trame = une succession de slots (de 53 octets)
- Un slot = adresse + données (longueur fixe)
- Un fanion (busy) permet de connaître l'état du slot (libre/occupé)
- Pour éviter les blocages (deux stations privilégiées qui monopoliseraient 1 slot), on interdit à une station qui reçoit de recharger immédiatement le slot.

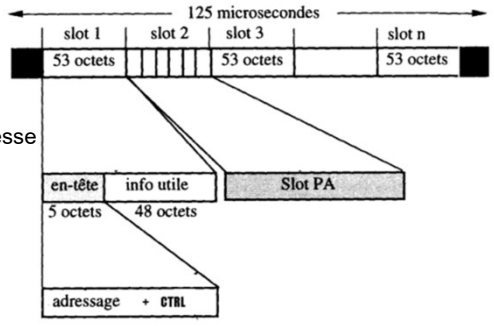
Θ Les stations proches du générateur sont privilégiées



MAC : Méthodes Déterministes

- Algorithme :

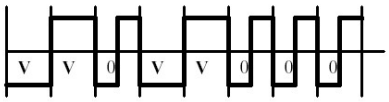
si arrivée_slot alors
  si fanion_libre alors
    si information_à_transmettre
    alors remplir le conteneur avec le message
      fanion ← occupé
    sinon pas d'examen du contenu
  sinon
    si adresse_destinataire = mon_adresse
    alors récupérer l'information
    sinon passer au suivant



Services de la couche LLC

- **Séparation des trames :**
  - **par caractères spéciaux (BSC)**
  - **par Fanions (HDLC)**
  - **par Violation de codage**

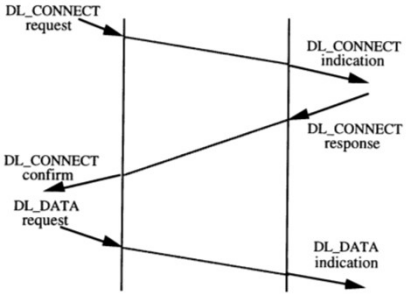
PB : présence de codes identique aux fanion dans les données



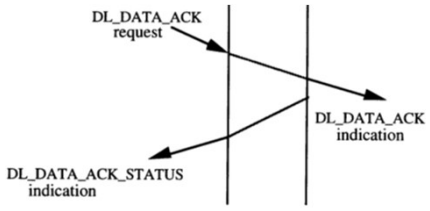
- **Détection et correction des erreurs**
- **Contrôle de flux**
- **Gestion de la liaison (initialisation des paramètres, fenêtre, …)**

Liaison de données - Couche LLC : 802.2

Primitives de type LLC1



Primitives de type LLC2



- Primitives de type LLC3

DIAPO EN ANNEXES

Liaison de données - Couche LLC : 802.2

• Sans connexion - Mode LLC1 et LLC3

• Les trame contiennent toutes l'adresse source et destination.

• Utile pour envoyer un message à plusieurs stations → **diffusion.** Celle-ci peut être totale (broadcast), partielle (multicast) ou point à point.

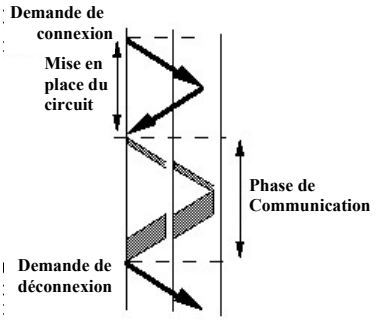
• **LLC3:** chaque trame est acquittée / **LLC1:** Pas de contrôle de flux

Liaison de données - Couche LLC : 802.2

La couche LLC doit assurer le **contrôle de flux** et le **contrôle d'erreurs** suivant le **mode de communication** choisi :

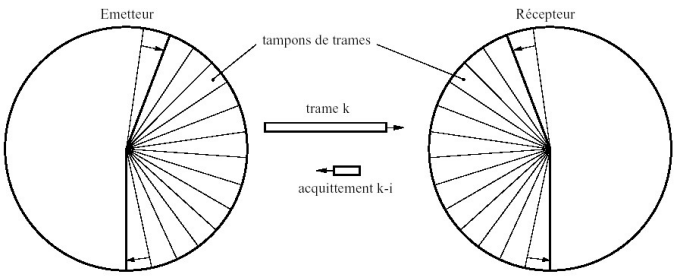
• Avec connexion - Mode LLC2

Une demande de connexion établie une communication entre 2 stations (end systems). Cette connexion reste ouverte durant toute la communication.



LLC : Gestion de la communication

- **Gestion de fenêtres d'anticipation :**
  - Fenêtre en émission : Les trames émises sans retour d'ACK garder en mémoire tampon
  - Fenêtre en réception : Permet la vérification des trames avant envoi au niveau supérieur (3)



Gestion de la communication

- **Exemple de protocole : BSC (Binary Synchronous Communication) :**
  - Protocole envoyer et attendre orienté caractère (entre PC et Terminal)
  - Code de supervision = code ASCII
    - SYN = 0101 0101 pour la synchronisation
    - ENQ = ouverture de connexion
    - EOT = déconnexion
    - SOH = début d'entête
    - STX = début des données
    - ETB = fin des données
    - ETX = fin du message
    - ACK
    - NAK
    - DLE = gestion de l'envoi de caractères spéciaux dans les données
    - BCC = contrôle d'erreur (parité)

    - Notion de time out

Gestion de la communication

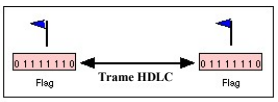
- **Exemple de Protocole : HDLC (High level Data Link Control) :**
  - Orienté bit / Fanion pour la synchronisation (01111110)
  - 7 bits à 1 consécutifs → trame erronée
  - + de 15 bits consécutifs → arrêt complet
  - Avec ou sans connexion
  - Mode étendu (2 octets) ou normal (1 octet)
  - Half ou Full duplex :
    - LAPB (Link Access Protocol Balanced) : avec connexion, full duplex, point à point →Utilisé dans X25
    - LAPD (D-channel) : LAPB en multipoint et sans connexion
      →canal D de RNIS (supervision)

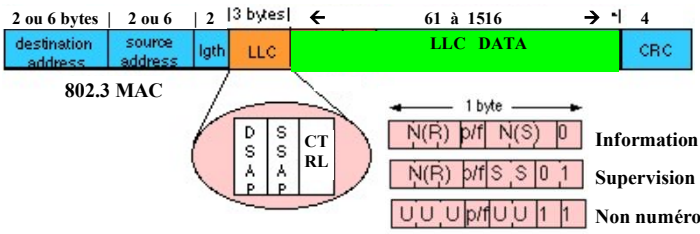
Gestion de la communication

- La norme HDLC fournit un service de transmission synchrone transparent de niveau 2

  → Voir le Cours de Transmission de l'information

- **La trame HDLC :**





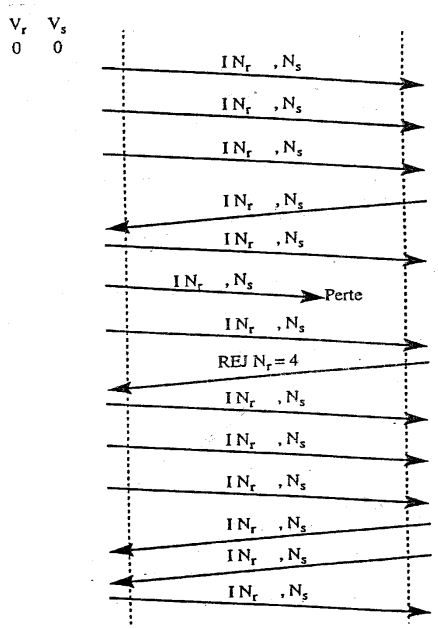
N(S) : Numéro de trame émise

N(R) : Numéro de trame attendue

Information : I(r,s)

Supervision : RR,RNR,REJ,SREJ

Non numérotée : SABM, DISC

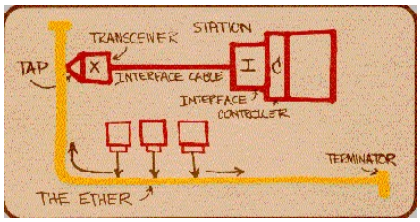


Chapitre 4

Ethernet et ses évolutions

Ethernet : Introduction

- Développé à l'origine par le groupe Dec, Intel Xerox (1980)



Conception originale de R. Metcalfe (1976)

- Proche de la norme 802.3 ➔ bus

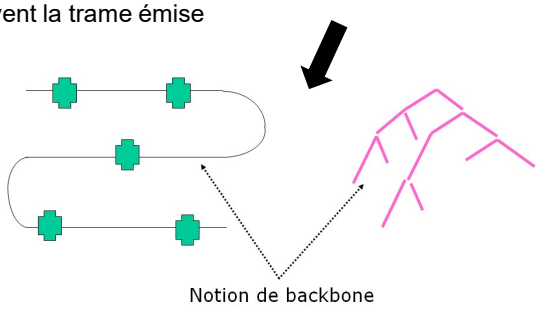
Buts	Non-buts
réseau multipoint	contrôle d'erreur
sans priorité	full duplex
avec collisions	sécurité
faible coût	priorité
	déterminisme

Ethernet : Principes de départ

- **PRINCIPE DE FONCTIONNEMENT ➔ Voir 802.3**
  - N stations sur le même support
  - une station écoute avant d'émettre
  - si deux stations émettent simultanément, il y a collision
  - une seule trame à un instant donné
  - toutes les stations reçoivent la trame émise

TOPOLOGIE
- De linéaire (bus)
- A arborescente

- **SUPPORT PARTAGE :**
  - permet la diffusion
  - bus passif
  - bus linéaire
  - bande de base



Ethernet : couche physique

- **RÔLE :**
  - détecter l'émission d'une autre station sur le médium (Carrier Sense), alors que la station est en écoute
  - transmettre et recevoir des bits sur le médium,
  - détecter l'émission d'une autre station pendant que la station émet **(Collision Detect)**

- **INTERFACE :**
  - transmission d'un bit (requête MAC)
  - réception d'un bit (requête MAC)
  - attendre N bits (requête MAC)
  - détection de porteuse (indication de la couche physique vers la couche MAC); la couche MAC doit déclencher la requête de réception d'un bit
  - détection de collision (indication de la couche physique vers la couche MAC); générée uniquement pendant une transmission

Ethernet : la trame

- 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**,
    - **8019 : Apollo**
    - **...**

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

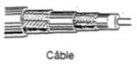
- Le constructeur reçoit une adresse dont :
  - les trois premiers octets sont fixés, code fabricant (Vendor Code) ou OUI (Organizationally Unique Identifier)
  - les trois suivants étant laissés à sa libre utilisation
- Ces adresses Ethernet sont alors unique dans le monde.
  - Les adresses étaient 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**

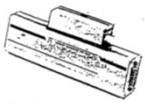
Norme de repérage des différents supports Ethernet

N1.IDEN.N2

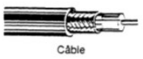
- N1 : vitesse de transmission en Mb/s ;
- IDEN : nature des signaux
- N2 : $\begin{cases} T : paire\_torsadée \quad F : Fibre \\ taille\_du\_réseau\_(5,2,36)\_en\_hectomètre \\ nombre\_de\_noeuds\_sur\_une\_branche \end{cases}$
- Exemples :
  - 10 BASE 5 : version standard (Ethernet épais jaune)
  - 10 BASE 2 : Ethernet fin (RG 58)
  - 10 BASE T : version sur 2 paires torsadées
  - 10 BASE F : fibre optique (liaison bipoint)
  - 1 BASE 5 : version Starlan
  - 10 BROAD 36 : version large bande
  - 100 BASE T4 : version sur 4 paires torsadées (cat 3/4)
  - 100 BASE TX : version sur 2 paires torsadées (cat 5)

Norme 10 BAS 5
"Câble jaune",
Coaxial 50 Ω,
Câble semi rigide
Rayon de courbure 30 cm
Vitesse de propagation mini o,65
Utilisation de prises piquées
Segment:
500 m maxi
100 MAU (prises utilisées)


Câble


Prise piquée et transceiver

Norme 10 BAS 2
"Ethernet mince", "Ethernet thin wire"
Coaxial 50 Ω, Type RG 58 (noir)
Câble souple
Vitesse de propagation mini o,65
Utilisation de T vissés BNC
Segment:
200 m maxi
30 MAU (prises utilisées)

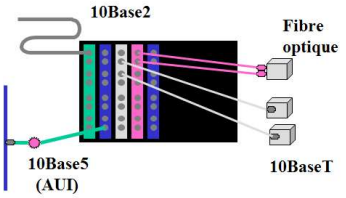

Câble


Prise T et transceiver

HUB Ethernet

HUB = concentrateur (ou étoile, multi-répéteur)
fonction de répéteur
permet de mixer différents médias
«empilables» (un seul domaine de collision)
«cascadables» (plusieurs domaines de collisions)
comprend généralement un agent SNMP

Hub plat : 8, 16, 24, 32 ports
Carte dans chassis : 8,16,24 ports.



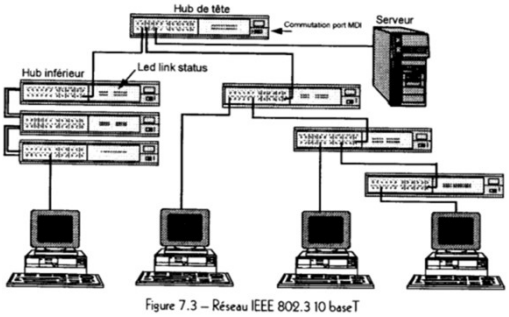


Figure 7.3 – Réseau IEEE 802.3 10 baseT

Ethernet 100Mbits / Fast Ethernet (802.3u)

- Même principe du CSMA/CD, mais 10 fois plus vite
- Paire torsadée Catégorie 5 - 100BASE TX (2 paires)
- Fibre optique 100BASE FX
- Paire torsadée de catégorie 2 et 4, mais sur quatre paires, 100BASE T4
- Plus de transmission sur câble coaxial.

- **Physical Layer Device - PHY :** L'adaptateur au media (Fibre ou paire torsadée), équivalent du transceiver s'appelle un PHY - *Physical Layer Device.* Il est connecté à un device au moyen d'un câble MII (correspondant à l 'ancien AUI) ou est installé sur la carte réseau. C'est lui qui code et décode les messages en 4B/5B, NRZI (TX et FX).
- Il existe des transceivers PHY pour 100Base TX, 100Base T4 et 100Base FX

- Gigabit Ethernet (802.3z) → Paires torsadéés ou F.O.

Ethernet Full duplex

- Exploitation des liaisons **point à point** pour les Paires Torsadées ou les F.O. :
  - Modification des cartes d'interface (inhibition de la détection de collision)
  - Le **hub (concentrateur)** est remplacé par un **switch (commutateur)** capable de traiter plusieurs trames simultanément
- Offre une bande passante de 20 Mbit/s (10 Mbits/s en émission et 10 Mbits/s en réception)
- Cette technologie peut s'appliquer à 100 Mbits/s → 200Mb/s
- **Il n'y a plus de collisions !!!**
- **Mais pb de compatibilité (HUB interdit ! Carte reseau FullD)**

Compatibilité entre les Ethernets

- **Auto-négociation :**
  - 1. 100BASE TX Full Duplex
  - 2.100BASE T4
  - 3.100BASE TX
  - 4.10BASE T Full Duplex
  - 5.10BASE T

- **Contrôle de flux :** Losrqu'un coupleur 10Mb/s communique avec un coupleur 100Mb/s

Ethernet commuté

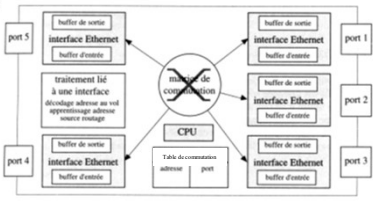
- Le Hub est remplacé par un **commutateur (Switch)**

→ L'interface de chaque port est intelligente, elle :

- détecte l'adresse destination "à la volée" **(Cut through)** sans attendre la vérification du CRC
- commute ensuite la trame sur le port destination
- établit un circuit à 10 ou 100 Mb/s entre 2 stations

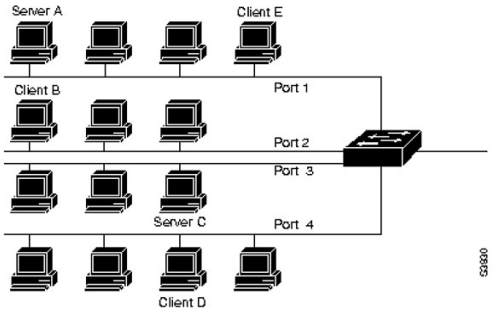
- La bande passante du bus du Switch lui permet d'établir ces circuits simultanément entre tout couple de stations.

- **Méthode " store and forward "** : méthode permet de mémoriser les trames et de vérifier le CRC avant de les commute



Ethernet : Commutateurs / Switchs

- Relie plusieurs segments physiques
- Equipement configuré de manière à gérer un ou plusieurs PC par port



Extrait de la documentation Cisco

Echanges simultanés :

A (port 1) <--> B (port 2)

C (port 3) <--> D (port 4)

Echange non commuté :

A (port 1) <--> E (port 1)

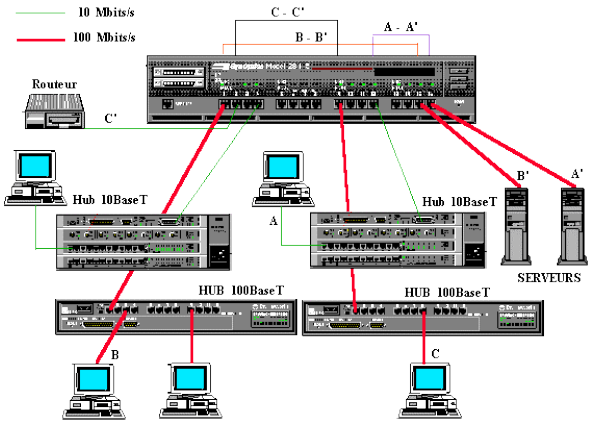
Ethernet : Commutateurs / Switchs

- **Technologies :**
  - Logiciel (ex: 3com, Atlantec)
    - Processeurs RISC à l'instar des routeur
    - Difficulté de gérer les Broadcasts (pas de process parallèle)
    - lenteur
    - flexible et administrable
  - Matériel (ex: LANNET, MULTINET)
    - ASICs comme pour les ponts
    - rapiditè
    - flexible et administrable
- **Protocoles spécifiques**
  - Trunk 802.3ad → agrégation de liens
  - Administration et sécurité 802.10 → login +mdp

Ethernet commuté : Qq PB

Quelques Problèmes :

- ❑ Commutation de trames erronées
- ❑ Multicast et Broadcast : Bootp, DHCP relay, …
- ❑ La commutation doit émuler les fonctionnements du mode « diffusion »

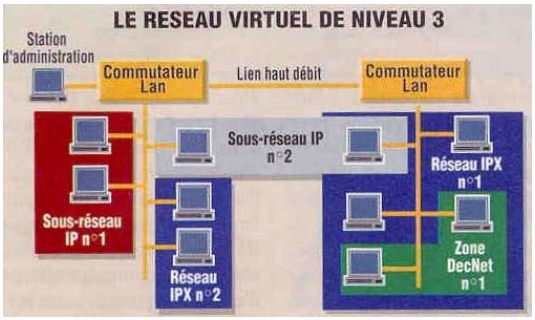


Ethernet : VLANS

- **Réseaux Virtuels** : Regrouper les stations par commutation suivant certains critères.
- Les paquets entre stations d'un même réseau virtuel ne sont pas diffusés sur les autres réseaux virtuels
- **Critères de création des réseaux virtuels :**
  - Par numéro de port . un même réseau virtuel peut être constitué de ports appartenant à des commutateurs différents.
  - Par adresse Ethernet (adresse MAC) : L'adresse Ethernet étant spécifique à la station, le déplacement d'une station ne nécessite pas la reconfiguration du commutateur.

Ethernet : VLANS

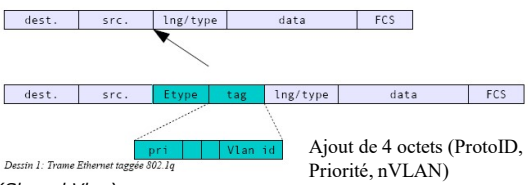
- **Par les informations contenues dans la couche 3 :**
- On peut utiliser le type de protocole ou l'adresse réseau pour définir l'appartenance à un réseau virtuel.
- Le déplacement d'une station n'oblige pas à changer d'adresse réseau (dans le cas de TCP/IP).
- Les performances sont moindres, il faut analyser le paquet jusqu'au niveau 3.



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 ?

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



Dessin 1: Trame Ethernet taggée 802.1q

Ajout de 4 octets (ProtoID, Priorité, nVLAN)

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

Ethernet : VLANS

Vlan inconnu = destruction

Format de la trame de sortie = aware ou pas

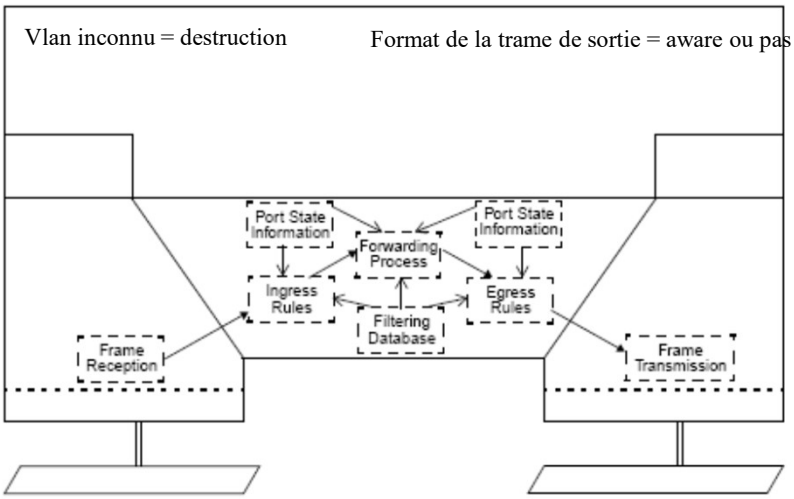


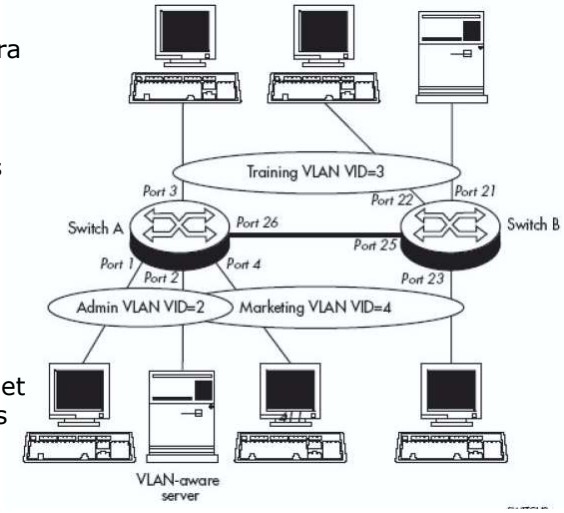
Figure 8-4—Relaying MAC frames

Ethernet : Exploitation du réseau

- Ethernet = réseau à diffusion et à débit fixe
- niveau de performance inversement proportionnel au nombre d'acteurs
- plus on est nombreux à parler, moins on a de bande , plus le réseau est dégradé jusqu'à l'écroulement possible (version avec HUB).
- Les solutions :
  - Supprimer les HUB → utiliser des Switchs
  - segmenter le réseau : une valeur raisonnable en débit constant se situe autour de 10% du débit nominal.
  - identifier des raisons de charge anormale : utiliser un analyseur (analyse la charge et identifie l'auteur de la charge anormale).
  - mesurer le taux de collisions moyen du réseau; si celui-ci est trop élevé (au delà de 10% des trames transmises), vérifier le matériel (transceiver, répéteur, etc), analyser chaque segment, envisager une nouvelle segmentation.

Exercice 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.



Exercice matériel Niveau 2

COMMUTATEUR 12 OU 24 PORTS 10/100 MBPS EVOLUTIF

- Commutateur 12 ou 24 ports 10/100 Base TX auto-sensing supportant également 2 modules non équipés.
- Chaque module d'extension peut supporter 4 ports 10/100 Base TX auto-sensing, 2 ports 100 Base FX ou 1 port Gigabit Ethernet.
- Les commutateurs 510 T, 520 T, 550 T et 550 F peuvent être regroupés au sein d'une même pile.
- Module de liaison pour interconnecter 2 commutateurs.
- Supporte jusqu'à 128 VLANS, 8164 adresses MAC
- Module d'empilage en étoile pour regrouper jusqu'à 7 commutateurs au sein d'une même pile.
- Détection du débit et configuration automatique de la vitesse de chaque port (10/100 Mbps).
- Support redondant du fond de panier de l'alimentation et des connexions réseaux.
- Commutation cut through ou store and forward par port.
- Contrôle de flux paramétrable.
- Device View est un outil d'administration livré en standard.
- Sonde RMON intégrée.
- Garantie : 1 an.

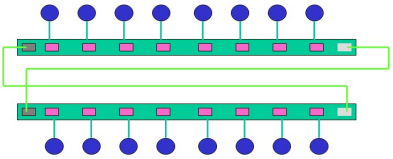
HUB ET MINI HUB FAST ETHERNET 100 MBPS - 100 BASE TX

- Hub Fast Ethernet 100 Mbps équipé de 4 ou 8 ports 100 Base TX RJ45.
- Peut être cascadé à un autre Hub 100 Mbps permettant alors jusqu'à 14 ports 100 Base TX.
- Un port est configurable par commutateur en cas de cascade avec un autre Hub.
- Conforme aux normes 802.3u, répéteur Classe II.
- Distance maximum entre la station et le Hub :
  100 m (câblage en catégorie 5) entre 2 Hubs 100 Base T : 10 m (catégorie 5).
- Rackable 19 pouces.
- Solution "Plug and Play".
- Dimensions : 43,7 x 20,6 x 4,4 cm.
- Poids : 3,62 Kg.
- Les modèles CTX 8101 et CTX 4101 sont nouveaux. Ce sont des mini hubs 100 base TX (nous consulter pour dimensions et caractéristiques).
- Garantie : 2 ans.

Autres réseaux locaux

- TOKEN-RING d'IBM
  - Réseau de transmission **en anneau** interconnectant des stations entre elles par une succession de liaisons point à point.
  - **Réseau déterministe**, asynchrone, avec acquittement
  - vitesse = 4 / 16 Mbs au depart puis High Speed Token-Ring
  - Normalisée par l'IEEE sous la norme 802.5
  - Plus complexe qu'un réseau Ethernet
  - ➔ Plus cher qu'un réseau Ethernet
  - ➔ Moins utilisé ➔ En cours de disparition (sauf banques)

Modules T.R BayNetworks



MAU Olicom

Autres réseaux locaux

- Token-Ring : Principes de base ➔ Voir 802.5
  - Jeton sur anneau
  - Une station peut émettre pendant 10 ms
  - Après émission d'une trame, la station peut émettre une nouvelle trame s'il reste suffisamment de temps pour le faire (10 ms d'émission max)
  - Lorsque toutes les trames en attente ont été transmises ou que le temps imparti est écoulé, la station cesse le processus d'émission et génère un nouveau jeton
  - **Des priorités** peuvent être affectées aux stations
    - le jeton comporte une indication de priorité
    - si le message à émettre a la priorité requise lors du passage du jeton, la station peut émettre, sinon elle passe le jeton à la station suivante.
  - un moniteur de contrôle supervise le fonctionnement du réseau

Autres réseaux locaux

- TOKEN-RING : Cablage
  - C'est la spécification d'IBM qui fait référence
  - Régit l'interconnexion de PC, terminaux, mainframes, ...
  - Câbles de type paires torsadées blindées (Shielded Twisted Pairs ou STP).
    - type 1 : double paire blindée (une paire est prévue pour le câblage intérieur et une autre pour l'extérieur). Il est recommandé pour les liaisons inter concentrateurs (MAUs).
    - type 3 : 4 paires téléphoniques dont 2 sont prévues pour le réseau et 2 autres pour le téléphone. Il est utilisé dans le câblage des bureaux.
    - type 2 : contient dans la même enveloppe un câble de type 1 et un câble de type 3; il permet le précablage des immeubles pour les installations téléphoniques et réseaux.
    - Le câble de type 5 contient deux fibres optiques et est dédié à l'interconnexions de MAUs éloignés (jusqu'à 2 kms).
    - Le câble de type 9 est un câble de type 1 économique, la distance autorisée étant inférieure d'un tiers.
    - Utilisation de UTP ethernet possible

Autres réseaux locaux

- FDDI (*Fiber Distributed Data Interface*)
  - **Topologie :**
    - Support (fibre optique) Double anneau - Débits beaucoup plus élevés (jusqu'à 100 Mb/s) - Circonférence de 100 km, jusqu'à 2 km entre les stations
    - La norme définit 3 types de stations :
    - DAS (Dual Attachment Stations) - classe A - Elles sont connectées à l'anneau actif et à l'anneau de secours.
    - SAS (Single Attachment Stations) - classe B - Elles sont uniquement connectées à l'anneau actif (primaire)
    - Concentrateurs - classe C
  - **Différences avec Token Ring :**
    - Le jeton est libéré après l'émission de la trame alors que pour token ring il n'est libéré qu'après son retour à la station émettrice.
    - Le jeton n'est pas attribué par une station maître mais négocié par l'ensemble des stations

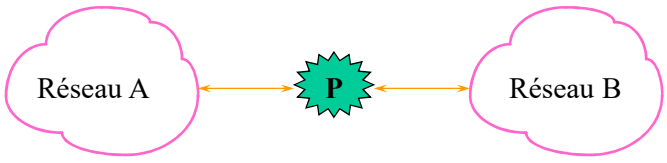
Chapitre 5

INTERCONNEXION DE LANs

TCP/IP & ATM
Les standards actuels
de l'interconnexion ?

Concepts de l'interconnexion

- Certaines machines possèdent une connexion sur plusieurs réseaux:



Le noeud P interconnecte les réseaux A et B.

- Le rôle de P est de transférer sur le réseau B, les paquets circulant sur le réseau A et destinés au réseau B et inversement.
- **Possible au niveau 2 ➔ Pont / switch ➔ Commutation / Filtrage**

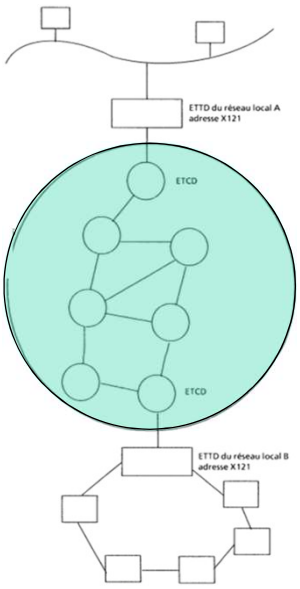
Concepts de l'interconnexion

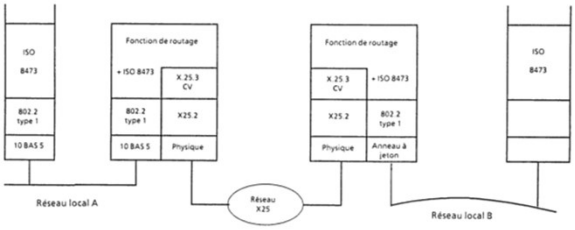
- P1 transfère sur le réseau B, les paquets circulant sur le réseau A et destinés aux réseaux B et C
- P1 doit avoir connaissance de la topologie du réseau; à savoir que C est accessible depuis le réseau B.
- **Difficile au niveau 2, donc déconseillé ➔ Routeur /Routage (Niv 3)**

Concepts de l'interconnexion

Commentez ces 2 figures

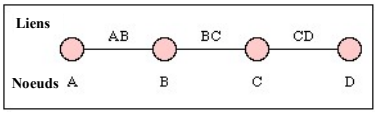
Routeurs = Nœuds d'interconnexion

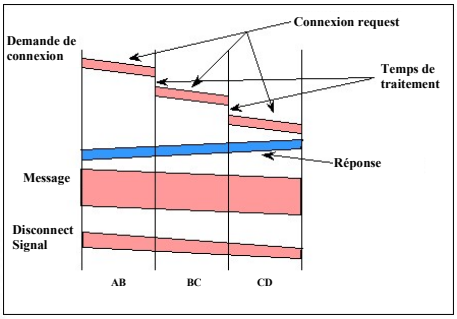


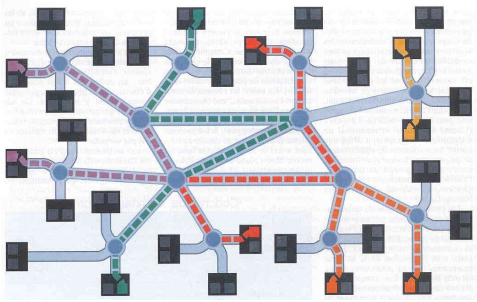


Les différents modes de communication de bout en bout

- Circuits virtuels:

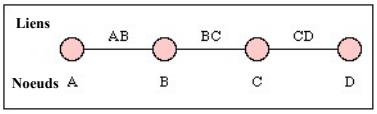


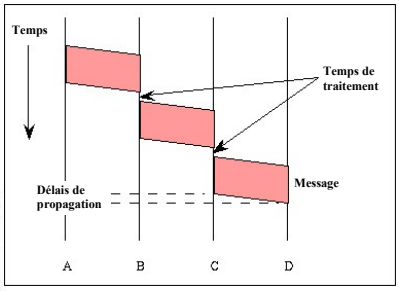


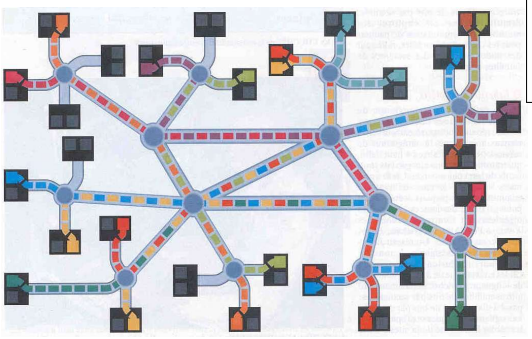


Les différents modes de communication de bout en bout

- Datagrammes :







Commençons par IP

IP : Tout le monde connait…
Non ?

La philosophie initiale TCP/IP

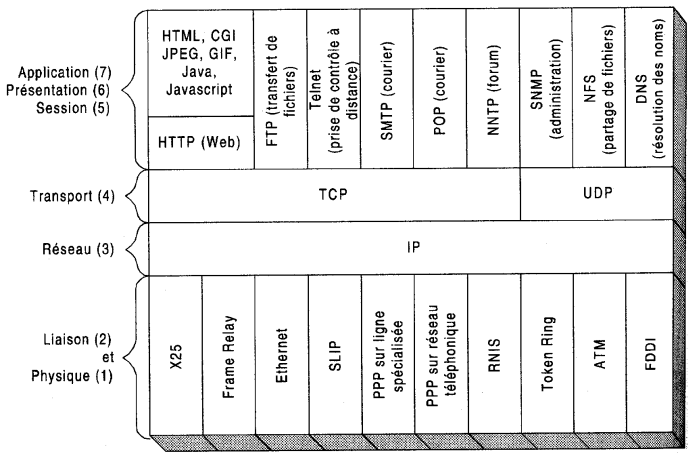
- TCP/IP : but = interconnexion de réseaux sur une base planétaire
- Aujourd'hui : 100000 réseaux interconnectés, plusieurs millions de machines, plusieurs dizaines de millions d'utilisateurs de "l'Internet".
- Interconnecte divers réseaux : Ethernet, T.R., X25, FR, FDDI, etc.
- La technologie est constituée par des protocoles de base (suite TCP/IP) qui offrent les services de base du transfert des données :
- Transport de datagrammes : service élémentaire du routage de paquets.
- Transport de messages sécurisés (TCP) : service orienté connexion permettant d'acheminer des données en garantissant leur intégrité

- Ces services de base sont indépendants du support de

La philosophie initiale TCP/IP

- Interconnexion universelle : les machines ont une adresse unique sur l'Internet. Deux machines reliées au réseau, communiquent grâce aux autres nœuds du réseau qui routent de manière coopérative sur la base de l'adresse destinataire.
- Interconnexion d'égal à égal (peer to peer systems) : il n'y a pas de machines prioritaires (en opposition à une structure hiérarchique).
- Dans le cadre du transport sécurisé, les acquittements sont effectués entre les systèmes finaux (source et destinataire) plutôt que continuellement entre chaque noeud relayant les messages.
- Technologie publique et largement diffusée au travers de RFC's.
- Indépendante des constructeurs et disponible sur tous types de matériel Largement validée depuis de nombreuses années dans un monde hétérogène.

Concepts de l'internet / Notion d'Intranet



L'adressage IP

- But : fournir un service de communication universel permettant à toute machine de communiquer avec toute autre machine de l'interconnexion
- Une machine doit être accessible aussi bien par des humains que par d'autres machines
- Une machine doit pouvoir être identifiée par :
  - un nom (mnémotechnique pour les utilisateurs),
  - une adresse qui doit être un identificateur universel de la machine,
  - une route précisant comment la machine peut être atteinte.

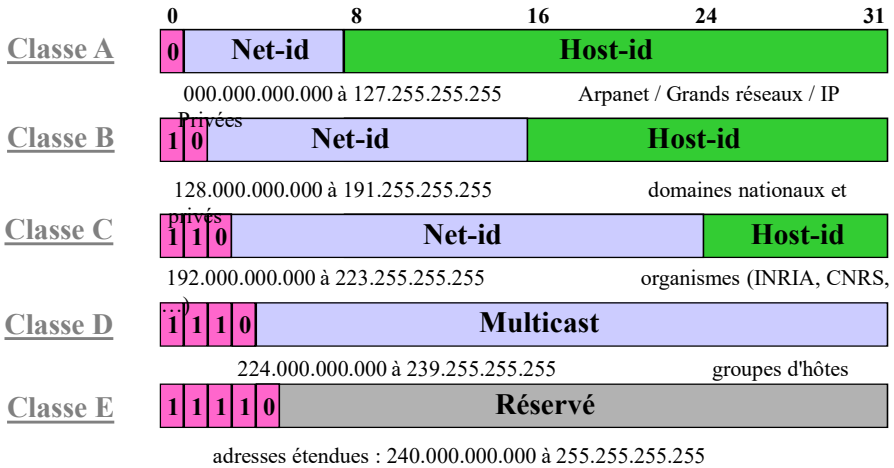
Adressage Internet

- **Ne mélangeons pas tous :**
  - numéro IPv4 et IPv6
  - adresse FQDN
  - adresse URL

Toujours l'adressage IPv4

- Solution 1 : adressage binaire compact assurant un routage efficace
- Adressage "à plat" par opposition à un adressage hiérarchisé permettant la mise en oeuvre de l'interconnexion d'égal à égal
- Utilisation de noms pour identifier des machines (réalisée à un autre niveau que les protocoles de base)
- Les classes d'adressage
  - Une adresse = 32 bits dite "internet address" ou "IP address" constituée d'une paire (netid, hostid) où netid identifie un réseau et hostid identifie une machine sur ce réseau.
  - Cette paire a été structurée de manière à définir cinq classes d'adresse (au départ)

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

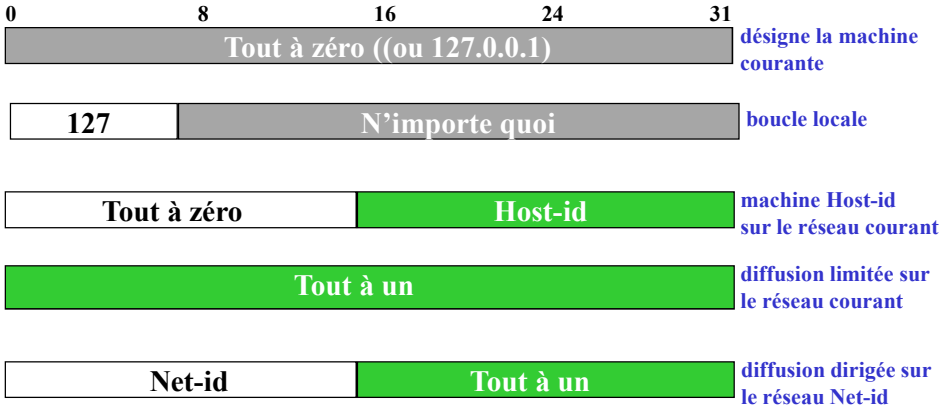
- Adresses particulières
  - Adresses réseau : adresse IP dont la partie hostid ne comprend que des zéros; => la valeur zéro ne peut être attribuée à une machine réelle : 191.20.0.0 désigne le réseau de classe B 191.20.
  - Adresse machine locale : adresse IP dont le champ réseau (netid) ne contient que des zéros;
  - **Adresses IP privée : 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 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



Manque d'Adresses IP v4

Pour pallier aux manques d'adresses IP :

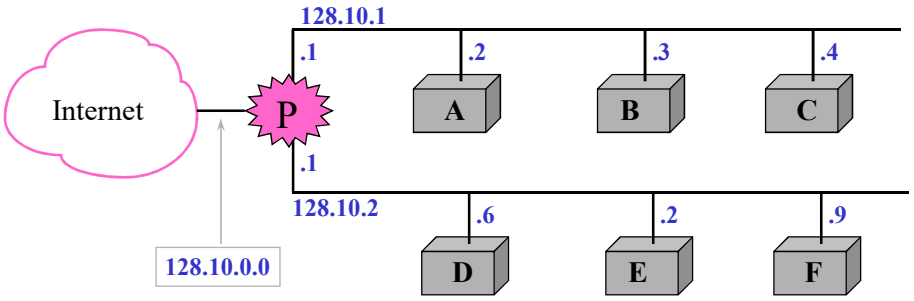
- IP privées (déjà vu)
- Sous / Sur – Adressage ➔ CIDR (cf après)
- DHCP : Dynamic Host Configuration Protocol (CF BM)
- NAT : Network Address Translation (CF BM)
- Adresses IP V6 sur 128 bits ➔ CF IPV6 (BM)

Le sous-adressage

- Le sous-adressage est une extension du plan d'adressage initial
- Devant la croissance du nombre de réseaux de l'Internet, il a été introduit afin de limiter la consommation d'adresses IP qui permet également de diminuer :
  - la gestion administrative des adresses IP,
  - la taille des tables de routage des passerelles,
  - la taille des informations de routage,
  - le traitement effectué au niveau des passerelles.

Le sous-adressage

Les sous-réseaux 128.10.1.0 et 128.10.2.0 sont notés seulement avec le NetId, les machines seulement avec le Hostid ; exemple IP(F) = 128.10.2.9



Un site avec deux réseaux physiques utilisant le sous-adressage de manière à ce que ses deux sous-réseaux soient couverts par une seule adresse IP de classe B.
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	Partie locale	
Partie Internet	**Réseau physique**	**Identifieur Machine**

- «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**
- la RFC 1860 (remplacée par la RFC 1878) stipulait qu'un numéro de sous réseau ne peut être composé de bits tous positionnés à zéro ou tous positionnés à un.

Et pourquoi pas du sur-adressage (RFC 1517-1520)

- Idem sous adressage mais sur la partie Net id
  → On concatène des réseaux (de classes C souvent)

Partie Internet	Partie locale

Partie Internet	Sur Réseau	Identifieur Machine

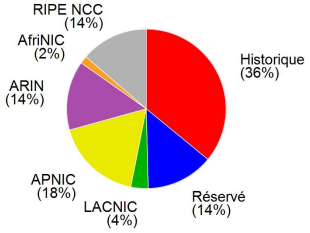
- «Partie Internet» correspond au NetId (plan d'adressage initial)
- «Partie locale» correspond au hostid (plan d'adressage initial)
- les champs «Sur-reseau» est toujours de taille faible. Il permet d'ignorer les derniers bit de la partie Net-Id
- PB pour le routage mais OK pour RIPv2, OSPF, BGPv4

Classless Inter-Domain Routing (CIDR)

- **RFC 1338 : Abolition de la notion de classe**
  - Afin de diminuer la taille de la table de routage
  - La totalité de l'espace d'adressage unicast est gérée comme une collection unique de sous-réseaux indépendamment de la notion de classe
  - Les Protocoles de routage compatibles avec CIDR sont dits classless (BGPv4, OSPF, EIGRP ou RIPv2

Adresse IP = Prefixe + Suffixe
Prefixe / Masque

→ 192.33.11.0 / 22



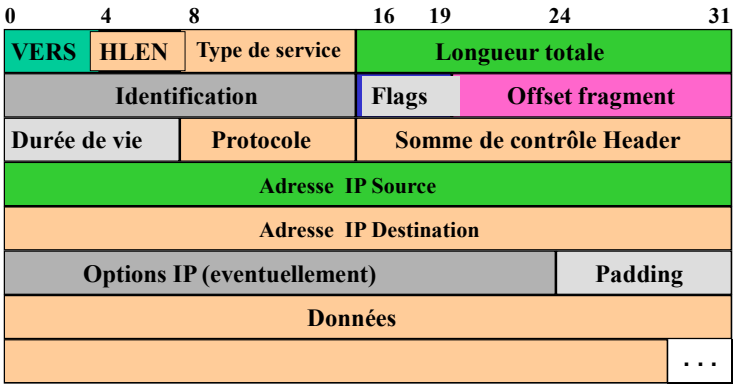
Bloc	Usage	Référence
0.0.0.0/8	*Adresse réseau par défaut*	RFC 1700
10.0.0.0/8	Adresses privées	RFC 1918
127.0.0.0/8	adresse de bouclage (localhost)	RFC 1122
169.254.0.0/16	adresses locales autoconfigurées (APIPA)	RFC 3927
172.16.0.0/12	Adresses privées	RFC 1918
192.0.0.0/24	Réservé par l'IETF	RFC 5736
192.0.2.0/24	Réseau de test TEST-NET-1	RFC 5737
192.88.99.0/24	6to4 anycast	RFC 3068
192.168.0.0/16	Adresses privées	RFC 1918
198.18.0.0/15	Tests de performance	RFC 2544
198.51.100.0/24	Réseau de test TEST-NET-2	RFC 5737
203.0.113.0/24	Réseau de test TEST-NET-3	RFC 5737
224.0.0.0/4	Multicast	RFC 5771
240.0.0.0/4	Réservé à un usage ultérieur non précisé	RFC 1112
255.255.255.255/32	broadcast limité	RFC 919

Le protocole IP : Internet Protocol

- Le protocole IP définit :
  - l'unité de donnée transférée dans les interconnexions (datagramme),
  - la fonction de routage (les règles qui mettent en œuvre la remise de paquets en mode non connecté)

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:



IP : le datagramme

Signification des champs du datagramme IP :

- VERS : numéro de version de protocole IP, actuellement version 4,
- HLEN : longueur de l'en-tête en mots de 32 bits, généralement égal à 5 (pas d'option),
- Longueur totale : longueur totale du datagramme (en-tête + données)
- Type de service : indique comment le datagramme doit être géré :

- PRECEDENCE (3 bits) : définit la priorité du datagramme; en général ignoré par les machines et passerelles (pb de congestion).
- Bits D, T, R : indiquent le type d'acheminement désiré du datagramme, permettant à une passerelle de choisir entre plusieurs routes (si elles existent) : D signifie délai court, T signifie débit élevé et R signifie grande fiabilité.

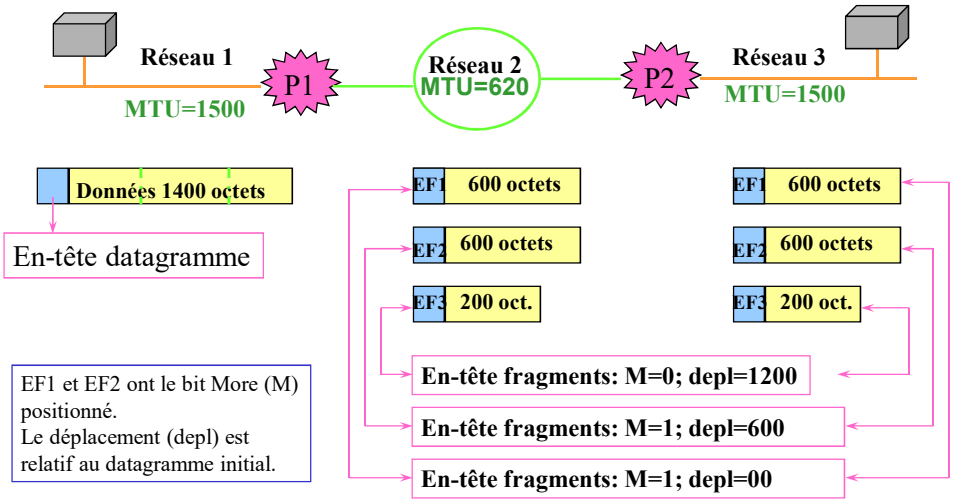
IP : le datagramme

- FRAGMENT OFFSET, FLAGS, IDENTIFICATION : les champs de la fragmentation.
  - Sur toute machine ou passerelle mettant en oeuvre TCP/IP une unité maximale de transfert (*Maximum Transfert Unit* ou **MTU**) définit la taille maximale d'un datagramme véhiculé sur le réseau physique correspondant
  - lorsque le datagramme est routé vers un réseau physique dont le MTU est plus petit que le MTU courant, la passerelle fragmente le datagramme en un certain nombre de fragments, véhiculés par autant de trames sur le réseau physique correspondant,
  - lorsque le datagramme est routé vers un réseau physique dont le MTU est supérieur au MTU courant, la passerelle route les fragments tels quels (rappel : les datagrammes peuvent emprunter des chemins différents),
  - le destinataire final reconstitue le datagramme initial à partir de l'ensemble des fragments reçus; la taille de ces fragments correspond au plus petit MTU emprunté sur le réseau. Si un seul des fragments est perdu, le datagramme initial est considéré comme perdu : la probabilité de perte d'un datagramme augmente avec la fragmentation.

IP : le datagramme

- FRAGMENT OFFSET : indique le déplacement des données contenues dans le fragment par rapport au datagramme initial. C'est un multiple de 8 octets; la taille du fragment est donc également un multiple de 8 octets.
- chaque fragment a une structure identique à celle du datagramme initial, seul les champs FLAGS et FRAGMENT OFFSET sont spécifiques.
- IDENTIFICATION : entier qui identifie le datagramme initial (utilisé pour la reconstitution à partir des fragments qui ont tous la même valeur).
- FLAGS contient un bit appelé "*do not fragment*" (01X)
- un autre bit appelé "*More fragments*" (FLAGS = 001 signifie d'autres fragments à suivre) permet au destinataire final de reconstituer le datagramme initial en identifiant les différents fragments (milieu ou fin du datagramme initial)

IP : le datagramme



IP : le datagramme

- Durée de vie
  - Ce champ indique en secondes, la durée maximale de transit du datagramme sur l'internet. La machine qui émet le datagramme définit sa durée de vie.
  - Les passerelles qui traitent le datagramme doivent décrémenter sa durée de vie du nombre de secondes (1 au minimum) que le datagramme a passé pendant son séjour dans la passerelle; lorsque celle-ci expire le datagramme est détruit et un message d'erreur est renvoyé à l'émetteur.
- Protocole

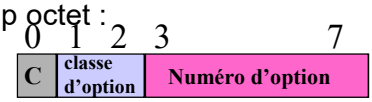
  Ce champ identifie le protocole de niveau supérieur dont le message est véhiculé dans le champ données du datagramme :
  - 6 : TCP,
  - 17 : UDP,
  - 1 : ICMP.

IP : le datagramme

- Somme de contrôle de l'en-tête
  - Ce champ permet de détecter les erreurs survenant dans l'en-tête du datagramme, et par conséquent l'intégrité du datagramme.
  - Le total de contrôle d'IP porte sur l'en-tête du datagramme et non sur les données véhiculées. Lors du calcul, le champ HEADER CHECKSUM est supposé contenir la valeur 0
  - Checksum = CRC → cf transmission de l'info.

IP : le datagramme

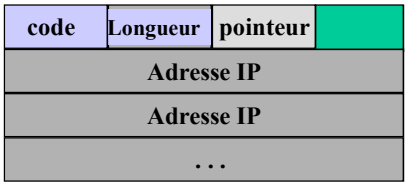
- OPTIONS
  - Le champ OPTIONS est facultatif et de longueur variable. Les options concernent essentiellement des fonctionnalités de mise au point. Une option est définie par un champ octet :



- copie (C) indique que l'option doit être recopiée dans tous les fragments (c=1) ou bien uniquement dans le premier fragment (c=0).
- les bits classe d'option et numéro d'option indiquent le type de l'option et une option particulière.

IP : le datagramme

- Enregistrement de route (classe = 0, option = 7) : permet à la source de créer une liste d'adresse IP vide et de demander à chaque passerelle d'ajouter son adresse dans la liste.



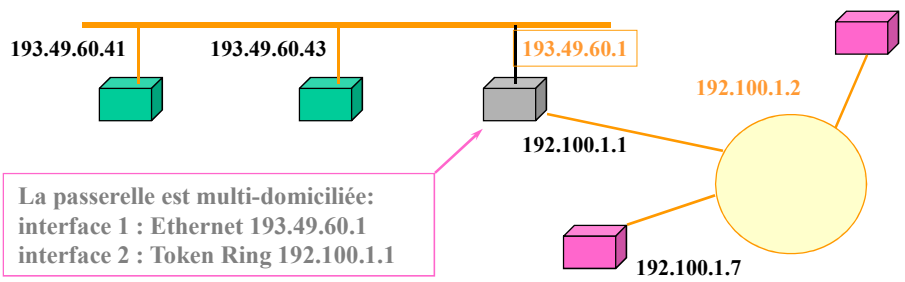
Routage 1ere approche : Routage direct VS indirect

- Le routage est le processus permettant à un datagramme d'être acheminé vers le destinataire lorsque celui-ci n'est pas sur le même réseau physique que l'émetteur.
- Le chemin parcouru est le résultat du processus de routage qui effectue les choix nécessaires afin d'acheminer le datagramme.
- Les routeurs forment une structure coopérative de telle manière qu'un datagramme transite de passerelle en passerelle jusqu'à ce que l'une d'entre elles le délivre à son destinataire. Un routeur possède deux ou plusieurs connexions réseaux tandis qu'une machine possède généralement qu'une seule connexion.
- **Machines et routeurs** participent au routage :
  - les machines doivent déterminer si le datagramme doit être délivré sur le réseau physique sur lequel elles sont connectées (routage direct) ou bien si le datagramme doit être acheminé vers une passerelle; dans ce cas (routage indirect), elle doit identifier la passerelle appropriée.
  - les passerelles effectuent le choix de routage vers d'autres passerelles afin d'acheminer le datagramme vers sa destination finale.

Routage 1ere approche : Routage direct VS indirect

Adresses et connexions

- Une adresse IP => une interface physique => une connexion réseau LAN
- A une machine, est associé un certain nombre N d'adresses IP. Si N > 1 la machine (ou passerelle) est multi-domiciliée ➔ appartient à plusieurs reseaux.

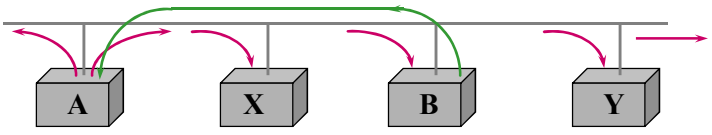


ARP : Address Resolution Protocol

- Le besoin
  - La communication entre machines ne peut s'effectuer qu'à travers l'interface physique
  - Les applicatifs ne connaissant que des adresses IP, comment établir le lien adresse IP / adresse physique?
- La solution : ARP
  - Mise en place dans TCP/IP d'un protocole de bas niveau appelé Adress Resolution Protocol (ARP)
  - Rôle de ARP : fournir à une machine donnée l'adresse physique d'une autre machine située sur le même réseau à partir de l'adresse IP de la machine destinatrice
- La technique :
  - Diffusion d'adresses sur le réseau physique
  - Les machines non concernées ne répondent pas
  - Gestion cache pour ne pas effectuer de requête ARP à chaque émission

ARP : Address Resolution Protocol

- L'association adresse physique - adresse IP de l'émetteur est incluse dans la requête ARP de manière à ce que les récepteurs enregistrent l'association dans leur propre mémoire cache



- Pour connaître l'adresse physique de B, PB, à partir de son adresse IP IB, la machine A diffuse une requête ARP qui contient l'adresse IB vers toutes les machines; la machine B répond avec un message ARP qui contient la paire (IB, PB).

RARP : Reverse Address Resolution Protocol

- Le besoin
  - L'adresse IP d'une machine est configurable (elle dépend du réseau sur lequel elle se trouve) et est souvent enregistrée sur la mémoire secondaire où le système d'exploitation l'accède au démarrage.
  - Ce fonctionnement usuel n'est plus possible dès lors que la machine est une station sans mémoire secondaire.
- Problème : déterminer un mécanisme permettant à la station d'obtenir son adresse IP depuis le réseau.
- La solution
  - Protocole de bas niveau appelé Reverse Adress Resolution Protocol
  - Permet d'obtenir son adresse IP à partir de l'adresse physique qui lui est associée.
- Fonctionnement

  Serveur RARP sur le réseau physique; son rôle: fournir les adresses IP associées aux adresses physiques des stations du réseau (BD).

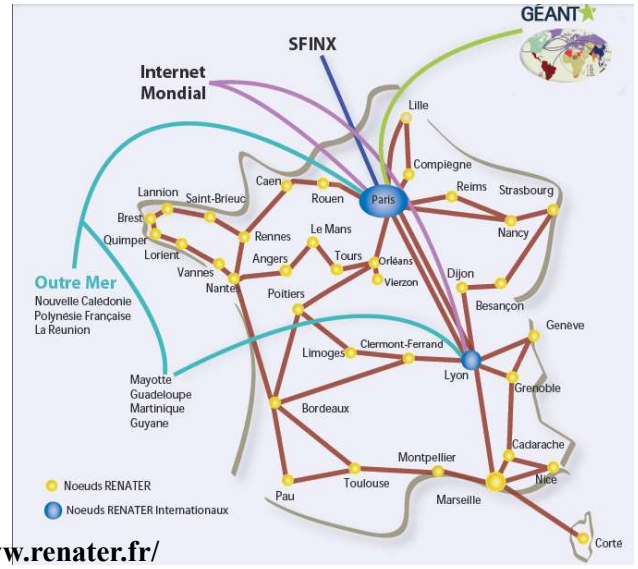
Introduction : Gestion du réseau

- ***Les organismes de coordination :***
  - L'ISOC : l'Internet Society : promotion, coordination des développements de l'Internet. Il coordonne :
    - L'IAB : l'Internet Architecture Board : coordination stratégique des développements techniques (à long terme) de l'Internet (recherche).
    - L'IETF : l'Internet Engineering Task Force, qui coordonne les développements techniques de l'Internet. Il produit, valide :
  - Les RFC (Request For Comment) sont les "standards" de l'Internet

Introduction : Gestion du réseau

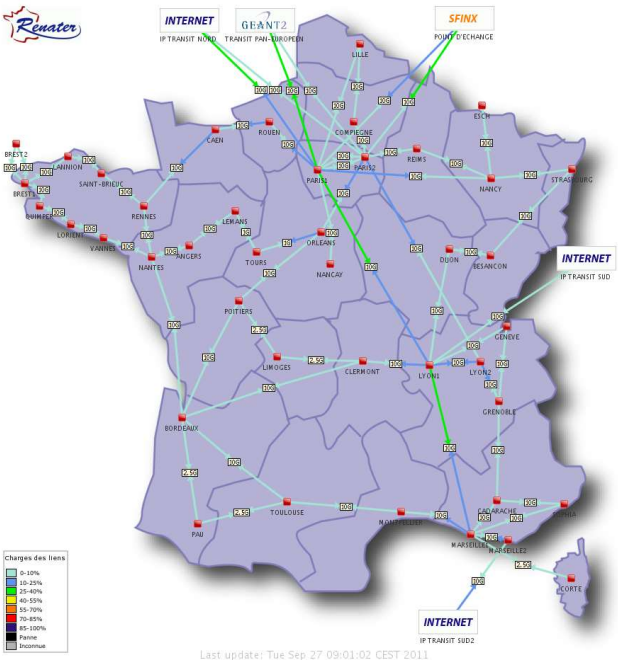
- ***Adresses IP et des noms de domaine :***
  - ICANN via IANA est l'organisme qui coordonne au niveau mondial les adresses IP , les ports et les noms de domaine
  - IP distribuées aux registres Internet régionaux (RIR) qui gèrent les ressources d'adressage IPv4 et IPv6 dans leur région
  - Les adresses IP sont gérées par l'ARIN pour l'Amérique et par l'APNIC pour la zone Asie - Pacifique.
  - RIPE : l'organisme qui attribue et gère les adresses IP pour l'Europe.
  - Le NIC France : la gestion des noms de domaines du "top-level domain" .fr, par l'association AFNIC.

Internet public en France 2010

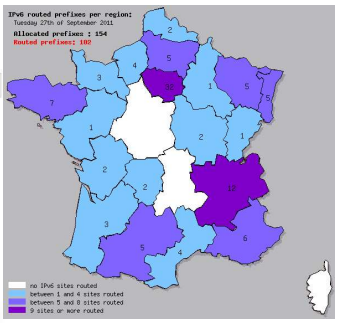


http://www.renater.fr/

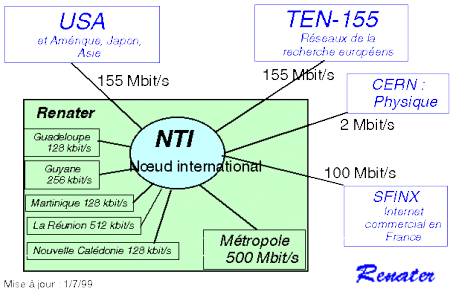
2010

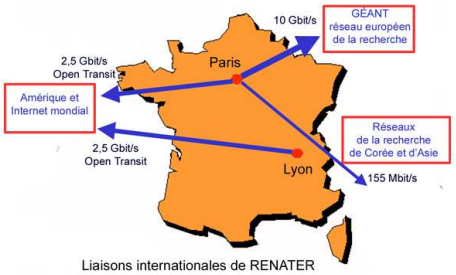


IPv6



Liaisons internationales





Liaisons internationales de RENATER

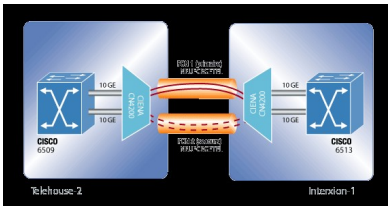
Autres NTI

Tarifs d'accès RENATER

Interface	Correspondance en terme de bande passante	Tarif en €/an HT jusqu'au 30/06/11	Tarif en €/an HT à partir du 01/07/2011
Ethernet (E)	jusqu'à 10 Mb/s	5674	5674
Fast Ethernet (FE)	Au delà de 10 Mb/s et jusqu'à 100 Mb/s	44 491	20 000
Giga Ethernet (GE)	Au delà de 100 Mb/s et jusqu'à 1 Gb/s	145 009	80 000
10 Giga Ethernet (10 GE)	Au delà de 1 Gb/s et jusqu'à 10 Gb/s	pas d'offre	320 000

L'internet Privé

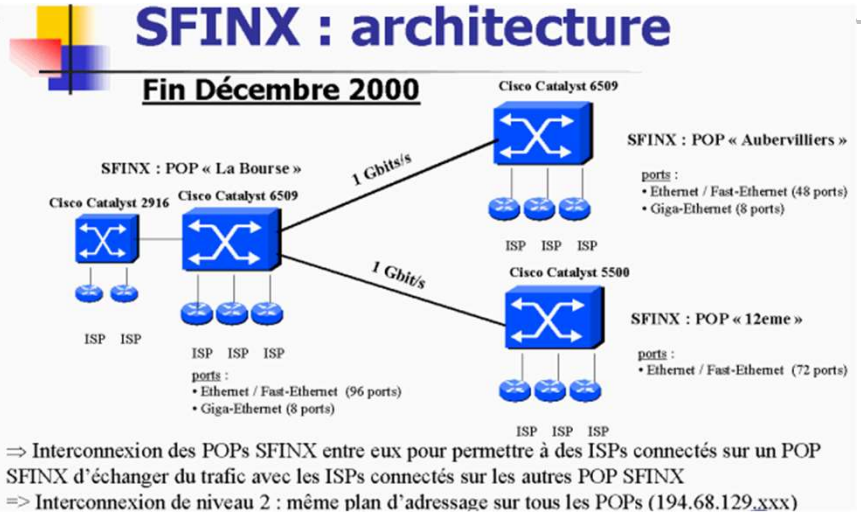
- Internet Exchange Point : Peering entre providers
- Accord point à point entre providers
- En France :
  - SFINX est un GIX (Global Internet eXchange point) ou IXP (Internet eXchange Point) géré par RENATER. Créé en 1995, au début de l'internet, le SFINX a été un des premiers IXP en France. Son objectif est d'optimiser le trafic internet en France, en toute **neutralité** par rapport aux acteurs du marché.
  - IX-France …



SFINX – Principes

- Les ISPs arrivent avec une ou plusieurs liaisons sur un routeur (qu'ils font héberger dans les baies du SFINX) et depuis ce routeur se raccordent sur le switch du SFINX (ports Ethernet/Fast-Ethernet/Giga-Ethernet).
- Les ISPs établissent ensuite des accords de peering (accords deux à deux) pour s'échanger du trafic de routeur à routeur via le switch (échange de tables de routage avec BGP4).

SFINX : architecture



⇒ Interconnexion des POPs SFINX entre eux pour permettre à des ISPs connectés sur un POP SFINX d'échanger du trafic avec les ISPs connectés sur les autres POP SFINX

=> Interconnexion de niveau 2 : même plan d'adressage sur tous les POPs (194.68.129.xxx)

SFINX : services

- **Accès 24/24-7/7 sur les POPs SFINX pour les personnes habilitées :** http://www.sfinx.tm.fr/Sfinx-Access-Procedures.html
- **Service hébergé** : offre « bring your box => routeurs (niveau 3 seulement, pas d'équipements de niveau 2) + modems (accès Out-of-Band).
- **Port Ethernet/Fast-Ethernet** sur le switch + une adresse ip fournie pour le peering avec les autres ISPs
- **Service de DNS secondaire** (via peering avec AFNIC)
- **Accès à la mailing-list du SFINX** (hosted-sfinx@renater.fr, ou sfinx@renater.fr), seulement utilisée par Renater et les ISPs pour les échanges d'informations techniques (annonce de nouveaux numéros par exemple)

SFINX : services

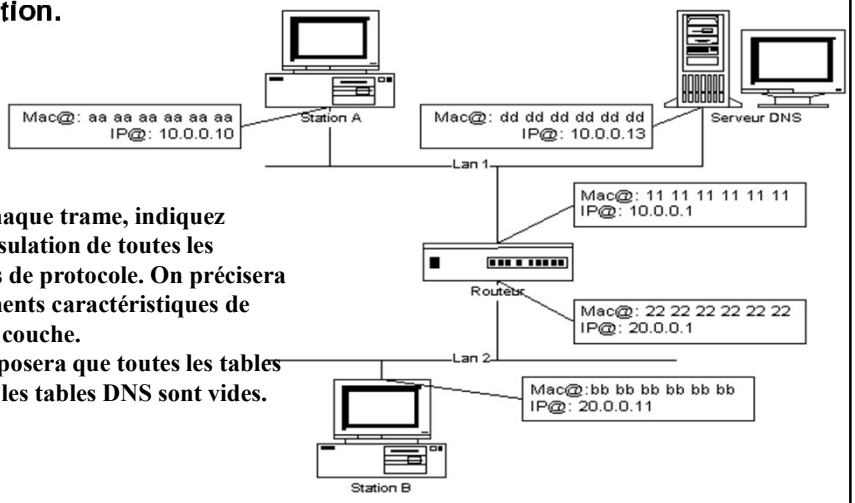
- **Statistiques** / par port / par ISP
- **Service de VLAN** (possibilité pour un ISP de dédier de la bande passante pour un peering ou un groupe de peering) + fonctionnalité « Ether-Channel »
- « **route reflector** » (une seule session BGP avec le « route reflector » et sélection des routes BGP par filtrage)
- « **route server** » : participation au projet européen du RIPE-NCC : RIS (Route Information Server) & RCC (Route Control Check)
- **Service NTP**
- **IPv6 peering** avec Renater
- **Ports supplémentaires**
- **Gigabit Ethernet ports** (sauf sur SFINX 12eme)
- **Service Multicast** (RGMP et PIM/SM)

Exercice

- Ayant obtenu un PC de votre directeur de département, on vous attribue (pour sa connexion au réseau) le numéro IP : 193.49.8.98. et son masque de sous-réseau associé 255.255.255.192. Le logiciel de configuration IP vous signale que vous êtes sur le réseau local de numéro 193.49.8.64.
- ① A quelle classe appartient ce réseau ? Quel est le numéro de ce réseau. Expliquez.
- On vous précise aussi que votre numéro de Broadcast est 193.49.8.127. ② A quoi sert ce numéro ?
- Le serveur web du département a pour numéro IP : 193.49.8.171 sur le réseau numéro 193.49.8.128.
- On vous précise que, pour vous y connecter, vous devez fournir au logiciel de configuration, le numéro IP : 193.49.8.65.③ Expliquez.
- Le logiciel de configuration IP, vous demande également de préciser le numéro IP d'un Domain Name Server. ④ Peut on prédire son adresse IP ? Expliquez.

Exercice de IP aux trames

Sur le schéma ci-dessous, la station A veut tester la présence de la station B en lançant la commande : ping IPstationB
Indiquez les principales trames émises sur Lan1 lors de cette opération.



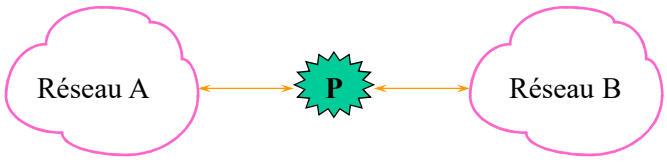
Pour chaque trame, indiquez l'encapsulation de toutes les couches de protocole. On précisera les éléments caractéristiques de chaque couche.
On supposera que toutes les tables ARP et les tables DNS sont vides.

Chapitre 5

INTERCONNEXION DE LANs

Concepts de l'interconnexion

- Certaines machines possèdent une connexion sur plusieurs réseaux:



Le noeud P interconnecte les réseaux A et B.

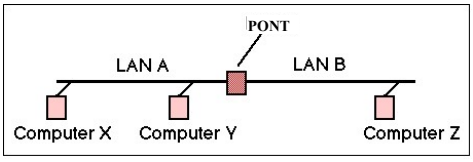
- Le rôle de P est de transférer sur le réseau B, les paquets circulant sur le réseau A et destinés au réseau B et inversement.
- Possible au niveau 2 ➔ Pont / switch

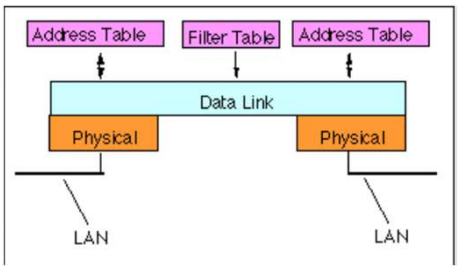
Concepts de l'interconnexion

- P1 transfère sur le réseau B, les paquets circulant sur le réseau A et destinés aux réseaux B et C
- P1 doit avoir connaissance de la topologie du réseau; à savoir que C est accessible depuis le réseau B.
- Difficile au niveau 2, donc déconseillé ➔ Routeur (Niv 3)

Interconnexion de niveau 2 : Les Ponts

- . Rôles de filtrage des trames
  - Couches 1 différentes.
  - Sous-couches 2 / MAC différentes.
  - Interconnection au niveau de la sous-couche 2 / LLC
  - Transparence à partir du niveau 3.
- **Commutateur :** Pont avec plusieurs entrée/sorties : les Ports





Les Ponts et Switchs

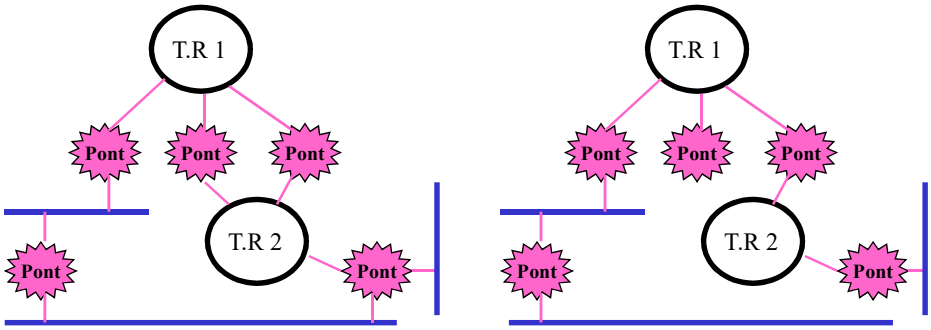
- fonctionnent aujourd'hui en "auto-apprentissage"
- découvrent automatiquement la topologie du réseau
- le pont/switch construit au fur et à mesure une table de correspondance entre adresses sources et segments sur lesquels les trames correspondantes sont acheminées.
- lorsque les ponts/switchs sont connectés pour la première fois, les tables de correspondance ne sont pas initialisées; les ponts utilisent l'algorithme d'inondation (retransmission sur tous les segments auxquels ils sont connectés) pour relayer la trame.
- un pont/switch examine toutes les trames des segments qui lui sont connectés; lorsqu'une trame arrive, le pont sait ainsi la relayer vers le segment approprié; un autre pont/switch éventuellement relayera à nouveau cette trame avant qu'elle ne parvienne à son destinataire.

Les Ponts et Switchs

- les ponts/switchs maintiennent l'heure d'arrivée (avec mise à jour continue) des trames dans les tables de correspondance; ceci permet d'invalider certaines entrées périmées et par conséquent permet de gérer l'arrêt ou le déplacement de stations dans le réseau
- les ponts/switch doivent laisser passer les messages de diffusion (broadcast, multicast)
- algorithme de fonctionnement
  - extraire l'adresse @ destination de la trame
  - si aucune entrée relative à @ dans la table de correspondance, reémettre la trame sur tous les segments (sauf le segment émetteur)
  - sinon acheminer la trame vers le segment identifié par l'entrée relative à @ dans la table de correspondance.

Gestion des boucles

- Le problème des boucles a été résolu par l'IEEE par la norme 802.1D en standardisant un algorithme connu sous le nom de « Spanning Tree Protocol» (STP).
- L'algorithme STP est basé sur la théorie des graphes et convertit la topologie physique en une topologie active en supprimant les boucles. Ceci garantit l'unicité du chemin entre deux noeuds; Exemple :



Gestion des boucles

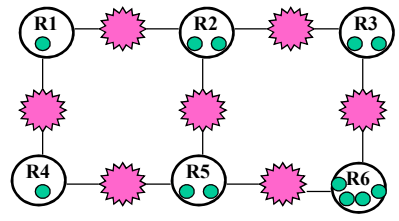
- Malgré l'élimination des problèmes de boucles le «Spanning Tree» apporte ses propres inconvénients :
  - la procédure complexe d'élimination des boucles induit un trafic non négligeable entre les ponts/switchs du réseau,
  - les chemins alternatifs ne sont plus accessibles,
  - le fonctionnement est inadapté aux interconnexions distantes car pas de gestion des coûts d'acheminement (métrique).
- En conclusion, les ponts/switchs constituent une solution acceptable pour les réseaux de petite et moyenne taille; au delà de cette limite, les coûts induits risquent d'être supérieurs à la mise en place d'une autre architecture de réseau.

Source Routing

- La méthode Source Routing (SR) :
  - Développé au départ par IBM pour interconnecter les réseaux Token Ring
  - la station détermine elle-même le chemin la reliant à son destinataire
  - la station utilise une trame « de découverte » (*discovery frame*) qu'elle émet sur le réseau
  - au fur et à mesure que la trame se propage dans le réseau, les noeuds indiquent dans le RIF (Routing Information Field), le numéro de l'anneau (Ring #) depuis lequel ils ont reçu le message ainsi que leur identifieur (numéro de noeud)
  - le noeud transmet alors, à son tour, le message sur toutes les connexions qui lui sont adjacentes à l'exception de celle à partir de laquelle, il a reçu le message
  - ce procédé utilise la technique d'inondation et plusieurs messages finaux peuvent arriver vers la destination, selon la topologie utilisée.

Source Routing

- **La structure du champ RIF impose les limitations suivantes :**
  - 16 noeuds maximum
  - La technique de l'inondation peut engendrer, un trafic important jusqu'à saturation du réseau.
  - Une station de l'anneau R1 désire communiquer avec une station de l'anneau R6 :



Copie de la trame All-route Broadcast

La trame initiale est copiée 12 fois

R6 reçoit les 4 routes suivantes :
- **R1-R2-R3-R6**
- **R1-R4-R5-R6**
- **R1-R2-R5-R6**
- **R1-R4-R5-R2-R3-R6**

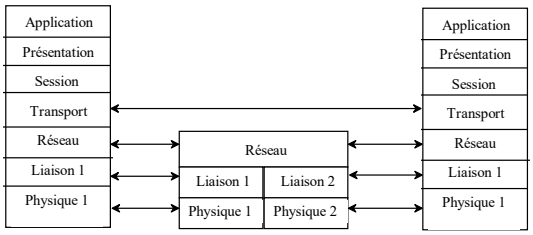
R6 répond pour chaque trame en sens inverse
==> 24 trames pour que R1 détermine le chemin pour aller à R6
Devient drastique avec un grand nombre de stations (surtout après un reboot général)

Source Routing

- Avantages du Source Routing :
  - permet d'utiliser des chemins redondants avec possibilités de boucles
  - garantit une certaine tolérance aux pannes du réseau
  - les informations de « routage » contenues dans les trames d'information peuvent être exploitées à des fins statistiques ou de surveillance
- Inconvénients du Source Routing :
  - incompatibilité avec les réseaux Ethernet
  - limite de traversée à 7 ponts
  - surplus de trafic important sur les réseaux
  - surplus de traitement au niveau des stations

Interconnexion de niveau 3

- Par **les routeurs** (notion de passerelle par défaut)
- Gestion de l 'Interconnexion au niveau des couches **réseaux**
- Transparence pour les niveaux supérieurs
- 3 travaux :
  - Gestion des tables de routage
  - Recherche chemin optimal
  - **Reformatage des paquets avant retransmission**
- 2 critères de selection :
  - Délais de latence
  - Nombres de paquets/s



Interconnexion de niveau 3 : Routeur

- Aujourd'hui grosse concurrence des commutateurs (pour la segmentation)
- Les routeurs sont très employés dans les réseaux publics
- Gros routeurs : 15 000Euros/ports à 100Mb/s
- Petits routeurs (PME) : 300 Euros pour 10 ports (ethernet) + RNIS ou ADSL

On les retrouvent à la périphérie : Non plus pour diviser les grands réseaux

Ou lorsque les protocoles sont différents (Gateway)

Plus performants et moins chers

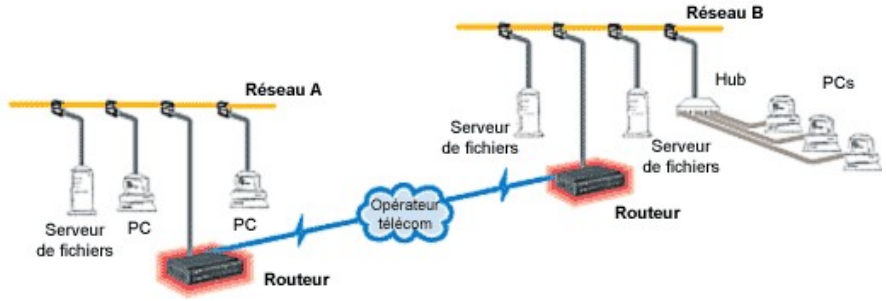
	Ancien routeur	Commutateur couche 3
Protocoles IP, IPX, Appletalk	oui	oui
Méthode de transfert	logicielle	matérielle
Taux de transfert	faible < –1 million de paquets/s	bon > 1 million de paquets/s
Accès distant	oui	non
Support de sonde RMON	non	oui
Prix	± 50 000 F	± 5 000 F

Les Routeurs

- Equipement complexe comprenant les couches de protocoles de niveau physique, liaison et réseau
- Souvent équipement dédié (CISCO, TRT-EXPERTdata, ...)
- Parfois ordinateur (SUN, PC, etc)
- Supporte toute topologie (y compris boucles et liens redondants)
- Comprend des tables de routage construites soit manuellement, soit dynamiquement par l'intermédiaire de protocoles spécialisés
- Filtre : ne laisse pas passer les collisions, les messages de diffusion
- N'examine pas tous les paquets des sous-réseaux qui lui sont connectés (filtrés au niveau 2)

Les Routeurs

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



Notion de passerelle par défaut – default gateway
Passerelle VS Modèle OSI (à illustrer ici)

Les Routeurs coupe-feux

- Routeurs aux fonctionnalités étendues et offrant une sécurité accrue
- Placés en front d'accès extérieur pour protéger le(s) réseau(x) interne(s);
  - Mise en oeuvre des fonctionnalités étendues entre la couche liaison ethernet et la couche réseau IP par **filtrage au niveau trame ethernet**
  - **Vérification du respect des règles de sécurité** (définies par l'administrateur) autorisent le transfert du paquet vers le destinataire
  - **Filtrage des services (ports)** internet (ftp et autres services …)
  - Prévention contre les chevaux de Troie ou virus par **analyse des contenus** ftp, E-mail, http, …
  - Filtrage des paquets **UDP et TCP** contre les accès non autorisés,
  - Vérification et **enregistrement** de toutes les communications
  - **Redirection** / modification des paquets
- Logiciel spécialisé (Exemple: IPtable)
- Cf DI5

Services offerts par le niveau 3

- **Routage :** acheminement optimisé des paquets entre stations non nécessairement directement interconnectées
- **Adressage des machines**
- **Contrôle de flux** : gestion des **congestions**, fragmentation /groupage
- Négociation de **Qualité de services :** fonction très importante dans les réseaux grandes distances

Routage / Acheminement

- Le **routage** concerne l'ensemble des techniques permettant de **fixer l'itinéraire suivi par un message sur le réseau**.
- Pour déterminer le routage, il faut connaître
  - la topologie du réseau
  - d'autres paramètres caractérisant le coût.
- Le choix d'un chemin se fera donc sur un critère de **coût minimal**.
- Le calcul des **routes** fournit **la (les) table(s) de routage** qui sont transmises sur tous **les nœuds** (systèmes intermédiaires).
- Le problème majeur est celui de la prise en compte des modifications dues à des pannes.

Routage / Acheminement

- **2 grandes catégories d'algorithmes de routage :**
  - **fixes**
  - **adaptatifs**

- **a) Fixe-déterministe**
  - La fonction de coût est proportionnelle au nombre d'étapes (ou noeuds intermédiaires). Elle est donc uniquement fonction de la topologie.

  → détermination des chemins optimaux a priori.

  → dégradation très importante si le réseau subit une modification

- **b) Fixe avec alternative**
  - Fixe-déterministe avec mémorisation de quelques chemins sous-optimaux pour limiter les dégradations en cas de modifications du réseau ou surtout en cas de pannes.

Routage / Acheminement

- **c) Fixe par inondation**
  - chaque station retransmet le message reçu à tous ses voisins à l'exception du précédent.

  → Il faut bien sûr noter les références des messages transmis

  → ce principe induit une très grande sureté de fonctionnement

  → augmentation intempestive du trafic.

- **d) Adaptatif centralisé**
  - Un nœud central décide du plus court chemin

  → il doit avoir des informations sur le trafic en tout point du réseau.

  → il faut répondre très vite pour ne pas être sensible aux variations brutales de trafic.

- **f) Adaptatif distribué**
  - Chaque nœud reçoit des informations sur l'état global du réseau (de tous les autres nœuds) et recalcule sa propre table de routage. Problème d'incompatibilité entre les différentes solutions optimales.

Calcul du plus court chemin

- Il faut connaître la topologie et définir une **métrique** → fonction de coût = distance entre nœuds.

- 2 types de métriques :
- - les métriques de coût (coût de fonctionnement)
- - les métriques de performances (délais de transmission).

Calcul du plus court chemin

- Soit A la matrice de connexion telle que $a_{ij} = 1$ ssi il existe un chemin entre les noeuds i et j.
- Pour trouver tous les chemins de longueur ≥ 2, on multiplie la matrice par elle-même :
  $a^2_{ij} = \vee (a^1_{ik} \wedge a^1_{kj})$ où $\vee$ et $\wedge$ sont les opérateurs logiques "ou" et "et".
- Pour trouver les chemins de longueurs $\leq k$, il faut calculer $A^{(k)}$. Opération extensive : si $a^k_{ij} = 1$ alors $a^{k+1}_{ij} = 1$
- Les chemins de longueur exactement égal à k sont obtenus par soustraction de deux matrices successives $A^{(k)}$ et $A^{(k-1)}$.

- **Attention**, la matrice ne permet que de répondre à la question sur l'existence d'un chemin. Pour avoir le chemin, il faut garder une trace des calculs.

Calcul du plus court chemin avec fonction de coût

Balayage/Propagation (Dijktra)

- **Soient :**
  - **N_i le noeud courant, N_a le noeud départ, N_b le noeud arrivée.**
  - **d une distance ou coût**

- **Pour chaque noeud N_i, on détermine un couple (n_i , d_i) où n_i est le précédent sur le chemin le plus court (* si inconnu) et d_i la distance à N_a par le chemin le plus court connu.**
- **On note d_{ij} la distance entre deux noeuds N_i et N_j.**
- **On part de N_a et on propage pour tous les voisins le coût de chaque lien :**
  $N_a \rightarrow N_i$: (N_a, d_{ai})
- **Chaque noeud N_i compare le message reçu (n_k, d_k) avec son couple courant (n_i , d_i)**
  si $d_k < d_i$ alors (n_i , d_i) ← (n_k, d_k) ;
  émettre (N_i, $d_i + d_{ij}$) à tout voisin N_j ($N_j \neq n_k$) ;

- **On répète la procédure jusqu'à stabilisation**
- **Pour trouver un chemin (N_a, N_b), on part de N_b et on remonte vers N_a. Si on modifie N_b, il suffit de reparcourir le graphe en partant du nouveau noeud arrivée.**
- **Si N_a change, il faut tout refaire.**

L'évolution du routage

1. Routage par défaut

Arpanet : interconnexion de réseaux locaux -> Routage circulaire pour mettre en œuvre le routage par défaut.

R.L 2 vers R.L 1 ==> P2->P3->P1

Inefficacité du routage par défaut

2. Le Core System : système centralisé évitant le routage par défaut

- les passerelles internes au Core system connaissent la route pour atteindre n'importe quelle station (pas de route par défaut)
- Les passerelles externes routent par défaut vers le Core.
- Devient impossible à gérer quand le système est de taille importante

3. Autonomous system

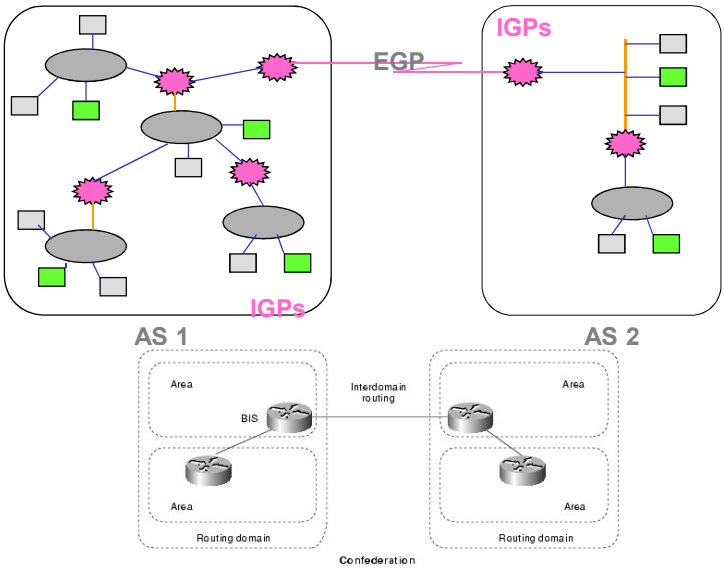
Autonomous System

- **Les limites imposées par le «Core» :**
  - impossibilité de connecter un nombre arbitraire de réseaux,
  - le core ne connaît qu'un seul réseau (local) par passerelle connectée
  - les tables de routage et le trafic associé deviennent gigantesques
  - quasi impossibilité de modifier les algorithmes de routage (base installée)
- **amenèrent le concept de «Système Autonome» (AS) :**
  - Domaine de routage (réseaux + routeurs) sous la responsabilité d'une autorité unique.
  - Architecture de routage indépendante des autres systèmes autonomes
  - correspond à un découpage de l'Internet.
  - Un AS est identifié par un numéro unique (16 Bits) attibué par le NIC.

Autonomous System

- La connexité implique que les routeurs d'un AS échangent les informations de routage:
  - le protocole de routage entre «external gateways» est appelé «Exterior Gateway Protocol» Exemple : EGP.
  - un routeur dans un AS est dit «internal gateway»
  - le protocole de routage à l'intérieur d'une AS est appelé «Interior gateway Protocol»; Exemple de IGP's: RIP, OSPF, IGRP.
- Les IGP's n'échangent que les tables de routage internes à l'AS, mais certains routeurs doivent d'autre part, dialoguer avec les «exterior gateways» pour découvrir les réseaux externes à l'AS.
- EGP (External Gateway Protocol) a pour fonction l'échange d'information sur la connectivité entre AS's. Cette information exprime un ensemble de réseaux connectés.

Autonomous System



Les algorithmes de routage

Deux classes d'algorithmes existent :
les algorithmes *Vector-Distance*
et les algorithmes *Link-State*.

- **Algorithmes Vector-Distance**
  - Un routeur diffuse régulièrement à ses voisins les routes qu'il connaît.
  - Une route est composée d'une adresse destination, d'une adresse de passerelle et d'une métrique indiquant le nombre de sauts nécessaires pour atteindre la destination.
  - Une passerelle qui reçoit ces informations compare les routes reçues avec ses propres routes connues et met à jour sa propre table de routage :
    - si une route reçue comprend un plus court chemin (nombre de prochains sauts +1 inférieur),
    - si une route reçue est inconnue.

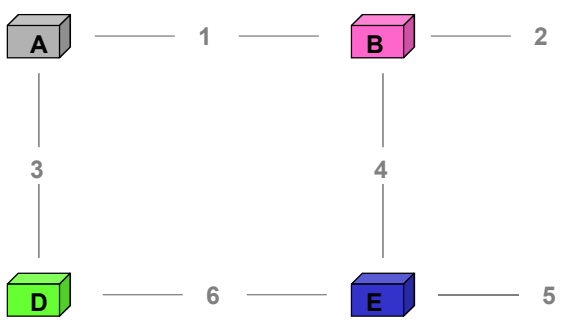
Algorithme V-D : Inconvénients

- La taille des informations de routage est proportionnelle au nombre de routeurs du domaine,
- Métrique difficilement utilisable : lenteur de convergence,
- Bouclage, éventuellement à l'infini,
- Pas de chemins multiples
- Coût des routes externes arbitraire.

Algorithme *Link State*

- Basés sur la technique *Shortest Path First (SPF)* :
  - les passerelles maintiennent une carte complète du réseau et calculent les meilleurs chemins localement en utilisant cette topologie.
  - les passerelles ne communiquent pas la liste de toutes les destinations connues (cf *Vector-Distance*),
  - une passerelle basée sur l'algorithme SPF, teste périodiquement l'état des liens qui la relient à ses routeurs voisins, puis diffuse périodiquement ces états (*Link-State*) à toutes les autres passerelles du domaine.
  - Les messages diffusés ne spécifient pas des routes mais simplement l'état (up, down) entre deux passerelles.
  - Lorsque un message parvient à une passerelle, celle-ci met à jour la carte de liens et recalcule localement pour chaque lien modifié, la nouvelle route selon l'algorithme de Dijkstra *shortest path algorithm* qui détermine le plus court chemin pour toutes les destinations à partir d'une même source.

Algorithme *Link State:* principes



De	à	L	D
A	B	1	1
A	D	3	1
B	A	1	1
B	C	2	1
B	E	4	1
C	B	2	1
C	E	5	1
D	A	3	1
D	E	6	1
E	B	4	1
E	C	5	1
E	D	6	1

Tous les noeuds ont la même base de donnée
==> pas de boucle.

Paquet de A vers C ==> calcule le + court chemin
et sélectionne B, qui calcule à son tour
le + court chemin vers C.

Algorithme *link state*

- Cohérence des bases
  - les copies de chaque nœud doivent être identiques aux périodes de transition près.
  - on améliore le processus en protégeant les bases contre les erreurs :
    - procédure d'inondation avec acquittement,
    - transmission des paquets sécurisés,
    - enregistrements de la base protégés par cheksum,
    - enregistrements de la base soumis à temporisation et supprimés si non rafraîchis à temps.
    - messages pouvant être authentifiés.
- Métriques multiples :
  - plus haut débit,
  - plus bas délai,
  - plus bas coût,
  - meilleure fiabilité.

Algorithme *Link State*

- Avantage des algorithmes Link State :
  - convergence rapide sans boucle,
  - possibilités de chemins multiples,
  - métriques précises et couvrant plusieurs besoins,
  - chaque passerelle calcule ses routes indépendamment des autres.

- En conclusion, les algorithmes SPF sont mieux adaptés au facteur d'échelle que les algorithmes *Vector-Distance.*

EGP : Protocole de routage extérieur

- EGP (*Exterior Gateway Protocol)* : RFC827

- utilisé pour échanger les informations de routage relatives au systèmes autonomes
- essentiel dans la connectivité Internet (Core, inter-provider , ...)
-
- EGP a trois fonctions principales :
  - support d'un mécanisme d'acquisition permettant à une passerelles de requérir, auprès d'une autre passerelles, qu'elles échangent leurs informations de routage
  - test continu de l'accessibilité des passerelles EGP voisines
  - échange de messages d'information de routage avec les passerelles EGP voisines.

EGP : les contraintes

- Conçu pour un réseau hiérarchique de type BackBone (exemple Arpanet/Nsfnet -> Réseaux régionaux ->campus)
  - Aujourd'hui le réseau est maillé et des boucles apparaissent
  - Les routes multiples ne sont pas prises en compte
- La distance est utilisée uniquement comme évaluation d'accessibilité
- Successeur d'EGP : BGP développé fin des années 80

RIP : Routing Information Protocol

- Protocole intérieur, RFC 1058. Berkeley made … jusqu'à RFC 2080
- Conçu à l'origine pour les réseaux locaux, étendu aux réseaux distants
- Peu performant, mais le plus employé au monde
- De type Vector/Distance - Différentes versions 1.0, 2.0, …, RIPng
- Fonctionne au dessus d'UDP/IP ; port 520
- Si une route n'est pas rafraîchie dans les 3 Mns la distance=infini
- Les informations de routage sont émises toutes les 30 secondes et indiquent pour un routeur donné, la liste des réseaux accessibles avec leur distance (*next hop*).

RIP : les contraintes

- Inconvénients des techniques Vector-Distance :
  - taille des informations de routage (proportionnelle au nombre de routeurs)
  - Métrique difficilement utilisable, limitée à 16
  - Bouclage, éventuellement à l'infini,
  - Pas de chemins multiples
- Amélioration apportée par les nouvelles versions :
  - Gestion de sous-réseaux et super-réseaux
  - utilisation de Multicast IP (224.0.0.9) au lieu de Broadcast IP
- Problèmes résiduels importants
  - Boucles,
  - Métriques non appropriées aux réseaux modernes
  - Pas de chemins multiples

OSPF : Open Shortest Path First

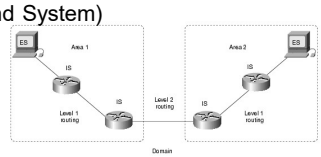
- Protocole *Link State* (RFC 1247 OSPF et 2740 OSPFv6) destiné à remplacer les protocoles intérieurs propriétaires et RIP.
- OSPF utilise la fonctionnalité "type de service" offerte par IP
  - permet d'installer plusieurs routes pour une même destination,
  - selon des critères différents (ex : délai court, débit important).
  - si plusieurs routes vers une même destination sont de coût équivalents, OSPF répartit la charge équitablement parmi ces routes.
- OSPF supporte l'adressage en sous-réseaux (subnets)
- Echanges entre routeurs authentifiés ==>intégrité des messages

OSPF : Fonctionnement

- Chaque routeur du système autonome où d'une area construit sa propre base d'information décrivant la topologie de l'AS complet ou bien de l'*area*.
- Au départ les routeurs utilisent des message "Hello" pour découvrir leurs voisins; une "adjacence" est formée lorsque deux routeurs communiquent pour échanger des informations de routage.
- L'information élémentaire échangée entre routeurs décrit l'état (*link state*) des adjacences; cette information est fournie par un routeur donné puis propagée dans l'*area* ou l'AS.
- A partir de sa base d'information (collection d'états des routeurs), chaque routeur construit un arbre du plus court chemin (*SPF tree*) dont il est la racine.
- Cet arbre indique toutes les routes pour toutes les destinations du système autonome, plus les destinations extérieures.

Conclusion sur le routage

- **Les principaux algorithmes :**
  - 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
- Autres, pour lien entre systèmes autonomes : GGP (gateway gateway Protocol) , EGP , BGP
  - **Routage et ISO : Dual IS-IS-ES** (Intermediate/End System)
  - Interdomain Routing Protocol (IDRP)



- **Quelques règles :**
  - Unn routage ne doit pas être hyper-sensible à la moindre panne → **Routage adaptatif**
  - Il faut minimiser les modifications car cela induit une augmentation artificielle du trafic et un risque d'incohérences temporaires (risque de perte de messages). Les états transitoires sont très importants : **congestion**
  - Interconnexion de LAN industriels → routage fixe-déterministe (simulation a priori → méthode fixe)

Chapitre 6

TCP/IP & ATM
Les standards actuels de l'interconnexion ?

Commençons par IP

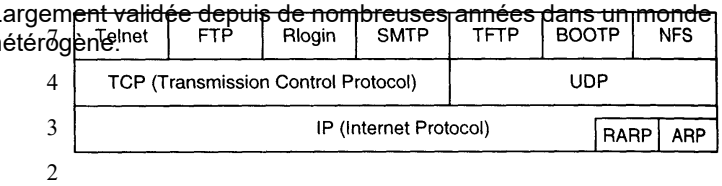
IP : Tout le monde connait…
Non ?

La philosophie initiale TCP/IP

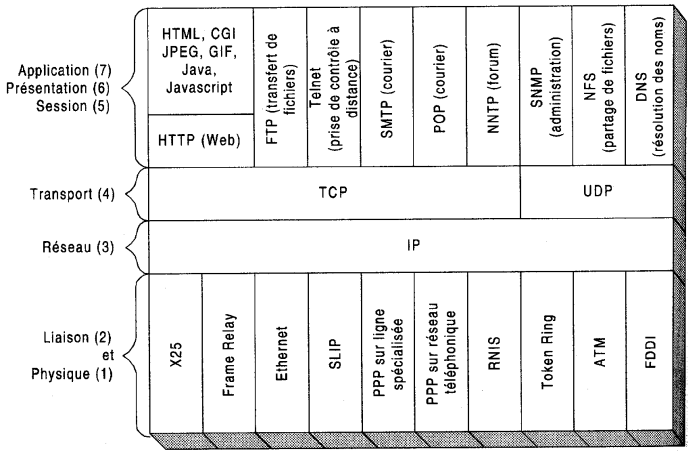
- TCP/IP : but = interconnexion de réseaux sur une base planétaire
- Aujourd'hui : 100000 réseaux interconnectés, plusieurs millions de machines, plusieurs dizaines de millions d'utilisateurs de "l'Internet".
- Interconnecte divers réseaux : Ethernet, T.R., X25, FR, FDDI, etc.
- La technologie est constituée par des protocoles de base (suite TCP/IP) qui offrent les services de base du transfert des données :
- Transport de datagrammes : service élémentaire du routage de paquets.
- Transport de messages sécurisés (TCP) : service orienté connexion permettant d'acheminer des données en garantissant leur intégrité
- Ces services de base sont indépendants du support de

La philosophie initiale TCP/IP

- Interconnexion universelle : les machines ont une adresse unique sur l'Internet. Deux machines reliées au réseau, communiquent grâce aux autres nœuds du réseau qui routent de manière coopérative sur la base de l'adresse destinataire.
- Interconnexion d'égal à égal (peer to peer systems) : il n'y a pas de machines prioritaires (en opposition à une structure hiérarchique).
- Dans le cadre du transport sécurisé, les acquittements sont effectués entre les systèmes finaux (source et destinataire) plutôt que continuellement entre chaque noeud relayant les messages.
- Technologie publique et largement diffusée au travers de RFC's.
- Indépendante des constructeurs et disponible sur tous types de matériel
- Largement validée depuis de nombreuses années dans un monde hétérogène.



Concepts de l'internet / Notion d'Intranet



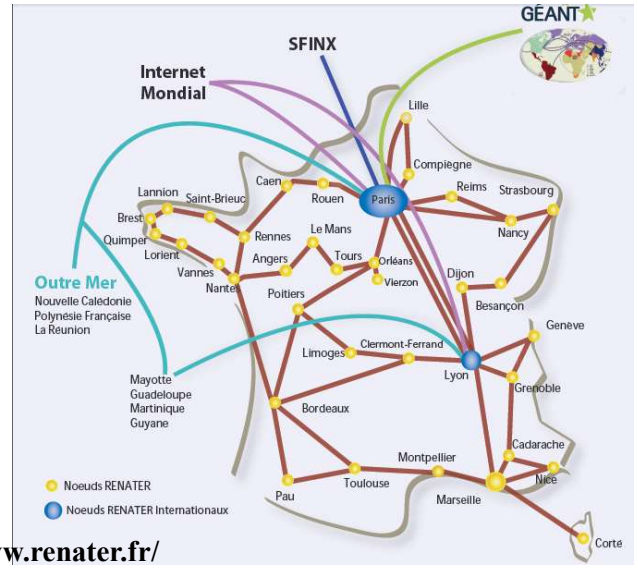
Introduction : Gestion du réseau

- ***Les organismes de coordination :***
  - L'ISOC : l'Internet Society : promotion, coordination des développements de l'Internet. Il coordonne :
    - L'IAB : l'Internet Architecture Board : coordination stratégique des développements techniques (à long terme) de l'Internet (recherche).
    - L'IETF : l'Internet Engineering Task Force, qui coordonne les développements techniques de l'Internet. Il produit, valide :
  - Les RFC (Request For Comment) sont les "standards" de l'Internet

Introduction : Gestion du réseau

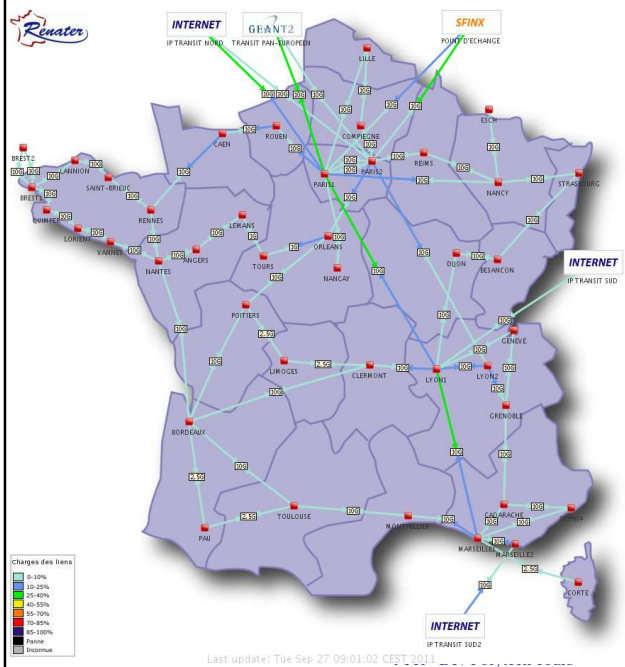
- ***Adresses IP et des noms de domaine :***
  - ICANN via IANA est l'organisme qui coordonne au niveau mondial les adresses IP , les ports et les noms de domaine
  - IP distribuées aux registres Internet régionaux (RIR) qui gèrent les ressources d'adressage IPv4 et IPv6 dans leur région
  - Les adresses IP sont gérées par l'ARIN pour l'Amérique et par l'APNIC pour la zone Asie - Pacifique.
  - RIPE : l'organisme qui attribue et gère les adresses IP pour l'Europe.
  - Le NIC France : la gestion des noms de domaines du "top-level domain" .fr, par l'association AFNIC.

Internet public en France 2010

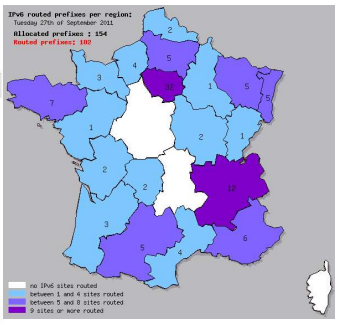


http://www.renater.fr/

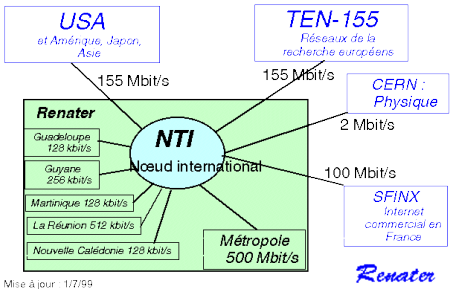
2010

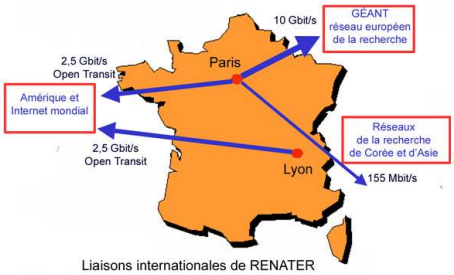


IPv6



Liaisons internationales





Liaisons internationales de RENATER

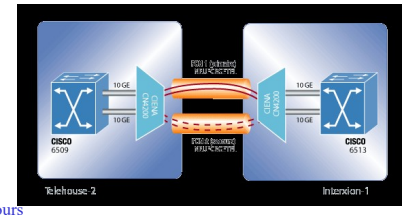
Autres NTI

Tarifs d'accès RENATER

Interface	Correspondance en terme de bande passante	Tarif en €/an HT jusqu'au 30/06/11	Tarif en €/an HT à partir du 01/07/2011
Ethernet (E)	jusqu'à 10 Mb/s	5674	5674
Fast Ethernet (FE)	Au delà de 10 Mb/s et jusqu'à 100 Mb/s	44 491	20 000
Giga Ethernet (GE)	Au delà de 100 Mb/s et jusqu'à 1 Gb/s	145 009	80 000
10 Giga Ethernet (10 GE)	Au delà de 1 Gb/s et jusqu'à 10 Gb/s	pas d'offre	320 000

L'internet Privé

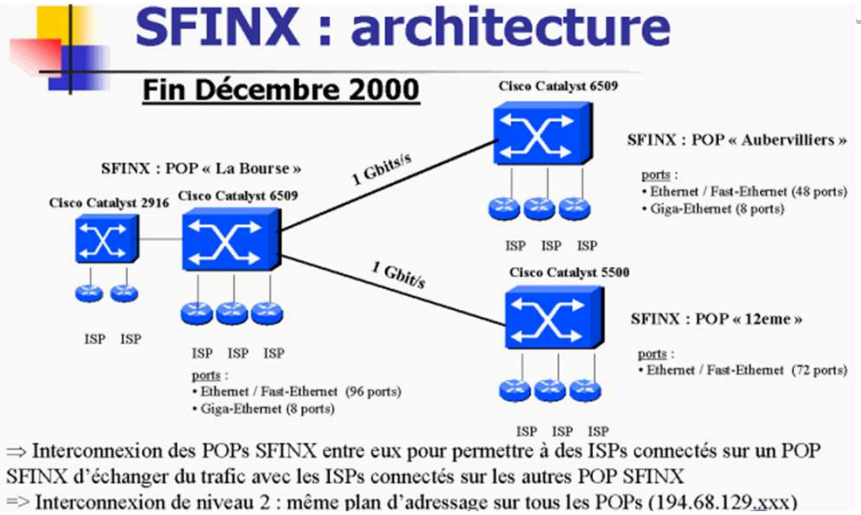
- Internet Exchange Point : Peering entre providers
- Accord point à point entre providers
- En France :
  - SFINX est un GIX (Global Internet eXchange point) ou IXP (Internet eXchange Point) géré par RENATER. Créé en 1995, au début de l'internet, le SFINX a été un des premiers IXP en France. Son objectif est d'optimiser le trafic internet en France, en toute **neutralité** par rapport aux acteurs du marché.
  - IX-France …



SFINX – Principes

- Les ISPs arrivent avec une ou plusieurs liaisons sur un routeur (qu'ils font héberger dans les baies du SFINX) et depuis ce routeur se raccordent sur le switch du SFINX (ports Ethernet/Fast-Ethernet/Giga-Ethernet).
- Les ISPs établissent ensuite des accords de peering (accords deux à deux) pour s'échanger du trafic de routeur à routeur via le switch (échange de tables de routage avec BGP4).

SFINX : architecture



⇒ Interconnexion des POPs SFINX entre eux pour permettre à des ISPs connectés sur un POP SFINX d'échanger du trafic avec les ISPs connectés sur les autres POP SFINX

=> Interconnexion de niveau 2 : même plan d'adressage sur tous les POPs (194.68.129.xxx)

SFINX : services

- **Accès 24/24-7/7 sur les POPs SFINX pour les personnes habilitées :** http://www.sfinx.tm.fr/Sfinx-Access-Procedures.html
- **Service hébergé** : offre « bring your box => routeurs (niveau 3 seulement, pas d'équipements de niveau 2) + modems (accès Out-of-Band).
- **Port Ethernet/Fast-Ethernet** sur le switch + une adresse ip fournie pour le peering avec les autres ISPs
- **Service de DNS secondaire** (via peering avec AFNIC)
- **Accès à la mailing-list du SFINX** (hosted-sfinx@renater.fr, ou sfinx@renater.fr), seulement utilisée par Renater et les ISPs pour les échanges d'informations techniques (annonce de nouveaux numéros par exemple)

SFINX : services

- **Statistiques** / par port / par ISP
- **Service de VLAN** (possibilité pour un ISP de dédier de la bande passante pour un peering ou un groupe de peering) + fonctionnalité « Ether-Channel »
- « **route reflector** » (une seule session BGP avec le « route reflector » et sélection des routes BGP par filtrage)
- « **route server** » : participation au projet européen du RIPE-NCC : RIS (Route Information Server) & RCC (Route Control Check)
- **Service NTP**
- **IPv6 peering** avec Renater
- **Ports supplémentaires**
- **Gigabit Ethernet ports** (sauf sur SFINX 12eme)
- **Service Multicast** (RGMP et PIM/SM)

L'adressage IP

- But : fournir un service de communication universel permettant à toute machine de communiquer avec toute autre machine de l'interconnexion
- Une machine doit être accessible aussi bien par des humains que par d'autres machines
- Une machine doit pouvoir être identifiée par :
  - un nom (mnémotechnique pour les utilisateurs),
  - une adresse qui doit être un identificateur universel de la machine,
  - une route précisant comment la machine peut être atteinte.

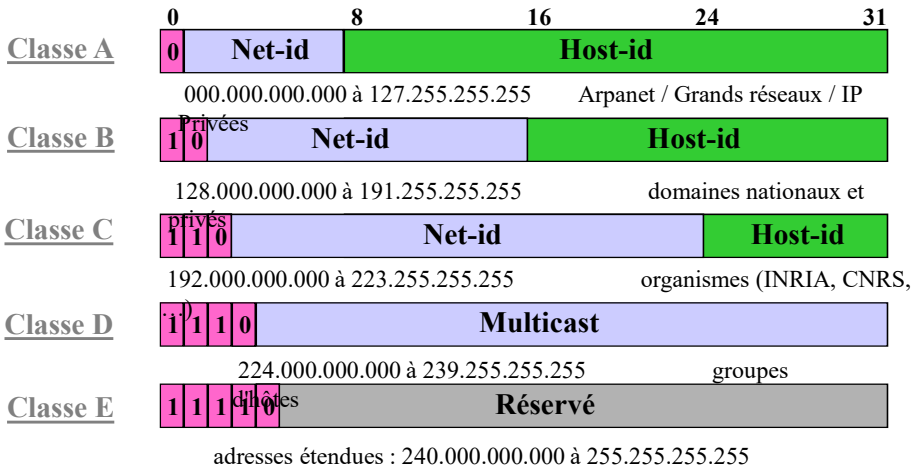
Adressage Internet

- **Ne mélangeons pas tous :**
  - numéro IPv4 et IPv6
  - adresse FQDN
  - adresse URL

Toujours l'adressage IPv4

- Solution 1 : adressage binaire compact assurant un routage efficace
- Adressage "à plat" par opposition à un adressage hiérarchisé permettant la mise en oeuvre de l'interconnexion d'égal à égal
- Utilisation de noms pour identifier des machines (réalisée à un autre niveau que les protocoles de base)
- Les classes d'adressage
  - Une adresse = 32 bits dite "internet address" ou "IP address" constituée d'une paire (netid, hostid) où netid identifie un réseau et hostid identifie une machine sur ce réseau.
  - Cette paire a été structurée de manière à définir cinq classes d'adresse (au départ)

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

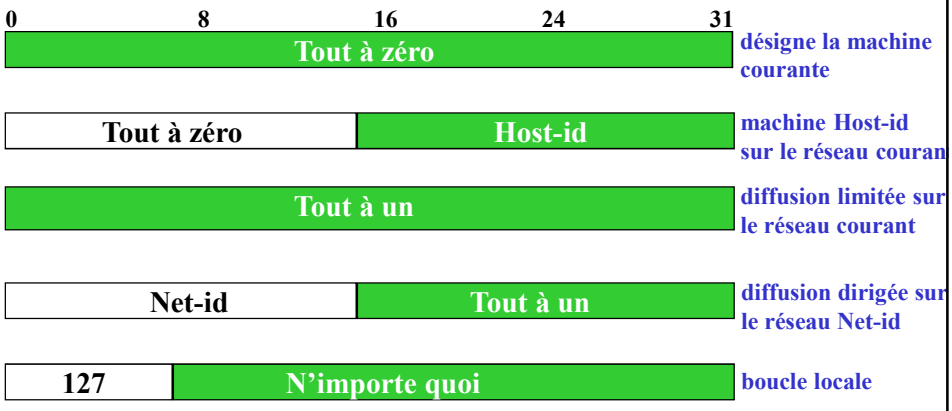
- Adresses particulières
  - Adresses réseau : adresse IP dont la partie hostid ne comprend que des zéros; => la valeur zéro ne peut être attribuée à une machine réelle : 191.20.0.0 désigne le réseau de classe B 191.20.
  - Adresse machine locale : adresse IP dont le champ réseau (netid) ne contient que des zéros;
  - **Adresses IP privée : 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

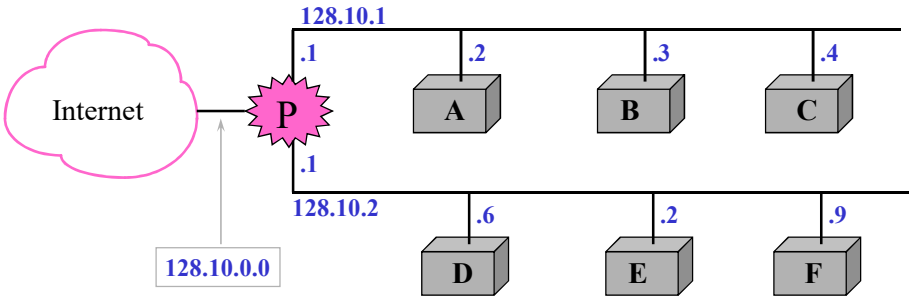


Le sous-adressage

- Le sous-adressage est une extension du plan d'adressage initial
- Devant la croissance du nombre de réseaux de l'Internet, il a été introduit afin de limiter la consommation d'adresses IP qui permet également de diminuer :
  - la gestion administrative des adresses IP,
  - la taille des tables de routage des passerelles,
  - la taille des informations de routage,
  - le traitement effectué au niveau des passerelles.

Le sous-adressage

Les sous-réseaux 128.10.1.0 et 128.10.2.0 sont notés seulement avec le NetId, les machines seulement avec le Hostid ; exemple IP(F) = 128.10.2.9



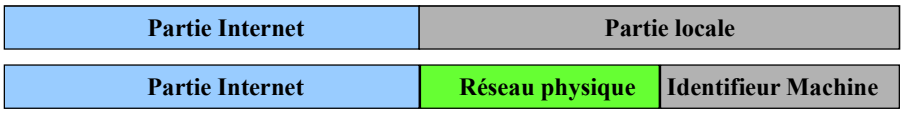
Un site avec deux réseaux physiques utilisant le sous-adressage de manière à ce que ses deux sous-réseaux soient couverts par une seule adresse IP de classe B.
La passerelle P accepte tout le trafic destiné au réseau 128.10.0.0 et sélectionne le sous-réseau en fonction du troisième octet de l'adresse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

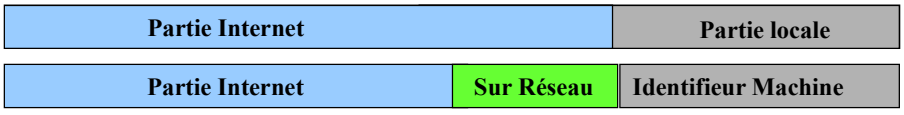
- Conceptuellement, la partie locale dans le plan d'adressage initial est subdivisée en "partie réseau physique" + "identification de machine (hostid) sur ce sous-réseau" :



- «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**
- la RFC 1860 (remplacée par la RFC 1878) stipulait qu'un numéro de sous réseau ne peut être composé de bits tous positionnés à zéro ou tous positionnés à un.

Et pourquoi pas du sur-adressage (RFC 1517-1520)

- Idem sous adressage mais sur la partie Net id
  → On concatène des réseaux (de classes C souvent)



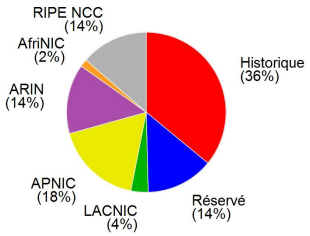
- «Partie Internet» correspond au NetId (plan d'adressage initial)
- «Partie locale» correspond au hostid (plan d'adressage initial)
- les champs «Sur-reseau» est toujours de taille faible. Il permet d'ignorer les derniers bit de la partie Net-Id
- PB pour le routage mais OK pour RIPv2, OSPF, BGPv4

Classless Inter-Domain Routing (CIDR)

- **RFC 1338 : Abolition de la notion de classe**
  - Afin de diminuer la taille de la table de routage
  - La totalité de l'espace d'adressage unicast est gérée comme une collection unique de sous-réseaux indépendamment de la notion de classe
  - Les Protocoles de routage compatibles avec CIDR sont dits classless (BGPv4, OSPF, EIGRP ou RIPv2

Adresse IP = Prefixe + Suffixe
Prefixe / Masque

→ 192.33.11.0 / 22



Bloc	Usage	Référence
0.0.0.0/8	*Adresse réseau par défaut*	RFC 1700
10.0.0.0/8	Adresses privées	RFC 1918
127.0.0.0/8	adresse de bouclage (localhost)	RFC 1122
169.254.0.0/16	adresses locales autoconfigurées (APIPA)	RFC 3927
172.16.0.0/12	Adresses privées	RFC 1918
192.0.0.0/24	Réservé par l'IETF	RFC 5736
192.0.2.0/24	Réseau de test TEST-NET-1	RFC 5737
192.88.99.0/24	6to4 anycast	RFC 3068
192.168.0.0/16	Adresses privées	RFC 1918
198.18.0.0/15	Tests de performance	RFC 2544
198.51.100.0/24	Réseau de test TEST-NET-2	RFC 5737
203.0.113.0/24	Réseau de test TEST-NET-3	RFC 5737
224.0.0.0/4	Multicast	RFC 5771
240.0.0.0/4	Réservé à un usage ultérieur non précisé	RFC 1112
255.255.255.255/32	broadcast limité	RFC 919

L'adressage IP : de IPv4 à IPv6

- Les adresses IPv6 **(128 bits)** peuvent être de 4 types :
  - Unicast
  - Multicast
  - Broadcast
  - Anycast : nouveau type d'adressage. Il identifie qu'un noeud, parmi un groupe de noeuds, doit recevoir l'information. Une adresse anycast, comme une adresse multicast, désigne un groupe d'interfaces, à la différence qu'un paquet émis avec comme destinataire une adresse anycast ne sera remis qu'à un seul membre du groupe, par exemple le plus proche au sens de la métrique des protocoles de routage, même si plusieurs interfaces ont répondu au message. L'interface de destination doit spécifiquement être configurée pour savoir qu'elle est anycast.
  - Pour l'instant, une seule adresse anycast est utilisée, elle est réservée au routeur mais dans l'avenir, d'autres pourraient être définies.

Bientôt l'adressage IPv6

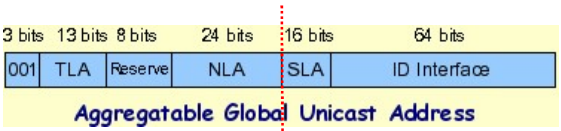
Les adresses unicast

- 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.
  - **Notation hexadécimale et :: remplace une suite de 0**
- Exemple : fe80::20d:61ff:fe22:3476
  - fe80:: en réalité fe80:0000:0000:0000 correspond au préfixe
  - 20d:61ff:fe22:3476 correspond au suffixe ou partie hôte (host)

Bientôt l'adressage IPv6

Les adresses unicast

- Adresse de boucle locale **::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. C'est une phase transitoire.
- Le préfixe d'une adresse de LAN (lien local) est **fe80::/10**
- Le préfixe d`1 adresse de site (Network) est **fec0::/10** → en cours d'abandon
- Mappage d'adresses IPv4 → ::ffff:147.30.20.10 et autres 6to4
- **Adressage global 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

Bientôt l'adressage IPv6

Les adresses multicast

- IPv6 généralise l'utilisation des adresses multicast qui remplacent les adresses de type "broadcast".
- un paquet broadcast était très pénalisant 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).

Continuons un peu avec IPv6 : 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

Adresses IP dynamiques

Pour pallier aux manques d'adresses IP :

- DHCP : Dynamic Host Configuration Protocol
- NAT : Network Address Translation

Dynamic Host Configuration Protocol

Le protocole DHCP sert à distribuer des adresses IP sur un réseau

- Il faut un serveur DHCP qui distribue des adr. IP.
- Le serveur doit avoir une adresse IP fixe.
- Complément au protocole BOOTP (Bootstrap Protocol = Installation d'une machine à travers un réseau).
- Un serveur DHCP peut renvoyer des paramètres BOOTP ou de configuration propres à un hôte donné

Fonctionnement du protocole DHCP :

- Le mécanisme de base de la communication est BOOTP (avec trame UDP).
- Pour trouver et dialoguer avec un serveur DHCP, la machine va simplement émettre un paquet spécial de broadcast (broadcast sur 255.255.255.255 avec d'autres informations comme le type de requête, les ports de connexion...) sur le réseau local.
- Lorsque le serveur DHCP recevra le paquet de broadcast, il renverra un autre paquet de broadcast contenant toutes les informations requises pour le client.

Dynamic Host Configuration Protocol

- **Il existe plusieurs types de paquets DHCP :**
  - DHCPDISCOVER (pour localiser les serveurs DHCP disponibles)
  - DHCPOFFER (réponse du serveur qui contient les premiers paramètres)
  - DHCPREQUEST (requête diverse du client pour par exemple prolonger son bail)
  - DHCPACK (réponse du serveur qui contient des paramètres et l'adr. IP du client)
  - DHCPNAK (le serveur signale au client que son bail est échu ou le client annonce une mauvaise configuration réseau)
  - DHCPDECLINE (le client annonce au serveur que l'adresse est déjà utilisée)
  - DHCPRELEASE (le client libère son adresse IP)
  - DHCPINFORM (le client demande des paramètres locaux, il a déjà son adresse IP)

- **Notion de bail**

Network Address Translation - RFC 1918

Plan

Description du principe de NAT

Utiliser NAT pour :

- Connexion à l'Internet de hosts qui n'ont pas d'adresses IP globales uniques
- Effectuer une distribution de charge
- Améliorer la sécurité
- Simplifier la maintenance des serveurs (chgmt d'adresses)

Bilan

NAT : 1er aperçu

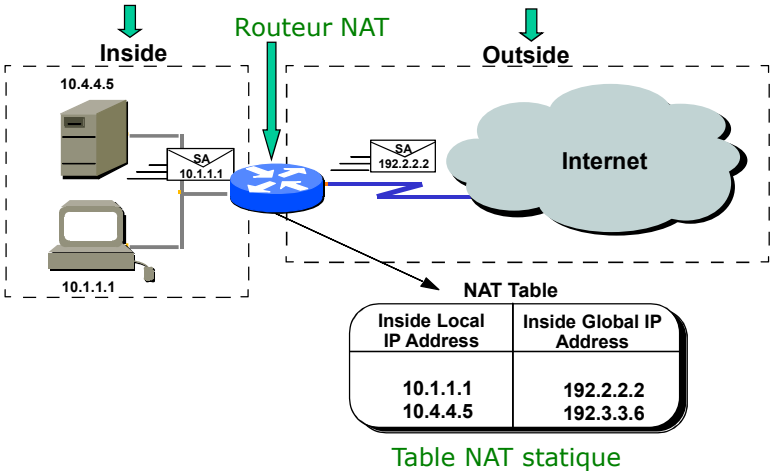
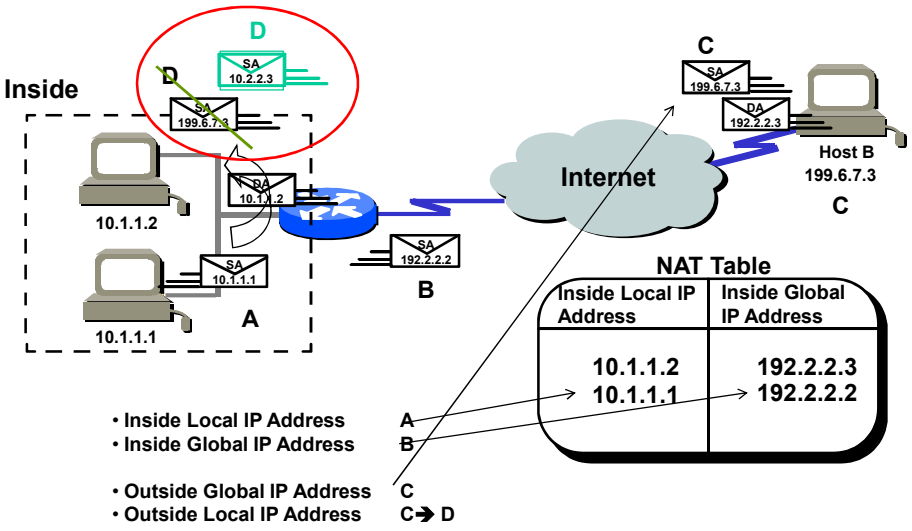


Table NAT statique

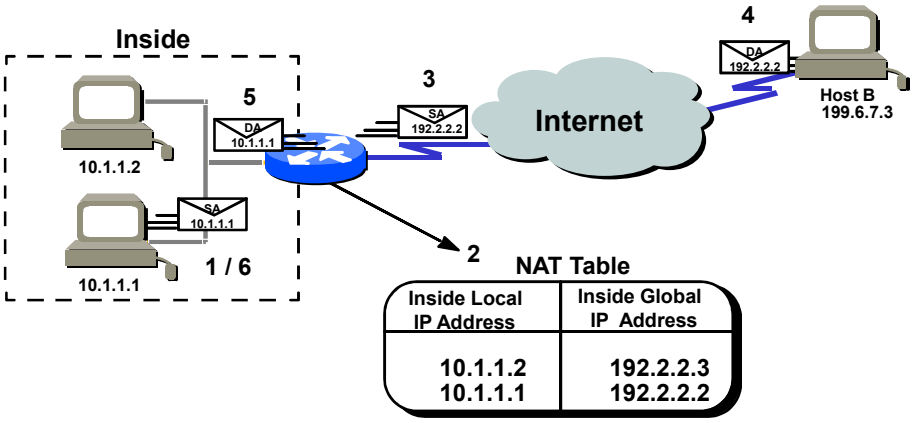
NAT : Inside vs Outside



- Inside Local IP Address — A
- Inside Global IP Address — B
- Outside Global IP Address — C
- Outside Local IP Address — C➔ D

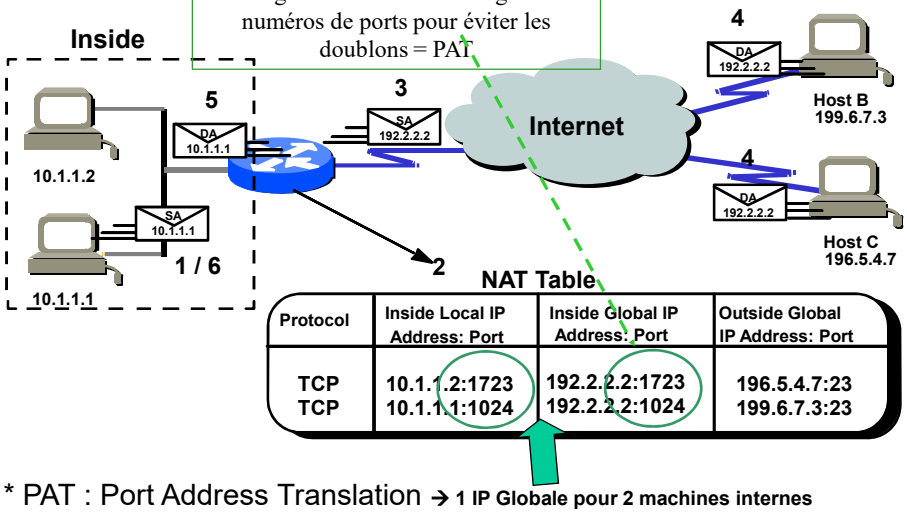
SNAT = NAT statique

Bijection (pour maintenance) ou Pool d'adresses globales à distribuer



DNAT = NAT Dynamique
Surcharge des adresses internes globales (overloading)

En général le routeur change les numéros de ports pour éviter les doublons = PAT

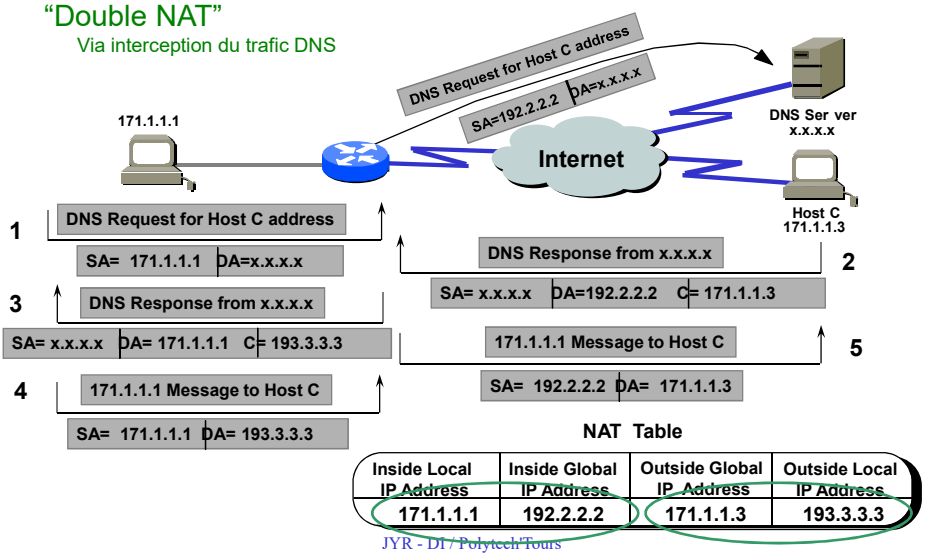


* PAT : Port Address Translation → **1 IP Globale pour 2 machines internes**

Traitement des réseaux qui se chevauchent (“overlapping”)

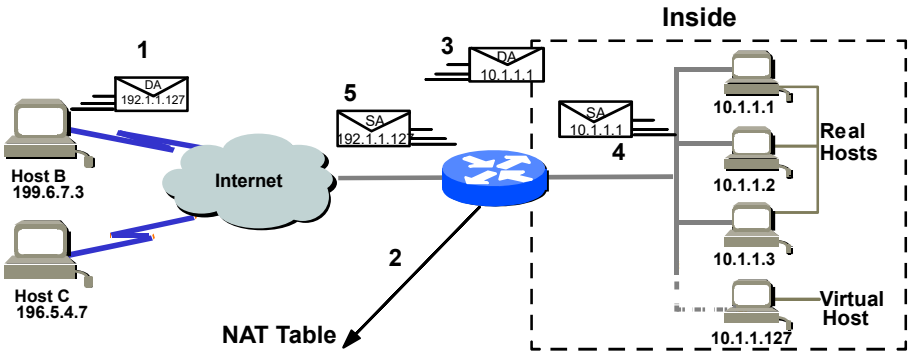
“Double NAT”

Via interception du trafic DNS



Inside Local IP Address	Inside Global IP Address	Outside Global IP Address	Outside Local IP Address
171.1.1.1	192.2.2.2	171.1.1.3	193.3.3.3

Distribution de charge TCP



Protocol	Inside Local IP Address: Port	Inside Global IP Address: Port	Outside Global IP Address: Port
TCP	10.1.1.1:23	192.1.1.127:23	199.6.7.3:3058
TCP	10.1.1.2:23	192.1.1.127:23	196.5.4.7:4371
TCP	10.1.1.3:23	192.1.1.127:23	199.6.7.3:3062

Quelques considérations

- **Port Fowarding** (1 port destination → 1 machine inside)
  - Tous 80 vers le serveur web (1 IP inside)
  - Tous 21 vers le serveur ftp (1 autre IP inside / machine)
- **Translation implique :**
  - modif des adresses IP et ports TCP, UDP
  - Recalcul et vérification du checksum IP
  - Recalcul et modification du checksum TCP
- **Transparence au niveau application uniquement !**
- **D'ou conversion de certains paquets**
  - FTP qui peut nécessiter une double connexion (21+20)
  - ICMP, SNMP, … qui n'utilisent pas de ports TCP UDP
- **Le routeurs NAT se rapprochent des Proxy applicatifs**

Quelques considérations

- La translation introduit plus ou moins de délais pendant la commutation
- NAT fait que certaines applications spécifiques qui utilisent les adresses IP fonctionnent difficilement ou sont impossibles à utiliser
- Ouverture de connexion depuis l'extérieur impossible
- NAT cache l'identité "réelle" des hosts
  - Pas de log → Perte de la traçabilité de bout-en-bout
- Tout paquet qui doit être translaté doit passer par le routeur NAT

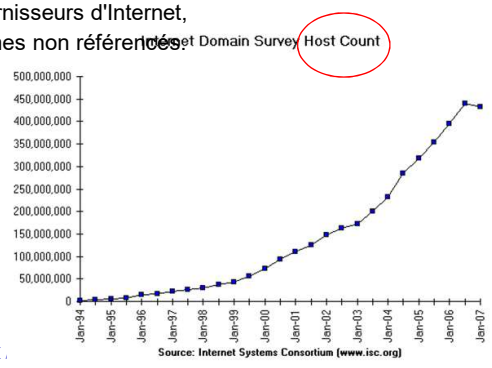
Quelques considérations

- Pas de gestion du Multicast
- Compatibilité avec DHCP
- Problématique du chiffrement (Niveau 3 et 4)
- NAT, outil de sécurité ?

Les adresses FQDN (Fully Qualified Domain Name)

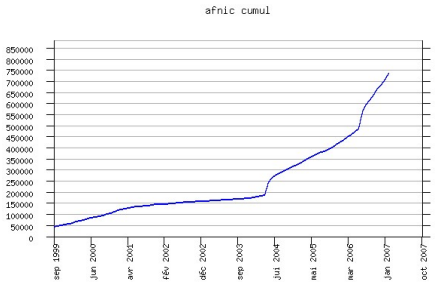
nom@**organisation.domaine**

- Les domaines sont regroupés en **grandes classes** (hiérarchie):
  - com : désigne les entreprises commerciales,
  - edu : désigne l'éducation,
  - gov : désigne les organismes gouvernementaux,
  - mil : désigne les organisations militaires,
  - net : désigne les organismes fournisseurs d'Internet,
  - org : désigne les autres organismes non référencés.
- Ils sont aussi regroupés en **pays** :
  - au : Australie,
  - ca : Canada,
  - fr : France,
  - uk : pour United Kingdom.



Les Noms de domaine

- Les noms de domaines doivent être uniques
- Ils sont attribués par des organismes centraux :
  - en France, on s 'adresse à un fournisseur d 'accès qui transmet :
    - à **l'association AFNIC** pour les .fr (charte de nommage .fr en annexe)
    - à **l 'InterNic** pour les autres : .cor



- Prix :
  - environ 30 Euros/an pour .fr en 2(
  - 30 Euros/an pour .com 2004
  - 5 Euros en 2007 (.fr = 700 000)
  - Aujourd'hui possible gratuitement

Noms de domaines

- **Nouveaux TLD :**
  - .info : sites d'information
  - .name : pour les particuliers
  - .biz : commerce
  - .aero : sociétés d'aéronautiques
  - .coop : coopératives
  - .museum : musées
  - .pro : professions libérales
  - **…**

Architecture : Des chiffres

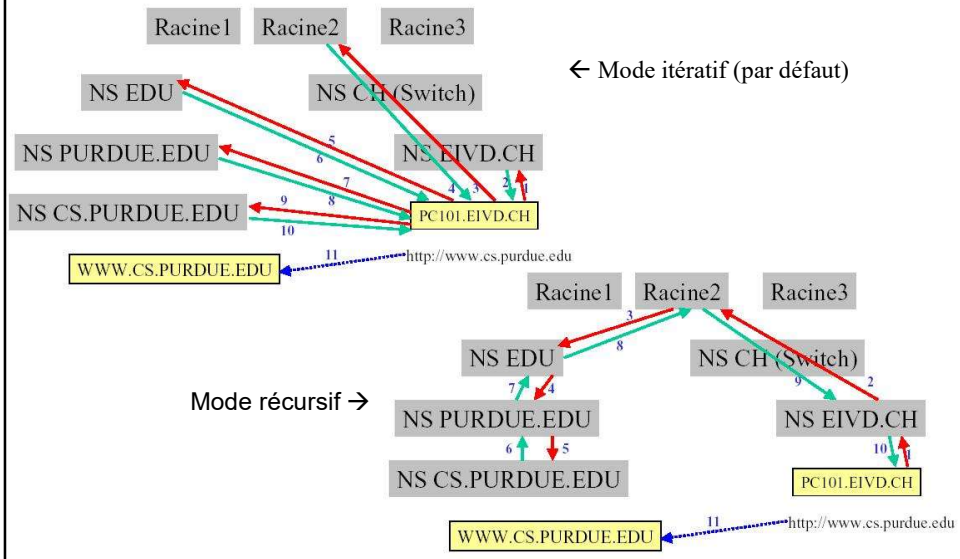
- Top DNS →

Extension	Octobre 2006	Février 2007	Progression d'octobre 2006 à février 2007
1.COM (Générique)	56 417 572	63 707 658	+13%
2.DE (Allemagne)	10 115 290	10 669 741	+5,4%
3.NET(Générique)	8 141 310	9 117 236	+12%
4.ORG (Générique)	5 116 285	5 637 549	+10%
5.UK (Royaume-Uni)	5 215 373	5 488 177	+5%
6.INFO (Générique)	3 525 893	3 939 649	+11%
7.EU (Europe)	2 145 055	2 513 888	+17%
8.NL (Pays-bas)	2 040 128	2 246 725	+10%
9.CN (Chine)	1 296 294	**1 803 393**	+39%
10.AU (Australie)	1 543 045	1 644 955	+6%
11.BIZ (Générique)	1 485 882	1 604 627	+6,9%
12.IT(Italie)	1 247 257	1 310 339	+5%
13.US (Etats-Unis)	1 122 119	1 140 000	+1,6%
14. BR(Brésil)	988 189	**1 040 462**	+5,3%
15.CH (Suisse)	857 584	904 000	+5,4%
16.JP (Japon)	850702	889 456	+4,6%
17.CA (Canada)	750 000	**792 017**	+5,6%
18.DK (Danemark)	725 542	765 029	+5,4%
19.RU (Russie)	653 000	**744 537**	+14%
20.FR (France)	631 552	**737 559**	+16,8%
21.KR (Corée)	686 222	720 000	+4,9%
22.AT (Autriche)	664 503	709 452	+6,8%
23.BE (Belgique)	1 070 702	640 045	-40%
24.SE (Suède)	495 560	581 562	+17%
25.PL (Pologne)	504 842	547 642	+5%
26.ES (Espagne)	422 032	**521 207**	+23%
27.MOBI (tel.portable)	218 000	**370 000**	+69%
28.NO (Norvège)	294 000	312 000	+6,1%
29.CZ (République Tchèque)	267 722	288 283	+7,7%
30.HU(Hongrie)	260 000	280 000	+7%
31.NZ (Nouvelle Zélande)	250 000	265 000	+6%

Correspondance entre adresses : DNS

- L'adressage en décimal est complexe → Adressage hiérarchique logique par domaine pour simplifier
- DNSystem = répertoire distribué s'appuyant sur une structure de noms hiérachisée
- Au sommet de la hiérarchie, les Top Level Domain (generic + 240 countries) :
- Ex : fr, com, adm, org, gov, net, …
- Les Domain Name Server gèrent la correspondance
- Différents types de DNServer :
  - Locaux (informations locales à un site / ils sont des millions)
  - Racines (13 au total surtout au USA – RFC 2870)
  - DNR (Domain Names Resolvers) pour aider les serveurs Racines (DNS autorisés)
- Serveurs primaires + secondaires
- Client → Serveur par **méthode itérative ou récursive**
- rfai.univ-tours.fr ←→134.214.76.158

DNS : mode itératif ou récursif



DNS

- VeriSign Global Registry, Herndon, Virginia
- DISA, University of Southern California, Marina del Rey, California
- PSI, Herndon, Virginia
- University of Maryland, College Park, Maryland
- NASA Ames Research Center, Mountain View, California
- Internet Software Consortium, Palo Alto, California
- Department of Defense, Vienna, Virginia
- Army Research Lab, Aberdeen, Maryland
- Autonomica, Stockholm, Sweden
- VeriSign Global Registry, Herndon, VA
- RIPE, London, England
- DISA, University of Southern California, Los Angeles, California
- WIDE Project, Tokyo, Japan

Lettre	adresse IPv4	adresse IPv6	Ancien nom	Société	Localisation	Logiciel
A	198.41.0.4	2001:503:BA3E::2:30	ns.internic.net	VeriSign	Dulles, Virginie, Etats-Unis	BIND
B	192.228.79.201	2001:478:65::53	ns1.isi.edu	USC-ISI	Marina Del Rey, Californie, Etats-Unis	BIND
C	192.33.4.12		c.psi.net	Cogent Communications	trafic distribué par anycast	BIND
D	128.8.10.90		terp.umd.edu	University of Maryland	College Park, Maryland, Etats-Unis	BIND
E	192.203.230.10		ns.nasa.gov	NASA	Mountain View, Californie, Etats-Unis	BIND
F	192.5.5.241	2001:500:2f::f	ns.isc.org	ISC	trafic distribué par anycast	BIND
G	192.112.36.4		ns.nic.ddn.mil	Defense Information Systems Agency	Columbus, Ohio, Etats-Unis	BIND
H	128.63.2.53	2001:500:1::803f:235	aos.arl.army.mil	U.S. Army Research Lab	Aberdeen Proving Ground, Maryland, Etats-Unis	NSD
I	192.36.148.17		nic.nordu.net	Autonomica	trafic distribué par anycast	BIND
J	192.58.128.30	2001:503:C27::2:30		VeriSign	trafic distribué par anycast	BIND
K	193.0.14.129	2001:7fd::1		RIPE NCC	trafic distribué par anycast	NSD
L	199.7.83.42			ICANN	trafic distribué par anycast	NSD
M	202.12.27.33	2001:dc3::35		WIDE Project	trafic distribué par anycast	BIND

Les adresses URL

Les Adresses URL (Uniform Resource Locators)

- **Origine** : les hypertextes
- **Elle comprend** :
  - le type de service
  - l'adresse FQDN
  - l'emplacement sur le serveur
  - le nom du fichier

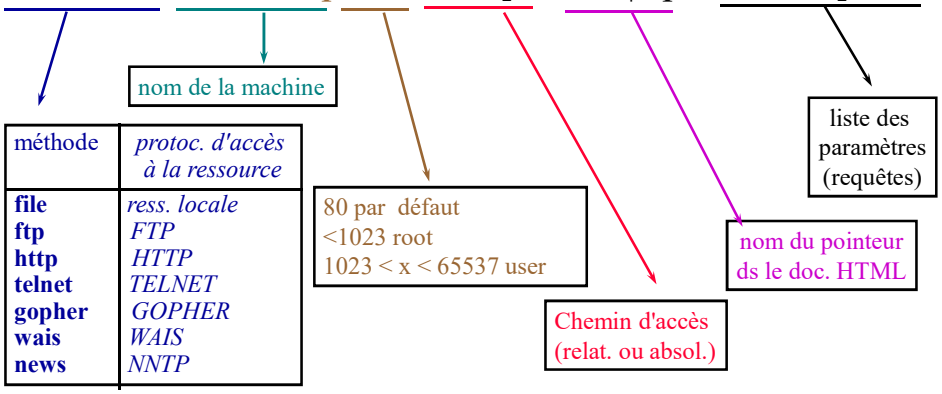
Types d'URL :

file:///repertoire/fichier.txt
http://serveur:port/repertoire/fichier.html
ftp://serveur/repertoire/fichier
mailto:nom@organisation.domaine
telnet://Nom:Password@serveur:port
gopher://serveur:port/repertoire/fichier#marqueur
news:nom.de.la.news
newsrc://serveur:port/repertoire/nom.de.la.news
wais://<host>:<port>/<database>?<search>

Identification des ressources URI/URL

(rfc 1738 : 1994)

méthode://machine:port/fichier[#ancre | ?paramètres]



Exercice

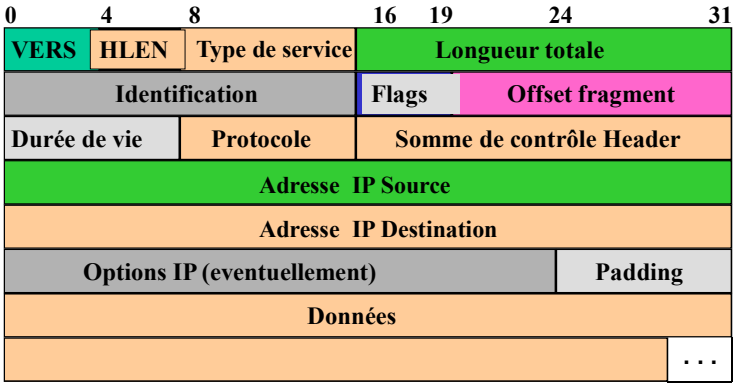
- Ayant obtenu un PC de votre directeur de département, on vous attribue (pour sa connexion au réseau) le numéro IP : 193.49.8.98. et son masque de sous-réseau associé 255.255.255.192. Le logiciel de configuration IP vous signale que vous êtes sur le réseau local de numéro 193.49.8.64.
- ① A quelle classe appartient ce réseau ? Quel est le numéro de ce réseau. Expliquez.
- On vous précise aussi que votre numéro de Broadcast est 193.49.8.127. ② A quoi sert ce numéro ?
- Le serveur web du département a pour numéro IP : 193.49.8.171 sur le réseau numéro 193.49.8.128.
- On vous précise que, pour vous y connecter, vous devez fournir au logiciel de configuration, le numéro IP : 193.49.8.65.③ Expliquez.
- Le logiciel de configuration IP, vous demande également de préciser le numéro IP d'un Domain Name Server. ④ Peut on prédire son adresse IP ? Expliquez.

Le protocole IP : Internet Protocol

- Le protocole IP définit :
  - l'unité de donnée transférée dans les interconnexions (datagramme),
  - la fonction de routage (les règles qui mettent en œuvre la remise de paquets en mode non connecté)

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:



IP : le datagramme

Signification des champs du datagramme IP :

- VERS : numéro de version de protocole IP, actuellement version 4,
- HLEN : longueur de l'en-tête en mots de 32 bits, généralement égal à 5 (pas d'option),
- Longueur totale : longueur totale du datagramme (en-tête + données)
- Type de service : indique comment le datagramme doit être géré :

- PRECEDENCE (3 bits) : définit la priorité du datagramme; en général ignoré par les machines et passerelles (pb de congestion).
- Bits D, T, R : indiquent le type d'acheminement désiré du datagramme, permettant à une passerelle de choisir entre plusieurs routes (si elles existent) : D signifie délai court, T signifie débit élevé et R signifie grande fiabilité.

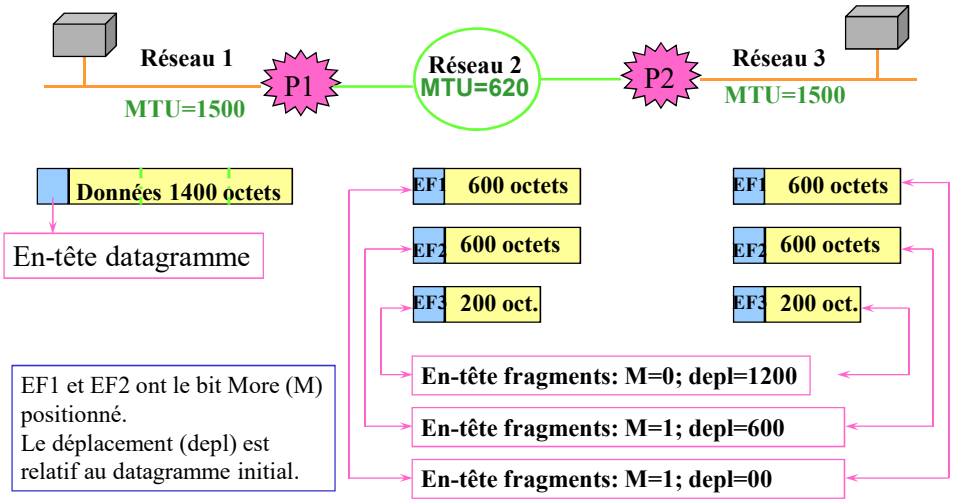
IP : le datagramme

- FRAGMENT OFFSET, FLAGS, IDENTIFICATION : les champs de la fragmentation.
  - Sur toute machine ou passerelle mettant en oeuvre TCP/IP une unité maximale de transfert (*Maximum Transfert Unit* ou **MTU**) définit la taille maximale d'un datagramme véhiculé sur le réseau physique correspondant
  - lorsque le datagramme est routé vers un réseau physique dont le MTU est plus petit que le MTU courant, la passerelle fragmente le datagramme en un certain nombre de fragments, véhiculés par autant de trames sur le réseau physique correspondant,
  - lorsque le datagramme est routé vers un réseau physique dont le MTU est supérieur au MTU courant, la passerelle route les fragments tels quels (rappel : les datagrammes peuvent emprunter des chemins différents),
  - le destinataire final reconstitue le datagramme initial à partir de l'ensemble des fragments reçus; la taille de ces fragments correspond au plus petit MTU emprunté sur le réseau. Si un seul des fragments est perdu, le datagramme initial est considéré comme perdu : la probabilité de perte d'un datagramme augmente avec la fragmentation.

IP : le datagramme

- FRAGMENT OFFSET : indique le déplacement des données contenues dans le fragment par rapport au datagramme initial. C'est un multiple de 8 octets; la taille du fragment est donc également un multiple de 8 octets.
- chaque fragment a une structure identique à celle du datagramme initial, seul les champs FLAGS et FRAGMENT OFFSET sont spécifiques.
- IDENTIFICATION : entier qui identifie le datagramme initial (utilisé pour la reconstitution à partir des fragments qui ont tous la même valeur).
- FLAGS contient un bit appelé "*do not fragment*" (01X)
- un autre bit appelé "*More fragments*" (FLAGS = 001 signifie d'autres fragments à suivre) permet au destinataire final de reconstituer le datagramme initial en identifiant les différents fragments (milieu ou fin du datagramme initial)

IP : le datagramme



IP : le datagramme

- Durée de vie
  - Ce champ indique en secondes, la durée maximale de transit du datagramme sur l'internet. La machine qui émet le datagramme définit sa durée de vie.
  - Les passerelles qui traitent le datagramme doivent décrémenter sa durée de vie du nombre de secondes (1 au minimum) que le datagramme a passé pendant son séjour dans la passerelle; lorsque celle-ci expire le datagramme est détruit et un message d'erreur est renvoyé à l'émetteur.
- Protocole

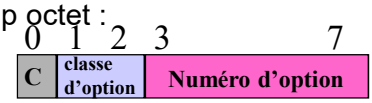
  Ce champ identifie le protocole de niveau supérieur dont le message est véhiculé dans le champ données du datagramme :
  - 6 : TCP,
  - 17 : UDP,
  - 1 : ICMP.

IP : le datagramme

- Somme de contrôle de l'en-tête
  - Ce champ permet de détecter les erreurs survenant dans l'en-tête du datagramme, et par conséquent l'intégrité du datagramme.
  - Le total de contrôle d'IP porte sur l'en-tête du datagramme et non sur les données véhiculées. Lors du calcul, le champ HEADER CHECKSUM est supposé contenir la valeur 0
  - Checksum = CRC → cf transmission de l'info.

IP : le datagramme

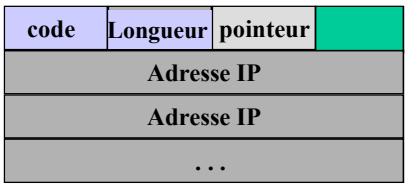
- OPTIONS
  - Le champ OPTIONS est facultatif et de longueur variable. Les options concernent essentiellement des fonctionnalités de mise au point. Une option est définie par un champ octet :



- copie (C) indique que l'option doit être recopiée dans tous les fragments (c=1) ou bien uniquement dans le premier fragment (c=0).
- les bits classe d'option et numéro d'option indiquent le type de l'option et une option particulière.

IP : le datagramme

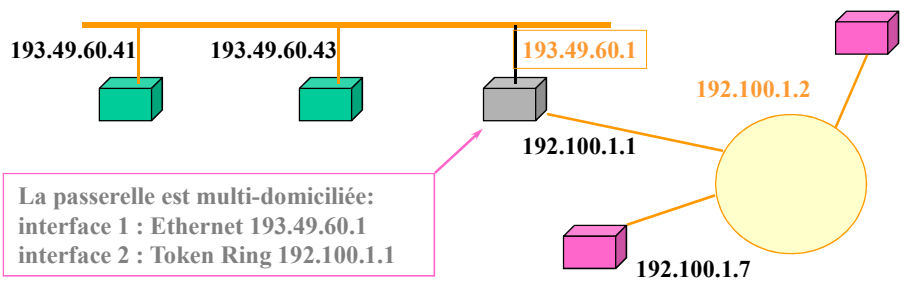
- Enregistrement de route (classe = 0, option = 7) : permet à la source de créer une liste d'adresse IP vide et de demander à chaque passerelle d'ajouter son adresse dans la liste.



Revenons un peu sur le routage

Adresses et connexions

- Une adresse IP => une interface physique => une connexion réseau LAN
- A une machine, est associé un certain nombre N d'adresses IP. Si N > 1 la machine (ou passerelle) est multi-domiciliée ➔ appartient à plusieurs reseaux.



Routage direct VS indirect des datagrammes

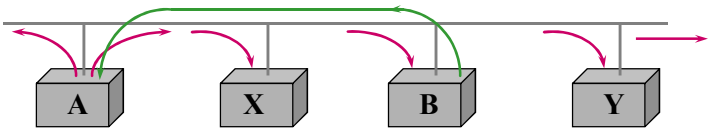
- Le routage est le processus permettant à un datagramme d'être acheminé vers le destinataire lorsque celui-ci n'est pas sur le même réseau physique que l'émetteur.
- Le chemin parcouru est le résultat du processus de routage qui effectue les choix nécessaires afin d'acheminer le datagramme.
- Les routeurs forment une structure coopérative de telle manière qu'un datagramme transite de passerelle en passerelle jusqu'à ce que l'une d'entre elles le délivre à son destinataire. Un routeur possède deux ou plusieurs connexions réseaux tandis qu'une machine possède généralement qu'une seule connexion.
- **Machines et routeurs** participent au routage :
  - les machines doivent déterminer si le datagramme doit être délivré sur le réseau physique sur lequel elles sont connectées (routage direct) ou bien si le datagramme doit être acheminé vers une passerelle; dans ce cas (routage indirect), elle doit identifier la passerelle appropriée.
  - les passerelles effectuent le choix de routage vers d'autres passerelles afin d'acheminer le datagramme vers sa destination finale.

ARP : Address Resolution Protocol

- Le besoin
  - La communication entre machines ne peut s'effectuer qu'à travers l'interface physique
  - Les applicatifs ne connaissant que des adresses IP, comment établir le lien adresse IP / adresse physique?
- La solution : ARP
  - Mise en place dans TCP/IP d'un protocole de bas niveau appelé Adress Resolution Protocol (ARP)
  - Rôle de ARP : fournir à une machine donnée l'adresse physique d'une autre machine située sur le même réseau à partir de l'adresse IP de la machine destinatrice
- La technique :
  - Diffusion d'adresses sur le réseau physique
  - Les machines non concernées ne répondent pas
  - Gestion cache pour ne pas effectuer de requête ARP à chaque émission

ARP : Address Resolution Protocol

- L'association adresse physique - adresse IP de l'émetteur est incluse dans la requête ARP de manière à ce que les récepteurs enregistrent l'association dans leur propre mémoire cache



- Pour connaître l'adresse physique de B, PB, à partir de son adresse IP IB, la machine A diffuse une requête ARP qui contient l'adresse IB vers toutes les machines; la machine B répond avec un message ARP qui contient la paire (IB, PB).

RARP : Reverse Address Resolution Protocol

- Le besoin
  - L'adresse IP d'une machine est configurable (elle dépend du réseau sur lequel elle se trouve) et est souvent enregistrée sur la mémoire secondaire où le système d'exploitation l'accède au démarrage.
  - Ce fonctionnement usuel n'est plus possible dès lors que la machine est une station sans mémoire secondaire.
- Problème : déterminer un mécanisme permettant à la station d'obtenir son adresse IP depuis le réseau.
- La solution
  - Protocole de bas niveau appelé Reverse Adress Resolution Protocol
  - Permet d'obtenir son adresse IP à partir de l'adresse physique qui lui est associée.
- Fonctionnement

  Serveur RARP sur le réseau physique; son rôle: fournir les adresses IP associées aux adresses physiques des stations du réseau (BD).

Le routage IP plus concrètement

- Les tables de routage IP, pour des raisons évidentes d'encombrement, renseignent seulement les adresses réseaux et non pas les adresses machines.
- Typiquement, une table de routage contient des couples (R, P) où R est l'adresse IP d'un réseau destination et P est l'adresse IP de la passerelle correspondant au prochain saut dans le cheminement vers le réseau destinataire.
- La passerelle ne connaît pas le chemin complet pour atteindre la destination.
- Pour une table de routage contenant des couples (R, P) et appartenant à la machine M, P et M sont connectés sur le même réseau physique dont l'adresse de niveau réseau (partie Netid de l'adresse IP) est R.

Plus concrètement les 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-HOP	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.

Comment sont créées les tables de routage ?

- Manuellement
  - Chaque routeur est configuré par un administrateur
  - La configuration manuelle initiale n'empêche pas les nœuds de participer à des phases de configuration dynamique
- Puis elles évoluent dynamiquement
  - Par des échanges automatiques de tables de routage à l'aide d'un des protocoles RIP, OSPF, EGP, BGP
  - Par réception de messages ICMP

Dynamic Routing Protocol

- 1. Un administrateur réalise un plan d'adressage, c'est-à-dire que des préfixes de sous réseaux sont donnés à chaque lien
- 2. En utilisant ce plan d'adressage, les routeurs de ce réseau sont configurés manuellement ; une adresse IP est donnée à chacune de leur interface, ainsi que la longueur des préfixes de sous réseaux associés à chaque lien
- 3. Les routeurs découvrent leur voisins, c'est-à-dire les routeurs qui peuvent être atteint en envoyant un paquet sur un lien connecté à l'une de leur interface

Dynamic Routing Protocol

- 4. Les routeurs échangent périodiquement des informations (routing updates) qui correspondent à la liste des entrées de leur table de routage associée (cf RIP et OSPF)
- 5. Les routeurs utilisent toutes les informations collectées pour mettre à jour leur table personnelle ; elle s'enrichit de cette façon d'information de routage vers des nœuds qui ne sont pas directement accessibles depuis l'une de ces interfaces.
- Note : ce type de protocole est permet d'etre robuste aux problèmes techniques dans les réseaux

Routage des datagrammes

- traceroute to bat710.univ-lyon1.fr (134.214.88.10): 1-30 hops, 38 byte packets
- 1 cisco-insa-cri.univ-lyon1.fr (134.214.76.1) 2.46 ms 1.1 ms 0.971 ms
- 2 cisco.univ-lyon1.fr (134.214.100.125) 2.63 ms 2.13 ms 2.9 ms
- 3 bat710.univ-lyon1.fr (134.214.88.10) 1.62 ms 2.90 ms 2.87 ms

- traceroute to nikhefh.nikhef.nl (192.16.199.1): 1-30 hops, 38 byte packets
- 1 cisco-insa-cri.univ-lyon1.fr (134.214.76.1) 2.40 ms 1.5 ms 1.1 ms
- 2 cisco.univ-lyon1.fr (134.214.100.125) 2.31 ms 3.34 ms 14.8 ms
- 3 u-1-cism-villeurbanne.aramis.ft.net (193.48.222.2) 12.3 ms 3.7 ms 2.82 ms
- 4 lyon.aramis.ft.net (193.48.66.13) 100 ms 121 ms 105 ms
- 5 lyon.renater.ft.net (193.48.66.233) 77.5 ms 111 ms 69.3 ms
- 6 stamand2.renater.ft.net (192.93.43.33) 107 ms 127 ms 61.8 ms
- 7 stamand1.renater.ft.net (195.220.180.43) 113 ms 103 ms 146 ms
- 8 rbs1.renater.ft.net (195.220.180.50) 101 ms 74.1 ms 108 ms
- 9 renater.FR.ten-34.net (193.203.228.5) 107 ms 108 ms 108 ms
- 10 FR.uk.ten-34.net (193.203.228.2) 153 ms 137 ms 144 ms
- 11 london6.att-unisource.net (195.206.64.69) 114 ms 109 ms 153 ms
- 12 london5.att-unisource.net (195.206.64.49) 132 ms 133 ms 155 ms
- 13 stockholm5.att-unisource.net (195.206.64.37) 169 ms 165 ms 149 ms
- 14 amsterdam5.att-unisource.net (195.206.64.33) 191 ms 222 ms 162 ms
- 15 amsterdam6.att-unisource.net (195.206.64.18) 183 ms 101 ms 114 ms
- 16 Amsterdam1.belsurf.net (192.12.54.1) 83.5 ms 106 ms 127 ms
- 17 Amsterdam11.router.surfnet.nl (192.12.54.10) 168 ms 95.4 ms 131 ms
- 18 hef-router.nikhef.nl (192.16.183.80) 128 ms 183 ms 165 ms
- 19 nikhefh.nikhef.nl (192.16.199.1) 195 ms 182 ms 189 ms

Exercice

- Maintenant que vous maitrisez les bases du réseau, représentez sur un schéma l'architecture du réseau du département Informatique de PolytechTours
- Puis décrivez un échange entre 2 machines positionnés sur 2 LAN ou VLAN différents (trames en circulation)

Le Protocole ICMP (Internet Control Message Protocol)

- Le protocole ICMP permet d'envoyer des **messages de contrôle ou d'erreur** vers d'autres machines ou passerelles (RFC 792 et 1256).
- ICMP rapporte les messages d'erreur à l'émetteur initial.
- Beaucoup d'erreurs sont causées par l'émetteur, mais d'autres sont dûes à des problèmes d'interconnexions rencontrées sur l'Internet :
  - **machine destination déconnectée,**
  - **durée de vie du datagramme expirée,**
  - **congestion de passerelles intermédiaires.**
- Si une passerelle détecte un problème sur un datagramme IP, elle le détruit et émet un message ICMP pour informer l'émetteur initial.
- Les messages ICMP sont véhiculés à l'intérieur de datagrammes IP et sont routés comme n'importe quel datagramme IP sur l'internet.

On passe à la couche 4 …

- Gestion des transferts applicatifs
- Communication de bout en bout
- Palliation des lacunes…

UDP : User Datagram Protocol

- UDP : protocole de transport sans connexion :
  - émission de messages applicatifs : sans établissement de connexion au préalable
  - l'arrivée des messages ainsi que l'ordonnancement ne sont pas garantis.
- Identification du service : les ports
  - les adresses IP désignent les machines entre lesquelles les communications sont établies. Lorsqu'un processus désire entrer en communication avec un autre processus, il doit adresser le processus s'exécutant sur cette machine.
  - L'adressage de ce processus est effectué selon un concept abstrait indépendant du système d'exploitation des machines car :
    - les processus sont créés et détruits dynamiquement sur les machines,
    - il faut pouvoir remplacer un processus par un autre (exemple reboot) sans que l'application distante ne s'en aperçoive,
    - il faut identifier les destinations selon les services offerts, sans connaître les processus qui les mettent en oeuvre,
    - un processus doit pouvoir assurer plusieurs services.

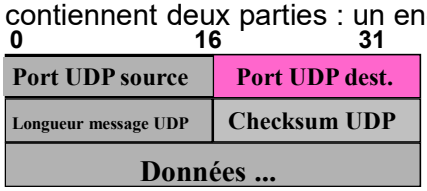
UDP : les ports

- Ces destinations abstraites permettant d'adresser un service applicatif s'appellent des **ports** de protocole.
- L'émission d'un **message se fait sur la base d'un port source et un port destinataire**.
- Les processus disposent d'une **interface système** leur permettant de spécifier un port ou d'y accéder ➔ **socket, ...**
- Les accès aux ports sont généralement synchrones, les opérations sur les ports sont tamponnés (files d'attente)

UDP : format des messages

Les messages UDP sont également appelés des datagrammes UDP.

Ils contiennent deux parties : un en-tête UDP et les données UDP.



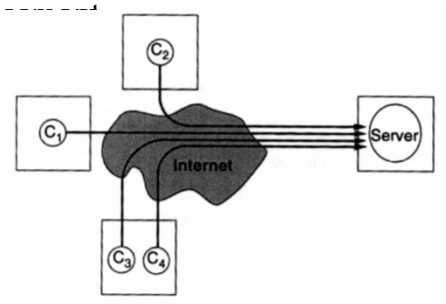
Format des messages UDP

Les ports source et destination contiennent les numéros de port utilisés par UDP pour démultiplexer les datagrammes destinés aux processus en attente de les recevoir.

La longueur du message est exprimée en **octets (8 au minimum)** (en-tête + données), le champ de contrôle est optionnel (0 si non utilisé).

TCP : Transmission Control Protocol

- Transport fiable :
  - fiabilité = illusion assurée par le service
  - transferts tamponnés : découpage en **segments**
  - connexions bidirectionnelles et simultanées
- Service en mode connecté
- Garantie de non perte de messages ainsi que de l'ordonnan[illegible]



TCP : La connexion

- une connexion est établie avant que les données ne soient échangées : appel + négociation + transferts
- Une connexion = une paire d'extrémités de connexion
- Une extrémité de connexion = couple (adresse IP, port)
- Exemple de connexion : **((124.32.12.1, 1034), (19.24.67.2, 21))**
- Une extrémité de connexion peut être partagée par plusieurs autres extrémités de connexions (multi-instanciation)
- La mise en oeuvre de la connexion se fait en deux étapes :
  - une application (extrémité) effectue une **ouverture passive** en indiquant qu'elle accepte une connexion entrante,
  - une autre application (extrémité) effectue une **ouverture active** pour demander l'établissement de la connexion.

TCP : Segmentation

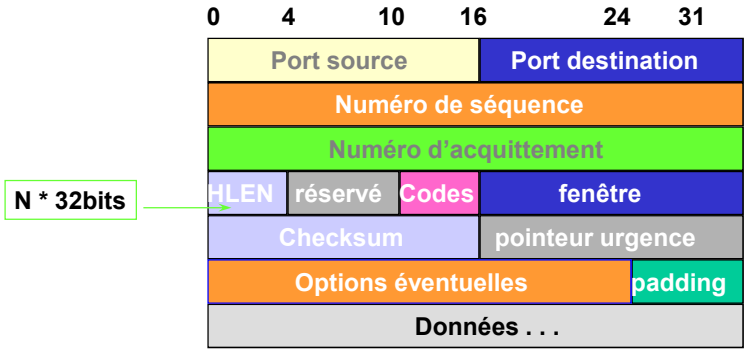
- Segmentation, contrôle de flux
  - Les données transmises à TCP constituent un flot d'octets de longueur variable.
  - TCP divise ce flot de données en segments en utilisant un mécanisme de fenêtrage.
  - Un segment est émis dans un datagramme IP.
- Acquittement de messages
  - Contrairement à UDP, TCP garantit l'arrivée des messages, c'est à dire qu'en cas de perte, les deux extrémités sont prévenues.
  - Ce concept repose sur les techniques d'acquittement de message : lorsqu'une source S émet un message Mi vers une destination D, S attend un acquittement Ai de D avant d'émettre le message suivant Mi+1.
  - Si l'acquittement Ai ne parvient pas à S, S considère au bout d'un certain temps que le message est perdu et reémet Mi :

TCP : Technique de fenêtrage

- Le mécanisme de fenêtrage mis en oeuvre dans TCP opère au niveau de l'octet et non pas au niveau du segment; il repose sur :
  - la numérotation séquentielle des octets de données,
  - la gestion de trois pointeurs par fenêtrage :

TCP : Segments

- Segment : unité de transfert du protocole TCP.
  - échangés pour établir les connexions (Syn),
  - transférer les données (Seq),
  - émettre des acquittements (Ack),
  - fermer les connexions (Fin);



TCP : Exemple

- On considère 2 stations A et B. On admet que les couches supérieures ont initialisée une demande de connexion auprès de leur couche transport respective, A demandant à se connecter sur B. L'état initial est donc : A demande l'ouverture d'une connexion vers la station B et B est en attente d'une demande d'ouverture de connexion. 1)A ⇒ B : SYN *SEQ200*

  2) B ⇒ A : ACK 201 - SYN *SEQ550*

  3)A ⇒ B : ACK 551

  4)A

- A souhaite envoyer 20 octets à B. La couche supérieure transmet à TCP_A les 20 octets à émettre. Les échanges entre TCP_A et sa couche supérieure font appel aux services et sont donc constitués de T_SDU.

  5) A ⇒ B : SEQ 201

  6) B ⇒ A : ACK 221

221 = 201 + longueur des données reçues (contrôle possible de A)

7) B

TCP : Exemple

- B souhaite à son tour envoyer 125 octets à A. La couche supérieure transmet à TCP_B les 125 octets à émettre.

  8) B ⇒ A : SEQ 551

  9) A ⇒ B : ACK 676

- Admettons que le transfert de cet acquittement subit un défaut et que le délai d'acquittement positif soit écoulé. TCP_B détecte une erreur de transmission et décide de retransmettre les données.

  10) B ⇒ A : SEQ 551

  11) A

- TCP_A réceptionne la nouvelle séquence. Comme il s'agit d'un numéro déjà reçu et transmis à la couche supérieure, ce paquet est détruit. Cependant, l'acquittement doit de nouveau être envoyé à TCP_B.

  12) A ⇒ B : ACK 676

- Fermeture de la connexion entre les stations A et B, en supposant que c'est A qui initie cette fermeture. La couche supérieure transmet à TCP_A une requête de déconnexion.

  13) A ⇒ B : FIN *SEQ221*

  14) B

  15) B ⇒ A : ACK 222 - FIN *SEQ676*

  16) A ⇒ B : ACK 677

TCP : la congestion

- TCP gère **le contrôle de flux de bout en bout** mais également les problèmes de congestion liés à l'interconnexion.
- La congestion correspond à la saturation de noeud(s) dans le réseau provoquant des délais d'acheminement de datagrammes jusqu'a leur pertes éventuelles.
- Les extrémité ignorent tout de la congestion sauf les délais. Habituellement, les protocoles retransmettent les segments ce qui aggrave encore le phénomène.
- Dans la technologie TCP/IP, les passerelles (niveau IP) utilisent la réduction du débit de la source mais TCP participe également à la gestion de la congestion en diminuant le débit lorsque les délais s'allongent

TCP : la congestion

- TCP maintient une **fenêtre virtuelle de congestion**
- TCP applique la fenêtre d'émission suivante:
  - fenêtre_autorisée = min (fenêtre_récepteur, fenêtre_congestion).
- Dans une situation de non congestion:
  - fenêtre_récepteur = fenêtre_congestion.
- En cas de congestion, TCP applique une diminution dichotomique :
  - à chaque segment perdu, la fenêtre de congestion est diminuée par 2 (minimum 1 segment)
  - la temporisation de retransmission est augmentée exponentiellement.

TCP : ports standards

No port		Mot-clé	Description
20	FTP-DATA		File Transfer [Default Data]
21	FTP		File Transfer [Control]
23	TELNET		Telnet
25	SMTP		Simple Mail Transfer
37	TIME		Time
42	NAMESERVER	Host	Name Server
43	NICNAME		Who Is
53	DOMAIN		Domain Name Server
79	FINGER		Finger
80	HTTP		WWW
110	POP3		Post Office Protocol - Version 3
111	SUNRPC		SUN Remote Procedure Call

Ports réserves =< 1024 - Ports libres > 1024

Protocole TCP

TCP_PDU = Segment. La taille maximale d'un segment MSS (Max. Segment Size) est fixée pour cet exercice à 800 octets.

L'utilisateur fournit 3 demandes d'émission de données respectivement de 700, 350 et 10 octets. Chacune de ces demandes provoque l'émission d'un PDU. Le premier PDU se perd.

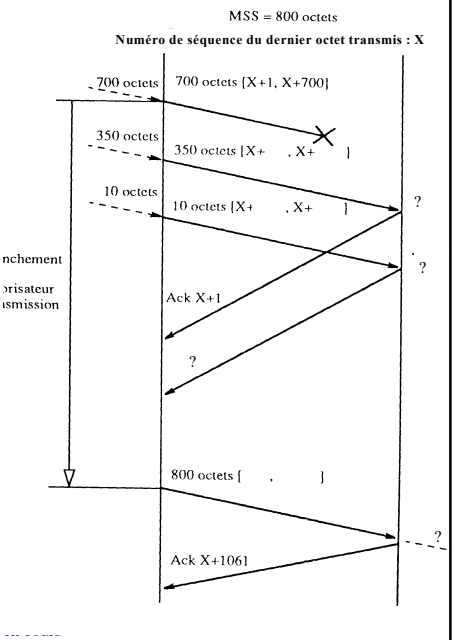
1. Complétez la figure.

2. Pourquoi le récepteur émet un acquittement pour les octets X+1 ?

3. Combien de fois, dans l'exemple précédent, les octets [X+701; X+800] sont-ils reçus ?

4. Pourquoi y a-t-il transmission du paquet de 800 octets ? Pourquoi le récepteur acquitte les données jusqu'à 1061 ?

5. La plupart des implantations de TCP considèrent que 3 acquittements positifs de suite portant la même valeur correspondent un acquittement négatif. Pourquoi ?



Mode Circuit Virtuel : de X25 à ATM

Un peu d'histoire : X25 / Transpac le premier réseau français

X25 Packet Layer Protocol = X25 niveau Réseau

→ **Notion de Circuit Virtuel**

- X25 est utilisé dans les réseaux à **commutation de paquets**
- En cours de disparition mais a inspiré les concepteurs d'ATM
- Il définit à la fois un protocole de communication entre ETCD (commutateur de Niveau 3) et ETTD (PC/Terminaux) et entre ETTD et ETTD.

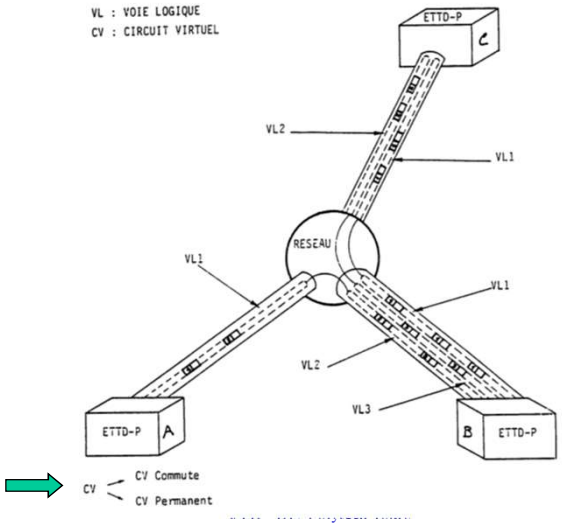
De X25 à ATM

- Le protocole X25 faisait référence de norme pour la couche 3 en **mode avec connexion**. 3 phases sont utilisées :
  - **Ouverture** d'une connexion : Création d'un **circuit virtuel** (entre 2 ETTD) par association de **voies logiques** (liaisons établies entre 2 ETCD). Envoi d'un paquet d'appel. Adressage X121.
  - **Transfert de données :** envoie des paquets de données (ordre respecté, même chemin).
  - **Fermeture** de la connexion : destruction du C.V., libération des ressources.
- Un commutateur de niveau 3 peut gérer plusieurs voies logiques simultanément (jusqu'à 4096 pour X25).
- Un circuit virtuel peut être commuté ou permanent

X25 ou ATM → réseau commuté → nœud : commutateur de niv. 3

De X25 à ATM

Voie logique / Circuit Virtuel



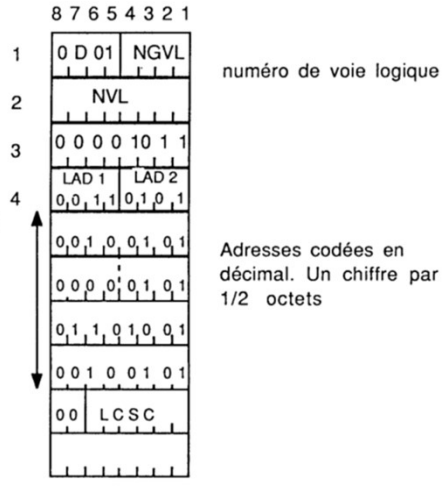
De X25 à ATM

Quel contenu pour un paquet d 'appel ?

Des adresses source et dest :

longueur adr appelant
LAD 1 = 3
longueur adr appelé
LAD 2 = 5

AD appelant = 250
AD appelé = 56925



De X25 à ATM

Et ensuite ?

8	7	6	5	4	3	2	1	
Ident. Général Q D L C				Numero				1
de Canal Logique								2
Ident. du type de Paquet								3
Champ Données ou Adresses ou Compte rendu ou absent selon le type								4

⇐ Types de paquets

Commentaire	Type du paquet	Ident. du type de Paquet 8 7 6 5 4 3 2 1	Correspondance avec HDLC
Ouverture	Demande d'ouverture	0 0 0 0 1 0 1 1	Trames non numérotées
	Appel accepté	0 0 0 0 1 1 1 1	
Fermeture	Demande de fermeture	0 0 0 1 0 0 1 1	
	Confirmation de fermeture	0 0 0 1 0 1 1 1	
Paquets Express	Demande d'interruption	0 0 1 0 0 0 1 1	U
	Confirmation d'interruption	0 0 1 0 0 1 1 1	
Nettoyage Circuit Virtuel	Reprise d'un CV	0 0 0 1 1 0 1 1	
	Confirmation de reprise	0 0 0 1 1 1 1 1	
	Redémarrage	1 1 1 1 1 0 1 1	
	Confirmation de redémarrage	1 1 1 1 1 1 1 1	
Gestion flux et erreurs	RR	X X X 0 0 0 0 1	supervision
	RNR court	X X X 0 0 1 0 1	
	REJ	X X X 0 1 0 0 1	
deux formats	Long 2 octets 3 et 4 N(r) est dans le 4eme octet		S
Données	Paquet de données format court	R R R M S S S 0 (N(r), N(s))	Données
	format long octet 3 octet 4	S S S S S S S 0 / R R R R R R R M	I

Commutation / Relais de Trames / Cellules

Principe

- Au départ, la fiabilisation des supports de transmission, d'où :
  - détection d'erreurs réalisée uniquement sur les organes d'extrémité
  - diminuer les opérations de couches (acheminement au niveau 1 et 2)
  - pas de contrôle de flux entre les noeuds
  - acquittement de bout en bout uniquement
- 3 techniques appliquent ces principes :
  - la commutation de trames (frame switching)
  - le relais de trames (frame relay)
  - le commutation de cellules (ATM)

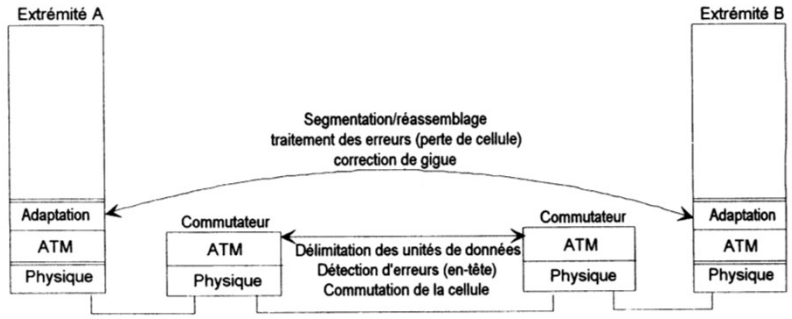
Travail des nœuds intermédiaires

	Paquet (X.25)	Commutation de trames	Relaisde trames
Formatage	Oui	Oui	Oui
Transparence	Oui	Oui	Oui
Existence d'un CRC	Oui	Oui	Oui
Contrôle d'erreurs	Oui	Oui	Non
Contrôle de flux	Oui	Oui	Non
Reprise et Redémarrage	Oui	Non	Non

ATM (Asynchronous Transfert Mode)

Un réseau à commutation de **cellules** :

- Trames très courtes de longueur fixe → Commutation " hardware "

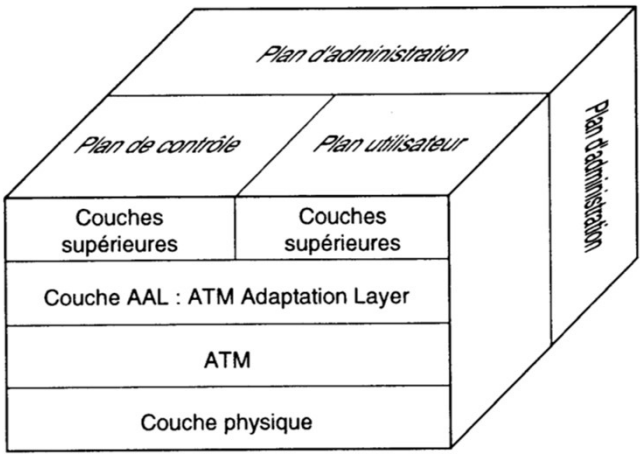


Architecture ATM

ATM (Asynchronous Transfert Mode)

- Cette technique consiste à transporter **de tout petits paquets** de 53 octets appelés cellules.
- ils passent par des nœuds de commutation rapide et les **temps de transport** des cellules d'un bout à l'autre du réseau sera pratiquement **constant**.
- Cette technique se rapproche donc du mode de communication **synchrone** ce qui est satisfaisant pour la communication de la voix et de la vidéo.
- Les cellules ATM sont remplies à l'émission par l'information arrivant de façon **asynchrone** depuis les applications.
- Les cellules ne sont envoyées qu'a la demande des applications. On alloue dynamiquement, selon la bande passante disponible, les différents débits nécessaires.

Architecture d'ATM



Architecture d'ATM

Couche Physique

Elle est composée de 2 sous-couches :

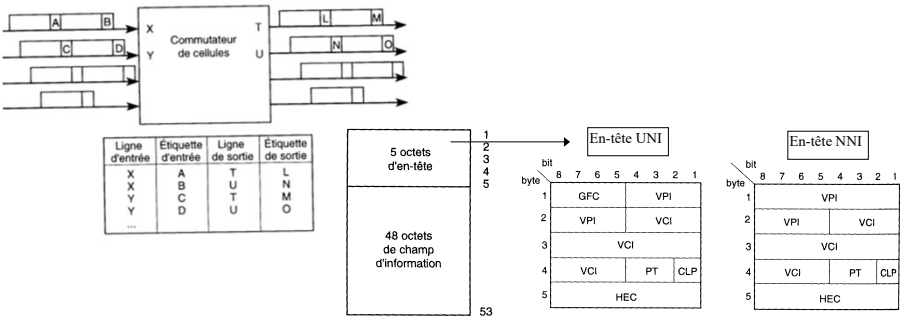
- La couche TC (Transmission Convergence) :
  - délimitation des cellules
  - adaptation de la vitesse de transmission
  - techniques SONET ou SDH sur fibre optique (envoi d'un "container de cellules" toute les 125 µs suivant le débit voulu)
- La couche Physical Medium :
  - Codage / Transmission des signaux
  - Gestion des horloges

Son rôle consiste à faire transiter en permanence toute les 125 µs une **trame** entre deux nœuds de commutation → un train qui circule en permanence entre deux gares, une cellule ATM peut monter dans ce train à n'importe quel moment et à n'importe quel endroit de ce train.

Architecture d'ATM

Couche ATM (Mode Transmission Asynchrone)

- Envoi des cellules de **53 octets de bout en bout**
- Adressage/commutation : proche de la méthode X25 (CV, CVP)
- **Contrôle de flux** : indicateur de congestion (1bit) + champ GFC



Architecture d'ATM

Couche AAL (ATM Adaptation Layer)

Elle comporte 2 sous-couches :

Sous-couche SAR (Segmentation And Rassembly)

Elle propose 4 types de services :

- AL1 (Constant Bit Rate) : débit constant en mode connecté (isochrone).
  → transport du son et de la vidéo (non compressée)
- AL2 (Variable Bit Rate) : débit variable en mode connecté
  → transport de vidéo compressée (MPEG)
- AL3/4 (Available Bit Rate) : mode connecté ou non
  → transport de données (voir sous-couche CS)
- AL5 (Simple and Efficient AL) : débit constant mode non-connecté
  → transport de données (voir sous-couche CS)

Architecture d'ATM

Sous-couche Convergence (CS)

- Au dessus de SAR, elle définit le bloc à transporter de bout en bout (de 1 à 65535 octets)
- Délimitation, séquencement, réservation mémoire et **détection d'erreurs pour AL1 et AL2**

Utilisation d'ATM

Comme LAN

- ATM est "**orienté connexion**" alors que les réseaux locaux classiques sont "sans connexion"
- Les réseaux locaux classiques utilisent la diffusion générale **(broadcast)** alors qu'ATM ne permet que des connexions point à point ou point à multipoint.
- Afin de protéger les investissements des utilisateurs au niveau des applications et des logiciels réseau, et pour rendre le support ATM utilisable par les protocoles existants …
- … ATM a défini un protocole d'émulation de réseaux locaux (LAN Emulation - LANE) : Une couche de traduction entre les couches hautes s'appuyant sur un service sans connexion et la couche basse ATM qui nécessite l'établissement d'une connexion avant toute communication.

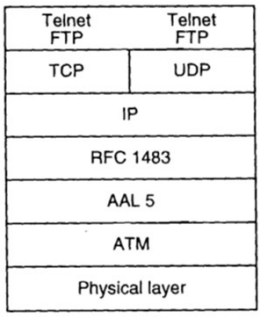
Utilisation d'ATM

Comme WAN

- Successeur de RNIS et X25
- Multimédia (son, image, ...)
- **Transport IP**

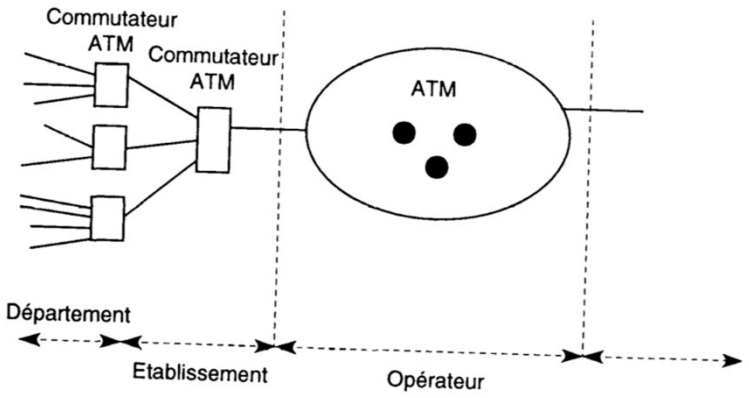
→ Communication inter réseaux locaux

- Seul concurrent potentiel :
  - Commutation IP - IP switching
- Période transitoire :
  - TCP/IP sur ATM : ATM entre routeurs IP



Utilisation d'ATM

ATM de bout en bout ???



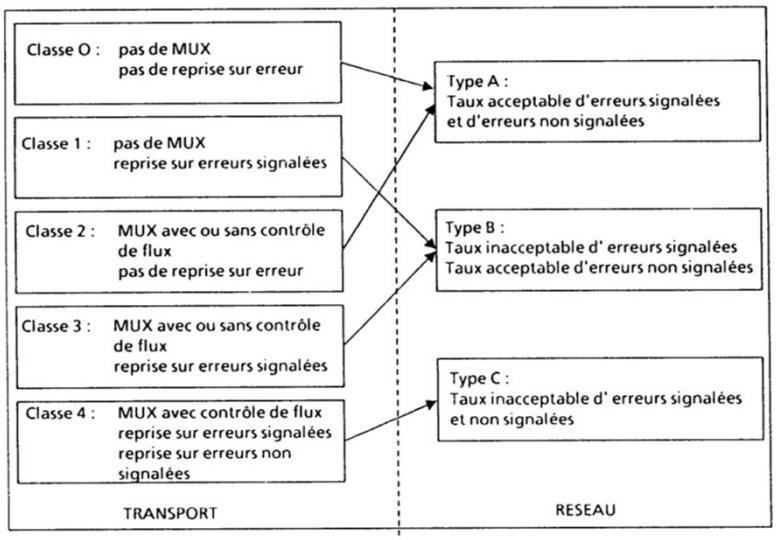
Chapitre 8

Couches 4 à 7 : Traitement des données

Couche 4 OSI : Transport

- Cette couche est **la charnière** entre les fonctions qui traitent de la communication et celle qui traitent de l'exploitation.
- Au dessus les caractéristiques du réseau n'apparaissent plus.
- La communication de **bout en bout** entre 2 usagers est assurée quelques soient les conditions.
- La couche gère les ressources de communications mis à disposition pour offrir le service avec les caractéristiques souhaités → Classes de services :

Couche 4 OSI : Transport



Couche 4 OSI : Transport

- Services rendus en fonction de la classe de la couche Transport :

Mécanismes prévus\Classes de transport	0	1	2	3	4
Segmentation et réassemblage (TSDU ↔ n TPDU)	oui	oui	oui	oui	oui
Concaténation et séparation (n TPDU ↔ NSDU)	non	oui	oui	oui	oui
Multiplexage et éclatement	non	non	oui	oui	oui
Contrôle de flux	non	non	option	oui	oui
Numérotation TPDU (séquencement)	non	oui	option	oui	oui
Données exprès	non	option	option	oui	oui
Reprise sur erreur détectée et signalée	non	oui	non	oui	oui
Utilisation de plusieurs connexions réseau	non	non	non	non	**oui**
Contrôle d'inactivité	non	non	non	non	**oui**
Détection d'erreurs sur TPDU	non	non	non	non	option

L'adéquation entre le niveau de qualité offert par la couche réseau et la classe de protocole transport :

Réseau	Transport	Caractéristiques principales de la classe de protocole de transport
A	0	Classe de base, la confiance faite à la couche réseau est totale
B	1	Numérotation TPDU, reprise sur erreur (détectée)
A	2	Numérotation TPDU, contrôle de flux, fonctions de multiplexage
B	3	Numérotation TPDU, contrôle de flux, reprise sur erreur et multiplexage
C	4	La confiance faite à la couche réseau est minimale

Couche 5 OSI : Session

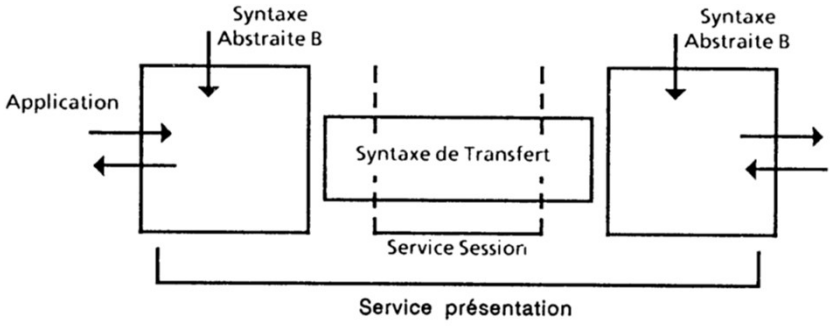
- Gestion des dialogues (activités) :
  - Synchronisation
  - Interruption
  - Reprise

Couche 5 OSI : Session

Primitive	*Rq.*	*Ind.*	*Response*	*Confirm*	Signification
S-CONNECT	X	X	X	X	Établissement d'une connexion
S-RELEASE	X	X	X	X	Libération ordonnée d'une session
S-U-ABORT	X	X			Libération brutale à l'initiative de l'utilisateur
S-P-ABORT		X			Libération brutale à l'initiative du fournisseur
S-DATA	X	X			Transfert de données normales
S-EXPEDITED-DATA	X	X			Transfert de données exprès
S-TYPED-DATA	X	X			Transfert de données typées
S-CAPABILITY-DATA	X	X	X	X	Transfert de données de capacité
S-TOKEN-GIVE	X	X			Passage d'un jeton
S-TOKEN-PLEASE	X	X			Jeton réclamé
S-CONTROL-GIVE	X	X			Passage de tous les jetons
S-SYNC-MAJOR	X	X	X	X	Insertion d'un point de synchronisation majeure
S-SYNC-MINOR	X	X			Insertion d'un point de synchronisation mineure
S-RESYNCHRONIZE	X	X	X	X	Retour à un point de synchronisation précédent
S-ACTIVITY-START	X	X			Démarrage d'une activité
S-ACTIVITY-END	X	X	X	X	Fin d'une activité
S-ACTIVITY-DISCARD	X	X	X	X	Abandon d'une activité
S-ACTIVITY-INTERRUPT	X	X	X	X	Suspension d'une activité
S-ACTIVITY-RESUME	X	X			Reprise d'une activité suspendue
S-U-EXCEPTION-REPORT	X	X			Rapport d'anomalie utilisateur
S-P-EXCEPTION-REPORT		X			Rapport d'anomalie fournisseur

Couche 6 OSI : Présentation

- Compréhension cohérente des informations échangées
- Syntaxe unifiée → ASN(1)



Couche 7 OSI : Application

- Cadre d'accueil pour les applications qui ont à communiquer
- 1 application utilise en ensemble d'ASE
- ASE : Application Service Element
- ACSE : Connexion entre 2 ASE (processus)
- Exemple de ASE normalisés ISO :
  - FTAM → FTP
  - MHS → SMTP
  - VTS →Telnet
  - DES → LDAP
  - …

Services Applicatifs associés à TCP/IP

- Courrier électronique
- Transfert de fichiers
- Telnet
- Web
- …

- Mode client / serveur

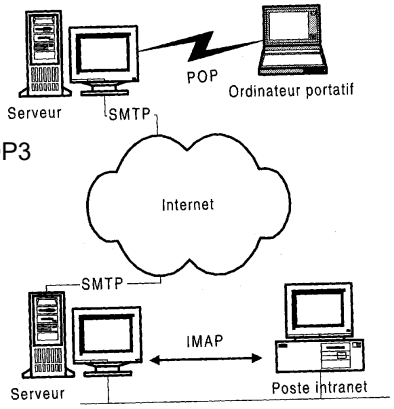
Service E-Mail

- Envoyer et recevoir des courriers
  - adresses de courrier Internet :
    nom@organisation.domaine.pays
- Le courrier électronique n'est pas anonyme
- Un mail contient toujours :
  - l'adresse du destinataire,
  - le sujet du mail parfois appelé aussi objet du courrier
  - Et de façon optionnelle :
    - les lignes correspondant au contenu du mail (ASCII)
    - un attachement (ASCII, Word, son etc).
- Les logiciels de lecture de courrier :
  - Eudora
  - Pegasus
  - ….

Service E-Mail

- **Les Protocoles Courrier**

- **La boîte aux lettres** de votre correspondant peut être située sur :
- . son ordinateur
- . sur un serveur de courrier
- **Pour expédier votre courrier :**
- → SMTP directement ou
- → une procédure extension de POP3



Service E-Mail

- **Les Protocoles Courrier**

- SMTP (Simple Mail Transport Protocol) :
- . Le protocole SMTP est un protocole point à point
- . Il met en communication deux serveurs
- → celui de la personne qui envoie le courrier et celui qui le reçoit
- . Ces serveurs sont chargées de la gestion des courriers
- . Le protocole SMTP spécifie:
  - le format des adresses des utilisateurs
  - le format des champs de vos courriers (from: to: etc.)
  - les possibilités d'envoi groupé
  - la gestion des heures

Service E-Mail

- **Les Protocoles Courrier**

- POP3 (Post Office Protocol)
- → Pour récupérer votre courrier sur une machine distante
- → Quand vous n'êtes pas connecté en permanence à Internet.

- Le protocole POP gère les messages suivants:
  - LIST donne le nombre de courriers présents sur le serveur
  - RETR numéro récupère le courrier numéro sur votre serveur
  - DELE numéro détruit le courrier numéro
  - NOOP vérifie la connexion
  - LAST récupère le dernier message arrivé sur le serveur
  - QUIT quitte la session et en autorise une autre

Service E-Mail

- **Les Protocoles Courrier**

- IMAP (Interactive Mail Access Protocol)
- → C'est un autre protocole moins utilisé que POP
- Il gère :
  - » plusieurs accès simultanés,
  - » plusieurs boîtes aux lettres sur le serveur
  - » recherches de courrier selon critères.
- → plus riche → plus complexe → moins utilisé

- MIME (Multi-purpose Internet Mail Extensions)
- → Gestion des types des documents attachés
- Listes de distribution :
  → Les Listservs : 1 programme (robot) gère la liste
- Les Services de changement d'adresse

Standardiser les formats : MIME

(rfc 1521, 1522 : 1993)

- **Multipurpose Internet Mail Extensions**
  - Format de mail universel, Documents attachés
  - Fichiers de correspondance format/suffixe
- **Le Web utilise un (petit) sous-ensemble de MIME**
  - Type de ressources
    - Content-type: text/html
    - Content-type: image/gif
  - Encodage de ressources
    - Content-Transfer-Encoding: base64
    - Content-Transfer-Encoding: x-gzip

MIME 2/2

- Serveur : trouve l'emballage

application/msword	doc
application/octet-stream	bin dms lha lzh exe class
audio/basic	au snd
chemical/x-pdb	pdb xyz
image/gif	gif
message/news	
multipart/mixed	
text/html	html htm
video/quicktime	qt mov
x-conference/x-cooltalk	ice
x-world/x-vrml	wrl vrml

- Client : trouver l'action à réaliser
  - Interprète la ressource (text/html, image/gif, plug-ins)
  - Transmet la ressource à une application externe
  - Demande à l'utilisateur

Service FTP

- **FTP (File Transfer Protocol)**
  - Le premier outil qui a été mis à la disposition des utilisateurs pour **échanger des fichiers** sur TCP/IP
  - Modèle client/serveur
  - Compression et format des données
  - Archie : fonctionnalité qui permet de se faire expédier le résultat de recherches par Email
  - Les serveurs Archie sont quotidiennement informés et mis à jour en temps réel

Service Telnet

- Connexion sur une machine distante en tant qu'utilisateur
- Modèle client/serveur
- En France, hier Minitel, aujourd'hui disponibles via Telnet
- L'adresse URL d'un service telnet est :
- . telnet://login:mot_de_passe@adresse:port
- . Terminal : VT100
- Les ports Telnet :
- . Par défaut, port = 23

Service World Wide Web

- Web = la toile d'araignée
- WWW=World Wide Web=toile d'araignée couvrant le monde entier

- le WWW relie des serveurs HTTP qui envoient des pages HTML à des postes dotés d'un navigateur
  - Le protocole de communication entre les navigateurs et les serveurs est HTTP (Hyper Texte Transfert Protocol)
  - Le langage permettant d'écrire les pages Web est le HTML (Hyper Text Markup Language)

HTTP

- **Comment récupérer une ressource : HTTP**

- **Comment décrire une ressource :**
  - Description interne : ML
  - Description des relations entre ressources HT

- *Remarque : WAP + WML idem pour les mobiles*

HTTP

- **HyperText Transfer Protocol :**
  - 1/0 rfc 1945 (05 1996) : Internet Informal
    - Tim Berners-Lee, Roy T. Fielding, Henry Frystyk
  - 1/1 rfc 2068 (01 1997) : Internet Proposed Standard
    - Fielding, Getty, Mogul, Frystyk, Berners-Lee
    - Connexions persistantes
- **Protocole de type Remote Procedure Call sur TCP**
  - Connexion
  - Requête du client
  - Réponse du serveur
  - Déconnexion

HTTP : Les requêtes

- Format d'une requête
  <Méthode><Chemin><Version_http>↙
  [<Champ_optionnel>: <Valeur>] ↙
  ↙
- Méthodes
  – GET, HEAD, POST, PUT
- Champs optionnels
  – User-Agent, If-Modified-Since, Authorization=XXX

HTTP Les réponses

- Format d'une réponse

  <Version_HTTP><Code_Réponse><Texte> ↙
  Content-Type: <Type_MIME> ↙
  [<Champ_optionnel>: <Valeur>] ↙
  ↙
  <Document>

- Code réponse
  - 100 - 199 : Informatif : 100 Continue
  - 200 - 299 : Requête client réussie : 200 OK, 201 Created
  - 300 - 399 : Requête client redirigée : 301 Moved Permanently, 302 Temporary
  - 400 - 499 : Erreur client : 400 Bad, 401 Unauthorized, 403 forbidden, 404 not found
  - 500 - 599 : Erreur du serveur : 500 Internal Server Error, 501 not implemented

HTTP

- Texte libre : description en anglais du code de réponse
- Champs optionnels du serveur
  - Date de la requête : date
  - Date de modification : Last-Modified
  - Identification du serveur : Server
  - Taille du document : Content-Length
- HTTP/1.1
  - Connexion « Keep-Alive »
  - Gestion fine des caches Web

Exemple HTTP

```
telnet lisiaix0 80
>GET /index.html HTTP/1.0
>User-Agent: libwww/2.12
>
=> HTTP/1.1 200 OK
=> Date: Fri, 11 Feb 1998 18:30:27 GMT
=> Server: Apache/1.2.4
=> Content-Length: 381
=> Content-Type: text/html
=>
=> <HTML>
=>   <BODY>
=>      Bonjour tout le monde ....
=>   </BODY>
=> </HTML>
```


XML : eXtensible Markup Language

- **Idée de base :**
  - Langage de description **générique** des 2 structures d'un document

    - Utiliser les balises pour décrire les données

      <roman>Notre dame de Paris</roman>

- **XSL : Feuille de style pour XML :**
  - Permet l'affichage d'un document XML (sur navigateur)
- **Les logiciels associés :**
  - Editeur de XML
  - Parser de XML

XML : eXtensible Markup Language

- **HTML, Balisage procédural :**
  - codes de formatage (gras, italiques) des traitements de texte traditionnels
  - Codes mélangés au contenu
  - spécifique à un logiciel et à une version du logiciel
  - Echange difficile entre applications hétérogènes

- **XML, Balisage descriptif**
  - Décrit la sémantique du contenu
  - Basé sur la structure hiérarchique du document
  - La structure arborescente du document XML (intitulé des balises, imbrications des balises, caractère obligatoire ou facultatif …) peut être déclarée formellement
  - Sépare le contenu des instructions de traitement (y compris le formatage)
  - Permet validation et navigation de la structure du document

XML : eXtensible Markup Language

- **Langage Ouvert et Extensible**
  - XML utilise le jeux de caractère Unicode (ISO 10646)
  - XML est un méta-langage qui permet d'inventer des jeux de balises et les règles syntaxiques d'utilisation de ces balises
  - Support des grands éditeurs de logiciels

- **Composantes d'une application XML**

  Le document ou instance XML comprend :
  - le prologue pouvant pointer vers une définition de type de document (DTD) (optionnel)
  - le texte balisé selon la structure définie par la DTD
  - Une feuille de style XSL qui transforme le document XML en HTML pour l'affichage sur le browser web

XML : eXtensible Markup Language

- **La Syntaxe d'une DTD**

Décrit rigoureusement la structure d'un document à l'aide des déclarations suivantes :

  - Eléments
  - Attributs
  - Entités générales et de paramètres
  - Commentaires
  - Instructions de traitement

- **Exemple de DTD :**

<!ELEMENT commande (no-pièce+, decription*, quantité, date-livraision?)>

- **Document XML conforme à la DTD ci-dessus :**

```
<commande>
<no-pièce> NAS1104-10D</no-pièce>
<description>Verrou</description>
<quantité>1</quantité>
<date-livraison>1998-04-07T21:30:00</date-livraison>
</commande>
```


XML : eXtensible Markup Language

- **Document XML bien formé :**
  - Sans DTD
  - Contient au moins un élément
  - Imbrication correcte des balises
- **Document Valide :**
  - Possède une DTD
  - L'instance XML suit les règles de la DTD

- **Feuille de Style**
  - Feuille de style référencée dans le document XML par son URL :

    <?xml-stylesheet href="article.xsl" type="text/xsl"?>
  - Permet de présenter le document XML sur un browser web sous format HTML
  - Le **processeur XSL peut être sur le client ou sur le serveur**

XML : eXtensible Markup Language

- **XSLT (*XSL Transformation*)** : langage de transformation normalisé qui va permettre, si nécessaire, de transformer une DTD (un arbre XML) "orientée contenu" en une autre DTD (un autre arbre XML) "orientée restitution" (c'est-à-dire constituée d"objets formateurs" (*formatting objects*).

- **XML Schema** : formalisme qui doit permettre définir des contraintes en matière de syntaxe, de structure et de valeurs applicables à une classe de documents. Il va permettre entre autres choses d'effectuer des contrôles de validité lors de la saisie/mise à jour de documents XML

- **DOM :** Modèle objet de document : un langage normalisé d'interface (API, *Application Programming Interface)* qui va permettre à un programme (Java, ECMAScript…) de naviguer dans un arbre XML (ou HTML) et d'en lire ou d'en modifier le contenu :

  ```
  Book = Doc.documentElement.firstChild;
  Sujet = Book.getAttributeNode("SUBJECT").text
  ...
  ```


XML : eXtensible Markup Language

- Les mécanismes de **lien (*linking*) et d'adressage associés à XML** sont en cours de spécification au sein de trois documents :
  - XPath (XML Path Language). XPath est le langage d'expression de chemins à l'intérieur d'un document XML, destiné à être utilisé à la fois par XSLT et par Xpointer.
  - XPointer (XML Pointer Language). XPointer est le langage d'adressage des contenus d'un document XML.
  - XLink (XML Linking Language). XLink spécifie les indications à insérer dans les ressources XML pour décrire des liens entre objets. Il utilise la syntaxe XML pour créer des structures qui peuvent décrire non seulement des hyperliens unidirectionnels tels que ceux permis aujourd'hui HTML mais aussi des liens plus complexes typés et à terminaisons multiple.

- **Resource Description Framework, Dublin Core, méta-données, ...**
- **Synchronized Markup Integration Language, ...**

XML : eXtensible Markup Language

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<BIBLIO SUBJECT="XML">
    <BOOK ISBN="9782212090819" LANG="fr" SUBJECT="applications">
        <AUTHOR>
            <FIRSTNAME>Jean-Christophe</FIRSTNAME>
            <LASTNAME>Bernadac</LASTNAME>
        </AUTHOR>
        <AUTHOR>
            <FIRSTNAME>François</FIRSTNAME>
            <LASTNAME>Knab</LASTNAME>
        </AUTHOR>
        <TITLE>Construire une application XML</TITLE>
        <PUBLISHER>
            <NAME>Eyrolles</NAME>
            <PLACE>Paris</PLACE>
        </PUBLISHER>
        <DATEPUB>1999</DATEPUB>
    </BOOK>
    <BOOK ISBN="9782212090529" LANG="fr" SUBJECT="général">
    <AUTHOR>
        <FIRSTNAME>Alain</FIRSTNAME>
        <LASTNAME>Michard</LASTNAME>
    </AUTHOR>
    <TITLE>XML, Langage et Applications</TITLE>
    <PUBLISHER>
        <NAME>Eyrolles</NAME>
        <PLACE>Paris</PLACE>
    </PUBLISHER>
    <DATEPUB>1998</DATEPUB>
    </BOOK>
</BIBLIO>
```


Caractéristiques d'un protocole

- **Nom** : Simple Mail Transfert Protocol
- **Rfc** : 1830, 1845, 1846
- **Mode de fonctionnement** : Connecté
- **Port de connexion** : 25
- **Commande / Requêtes** : EXPN, QUIT, HELO...
- **Client** : Eudora
- **Serveur** : Sendmail

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

Chapitre 9

Administration, Sécurité : Quelques mots . . .

La sécurité dans les Réseaux

- Risques et Menaces :
  - vulnérabilité : degré d'exposition à des dangers
  - sensibilité : caractère stratégique d'un élément
  - menaces passives : écoute des informations
  - menaces actives : modification de l'intégrité des données

La sécurité dans les Réseaux

- Des garanties doivent être fournies :
  - authentification
  - contrôle d'accès
  - confidentialité des données
  - intégrité des données
  - non répudiation

→ login + mot de passe
→ droits d'accés par utilisateur
→ signature de messages
→ chiffrement de message

- Certificats, SSL, … → ***Voir cours Transmission de l 'info***

Administration de réseau

L'administration de réseaux et de systèmes recouvre l'ensemble des activités de surveillance, d'analyse, de contrôle et de planification du fonctionnement des ressources d'un réseau dans le but de fournir aux usagers des services avec un certain niveau de qualité.

- 5 aires fonctionnelles :
  - **la configuration** : la capacité à maîtriser le système et à recueillir des informations sur son état.
  - la **détection et la correction des anomalies** dans le système. Les fautes proviennent des pannes de composants matériels et logiciels et se manifestent par des erreurs qui doivent être captés, analysés afin de dresser un diagnostic.
  - la **mesure de la performance** du système doit permettre d 'évaluer la charge du réseau et l'efficacité de la communication.
  - la **sécurité du réseau** notamment la gestion des privilèges d'accès, en rendant compte des tentatives d'accès illicite et intrusions dans le réseau
  - la **comptabilité** pour établir des relevés de taxation et surveiller l'évolution de l'utilisation du réseau.

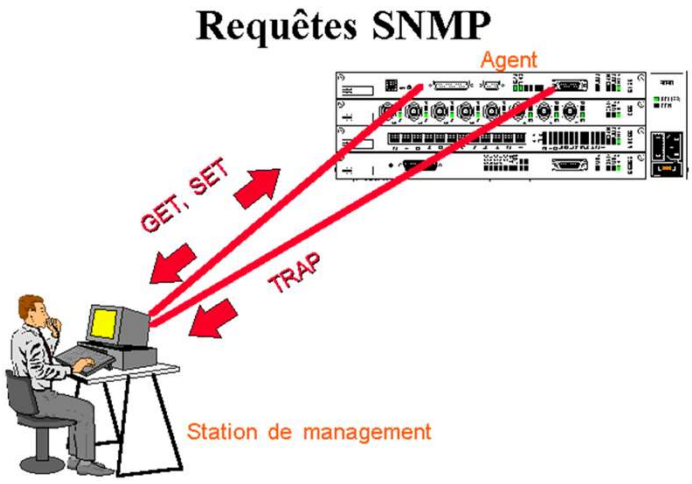
Administration de réseau

- Le Quoi ?
  - les équipements
  - les réseaux, les clients
  - les services, les applications
- Le Comment ?
  - des modèles
  - des normes (CMIP, MIB, SNMP, …)
  - des activités (maintenance, surveillance, planification, …)
  - des outils
- Le Pourquoi ?
  - QoS

Administration de réseau

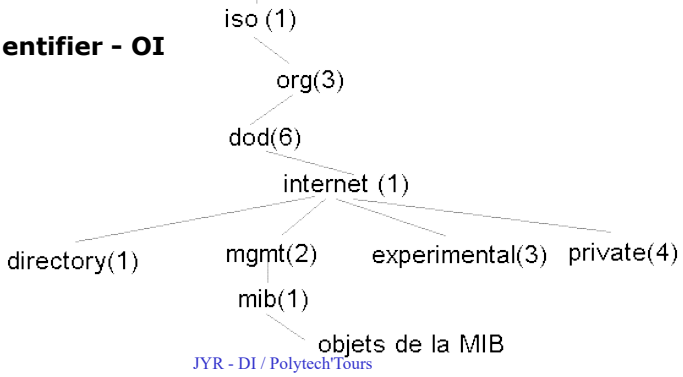
- La notion de Qualité de Services **QoS** est de plus en plus importante :
  - **délai et disponibilité :** le réseau choisi garantit-il une bande passante ?
  - **capacité et fiabilité :** Le réseau gère t il les congestions / les erreurs ?
  - **sécurité** : le réseau choisi est il sure/sécurisé ?
- Exemples :
  - Flux vidéo, audio, multimédia : RTP : Real Time Protocol, ATM, ...
  - Confidentialité des échanges : IPv6, IPsec, ...
  - C 'est la grosse différence entre **IP et ATM** ...

Administration SNMP (par IETF pour IP)



Administration SNMP

- **MIB - Management Information Base :**
  - La MIB : ensemble des variables permettant de définir l'état d'un nœud du réseau
  - Une partie standard, commune à tous les nœuds
  - Une partie optionnelle : spécificité d'un nœud
- **Object Identifier - OI**



Administration SNMP

- Chaque objet de la MIB est identifié par une suite de nombre qui indique une arborescence qui va de *ISO* à l'objet considéré en passant par *ORG* (Organisations), *DOD*, *INTERNET* et *MGMT*
- **Commandes :**
  - **get (var [,var,...])** requête de lecture de "var" qui déclenche une réponse de l'agent SNMP concerné
  - **get-next (var [,var,...])** retourne, le nom de la variable suivante, mais pas sa valeur. *get-next* permet de traverser toute la hiérarchie d'une MIB
  - **set (var,val, [, var,val,..])** modifie la valeur de la variable, donc son comportement (Ex.: configuration d'un port à distance)
  - **trap (code)** code envoyé à la station de management en cas d'événement exceptionnel
- **CMIP :** Common Management Info Protocol par ISO (idem SNMP)

Chapitre 9

Administration, Sécurité : Quelques mots . . .

La sécurité dans les Réseaux

- Risques et Menaces :
  - vulnérabilité : degré d'exposition à des dangers
  - sensibilité : caractère stratégique d'un élément
  - menaces passives : écoute des informations
  - menaces actives : modification de l'intégrité des données

La sécurité dans les Réseaux

- Des garanties doivent être fournies :
  - authentification → login + mot de passe
  - contrôle d'accès → droits d'accés par utilisateur
  - confidentialité des données → signature de messages
  - intégrité des données → chiffrement de message
  - non répudiation
- Certificats, SSL, … → ***Voir cours Transmission de l 'info***

Administration de réseau

L'administration de réseaux et de systèmes recouvre l'ensemble des activités de surveillance, d'analyse, de contrôle et de planification du fonctionnement des ressources d'un réseau dans le but de fournir aux usagers des services avec un certain niveau de qualité.

- 5 aires fonctionnelles :
  - **la configuration** : la capacité à maîtriser le système et à recueillir des informations sur son état.
  - la **détection et la correction des anomalies** dans le système. Les fautes proviennent des pannes de composants matériels et logiciels et se manifestent par des erreurs qui doivent être captés, analysés afin de dresser un diagnostic.
  - la **mesure de la performance** du système doit permettre d 'évaluer la charge du réseau et l'efficacité de la communication.
  - la **sécurité du réseau** notamment la gestion des privilèges d'accès, en rendant compte des tentatives d'accès illicite et intrusions dans le réseau
  - la **comptabilité** pour établir des relevés de taxation et surveiller l'évolution de l'utilisation du réseau.

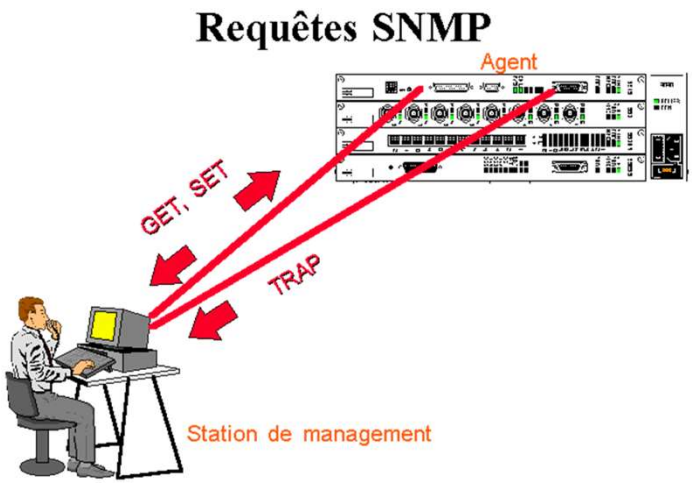
Administration de réseau

- Le Quoi ?
  - les équipements
  - les réseaux, les clients
  - les services, les applications
- Le Comment ?
  - des modèles
  - des normes (CMIP, MIB, SNMP, …)
  - des activités (maintenance, surveillance, planification, …)
  - des outils
- Le Pourquoi ?
  - QoS

Administration de réseau

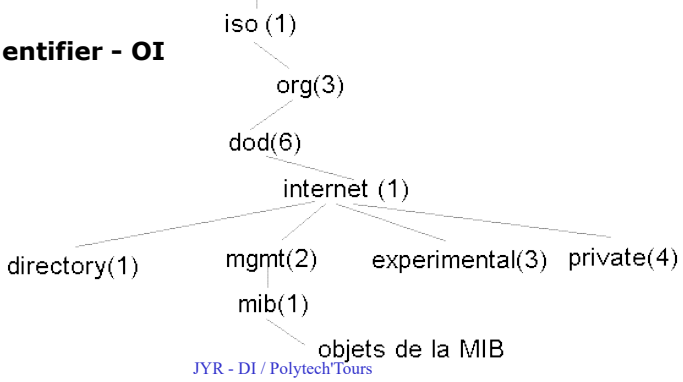
- La notion de Qualité de Services **QoS** est de plus en plus importante :
  - **délai et disponibilité :** le réseau choisi garantit-il une bande passante ?
  - **capacité et fiabilité :** Le réseau gère t il les congestions / les erreurs ?
  - **sécurité** : le réseau choisi est il sure/sécurisé ?
- Exemples :
  - Flux vidéo, audio, multimédia : RTP : Real Time Protocol, ATM, ...
  - Confidentialité des échanges : IPv6, IPsec, ...
  - C 'est la grosse différence entre **IP et ATM** ...

Administration SNMP (par IETF pour IP)



Administration SNMP

- **MIB - Management Information Base :**
  - La MIB : ensemble des variables permettant de définir l'état d'un nœud du réseau
  - Une partie standard, commune à tous les nœuds
  - Une partie optionnelle : spécificité d'un nœud
- **Object Identifier - OI**



Administration SNMP

- Chaque objet de la MIB est identifié par une suite de nombre qui indique une arborescence qui va de *ISO* à l'objet considéré en passant par *ORG* (Organisations), *DOD*, *INTERNET* et *MGMT*
- **Commandes :**
  - **get (var [,var,...])** requête de lecture de "var" qui déclenche une réponse de l'agent SNMP concerné
  - **get-next (var [,var,...])** retourne, le nom de la variable suivante, mais pas sa valeur. *get-next* permet de traverser toute la hiérarchie d'une MIB
  - **set (var,val, [, var,val,..])** modifie la valeur de la variable, donc son comportement (Ex.: configuration d'un port à distance)
  - **trap (code)** code envoyé à la station de management en cas d'événement exceptionnel
- **CMIP :** Common Management Info Protocol par ISO (idem SNMP)

Chapitre 10

Brèves descriptions d'autres réseaux

Dans les ateliers …

FIP (Flux d'Informations Processus)

Projet français lancé par le ministère de l'industrie

→ cible = réseaux de terrain

Objectif

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

2) Très faible coût => circuit intégré.

Bilan actuel : projet très bien menés → possibilité de normalisation pour les réseaux de terrains (déjà une norme française : AFNOR 46-601 à 607).

FIP (Flux d'Informations Processus)

Fonctionnement

- 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)

Architecture

Il existe uniquement les niveaux 1,2 et 7 :

- **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.

FIP (Flux d'Informations Processus)

Architecture

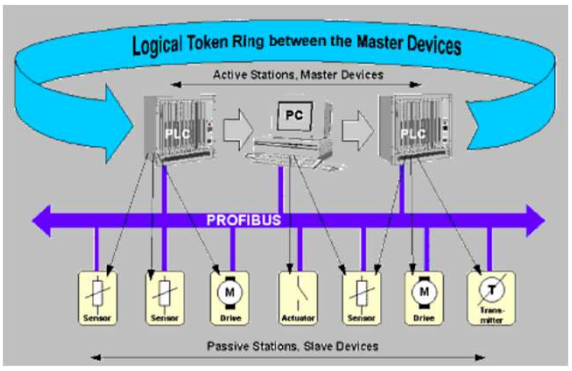
- **Couche application**
  - Cette couche offre à l'utilisateur des services de gestion des objets manipulés par les stations, de surveillance des transmissions, de synchronisation, et de communication point à point.

CAN

- Voir DI5 ….

Profibus

- **Un autre réseau de terrain :**
  - → Architecture en bus
  - → Maitre / Esclave entre automates et périphériques
  - → Jeton sur bus entre automates



→ Débits : 1Mb/s (RS485) jusqu'à 12 Mb/s (fibre optique)

→ Nombre de stations : 32 environs

Chapitre 5

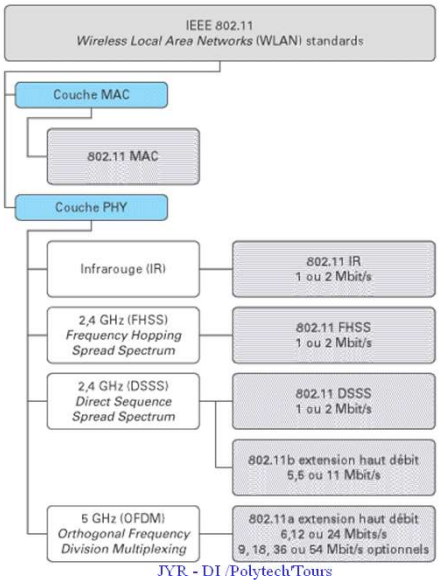
Réseaux sans fil :

Wifi (802.11), Bluetooth (802.15), ...

WiFi = *Wireless Fidelity*

- Standard international décrivant les caractéristiques d'un réseau local sans fil (*WLAN*)
- WECA (*Wireless Ethernet Compatibility Alliance*) : organisme chargé de maintenir l'interopérabilité entre les matériels
- Liaison haut débit (11 Mbps) 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.
- Zones d'accès appelées "hot spots"

WiFi = *Wireless Fidelity*



WiFi = *Wireless Fidelity*

- **Couche Liaison de données (MAC)**
  - 802.2 (CSMA/CA ou *Point Coordination Function - PCF*)
  - 802.11
- **Couche Physique(PHY)**
  - DSSS
  - FHSS
  - Infrarouges

- La norme *IEEE 802.11* est en réalité la norme initiale offrant des débits de 1 ou 2 Mbps.
  - Des révisions ont été apportées à la norme originale afin d'optimiser le débit (c'est le cas des normes 802.11a, 802.11b et 802.11g, appelées normes 802.11 physiques)
  - ou bien préciser des éléments afin d'assurer une meilleure sécurité ou une meilleure interopérabilité.

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 rééls) 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*)

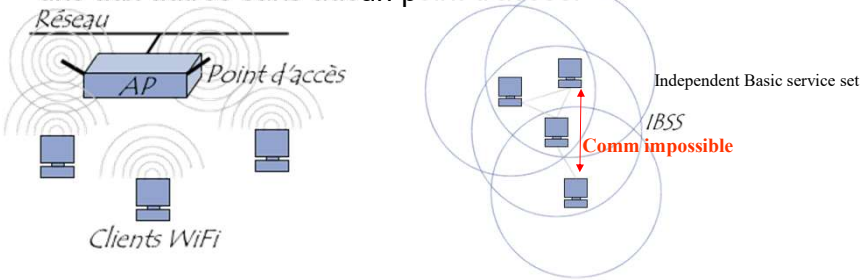
- **802.11e -** Amélioration de la qualité de service
  - La norme 802.11e vise à donner des possibilités en matière de qualité de service au niveau de la couche *liaison de données*. Ainsi cette norme a pour but de définir les besoins des différents paquets en terme de bande passante et de délai de 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 offrira un haut débit (54 Mbps théoriques, 30 Mbps réels) sur la bande de fréquence des 2.4 GHz. Cette norme n'a pas encore été validée, le matériel disponible avant la finalisation de la norme risque ainsi de devenir obsolète si celle-ci est modifiée ou amendée. 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
- **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

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 *802.11j* 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.

Modes opératoires

- Le standard 802.11 définit deux modes opératoires :
  - Le mode infrastructure 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 dans lequel les clients sont connectés les uns aux autres sans aucun point d'accès.

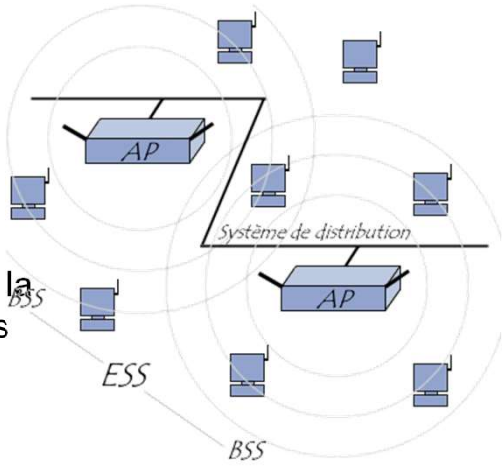


Mode Infrastructure

– *Station = trame probe request (arrivée)*

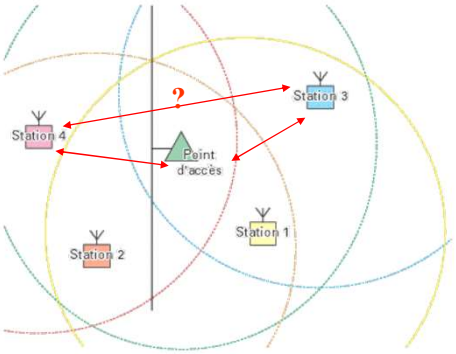
– AP = trame beacon (horloge)

– 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

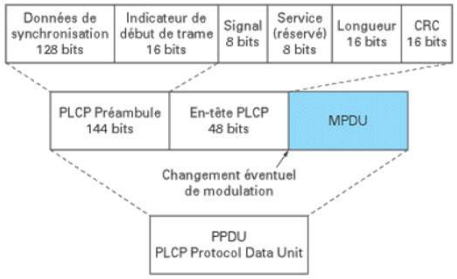


Mode Infrastructure

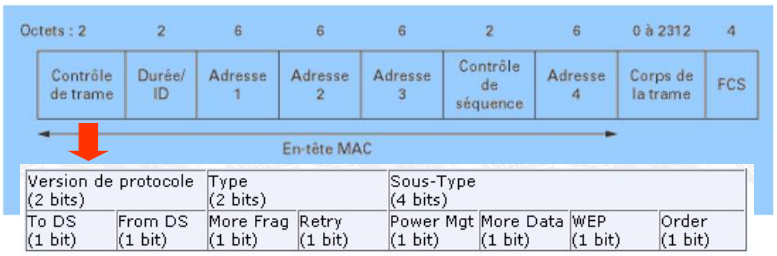
- Station cachée + parasitage :
  - RTS → CTS
  - ACK systématique



Format des Trames



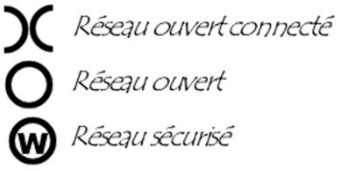
Physical Layer Convergence Protocol



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)

Sécurité

- 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
- Attaques :
  - War-driving
- Parades :
  - Pas de valeurs par défaut
  - Filtrage MAC
  - WEP - Wired Equivalent Privacy
  - VPN



Quelques mots sur

QUI ETAIT BLUETOOTH ?

- Harald Blaatand « Bluetooth » II
- Roi du Danemark de 940 à 981
- A toujours souhaité unir le Danemark et la Norvège
- Inspiration pour la technologie : unir des appareils différents
- Toujours les dents bleues car il mangeait des mûres …..

Historique

- ***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 2000 entreprises dans le SIG

CONCEPTS DE BLUETOOTH

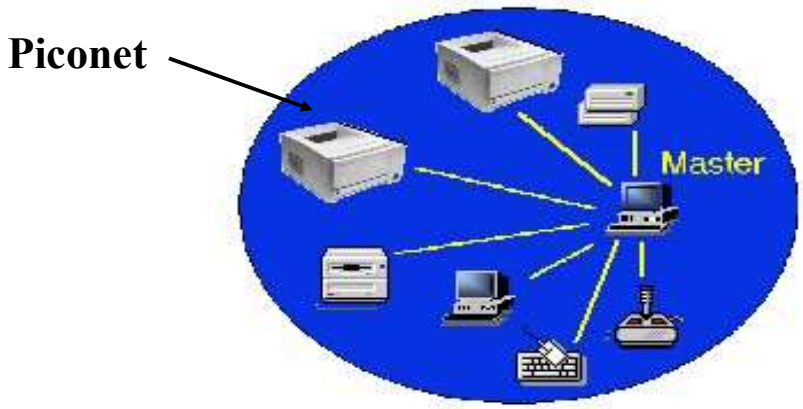
- Remplacement des câbles
- constitution de réseau sans fil
- faire communiquer tout type d 'appareils munis de carte Bluetooth
  - PC, ordinateurs portables
  - Téléphones Portables
  - PDA
  - montres …...

CONCEPTS DE BLUETOOTH

- 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
- 1 seul « maître », les autres sont des esclaves

  Plusieurs piconet forment un **scatternet**

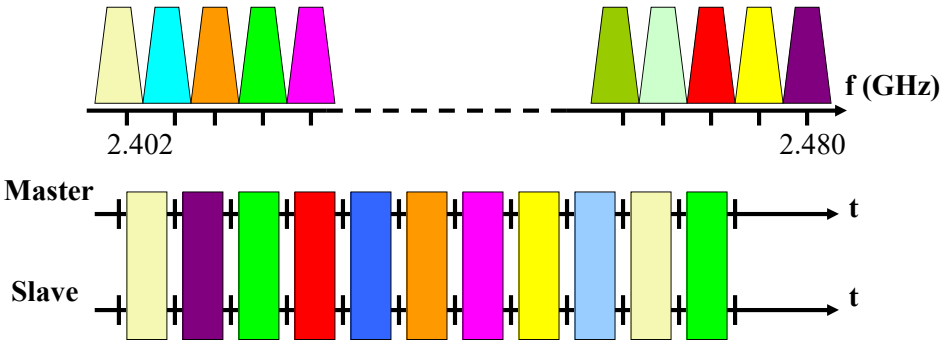
CONCEPTS DE BLUETOOTH



NOTIONS DE BASE

Transfert de données selon deux mécanismes :

- Frequency hopping (saut de fréquence)
- TDD (time duplex division)



TYPES D 'ECHANGES DE DONNEES

But : *communications multimédia*
(voix / data / image)

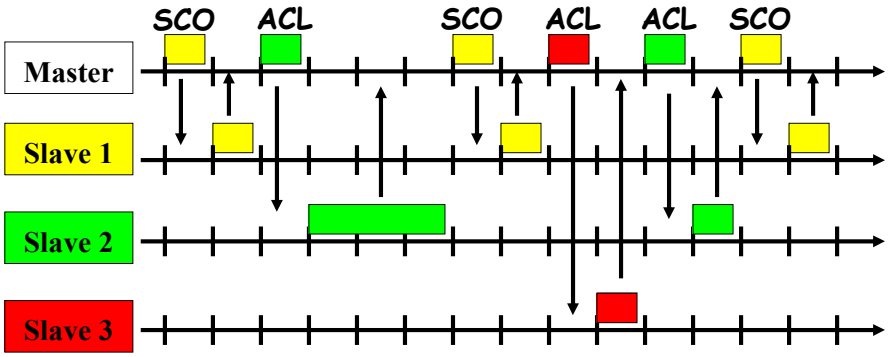
Mode connecté
principalement pour la voix

Mode non connecté
data et images

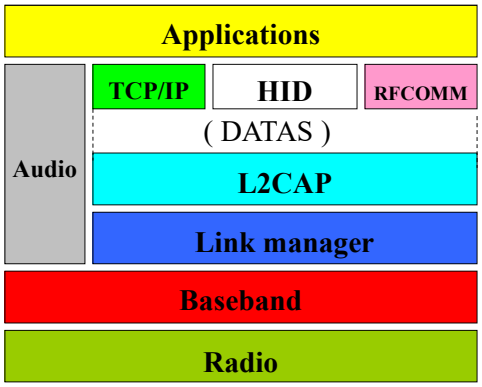
TYPES D 'ECHANGES DE DONNEES

- Les 2 modes existent sous Bluetooth :
  - ACL : asynchronous connection less link
    - Sans connexion
    - échanges asynchrones, (a)symétrique
    - accès au canal par polling
  - SCO : synchronous connection oriented link
    - Avec connexion
    - échanges symétriques et synchrones
    - accès au canal par réservation de slots à intervalles fixes

MULTIPLEXAGE DE LIAISONS



PILE PROTOCOLAIRE
VUE SIMPLIFIEE



COUCHE RADIO

- Couche la plus basse : assure la radio transmission (couche physique)
- FSK : modulation fréquentielle
- Opère dans la bande de fréquence des **2,4 GHz**
- ***Bande ISM*** : « industrial, scientific, Medical » : micro-ondes, téléphones sans fils, ouvertures de garage …. Bande sans licence d 'exploitation
- La bande ISM est mondiale donc Bluetooth est internationalement interopérable

COUCHE BASEBAND

Couche la plus importante de Bluetooth

- gère les canaux physiques
- contrôle les liens existants : synchrones ou asynchrones
- gère les ajouts d 'appareils dans le picoréseau
- Gère le Time Duplex Division et les sauts de fréquence

COUCHE BASEBAND

- Constitution de la trame « baseband »

- ***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

TYPES DE PDU ET DEBITS ASSOCIES

- Le champs « en-tête » permet de spécifier des adresses, champs de contrôle, le type de connexion (ACL ou SCO) ainsi que les débits associés :
  - SCO : les débits peuvent être 64 kbps, 128 kbps ou 196 kbps (typiquement pour la voix)
  - ACL : Débits symétriques ou assymétriques jusqu'à 196 kbps

TYPES DE PDU ET DEBITS ASSOCIES

- Le maître ne peut supporter que 3 liaisons SCO au maximum dans un piconet
- Il peut établir une liaison ACL avec chacun des esclaves
- Les paquets SCO ne sont jamais réémis (contraintes pour la voix)
- Paquets ACL réémis : contraintes des datas

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**

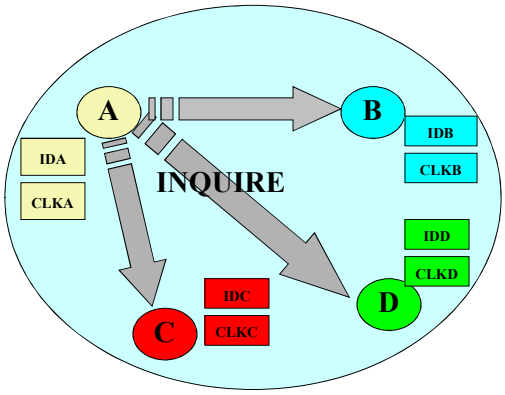
COUCHE L2CAP

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

EXEMPLE : AJOUT D ’UN APPAREIL DANS UN PICONET

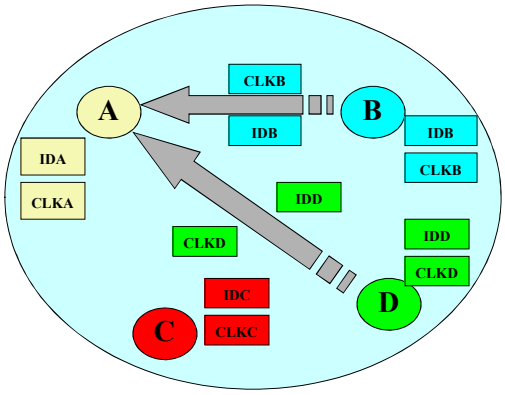
- (1) : Le maître scanne l ’espace :

« inquiring »



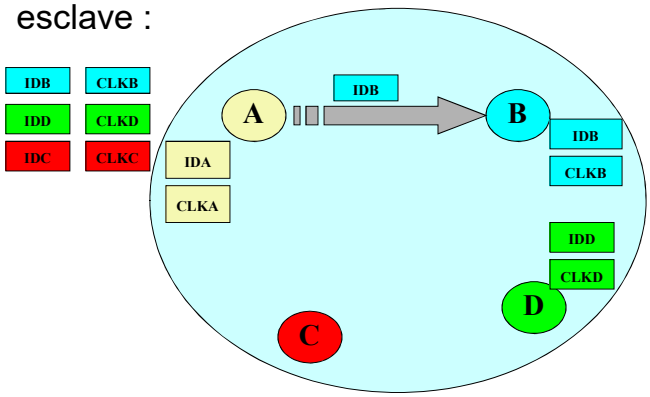
EXEMPLE : AJOUT D ’UN APPAREIL DANS UN PICONET

- (2) : Le maître écoute les réponses



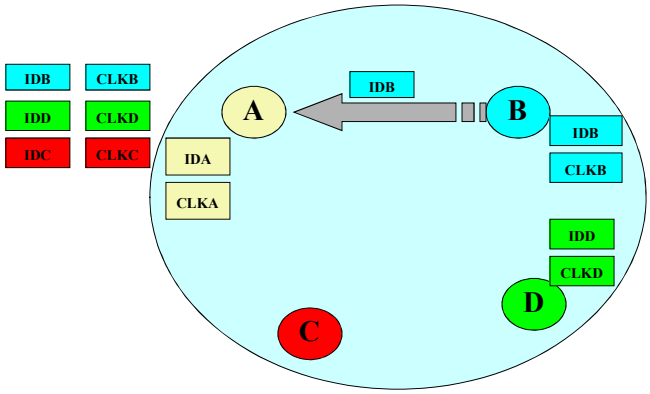
EXEMPLE : AJOUT D ’UN APPAREIL DANS UN PICONET

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



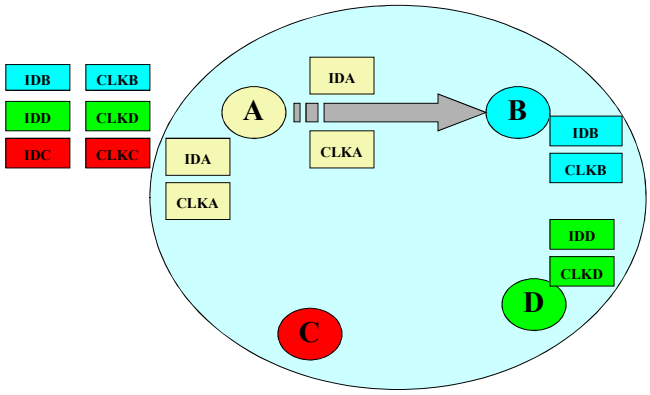
EXEMPLE : AJOUT D ’UN APPAREIL DANS UN PICONET

- (3) L ’esclave B est bien joignable



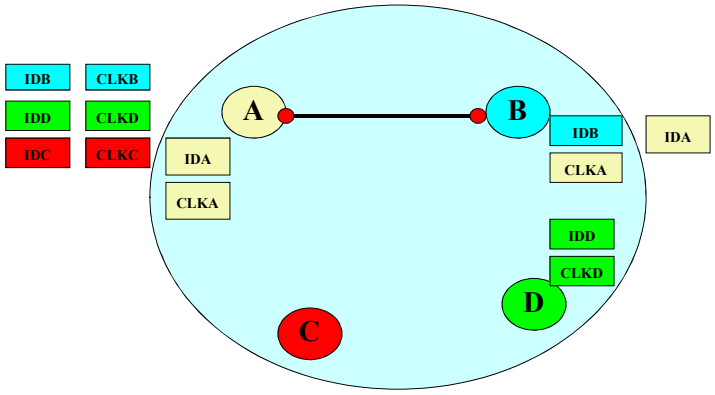
EXEMPLE : AJOUT D ’UN APPAREIL DANS UN PICONET

- (3) le maître ajoute l ’esclave B



EXEMPLE : AJOUT D ’UN APPAREIL DANS UN PICONET

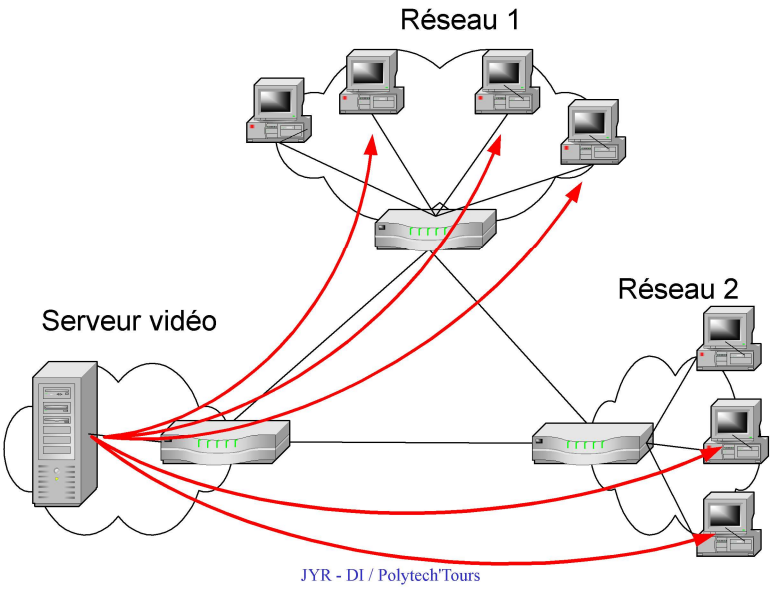
- (4) Liaison effective entre A et B



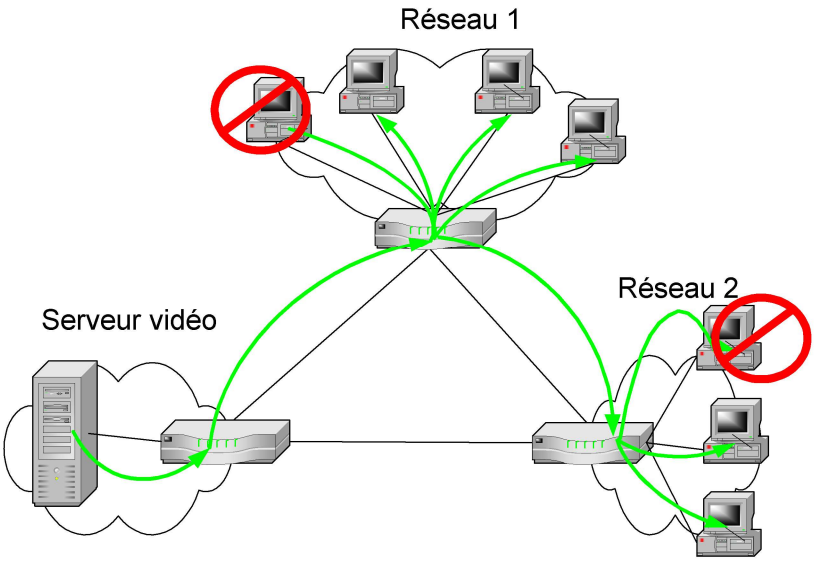
Chapitre 11 :
Le Multicast sur IP

Le multicast, Pourquoi ?

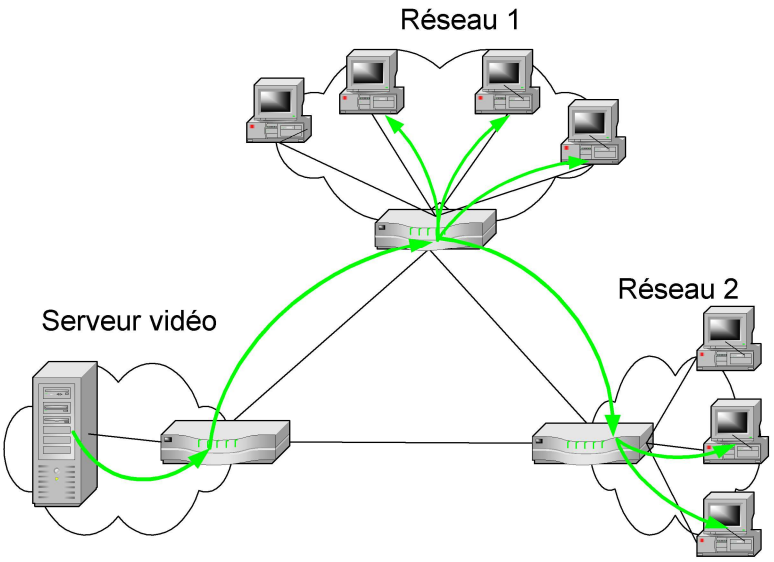
Multicast vs Unicast



Multicast vs Broadcast

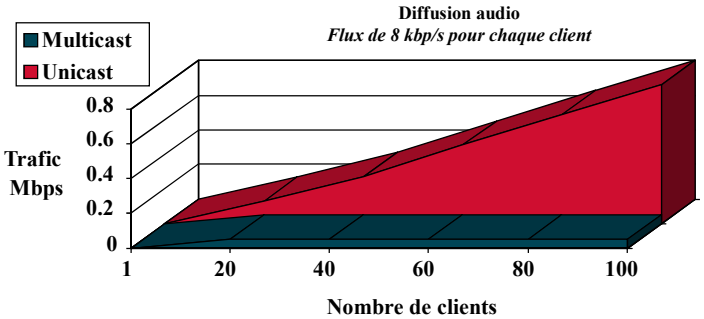


Multicast



Avantages du Multicast

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



Domaine d'application

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

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

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

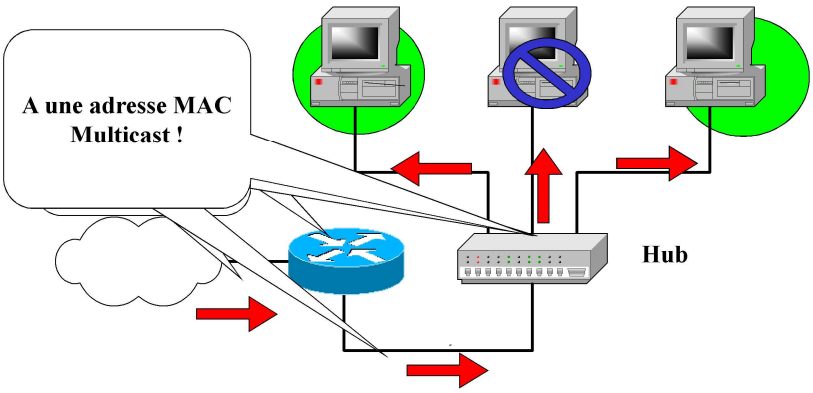
Adressage Multicast

L'adressage

- *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*

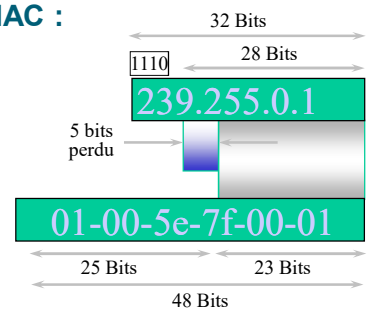


L'adressage

- **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 :**



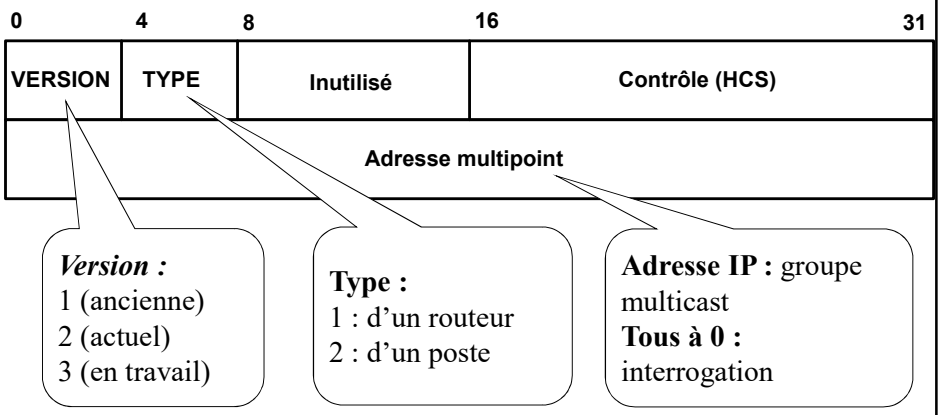
La signalisation : IGMP

IGMP

- **Signalisation entre routeurs et ordinateurs**
  - Choisir
  - Maintenir
  - et Quitter un groupe
- **Trames IGMP**
  - De même niveau qu'ICMP
  - Encapsulée dans des trames IP

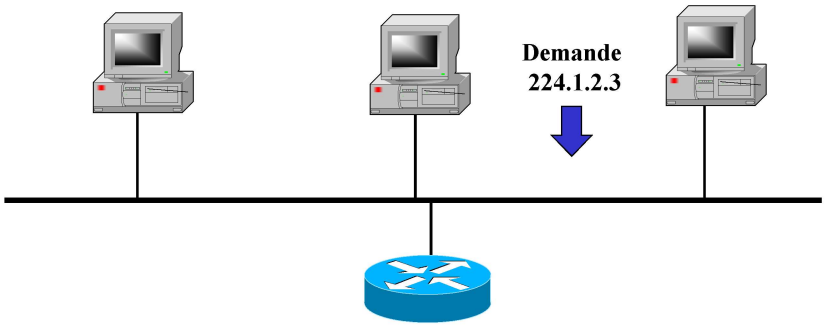
IGMP

- ***Trames IGMP :***



IGMP

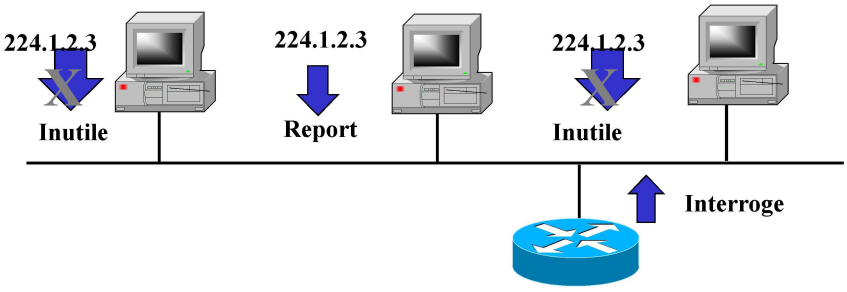
Rejoindre un groupe



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

IGMP

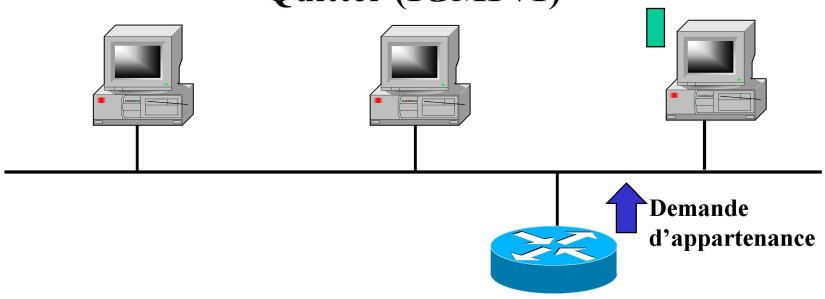
Maintenir



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

IGMP

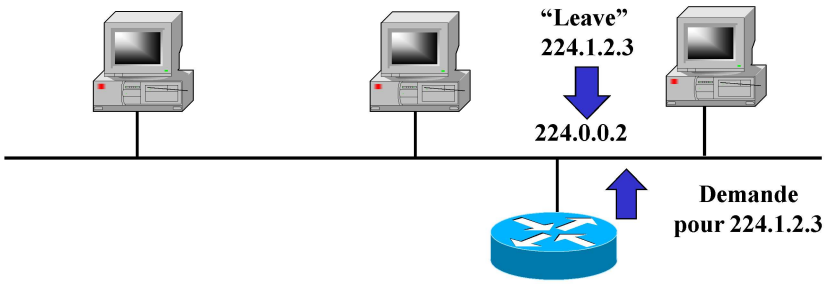
Quitter (IGMPv1)



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

IGMP

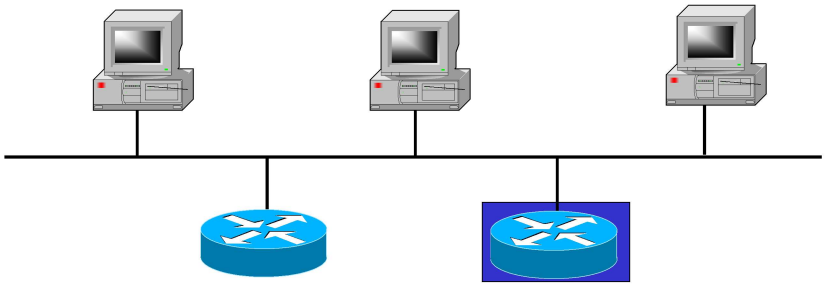
Quitter (IGMPv2)



- 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

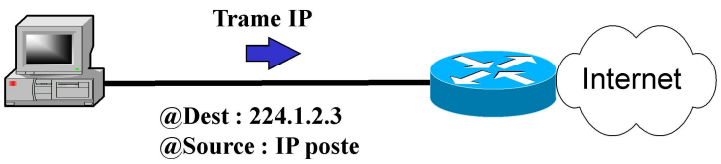
Cas de plusieurs routeurs



- **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

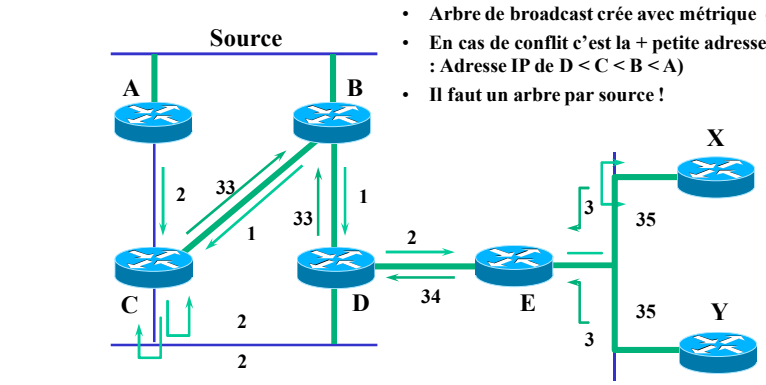
Types de protocoles

- **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



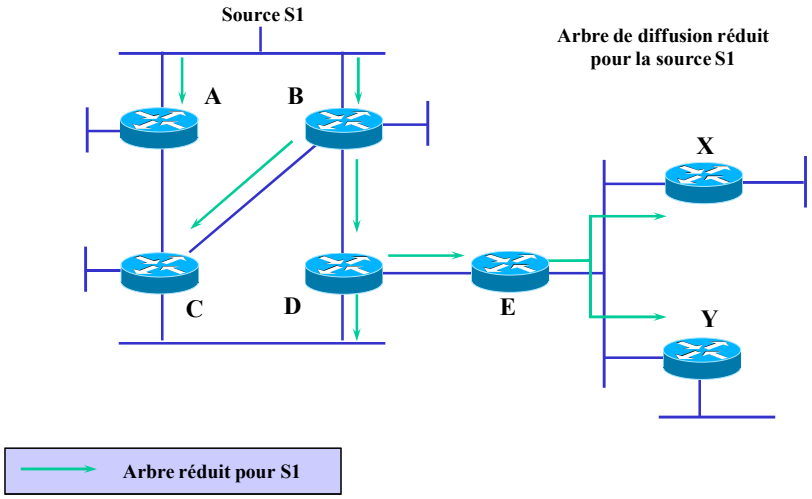
- **Arbre de broadcast crée avec métrique de chaque ligne**
- **En cas de conflit c'est la + petite adresse IP qui gagne. Ici : Adresse IP de D < C < B < A)**
- **Il faut un arbre par source !**

n — **Chemin depuis la source de métrique "n"**

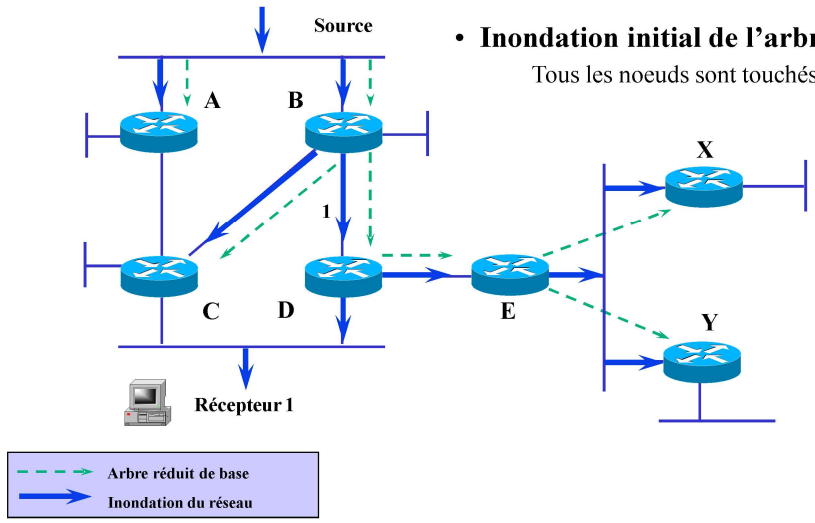
m — **Retour (métrique + 32 (infini)) envoyé aux parents après le choix.**

Arbre réduit pour LA source 1.

DVMRP : Création de l'arbre réduit

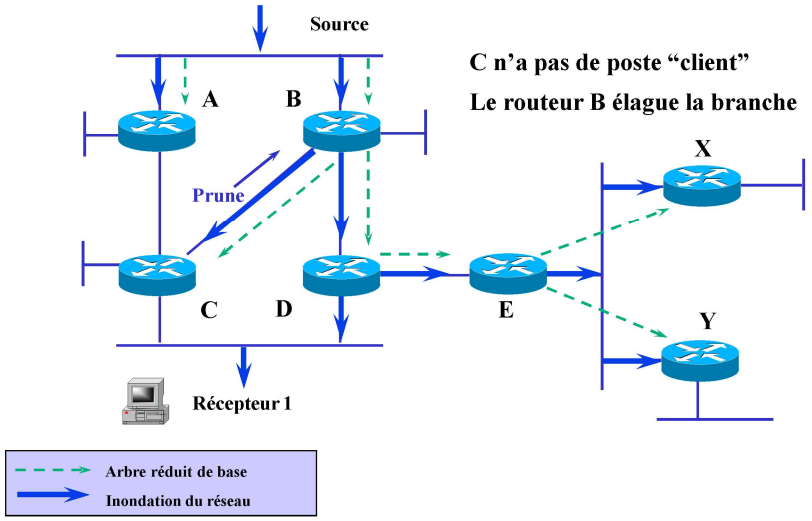


DVMRP : Élagage



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

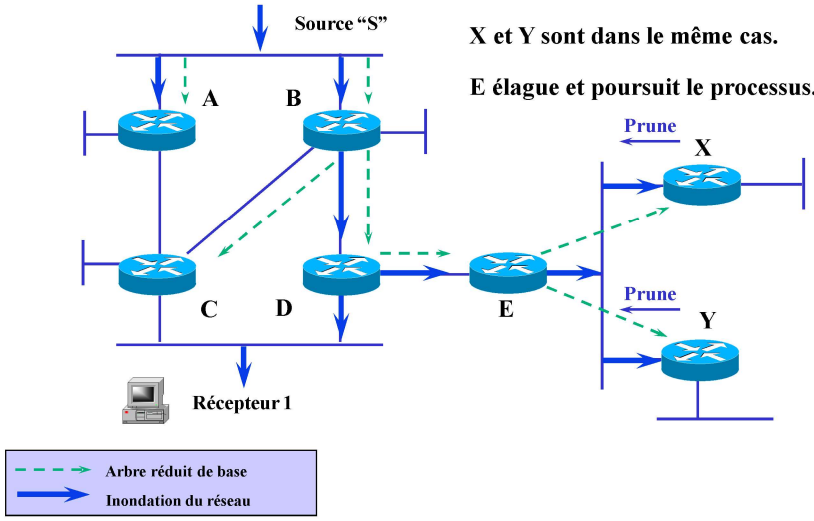
DVMRP : Élagage



C n'a pas de poste "client"

Le routeur B élague la branche

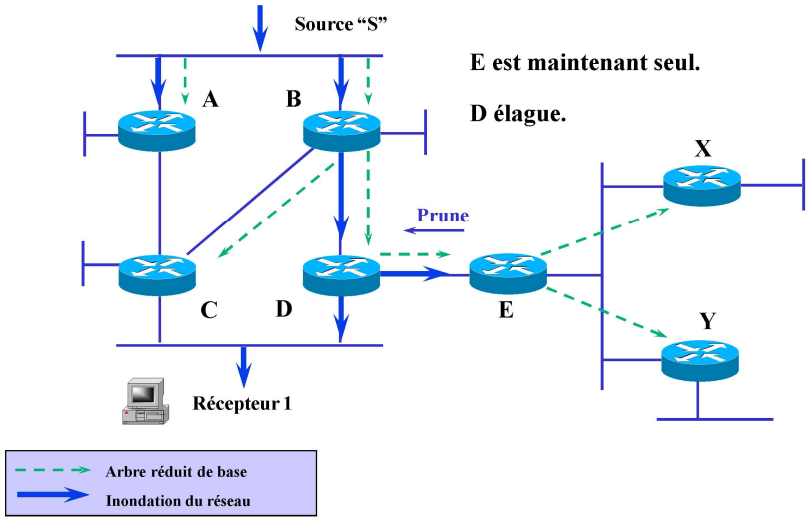
DVMRP : Élagage



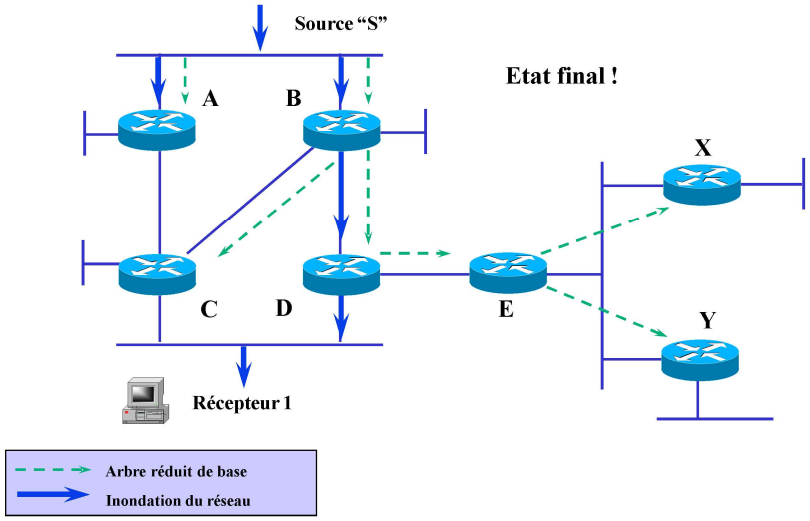
X et Y sont dans le même cas.

E élague et poursuit le processus.

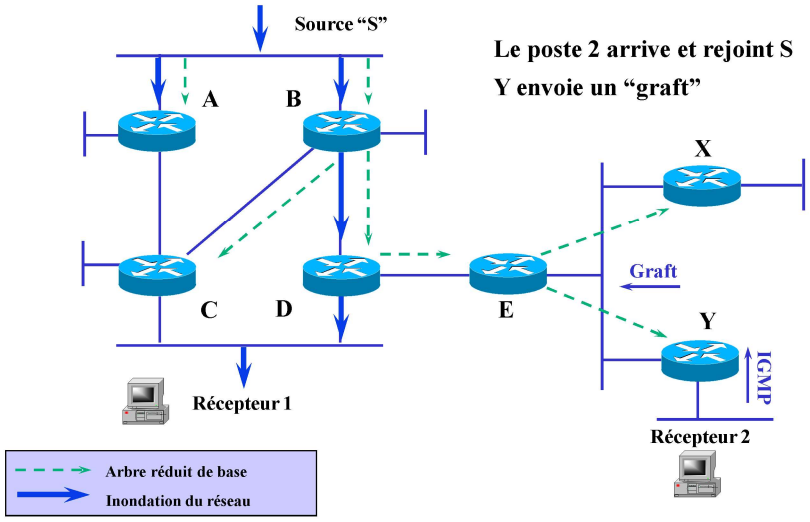
DVMRP : Élagage



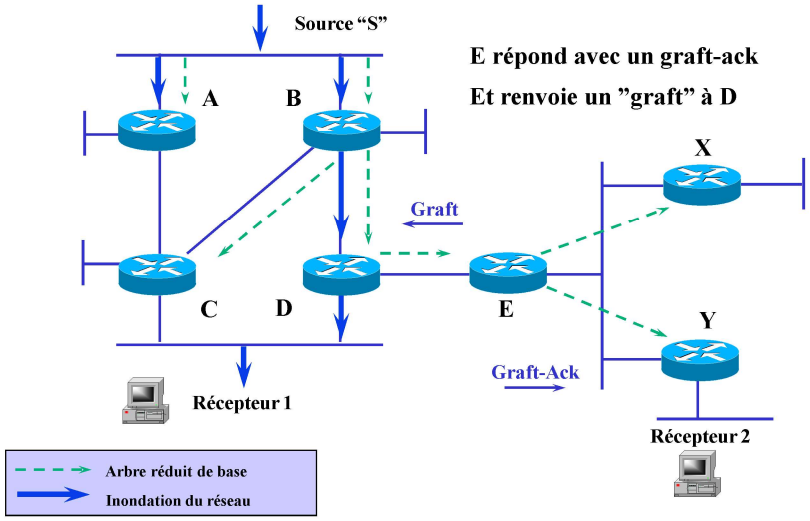
DVMRP : Élagage



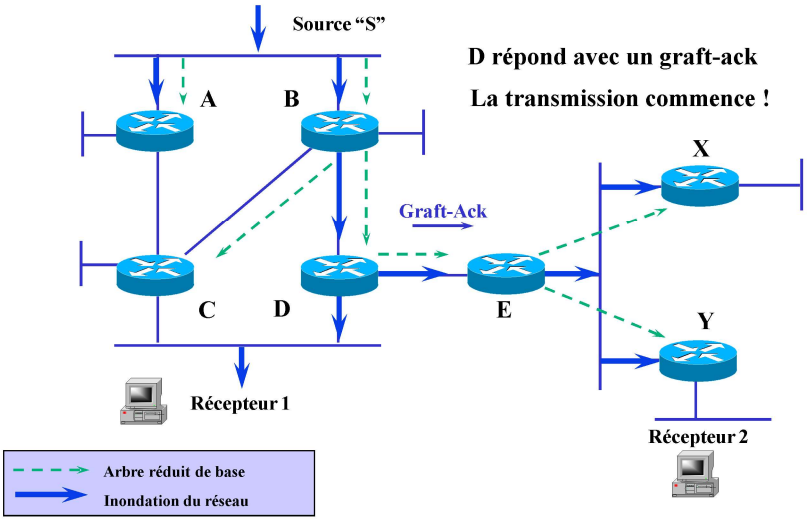
DVMRP : Greffe



DVMRP : Greffe



DVMRP : Greffe



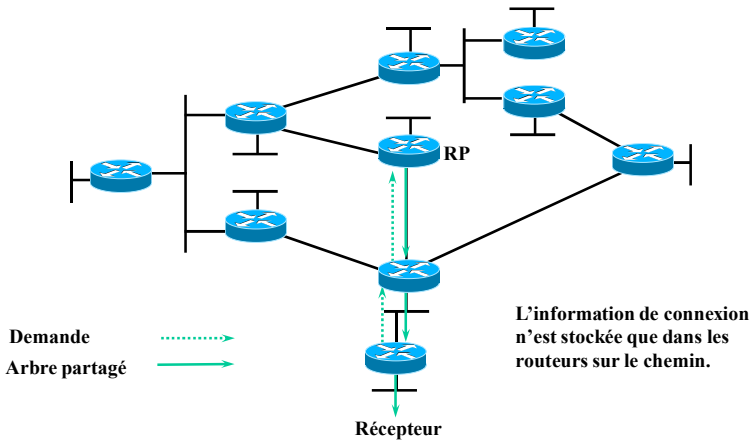
DVMRP

- 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)

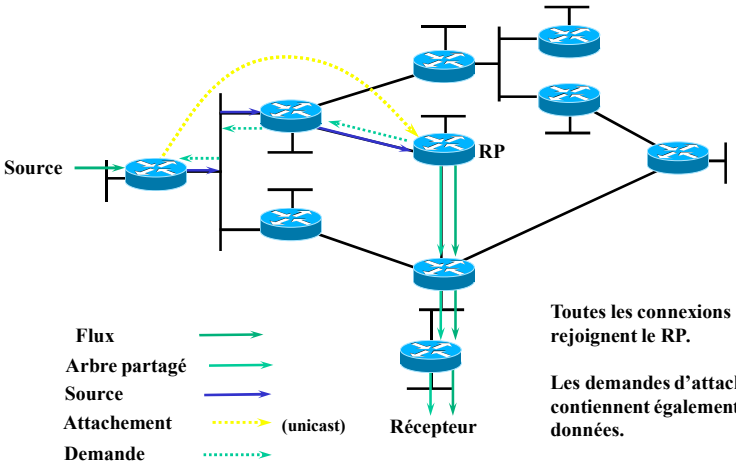
PIM : Protocol Independent Multicast

- **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



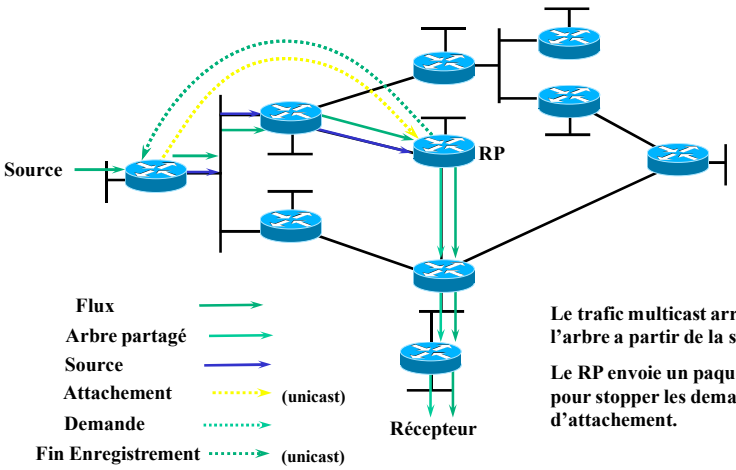
PIM SM : Enregistrement



Toutes les connexions rejoignent le RP.

Les demandes d'attachement contiennent également des données.

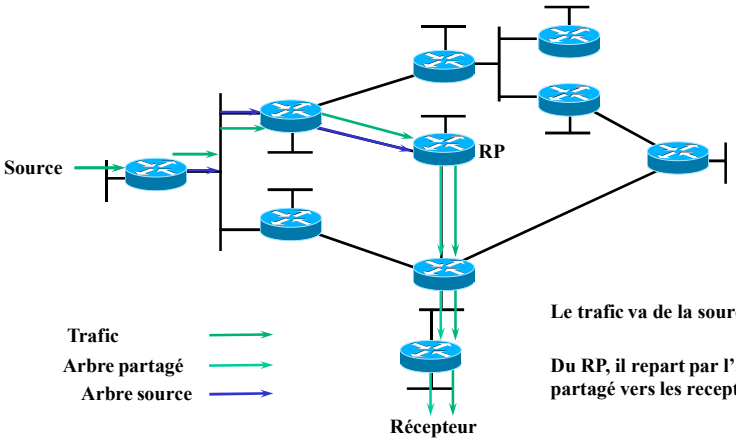
PIM SM : Enregistrement



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

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

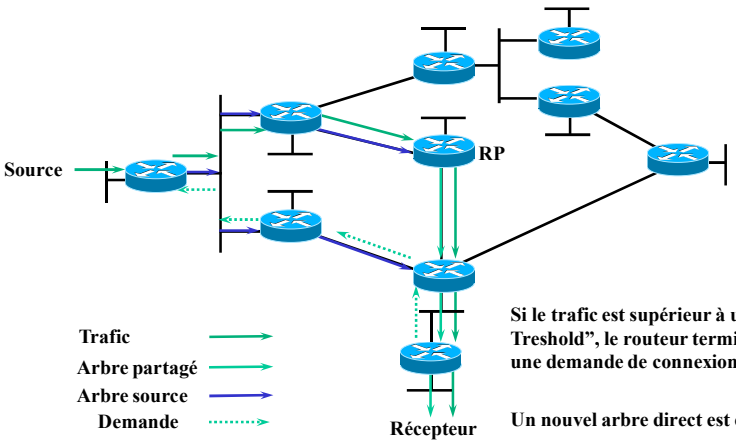
PIM SM : Enregistrement



Le trafic va de la source au RP.

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

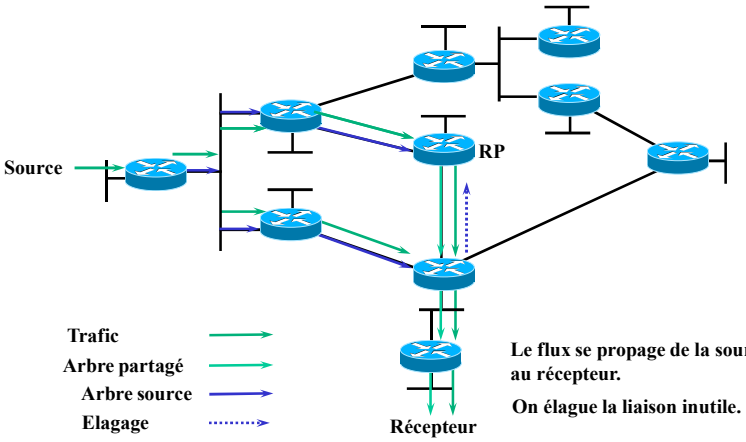
PIM SM : Saut du RP



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.

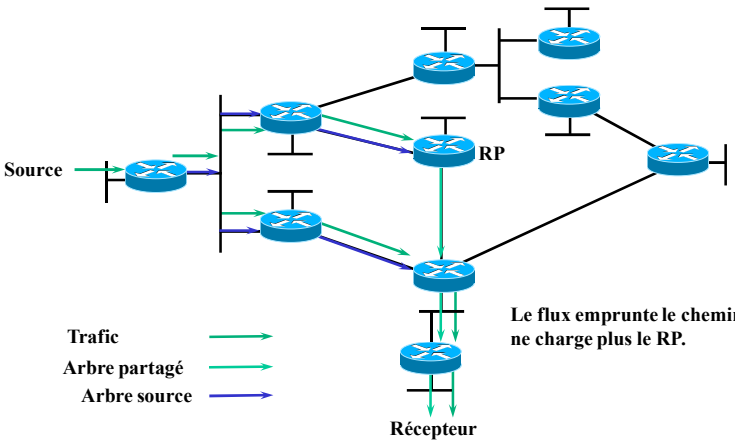
PIM SM : Saut du RP



Le flux se propage de la source au récepteur.

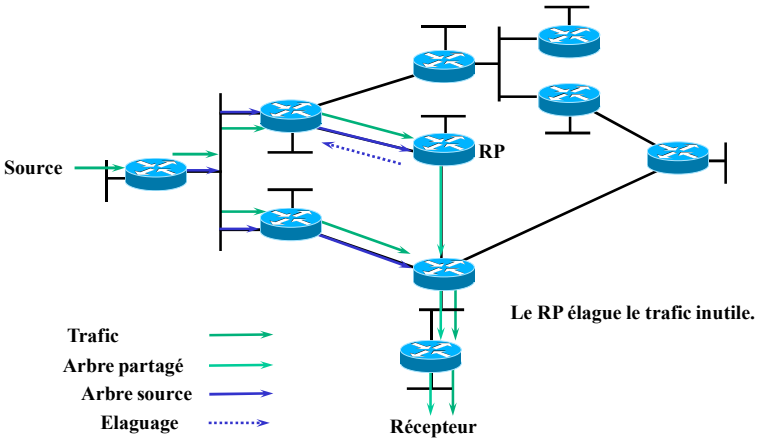
On élague la liaison inutile.

PIM SM : Saut du RP

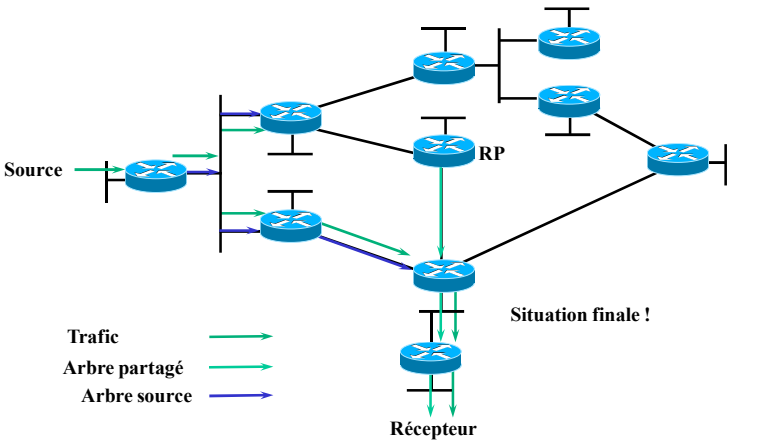


Le flux emprunte le chemin direct et ne charge plus le RP.

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

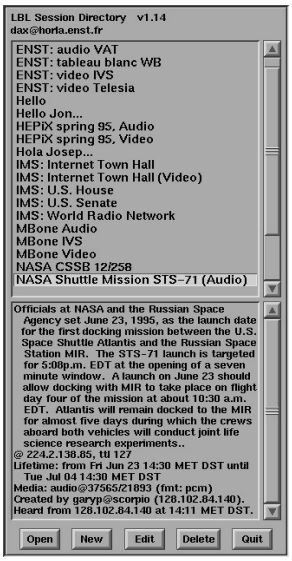
- **Contraintes :**
  - Niveau 2 : Ethernet (carte réseau)
  - Niveau 3 : IGMP, …

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

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

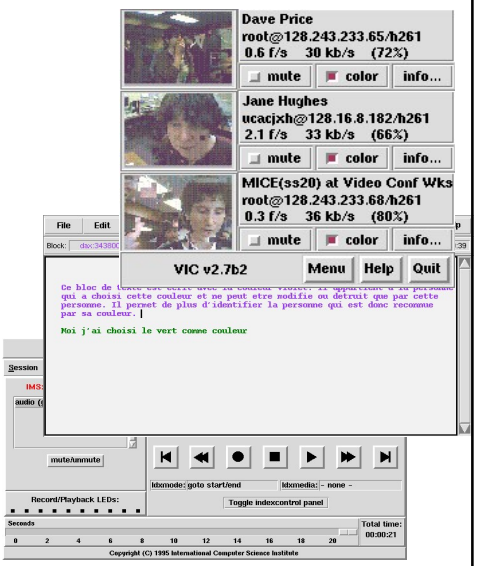
Applications : SDR

- **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

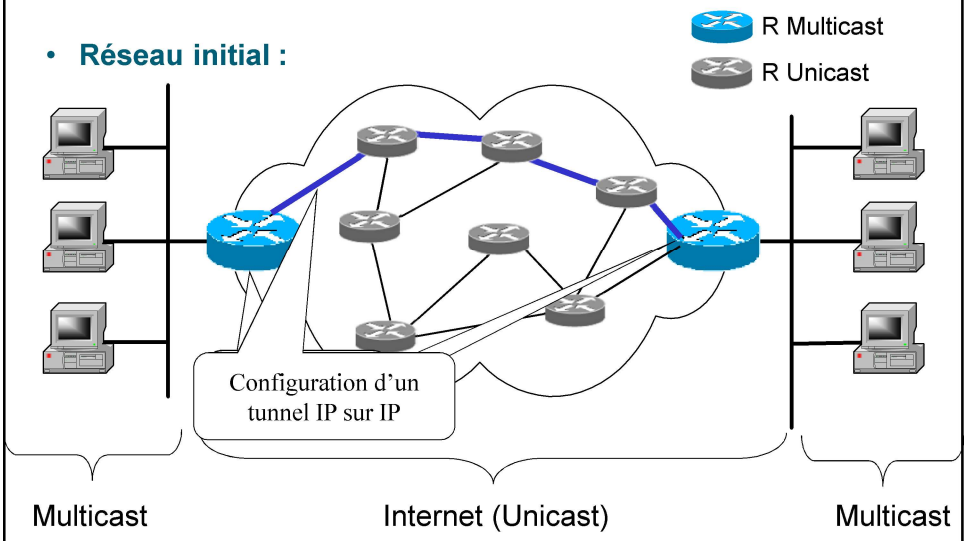
Le MBone

- **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

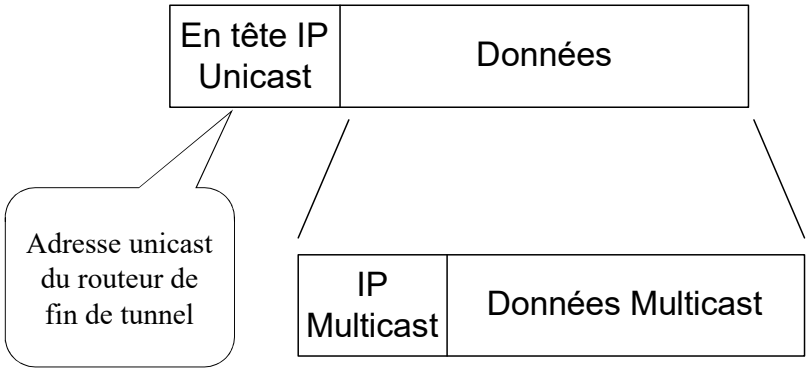
Le Mbone : Architecture

- **Réseau initial :**

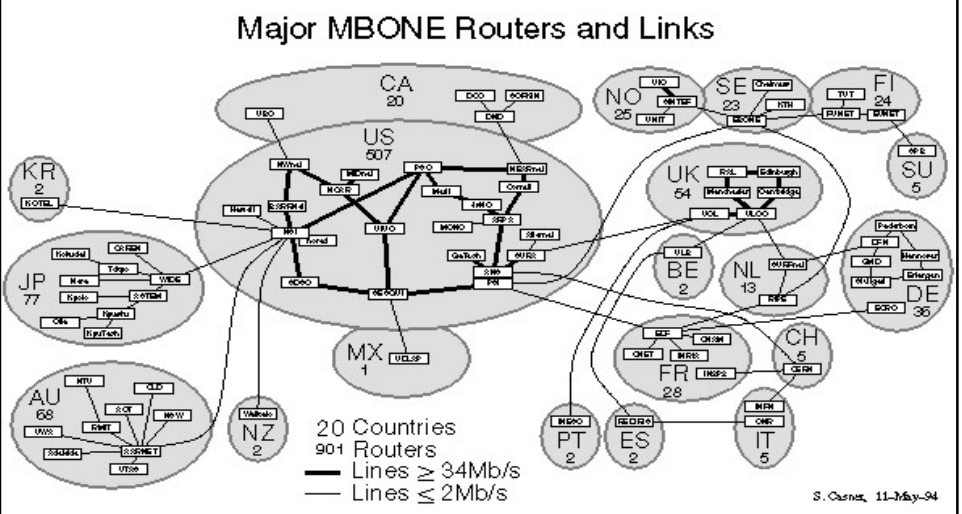


Le Mbone : IP sur IP

- **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 FMBone : The French Mbone**
  - Au dessus de Renater
  - Administré dans chaque centre réseau
  - Groupe de diffusion en français
- **En pleine évolution :**
  - Le FMBone 2 : architecturé sur Renater 2
  - Augmentation de débit et de qualité de service par la gestion sur Renater 2 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**

Chapitre 12

Méthodologie de conception

Méthodologie de conception

→ Prendre une démarche classique de conception
→ Rajouter quelques concepts plus spécifiques aux réseaux

Les 6 questions pour construire un système :

1) De quoi s'agit-il ?
   → Détermination du concept ou objectif
2) Quelle est sa finalité ?
   → Détermination de sa mission opérationnelle
3) Comment est-il structuré ?
   → Recherche de l'architecture et composants essentiels
4) Que fait-il ?
   → Liste de ses fonctionnalités
5) Dans quel milieu fonctionne-t-il ?
   → Nature de l'environnement et de l'interaction du système
6) Quelles sont les mutations possibles ?
   → Déterminer les évolutions souhaitées et/ou autorisées

Méthodologie de conception

→ Il existe de nombreuses méthodologies de conception

- **Méthode cartésienne (Descartes) :**

1- Identifier les objets du monde réel et leurs caractéristiques
2 - Identifier les actions de chaque objet et les ordonnancer
3. Etablir les relations inter-objets (Qui voit l'objet ? Que voit-il ?)
4. Etablir l'interface de chaque objet avec ce qui l'entoure
→ fonctionnalités accessibles
5. Décrire les objets à l'aide d'un langage de programmation

2 phases :
. une analyse descendante pour déterminer les composants
. une analyse ascendante pour reconstituer le système
Le formalisme type : langage orienté objet
Un exemple : SADT

Pour les réseaux :
. Fonctionnalités de chaque station privilégiées / aux interaction
. Cette approche ne semble donc pas très appropriée

Méthodologie de conception

- **Méthode systémique :**

→ Une approche globale

Cette démarche repose sur 3 modèles :

» Modèle conceptuel : **De quoi s'agit-il ?**

» Modèle organisationnel : **Comment est-il fait ?**
Comment fonctionne-t-il ?

» Modèle physique : D**e quoi est-il fait ?**
Q**ui le fait fonctionner ?**

- Exemple : Merise, Mega, Media, …

- **Méthode MACSI :**
- → un compromis entre les 2 approches précédentes

Méthodologie de conception

Les différentes étapes de la démarche / méthodologie **"Réseaux"** :

- Analyse
- Elaboration des spécifications
- Conception
- Codage et test unitaire
- Intégration - validation

- **L'analyse → Construire le cahier des charges utilisateur**
  - 1- Comprendre le problème, les motivations du demandeur
  - 2- Identifier les besoins **réels** → reformaliser la demande client
  - 3- Formuler les contraintes opérationnelles, technologiques, économiques, fonctionnelles
  - 4- Analyser les spécificités
  - 5- Etablir un calendrier approximatif

Méthodologie de conception

- **Elaboration des spécifications → cahier des charges concepteur**
  - → décrire le système en termes de fonctionnalités
  - → lister les applications requises : transfert de fichiers, controle de process, consultation de bases de données, bureautique, messagerie, ….
  - → vérifier l'intégrité des données :
  - Qui fait les mises à jour? Qui stocke? Comment assure-t-on la cohérence?
- **La conception → choix des produits utilisés :**

Conception architecturale (topologie du réseau) :

	Taille	Nature	Délais
pteurs tionneurs	1 à 100 b	périodique	1 à 50 ms
rmes	1 à 100 b	apériodique	0 ms
bots à vision	10^6 à 10^7 b	périodique	50 ms
rminaux tomates	10^2 à 10^3 b	apériodique	0,1 à 1 s
dinateurs (fichiers)	10^3 à 10^6 b	apériodique	1 à 5 s
éphone	300 à 2000 b	périodique/apériod.	5 à 30 ms

Méthodologie de conception

Conception fine (détermination du modèle physique) :

- le plan d'occupation physique de l'espace
- les algorithmes mis en oeuvre par les stations
- la structuration des données
- le choix des protocoles de communication
- les caractéristiques physiques fines du réseau

- **Codage et test unitaire**
- **Intégration et validation**