

Réseaux 1

Réseaux personnels

Damien Sauveron
damien.sauveron@unilim.fr
<http://damien.sauveron.fr/>

1

Intervenans dans le module

Damien Sauveron (Cours, TD et TP) :

- Membre de l'équipe « Sécurité de l'Information »
- Thème de recherche : sécurité des cartes à puce et des réseaux ad hoc

Pour me contacter :



Damien Sauveron
XLIM UMR CNRS 6172 -- Université de Limoges
Site Jide
83 rue d'Isle
87000 Limoges, FRANCE

Email: Damien.Sauveron@unilim.fr
Web: <http://damien.sauveron.fr/>
Phone: +33 (0) 5 55 43 69 83
Fax: +33 (0) 5 55 43 69 77

2004-2006 :

Visiteur/Postdoctorant dans le Smart Card Centre de l'Information Security Group du Royal Holloway, University of London (6 mois)

ATER à l'université de Limoges

2001-2004 :

Thèse au LaBRI – Université Bordeaux 1 sur la *Sécurité de la Technologie Java Card*

Ingénieur R&D dans le CESTI de SERMA Technologies (Pessac) spécialisé sur *les évaluations sécuritaires puces*

2

Plan du cours

Introduction aux réseaux

- Concept de réseau
- Historique
- Objectifs et intérêt d'un réseau
- Applications
- Modèle client/serveur
- Modèle peer-to-peer
- Mobilité
- Aspects sociaux
- Classification des réseaux par :
 - mode de transmission
 - réseaux « point à point »
 - réseaux à diffusion
 - taille du réseau
- LAN, MAN, WAN
- Réseaux sans-fil, domestique et interréseaux

Couches physique et liaison de donnée

- Les bases d'un réseau
 - lien physique et adressage
 - Échanges
- RTC / ADSL / Câble / Boucle locale radio
- Code correcteur d'erreur
- PPP
- Ethernet

La couche routage

- Adressage du réseau
 - adresse IP
 - classe d'adresse
 - notion de sous-réseau
 - correspondance MAC <-> IP
 - algorithme de routage
- Le protocole ICMP
- Le protocole DHCP
- Le NAT

La couche transport

- Client/Serveur
- Notion de ports
- Multiplexage
- Échanges en mode connecté : TCP
- Échanges en mode non-connecté : UDP

La couche application

- Protocole d'administration : DNS / SNMP
- Protocole utilisateur : HTTP / IRC / FTP / ...

La sécurité ?

3

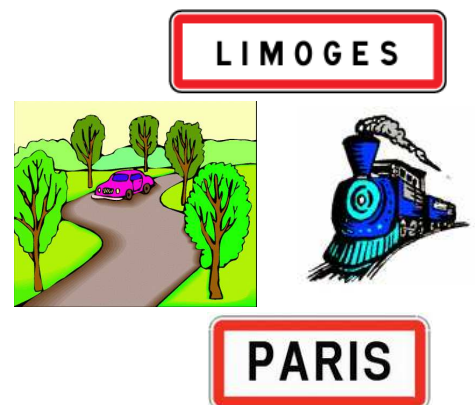
Concept de réseau

Exemple de réseaux :

- réseau de transport (autoroutier, ferroviaire, ...)
- réseau téléphonique
- réseau de neurones
- réseau de malfaiteurs
- réseau informatique

Intuitivement, plusieurs notions :

- structures physiques (routes, fils, ...)
- informations au sens large (véhicule, impulsion électrique, ...)
- échanges (déplacement du véhicule, des impulsions électriques, ...)
- adresse (nom de ville, numéro de téléphone, nom de personne, ...)



Qu'est ce qu'un réseau informatique ?

C'est un ensemble **interconnecté** d'ordinateurs **autonomes** au moyen d'une seule technologie.

Interconnecté : deux ordinateurs sont considérés comme interconnectés s'ils sont capables d'échanger des informations.

Autonomes : *pas de relation de type maître/esclave* (si une unité de contrôle peut déclencher l'arrêt ou le démarrage d'une autre unité de contrôle alors ces unités ne sont pas autonomes).

Un système composé d'une unité de contrôle et d'une ou plusieurs unités esclaves n'est pas un réseau.

Exemple : un ordinateur disposant de terminaux et d'imprimantes distants.



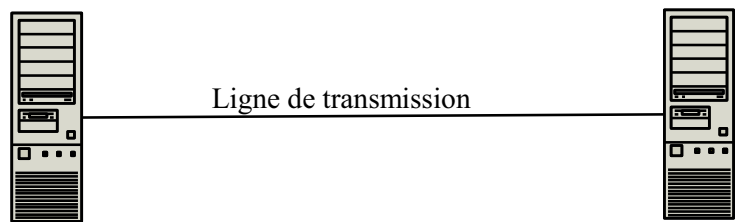
4

Les bases d'un réseau : des liens de connexion et un adressage

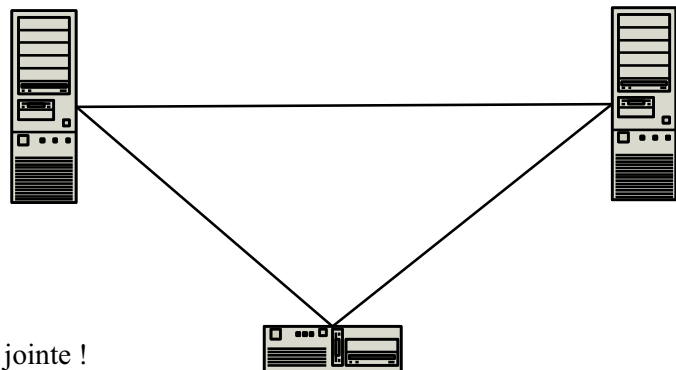
Pour communiquer physiquement

Deux machines doivent être reliées par une « ligne de transmission » :

- un câble série ou parallèle ;
- un câble USB ;
- modem analogique ;
- une connexion wifi ;
- un opérateur proche des deux ?



Dans le cas de trois machines et plus ?



Il faut disposer de :

- liens (pas de machine isolées) ;
- d'adressage !

Une machine doit avoir une adresse pour être jointe !

5

Historique

XVIII siècle :

Grands systèmes mécaniques issus de la révolution industrielle

XIX siècle :

Locomotive à vapeur

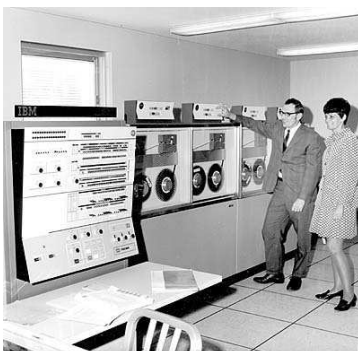
XX siècle :

Ère de la collecte, du traitement et de la distribution des informations : déploiement de réseaux à l'échelle mondiale (téléphone, invention de la radio, de la télévision, lancement de satellites de communication)

Avant :

Au départ un ou deux ordinateurs pour une société ou une université :

- *un système informatique centralisé, localisé physiquement dans une même pièce*



6

Historique

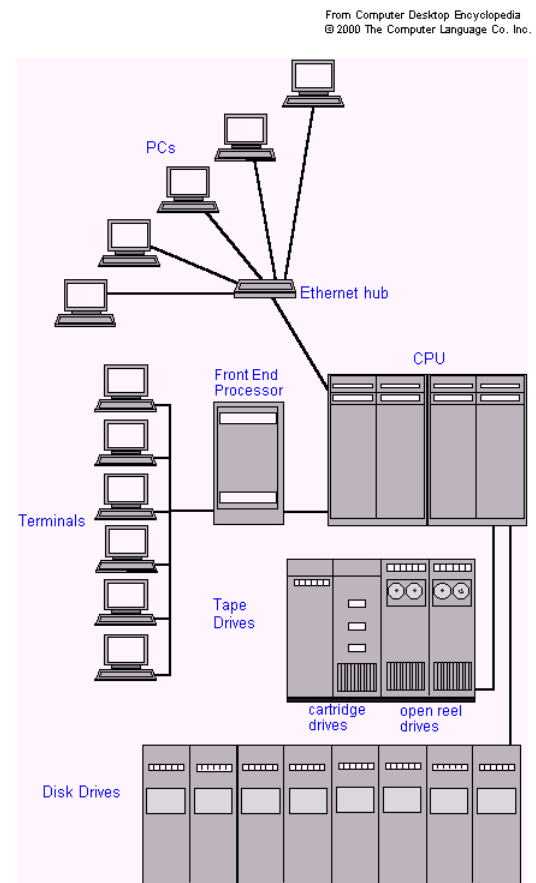
Maintenant :

Des dizaines d'ordinateurs décentralisés

Le réseau a permis la mutation des ordinateurs : du « MainFrame » vers le micro ordinateur

Concepts obsolètes :

- la « salle ordinateur » comme lieu où les utilisateurs apportent leur travaux est totalement obsolète.
- un ordinateur unique pouvant satisfaire tous les besoins de traitement est remplacé par le modèle d'un ensemble d'ordinateurs **séparés** mais **interconnectés** qui exécutent des tâches différentes.



Objectifs et intérêt des réseaux

Partager les ressources

Rendre accessible à chaque membre du réseau *programmes, données et équipements* indépendamment de leur localisation physiques

=> Affranchissement des contraintes géographiques : *même à 1000 km les données doivent être partagées.*

Plus grande fiabilité

- proposer des alternatives aux ressources employées (plusieurs imprimantes, etc.)
- surmonter les défaillances matériel : application militaire, bancaire,... l'exploitation doit pouvoir continuer même en cas de problèmes matériels.

Réduction des coûts

- les petits ordinateurs ont un rapport performance/coût supérieur aux gros ordinateurs.
- partage de périphériques (1 seule imprimante pour un groupe d'utilisateurs)

Moyen de communication

- les ordinateurs d'un réseau permettent l'échange d'information entre personnes séparées par de longue distance
- travail en commun, travail collaboratif (agenda, planning, ...), développement de coopération (vidéoconférence, tableau blanc, ...), ...

=> l'industrie des télécommunications devient un concurrent de l'industrie du transport



VS



Applications

Professionnelles

Partage de ressources matérielles et informationnelles distantes ou non (bases de donnée, ...).

- Il suit souvent un modèle client/serveur

Collaboration intra-entreprise et inter-entreprises

Réduction des coûts :

- Coûts des échanges (courrier, etc)
- Coûts de stockage (par exemple pièces pour une entreprise automobile)

Ventes directes en ligne

1977 : Ken Olsen président de Digital Equipment Corporation (2ième fabricant d'ordinateur après IBM)

Il déclare qu'il ne voit pas d'intérêt pour le particulier à disposer d'un ordinateur chez lui.

Aujourd'hui Digital a disparu !

Domestiques

L'accès a des informations distantes (web, journaux, bibliothèques numériques => mort de l'édition ?, ...)

La communication entre personnes (messagerie instantanée, chat, newsgroups, visio, téléphonie, téléformation, ...)

Les divertissements interactifs (casinos en ligne => légalité ?, jeux vidéo, vidéos à la demandes et interactives, ...)

Le commerce électronique

To be continued (exemple succès du SMS)

Que voit madame Irma ? :

- Téléformation
- Télémédecine
- Les réseaux domestiques (voir plus loin)

Le réseau a une fonction sociale ?

(réduction des inégalités géographiques)

Appellation	Modèle commercial	Exemple
B2C (Business-to-consumer)	Entreprise à client	L'achat de livres, de CD ou de DVD.
B2B (Business-to-business)	Entreprise à entreprise	Un fabricant d'automobiles commandant des pneus à un fournisseur.
G2C (Government-to-consumer)	Gouvernement à consommateur	Distribution de formulaires fiscaux.
C2C (Consumer-to-consumer)	Consommateur à consommateur	Vente aux enchères de produits d'occasion.
P2P (Peer-to-peer)	Égalitaire	Partage de fichiers.

9

Modèle client/serveur

Développement de l'architecture client/serveur

- un micro par utilisateur, les données étant partagées sur un ou plusieurs serveurs de fichiers.
- possibilité d'augmenter de manière graduelle ses performances ("scalability") par ajout de processeurs supplémentaires quand le travail augmente.

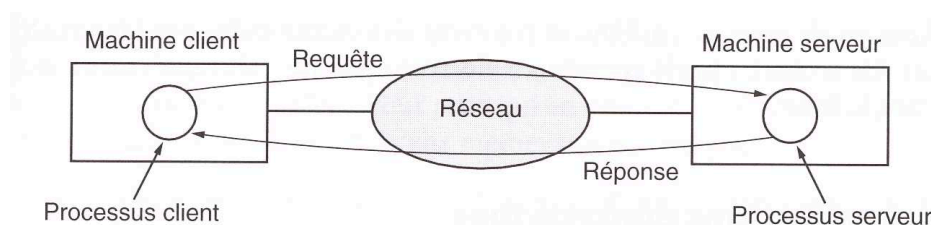
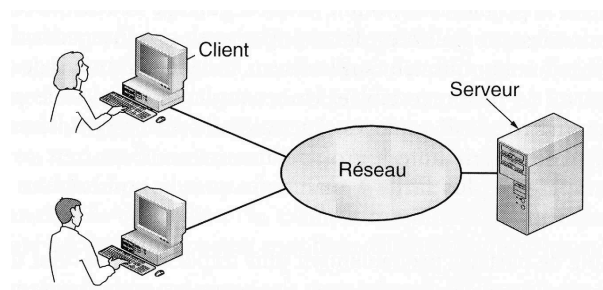
Dans le cas d'un gros ordinateur unique il faut changer l'ordinateur ce qui est coûteux et perturbant pour les utilisateurs.

- *flexibilité puisque l'utilisateur n'est plus dépendant de sa machine grâce à l'utilisation de serveur conservant ses données*

Le serveur est géré par l'administrateur système

Modèle le plus répandu pour les applications.

Par exemple, le web.



Le modèle client/serveur implique l'échange de requêtes et de réponses.

10

Modèle Peer-to-peer (poste à poste)

En opposition avec le modèle client/serveur

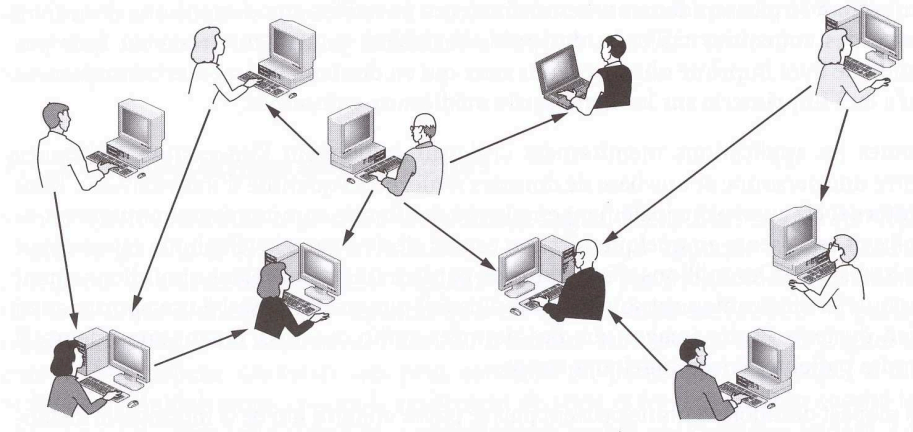
Communication interpersonnelle entre systèmes homologues (pairs)

Chacun peut communiquer avec tous les autres.

L'échange se fait sur un pied d'égalité. Les rôles de client et de serveur ne sont pas assignés de façon fixe.

Avantage : Résistant aux attaques

Exemple: Napster même si la base de donnée est centralisée. Mort à cause des problèmes d'atteintes aux droits d'auteurs



Dans les nouveaux systèmes, les bases de données sont complètement décentralisées.

Chaque client maintient sa propre BD et une liste des autres participants dans le voisinage du système.

Le nouvel utilisateur peut ainsi rendre visite à un membre existant pour voir ce qu'il propose et obtenir la liste des participants pour élargir son champ de recherche.

11

Mobilité

Accroissement des équipements mobiles :

PDA's, ordinateurs portables, téléphones portables, ...

Développement des réseaux sans-fils :

Wifi, Bluetooth, Wimax, ZigBee

Technologie

IEEE

Besoins mémoire

Autonomie avec pile

Nombre de nœuds

Vitesse de transfert

Portée

Zigbee

802.15.4

4-32 Kb

Années

65000+

250 Kb/s

100 m

Bluetooth

802.15.1

250 Kb +

Jours

7

1 Mb/s

10-100 m

Wi-Fi

802.11a/b/g/n/...

1 Mb +

Heures

32

11-54-108-320 Mb/s

300 m

Utilisation : en déplacement (bureau mobile), pour les flottes de véhicules, pour l'armée

=> quand une connexion filaire est impossible

Différence entre accès **fixe** sans fil et accès **mobile** sans fil.

Sans fil	Mobile	Applications
Non	Non	Ordinateurs personnels de bureau.
Non	Oui	Ordinateur portable utilisé dans une chambre d'hôtel.
Oui	Non	Réseaux dans des immeubles anciens sans câblage.
Oui	Oui	Bureau portable ; PDA pour l'inventaire de magasin.

Utilisations des réseaux sans fils :

m-commerce :

- WAP 1.0 et 2.0, i-mode => objectif : remplacer le porte-monnaie par un PDA + lecteur code barre

- géolocalisation de services => faire payer les utilisateurs (portable vs internet)

- ...

Parcmètres sans fils, distributeur de boissons, relevé de compteur gaz-électricité, montre d'IBM (PAN, ...)

12

Aspects sociaux

Légalité de certains contenus :

Les lois divergent selon les pays. Faut-il censurer ? Débat !

Responsabilité des contenus :

Est-ce le diffuseur (l'hébergeur, les FAI, les équipements intermédiaires) ou l'auteur qui est responsable ? (par exemple sur un forum)

La poste contrôle-t-elle le courrier des usagers ? Faut-il censurer ? Débat !

Droits des salariés/employeurs :

Vérification par les employeurs des mails rédigés par les salariés dans le cadre de l'entreprise mais également du domicile.

Droits des étudiants/universités :

Censure à l'université Carnegie-Mellon

Espionnage :

Système Carnovore installé par le FBI chez les FAIs pour espionner les messages => DCS1000

– Quid du 4eme amendement de la constitution américaine ?

Spyware, cookies, ... => fuites d'informations confidentielles : numéro de carte bancaire, sécurité sociale

Les réseaux sociaux : Facebook, twitter, etc.

Anonymat :

Positifs : Dénoncer des scandales

Négatifs : Dénonciation calomnieuses, Spam (CD-ROM d'adresses), ...

Usurpation d'identité :

Fishing, violation des droits d'auteurs, ...

NÉCESSITÉ D'AVOIR UNE SÉCURITÉ PLUS ÉLEVÉE

13

Classification des réseaux

Il existe deux caractéristiques pour établir la classification :

la technique de transmission utilisée

la taille du réseau

Il existe essentiellement deux techniques de transmission :

– la diffusion

– le point à point

La taille du réseau :

– petit

– moyen

– gros

14

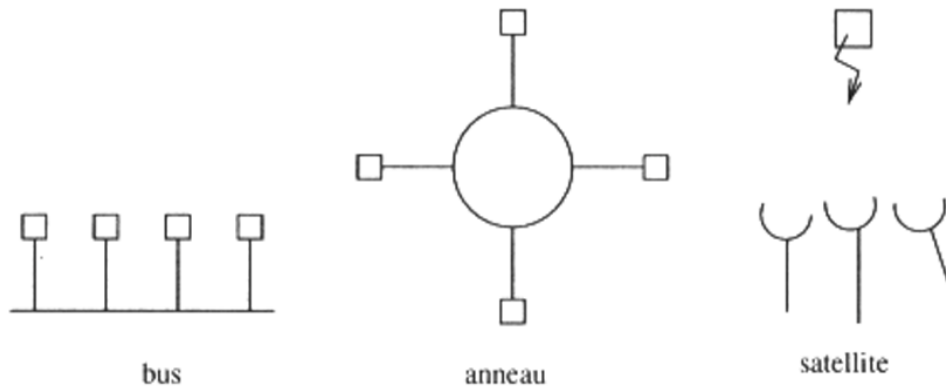
Réseau à diffusion

Les réseaux à diffusion (“*broadcast network*”) n’ont qu’un **seul canal de communication** que toutes les machines partagent.

Chaque machine appartenant au réseau dispose d’une adresse.

Une machine envoie de petits messages, appelés **paquets**, qui sont reçus par toutes les autres machines.

- dans le message un champ d’adresse permet d’identifier le destinataire
- à la réception du message, une machine teste ce champ :
si le message est pour elle, elle le traite sinon elle l’ignore.



Exemple : un couloir sur lequel débouche un certain nombre de portes de bureau
quelqu’un sort dans le couloir et appelle une personne,
tout le monde entend l’appel mais une seule personne répond à l’appel
(cas des annonces dans les gares ou les aéroports).

15

Les réseaux à diffusion

Il est possible dans un système de diffusion d’envoyer un message **vers tout le monde** en utilisant une adresse particulière :

- Ce message est alors traité par toutes les machines on appelle ce procédé « diffusion générale » ou **envoi broadcast** ou “*broadcasting*”

Certains systèmes permettent l’envoi à **un sous-ensemble** de machine du réseau : c’est la « diffusion restreinte » ou **envoi multicast**

Avantage :

Il est **facile d’ajouter** de nouveaux ordinateurs sans modifier la configuration de ceux déjà connectés.
La **panne d’un des éléments** connectés au réseau **ne provoque pas de panne** du réseau (en général).

Inconvénients :

La **rupture** du support de transmission entraîne l’**arrêt du réseau**.

Exemple :

LAN, MAN

Les réseaux point-à-point

Le support physique relie seulement **une paire d'équipements** à la fois.

La communication est **directe** si les deux équipements sont connectés entre eux.

La communication est **indirecte** sinon : quand deux équipements veulent communiquer, ils le font par l'intermédiaire des autres nœuds du réseau.

Exemples :

- Cas d'un réseau en « étoile », le site central reçoit et envoie tous les messages.
Le fonctionnement est simple, mais la panne du site central **paralyse** tout le réseau.
- Cas d'une « boucle simple », chaque nœud recevant un message de son voisin en amont le réexpédie à son voisin en aval.
Pour que le message ne tourne par indéfiniment, il est retiré par le nœud émetteur.
Si l'un des nœuds tombe en panne, le réseau est bloqué.
=> Une solution partielle est d'utiliser une « double boucle ».

Maillage **régulier** :

- l'interconnexion est totale ;
- la fiabilité est maximale ;
- le coût en câblage est maximal.

Maillage **irrégulier** :

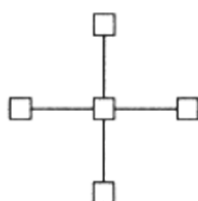
- l'interconnexion n'est plus totale ;
- la fiabilité diminue ;
- le routage des messages peut devenir complexe ;
- impossible de prévoir le temps de transfert d'un nœud à l'autre.

17

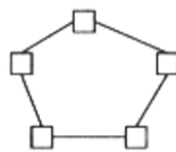
Les réseaux point-à-point

Ces réseaux sont formés d'un **grand nombre de connexions** entre les machines prises deux à deux.

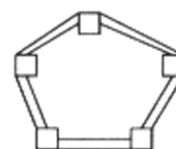
Une transmission point-à-point entre un expéditeur et un destinataire est appelée diffusion individuelle ou **envoi unicast**



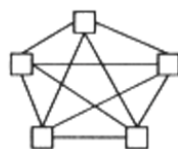
étoile



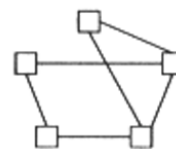
boucle simple



boucle double



maillage régulier



maillage irrégulier

Le trajet des communications est affecté par :

- les intermédiaires : pour aller de la source au destinataire, un message doit alors passer par un ou plusieurs intermédiaires ;
- le routage : il existe plusieurs routes de *longueurs différentes* pour joindre ces deux machines, il est nécessaire d'utiliser de **bons algorithmes d'acheminement des messages** ;
- le temps de transfert du message : il devient presque impossible à prévoir.
maillage régulier contre maillage irrégulier.

18

Les réseaux suivant leur taille

En fonction de la distance des ordinateurs entre eux, les réseaux sont classés de différentes façons :

Distance entre processeurs	Localisation des processeurs	Exemple
0,1 m	Un circuit imprimé	Machine à flots de données
1 m	Un ordinateur	PAN ou Multiprocesseur
10 m	Une salle	Réseau local
100 m	Un immeuble	
1 km	Un campus	
10 km	Une ville	Réseau métropolitain
100 km	Une région	Réseau longue distance
1 000 Km	Un continent	
10 000 km	La terre entière !	Internet

En général, la **taille du réseau** et le **mode de transmission** sont liés :

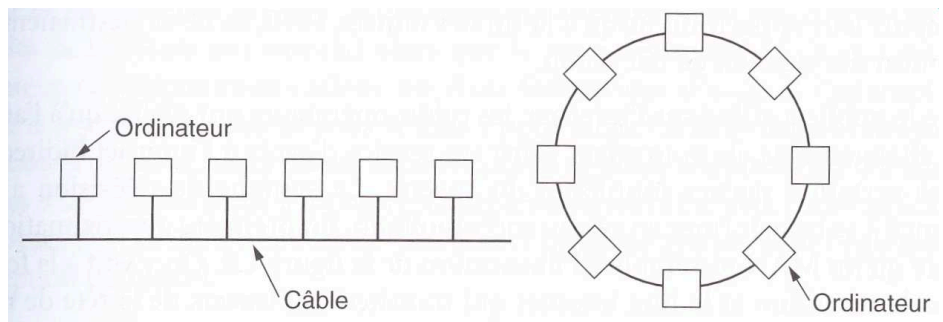
- Petits réseaux : réseaux à diffusion
- Gros réseaux : réseaux « point à point »

19

LAN (Local Area Network)

C'est le type de réseau est le plus répandu, il correspond aux réseaux locaux ou « LAN », “local area network” :

- réseaux privés dont la taille ne dépasse pas quelques kilomètres (réseau d'une entreprise réparti entre plusieurs bâtiments, campus, ...) ;
- les LAN étant de taille restreinte, le délai de transmission est borné et connu ce qui permet de simplifier la conception et la gestion du réseau ;
- Caractéristiques des transmissions :
 - Débit : de 10 Mbps (10 Mbit/s) à 1 Gbps (1 Gbit/s)
 - Faible délai de transmission : de l'ordre de la dizaine de microsecondes ou nanosecondes
 - Très peu d'erreurs de transmission.
 - Topologie : bus, anneau, ...



Problème de l'accès au canal : 1 seule machine est autorisée à transmettre dans un instant donné

- Sinon il y a collision => il faut un mécanisme d'arbitrage (centralisé ou décentralisé)
- Exemple : attente aléatoire pour Ethernet, jeton pour TokenRing
- Allocation statique (tranches de temps => gaspillage) ou dynamique du canal (à la demande)
 - Dynamique centralisé = unité maître sur le bus ; dynamique décentralisé = chacun décide => Pas de chaos

Le plus connu : le réseau Ethernet (IEEE 802.3) !

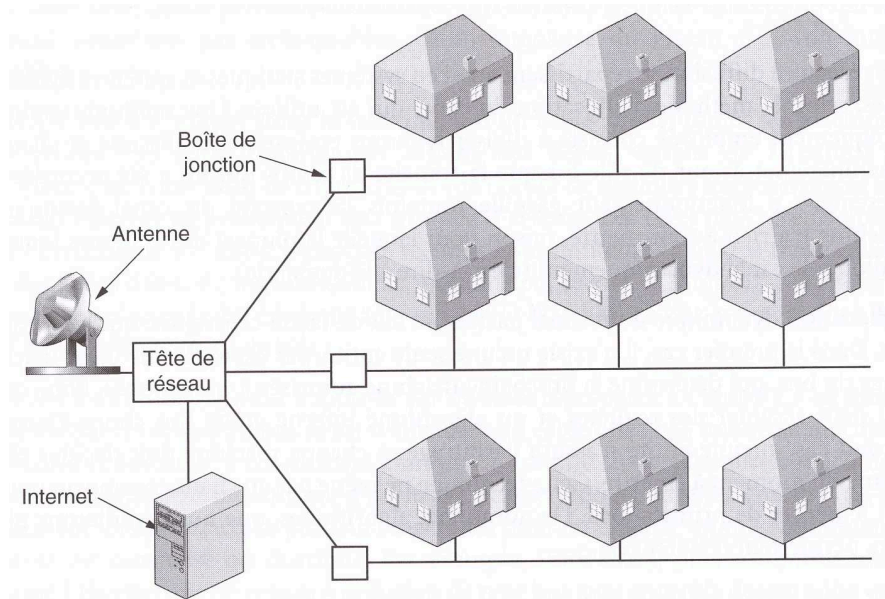
20

MAN (Metropolitan Area Network)

Le réseau métropolitain couvre une ville.

Le plus connu des MAN est le réseau de télévision par câble

- Il s'est développé à partir de l'ancien système d'antenne collective utilisé dans les zones qui souffraient d'une mauvaise réception
- Initialement (jusqu'à la fin des années 1990) : seulement pour la TV avec un choix d'émissions spécialisées
- Possibilité d'offrir un accès à l'internet bidirectionnelle en utilisant des parties inutilisées du spectre



Autre MAN : le réseau haut débit sans fil (IEEE 802.16)

21

WAN (World Area Network) (1/2)

Le réseau longue distance s'étend sur une vaste zone géographique (pays, continent, ...).

Il est constitué :

D'ensemble d'ordinateurs appelés **hôtes**.

D'un **sous-réseau de communication** pour relier ces hôtes souvent abrégé en **sous-réseau**.

Propriété :

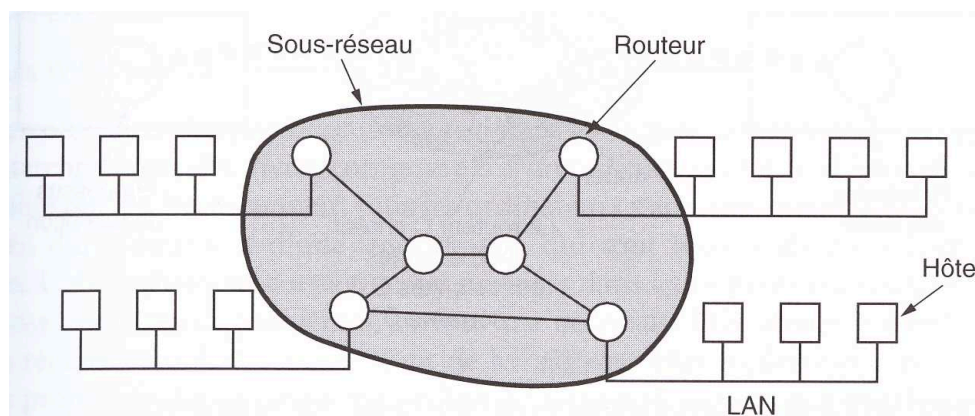
Hôtes : appartiennent aux clients (vous, une entreprise, etc.)

Le sous-réseau : appartient à un opérateur télécom ou à un FAI

Tâche d'un sous réseau : acheminement des messages d'un hôte à l'autre

=> séparation entre l'aspect communication (le sous réseau) et aspect application (les hôtes)

=> simplification de la conception du réseau (divide & conquer)



Exemple : Renater

22

WAN (World Area Network) (2/2)

Un WAN est composé de :

Lignes de transmissions qui transportent les bits (fils de cuivre, fibre optique, liaisons radio, ...)

Équipements de commutation (**routeur**) :

- ordinateurs spécialisés qui servent à interconnecter trois ou d'avantages lignes de transmission.
- En fonction des données entrantes il choisit vers quelle ligne de sortie les aiguiller.

Sous-réseau = ensemble des routeurs et des lignes de transmissions pour acheminer des paquets depuis un hôte source jusqu'à un hôte de destination. (Attention au contexte)

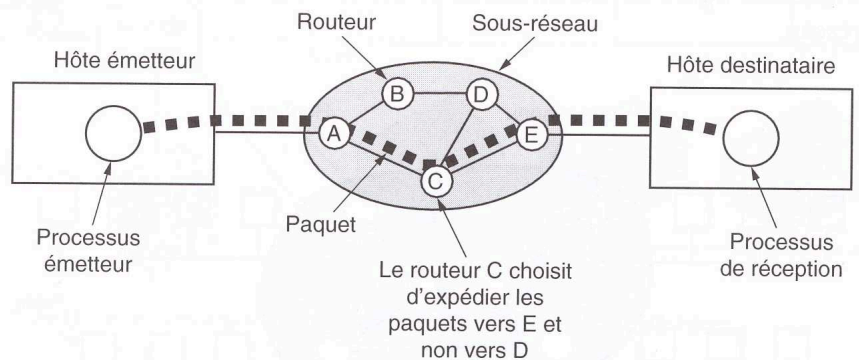
Une ligne de transmission relie 2 routeurs. Si 2 routeurs non directement reliés souhaitent communiquer le paquet passe par un routeur intermédiaire. Il est reçu en totalité par celui ci, mis en attente jusqu'à ce que la ligne de sortie se libère puis expédié.

C'est le fonctionnement le plus fréquent : c'est le **mode différé** (store-and-forward) ou **commutation de paquets**.

Dans la réalité c'est l'usage. Si les paquets ont tous la même taille, ils se nomment **cellules**.

Problèmes :

- Taille mémoire des équipements de commutations
- Découpage du message en paquet et numérotation
- Algorithme de routage



Réseaux sans fil

1901 : physicien italien Guglielmo Marconi expérimente une transmission télégraphique sans fil depuis un navire vers la côte au moyen du code Morse.

=> les systèmes numériques sans fil modernes offrent de meilleures performances mais l'idée de base reste la même

Trois grandes catégories de réseaux sans fil:

L'interconnexion de système

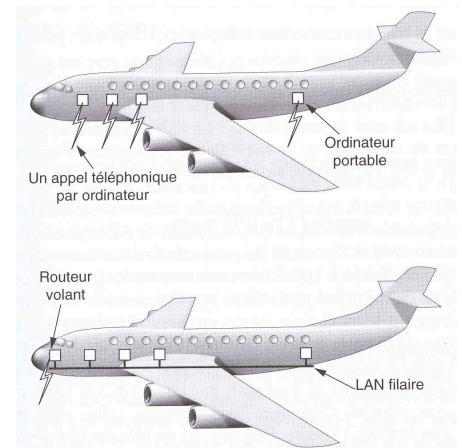
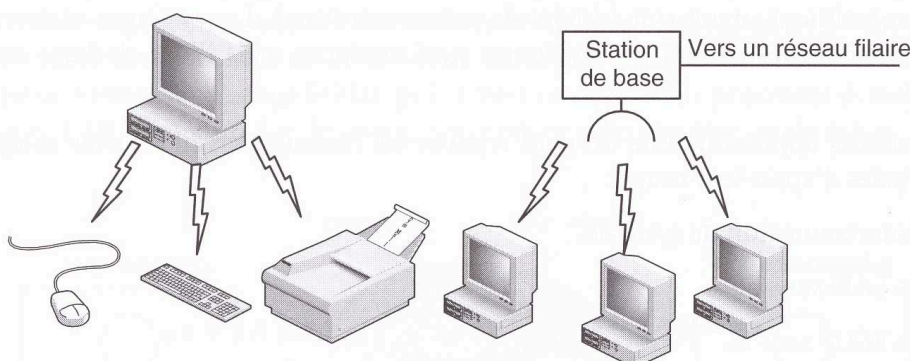
- Simplifier et supprimer les connectiques pour les utilisateurs avec par exemple Bluetooth (aucun pilote n'est nécessaire pour les matériels : caméras numériques, casques, scanners, ...)

Les LAN sans fil

- Ordinateur équipé de modem radio et d'une antenne : IEEE 802.11

Les WAN sans fil

- Réseaux cellulaires (téléphones 1G -> 2G -> 3G)
- IEEE 802.16



Presque tous les réseaux sans-fil sont connectés à un réseau filaire à un moment ou à un autre.

Réseaux domestiques

Idée de base :

Avoir un réseau dans les habitations pour permettre aux appareils de communiquer entre eux et d'être accessibles par l'internet.

Concept que personne ne réclame et dont on ne peut plus se passer après (exemple : la télécommande)

Appareils connectables :

- Les ordinateurs : PC, portable, PDA, périphériques partagés
- Les systèmes de divertissement (TV, DVD, magnétoscopes, caméscope, caméras, chaîne stéréo, lecteurs MP3)
- Les systèmes de télécommunication (téléphones, téléphones portables, dispositifs intercom, télécopieurs)
- Les appareils ménagers (micro-ondes, réfrigérateur, horloges, fours, climatiseurs, luminaires)
- Les systèmes de télémétrie et de surveillance (compteurs d'eau, alarme contre l'incendie et le vol, vidéo surveillance des bébés)

Conditions pour le succès :

- Connexion bidirectionnelle
- 1 seul réseau
- Simplicité et fiabilité (pas d'installation, pas de hotline, l'utilisateur traditionnel veut que ça fonctionne à 100% dès le départ, de 4 boutons sur un climatiseur on passera à 30 pages de manuel + une partie sur la sécurité)
- Bas prix (thermostat à 5€ ok mais pas à 50€)
- Capacité de réseaux importante (possibilité de faire du multimédia)
- Un standard stable pour l'interface (pas de IEEE 1394 – Firewire – puis de USB 2.0)
- Une sécurité très élevée (sinon le PDA deviendrait le pied de biche des futurs voleurs)

Seront-ils filaires ou sans fil ? (problème de sécurité mais aussi d'installation).

Déjà 6 réseaux par habitation (électricité, téléphone, TV par câble, eau, gaz, eaux usées)

25

Le rêve de toutes et tous



Quel plaisir de s'allonger sur le canapé tout en regardant d'un œil assoupi le **robot aspirateur** faire son travail sans jamais râler !!!

Grâce à des capteurs il passe l'aspirateur tout seul comme un grand et ne repasse jamais deux fois au même endroit.

Ce qu'on ne soupçonne pas, c'est que ce petit robot est aussi un espion, car il est aussi **muni d'une caméra digitale !!!**

Imaginez que vous soyez au bureau et que vous vouliez surveiller le professionnalisme de la baby-sitter, **c'est possible depuis votre écran d'ordinateur qui se connecte à l'i-robo et peut le contrôler à distance !!!**

Pour le look, il est tiré tout droit d'un film de sciences-fiction : design et futuriste !

26

Le frigo de demain

Sur cet écran vous retrouverez toutes les fonctions d'INTERNET sans avoir de PC : shopping et informations diverses, envoyer et recevoir du courrier électronique. En plus de l'écran tactile on peut également brancher un clavier.

La communication ne s'arrête pas là : on peut aussi faire de la visio-conférence, ou téléphoner aux gens qu'on aime tout en les voyant sur l'écran. Un réel face à face auditif et visuel !!! L'écran remplacera le post-it à la maison, ce réfrigérateur multi-tâches offre la possibilité aux membres de la même famille de communiquer et de s'organiser entre eux. Grâce à la fonction message sur l'écran, on peut laisser des messages vidéos, des mots écrits " n'oublie pas de sortir les poubelles !", ou encore des messages vocaux.

Pendant qu'on prépare la cuisine on peut également regarder sur ce même écran couleur LCD la télévision, ou des films provenant de votre magnétoscope ou lecteur DVD. Pendant qu'on a les mains dans la farine on peut encore brancher un caméscope pour surveiller la chambre du bébé qui dort ou encore contrôler l'accès à votre domicile (visiophone)...

Une autre fonction étonnante : l'album digital. Equipé d'une caméra on peut filmer les meilleurs moments en famille et les dîners les plus animés, puis regarder ce film à l'écran. On peut également télécharger des photos qui apparaîtront sur l'écran comme un album.

Et la cuisine dans tout ça ?

Vous pouvez télécharger ou consulter des recettes de cuisine enregistrées dans un programme et choisir celle qui s'adapte le mieux au contenu de votre réfrigérateur.

Parmi toutes ses facettes, l'écran peut également se transformer en tableau de bord pour une meilleure gestion du réfrigérateur : contrôle de la température, indicateur du niveau d'eau, contenu du réfrigérateur etc. ...

Mais aussi gérer votre emploi du temps (agenda et horloge).

La cuisine trouvera ainsi pleinement son rôle de cœur de la maison, qu'elle avait occupée dignement pendant tant de siècles...et constituera une véritable plate-forme de communication au sein de la famille.

En tant que réfrigérateur le modèle 2002 n'a rien à envier aux autres. Bien au contraire !

Basé sur la technologie professionnelle du froid ventilé, équipé du système Twin Cooling, il dispose d'un volume total de 680 litres, d'un distributeur d'eau fraîche purifiée, d'étagères anti-débordement en verre trempé, d'un compartiment fraîcheur 0-1°C, de tiroirs à légumes et fruits à humidité contrôlée et d'un éclairage naturel renforcé ...

Voilà un majordome que tout le monde aimerait avoir chez soi !
Étonnant, non ?



27

Interréseaux

Il existe de nombreux réseaux dans le monde et ils sont souvent incompatibles.

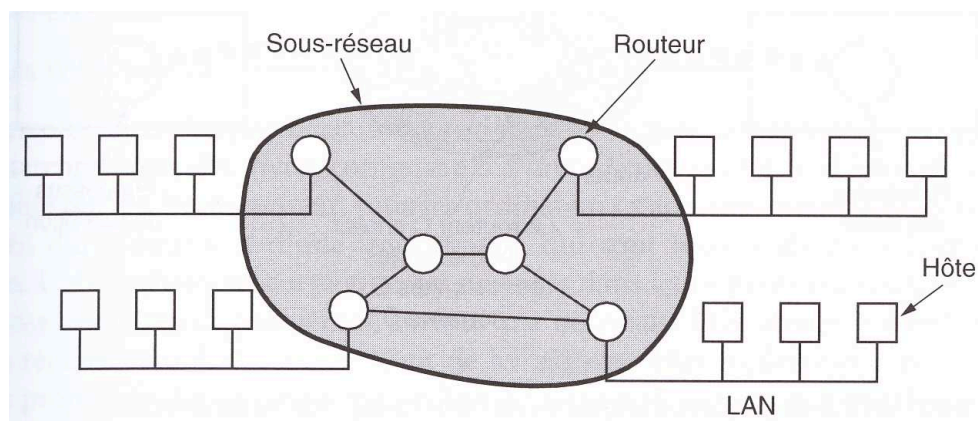
Ainsi pour que les personnes sur différents réseaux puissent communiquer entre elles on interconnecte les réseaux avec des machines appelées **passerelles** (gateway)

=> traduction au niveau matériel comme logiciel

Cet ensemble de réseau ainsi relié s'appelle un interrésseau

L'internet est le plus célèbre.

Un WAN interconnectant des LANs est aussi un interrésseau



Passage de réseaux à diffusion à du point à point.

28

Hiérarchies de protocoles (1/3)

Avant, pour les premiers réseaux :

Les ingénieurs se sont surtout concentrés sur l'aspect matériel reléguant l'aspect logiciel au second plan

Aujourd'hui cette stratégie ne tient plus et les logiciels réseaux sont hautement structurés

=> pour réduire la complexité de conception, les architectures sont organisées en strates, appelées **couches** ou niveaux

- Le nom, la fonction, le contenu des couches et leur nombre diffèrent selon les réseaux.
- Chaque couche a pour rôle de fournir un service au travers d'une **interface** à la couche immédiatement supérieure tout en lui dissimulant les détails de l'implémentation. (Cela s'appelle l'abstraction.)

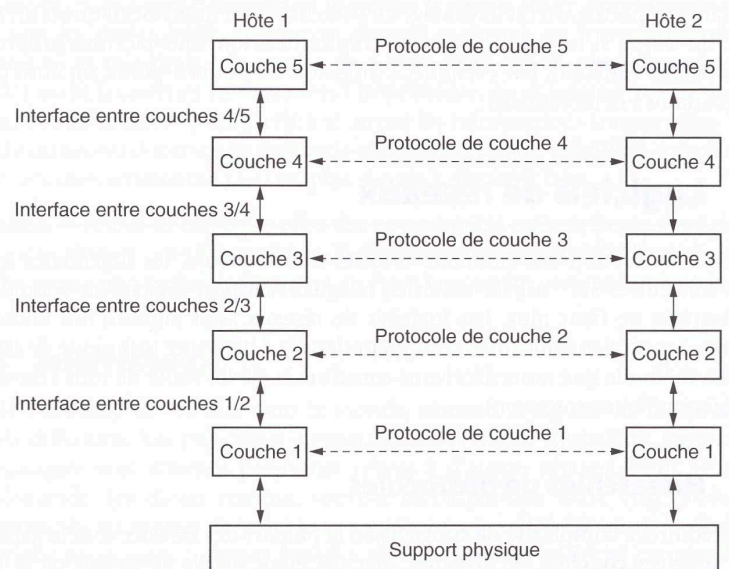
Virtuellement, la couche n d'une machine dialogue avec la couche n d'une autre machine. Pour se comprendre elles utilisent un **protocole**. Un protocole est un **langage commun** associé à des **règles** communes.

=> Une violation du protocole rend la communication impossible

Aucune donnée ne transite directement entre couche n . Elles passent par le **support physique**.

L'interface définit les services rendus à la couche supérieure. Elle offre la modularité (exemple remplacement de la ligne téléphonique par des canaux satellites).

Architecture de réseau = couches + protocoles
Pile de protocoles = ensemble des protocoles utilisé par un certain système.



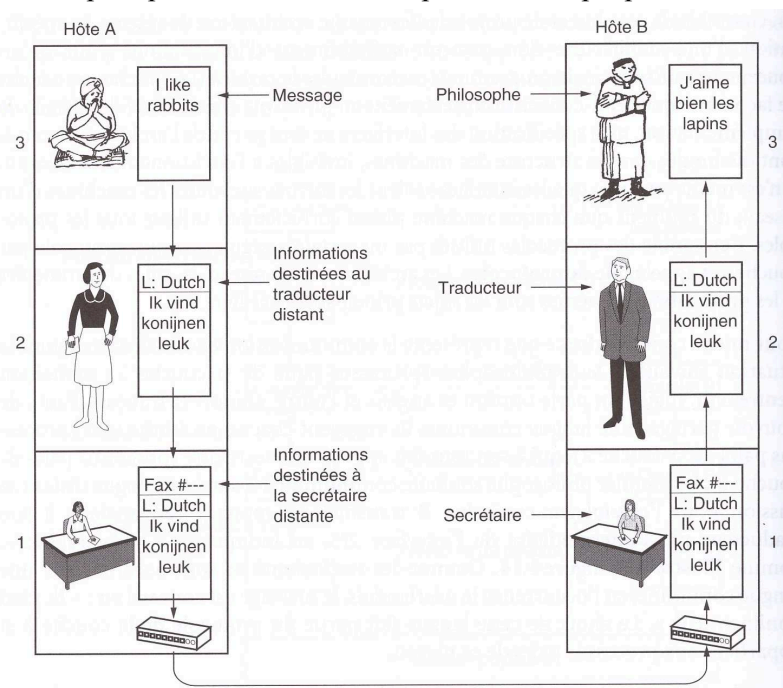
Hiérarchies de protocoles (2/3)

Exemple des philosophes

Le premier parle ourdou et anglais et le second chinois et français.

Le premier veut communiquer sa passion pour l'*oryctolagus cuniculus*.

Accord entre les traducteurs pour parler le néerlandais et pour la télécopie pour les secrétaires.



Indépendance du message vis-à-vis de la langue choisie, du support de transmission choisi. Les protocoles sont indépendants les uns des autres tant que les interfaces ne sont pas changées.

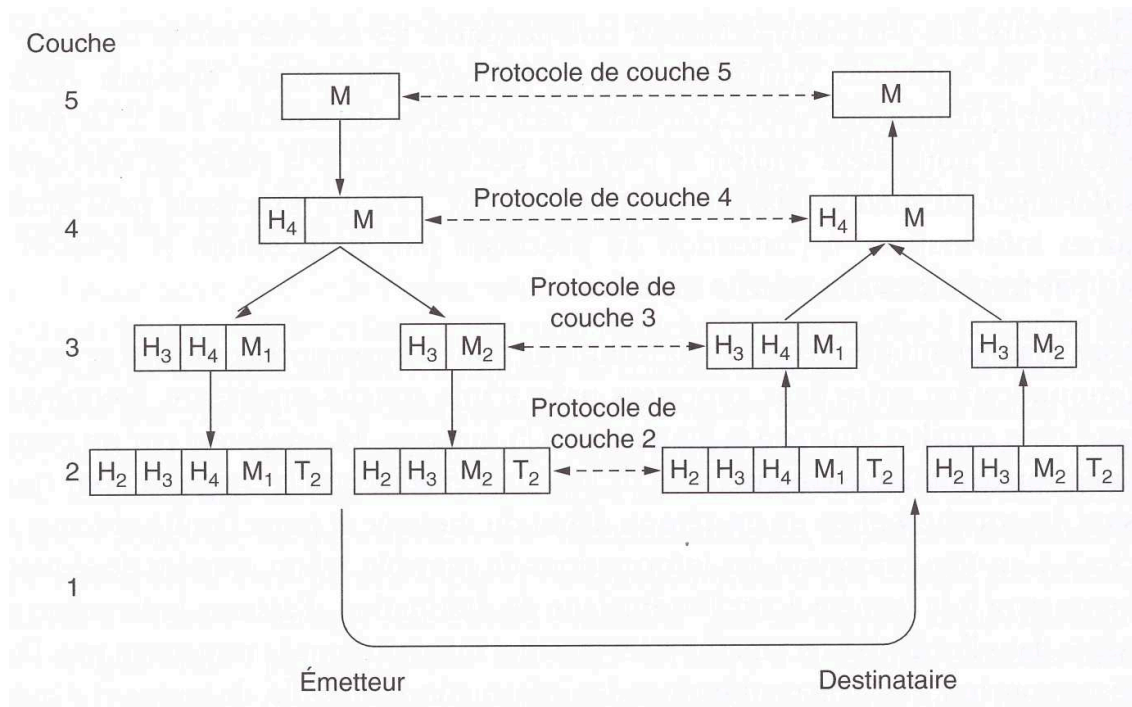
Hierarchies de protocoles (3/3)

Illustration

Cheminement d'un message à travers les couches.

- Ajout d'un en-tête, découpage et numérotation de la séquence du message, ajout d'information de taille.
- Vérification des tailles, recomposition du message et livraison

Notez la différence entre **communication virtuelle** et la **communication effective**.



31

Principes de conception des couches

Certains principes de conception des réseaux se retrouvent dans plusieurs couches :

Identification des processus émetteur et récepteur : il faut une forme d'**adressage**

Pour le transfert de données, selon les systèmes les données peuvent voyager dans une seule direction ou les deux:

- **simplex, half duplex, duplex, full duplex**

Le **contrôle d'erreur** est important car les circuits de communications ne sont pas parfaits :

- Code de détection et code de correction d'erreurs

Tous les canaux de communication ne préservent pas l'ordre des messages qu'ils transportent :

- Numérotation des paquets
- Comment traiter les paquets arrivant dans le désordre ?

Empêcher un émetteur rapide de submerger un récepteur lent.

- C'est le **contrôle de flux**.

Gestion de la fragmentation :

- Pour des raisons d'efficacité, si les messages sont trop gros ils peuvent être découpés, s'ils sont trop petits ils peuvent être rassemblés.

Multiplexage et demultiplexage :

- Comme l'établissement d'une communication peut être coûteuse, on peut utiliser la même connexion pour des conversations distinctes.

Lorsqu'il existe plusieurs itinéraires entre la source et la destination il faut choisir la bonne route.

- C'est le **routing**.

32

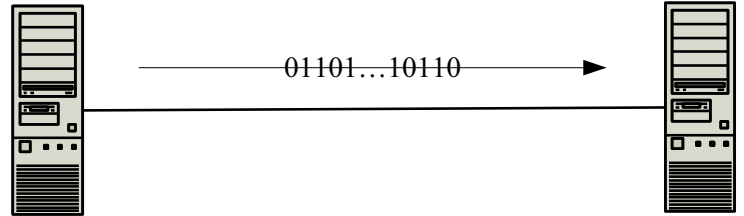
Les services avec connexion

On peut échanger des données :

- en mode connecté :

1. l'émetteur demande l'établissement d'une connexion ;
2. si le récepteur refuse cette connexion, la communication n'a pas lieu ;
3. si la connexion est acceptée, elle est établie ;
4. les données sont ensuite transférées d'un point à l'autre ;
5. la connexion est libérée.

Fonctionnement du réseau téléphonique.



Émetteur

Récepteur

La connexion fonctionne comme un **tuyau** : l'émetteur pousse des objets (1 bit) d'un côté et le récepteur les récupère dans le même ordre de l'autre côté.

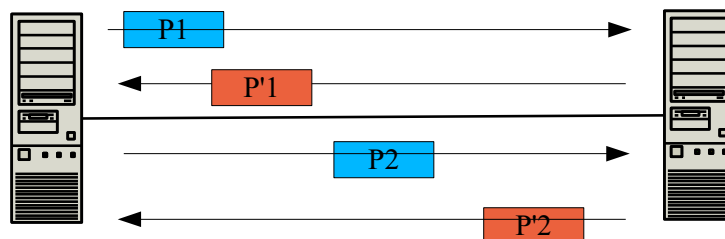
Le récepteur ne peut répondre que lorsque l'émetteur a fini !

33

Les services sans connexion

On peut échanger des données :

- en mode non connecté : les données sont découpées en paquet, chaque paquet est envoyé l'un après l'autre.



Il est possible d'alterner des paquets de l'émetteur avec ceux du récepteur sans attendre la fin des échanges.

C'est le fonctionnement du courrier postal :

- le client poste une lettre
- la lettre porte l'adresse du destinataire
- chaque client possède une adresse propre
- le contenu de l'information est inconnu du prestataire de service
- les supports de transports sont inconnus de l'utilisateur du service.

34

Fiabilité dans les services avec et sans connexion

Chaque service est caractérisé par une qualité de service.

Certains sont de qualités fiables et ne perdent jamais de données :

- système de notification dans lequel le récepteur accuse à l'émetteur la réception de chaque message
=> surcharge de services et donc parfois des délais indésirables mais ça peut en valoir la peine (exemple : transfert de fichier)
- 2 formes : par messages (les messages sont préservés) ou par flots d'octets (les messages sont mis bout à bout sans indiquer les limites de messages)

Un service non fiable sans connexion est appelée **service datagramme**.

Pourquoi préférer une communication non fiable ?

- Le service peut ne pas être disponible (exemple : Ethernet)
- Le problème doit alors être traité dans les couches supérieures
- Les délais introduits pour un service fiable peuvent ne pas être acceptables.

		Services	Exemples
Avec connexion		Flot de messages fiable	Suite de pages
		Flot d'octets fiable	Ouverture de session à distance
		Connexion non fiable	Voix numérique
Sans connexion		Datagramme non fiable	Prospectus électronique
		Datagramme acquitté	Messagerie avec accusé de réception
		Demande-réponse	Interrogation d'une base de données

35

Modèle OSI (1/4)

Développé par l'ISO

Modèle de référence OSI (Open Systems Interconnection)

Modèle général de conception

Couche physique :

Se charge de la transmission des bits à l'état brut sur le canal de communication.

Objectif de conception : s'assurer qu'un bit à 1 envoyé sur une extrémité arrive aussi à 1 de l'autre côté, et non à 0
Concernes le voltage pour représenter les états 0 et 1, la durée d'un bit, la possibilité de transmission dans les deux sens en même temps, l'établissement initial d'une connexion et sa libération lorsque les deux extrémités ont fini, le nombre de broche d'un connecteur et leur rôle, ...

Couche liaison de données :

Objectif : faire en sorte qu'un moyen de communication brut apparaisse à la couche réseau comme étant une liaison exempte d'erreurs de transmission.

Elle décompose les données en **trames de données** (quelques centaines ou milliers d'octets) et envoie les trames en séquence. S'il s'agit d'un service fiable, le récepteur confirme la bonne réception de chaque trame en envoyant à l'émetteur une trame d'acquiescement

Il est important d'éviter qu'un récepteur lent soit submergé de données par un émetteur rapide.

=> utiliser des mécanismes de régulation pour que l'émetteur connaisse la quantité d'espace disponible dans le tampon du récepteur.

=> intégration de mécanisme de contrôle de flux et de gestion des erreurs

Difficulté supplémentaire dans les réseaux à diffusion : **contrôler l'accès au canal partagé !**

- C'est la sous-couche d'accès au média qui gère ce problème

36

Modèle OSI (2/4)

Couche réseau :

Contrôle le fonctionnement du sous-réseau.

Objectif : déterminer comment les paquets sont routés de la source vers la destination.

- Statiquement avec des tables câblées dans le réseau et rarement modifiées
- Dynamiquement au début du dialogue pour la session ou pour chaque paquet selon la charge actuelle du réseau

Elle doit aussi régler tous les problèmes de qualité de service (délais, temps de transit, gigue, ...)

=> causé par exemple par des congestions (trop de paquets en même temps sur le sous-réseau)

Elle doit aussi gérer les problèmes concernant l'adressage (qui peut être différent entre le réseau d'origine et celui de destination), la taille des paquets (paquets trop grands), les protocoles différents, ...

Sur un réseau à diffusion le problème du routage est simple => peu ou pas de couche réseau

Couche transport :

Objectif : Accepter des données de la couche supérieure, de les diviser en unités plus petites si nécessaire, de les transmettre à la couche réseau et de s'assurer qu'elles arrivent correctement à l'autre bout.

Détermine le type de service à fournir à la couche session, et au final à l'utilisateur :

- Celui qui a le plus de succès est le canal point-à-point exempt d'erreur (en réalité très faible taux d'erreur) qui remet les messages ou les octets dans l'ordre dans lequel ils ont été envoyés
- Il existe aussi la remise de messages isolés sans garantie de l'ordre d'arrivée ou la diffusion de messages à plusieurs destinataires (multicast)

La couche transport offre un réel service de bout-en-bout, de la source à la destination.

=> C'est à dire qu'un programme sur la machine source entretient une conversation avec un programme similaire sur la machine de destination en utilisant les entêtes et les messages de contrôle.

Dans les couches plus basses les protocoles sont échangés entre chaque machine et ses voisins immédiats, et non entre les machines source et de destination qui peuvent être séparés par de nombreux routeurs.

37

Modèle OSI (3/4)

Couche session :

Elle permet aux utilisateurs de différentes machines d'établir des **sessions**.

Elle gère divers services comme :

- La gestion du dialogue (suivi du tour de transmission)
- La gestion du jeton (empêchant deux participants de tenter la même opération critique au même moment)
- La synchronisation (gestion de points de reprise permettant aux longues transmissions de reprendre là où elles en étaient suite à une interruption)

Couche présentation :

Elle s'intéresse à la syntaxe et à la sémantique des informations transmises.

Objectif : permettre la communication entre ordinateurs travaillant avec différents représentations de données

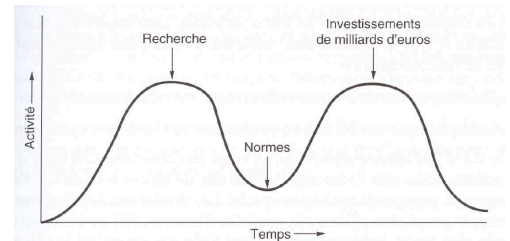
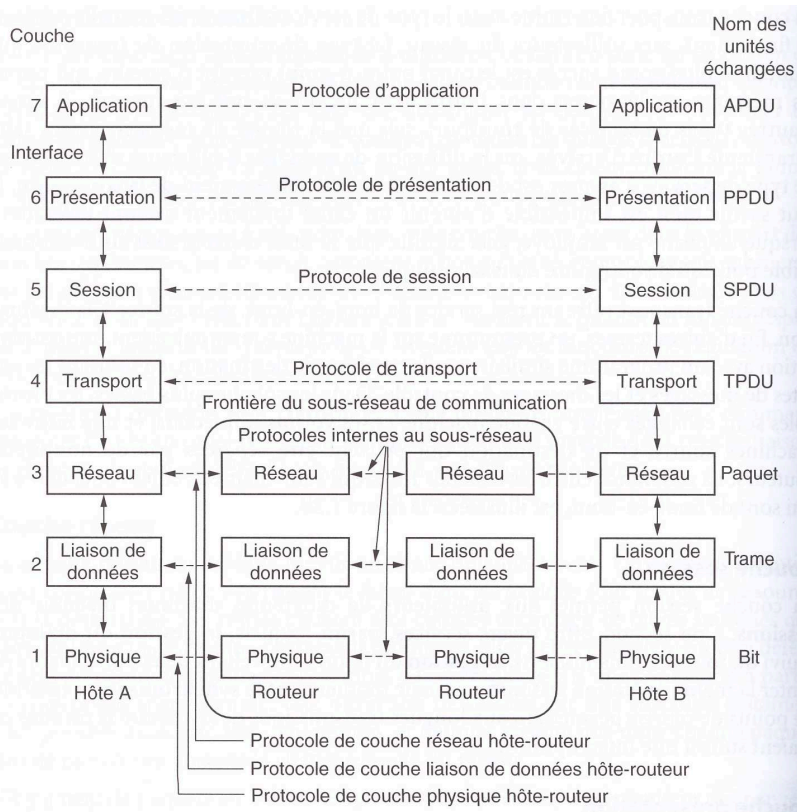
=> définition de structures d'encodage standard.

Couche application :

Elle contient une variété de protocoles qui sont utiles aux utilisateurs :

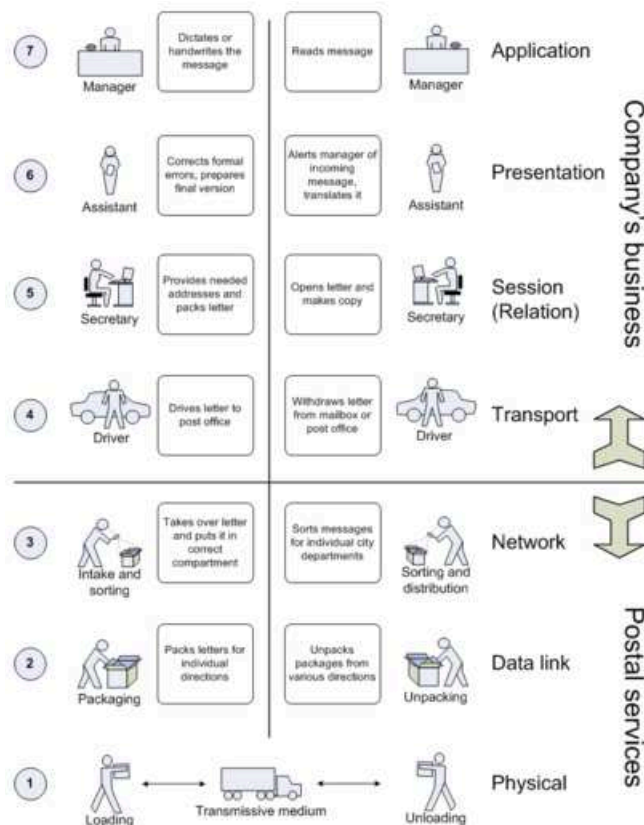
- HTTP => protocole du World Wide Web
- POP/IMAP/SMTP => protocoles pour le courrier électronique
- FTP => protocole pour le transfert de fichiers
- NNTP => protocoles pour les news
- ...

Modèle OSI (4/4)



39

Modèle OSI illustré



RM – OSI and letter communication parallel

40

Modèle TCP/IP

Développé par le DoD (Department of Defense)

Objectifs :

- maintenir la disponibilité du système même en cas de panne de sous-réseaux
- Permettre divers types d'applications (transfert de fichiers, transmission de la parole en temps réel, ...)

Modèle de référence TCP/IP

Déployé d'abord dans les universités américaines puis maintenant presque partout.

Couche internet :

Choix : un réseau à commutation de paquet fondé sur une couche d'interconnexion de réseaux **sans connexion**.

Ici le terme internet = inter-réseau

Cette couche permet aux hôtes d'introduire des paquets sur n'importe quel réseau et fait en sorte qu'ils soient acheminés indépendamment les uns des autres vers leur destination. Si les paquets arrivent dans le désordre les couches supérieures se chargeront de les réordonner si cela fait partie des exigences de livraison.

Analogie avec le courrier postal :

- Lorsqu'une personne envoie des lettres pour l'étranger, il y a de forte chance qu'elles arrivent à destination. Elles seront probablement traitées par un ou plusieurs centres de transit internationaux, mais cela reste transparent pour les utilisateurs, qui n'ont pas non plus à se préoccuper du fait que chaque pays (c'est à dire chaque réseau) dispose de ses propres timbres, formats d'enveloppes et règles de distribution.

La couche internet définit un format de paquet officiel et un protocole nommé IP (Internet Protocol). Son rôle étant d'acheminer les paquets IP jusqu'à leur destination, elle s'occupe donc principalement du routage et de l'évitement des congestions.

Semblable à la couche réseau du modèle OSI.

41

Modèle TCP/IP

Couche transport :

À l'instar de la couche transport OSI, son rôle est de permettre à des entités paires sur les hôtes source et destination de mener une conversation.

Deux protocoles ont été définis :

- TCP (Transmission Control Protocol) : protocole fiable avec connexion qui garantit la livraison sans erreur sur n'importe quel hôte de l'inter-réseau d'un flot d'octets émis par une machine. Il fragmente le flot d'octets entrant en messages qu'il passe à la couche internet. À l'arrivée, le processus TCP destinataire réassemble les messages reçus en flot de sortie (pour la couche application). TCP assure aussi un contrôle de flux.
- UDP (User Datagram Protocol) : protocole non fiable sans connexion qui permet d'assurer elles-mêmes le séquençement et le contrôle de flux plutôt que de faire appel à TCP. Il est utilisé largement par les applications de type demande-réponse dans des environnements client-serveur et pour celles pour lesquelles le plus important est d'avoir des données à temps comme la transmission de son ou de l'image.

Couche application :

Pas de couche session et de couche de présentation dans ce modèle.

De toute façon la plupart des applications ne les utilisent pas.

Elle contient de nombreux protocoles de haut niveau : Telnet (protocole de terminal virtuel), FTP, DNS (Domain Name System) pour associer des noms d'hôtes aux adresses de réseau, ...

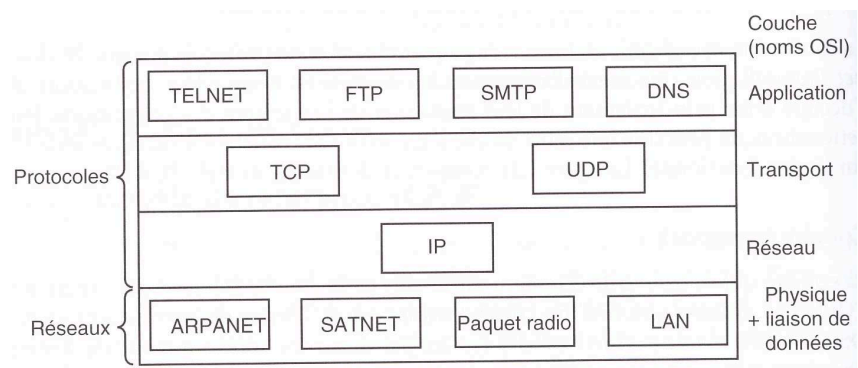
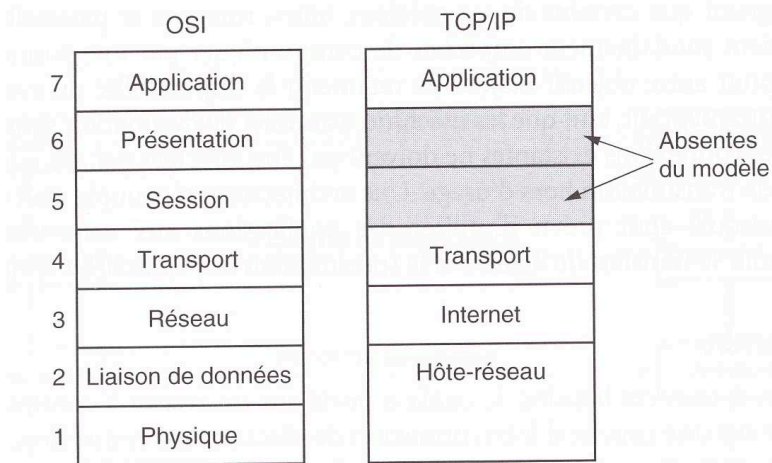
Couche hôte-réseau :

Grand vide pas vraiment défini.

L'hôte doit pouvoir se connecter au réseau en utilisant un protocole pour pouvoir envoyer des paquets.

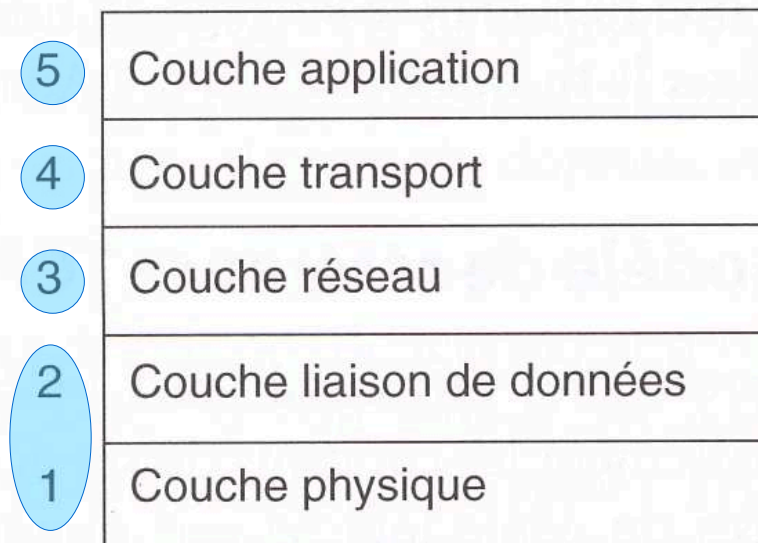
42

Modèle TCP/IP (vs OSI)



43

Suite du plan du cours



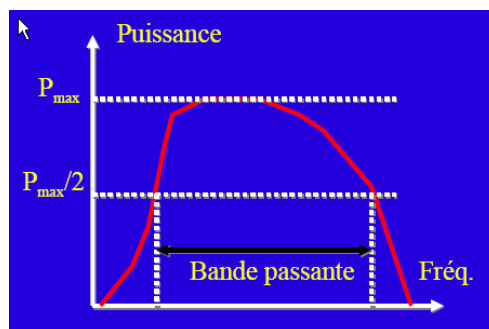
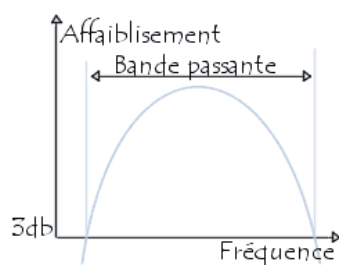
44

Couche physique

45

Bande passante

La bande passante d'une voie de transmission est l'intervalle de fréquence sur lequel le signal ne subit pas un affaiblissement supérieur à une certaine valeur (généralement 3db, car 3décibel correspondent à un affaiblissement du signal de 50%).



Notion de bande passante

désigne la différence en Hertz entre la plus haute et la plus basse des fréquences utilisables sur un support de transmission.

Dans la pratique, ce terme désigne le débit d'une ligne de transmission, calculé en quantité de données susceptibles de transiter dans un laps de temps donné (en général exprimé en secondes).

Plus la bande passante est large, plus le volume d'informations qui transitent est important.

On verra qu'il est possible de coder plusieurs bits par Hertz.

Bande passante d'un système de transmission:

- Paire métallique : ~ 10 MHz
- Câble coaxial : ~ GHz
- Fibre optique : ~ 100 GHz

46

Support de transmission guidés : la transmission filaire (1/2)

Support magnétique :

Bande magnétique, DVD, etc.

- Exemple : les sauvegardes d'une banque => réseau pas assez puissant et cher

Coût par bit versus délai de transmission

Ne sous-estimez jamais la bande passante d'une fourgonnette pleine de bandes magnétiques, lancée à fond sur l'autoroute.

Paire torsadée

Deux fils de cuivre isolés d'une épaisseur d'environ 1mm enroulés l'un sur l'autre de façon hélicoïdale pour réduire les radiations électromagnétiques perturbatrices.

=> les ondes rayonnées par chaque torsade s'annulent

Pas besoin d'amplification sur plusieurs kilomètres

=> au delà des répéteurs sont nécessaires

Utilisation : quand une connexion immédiate est requise.

- Exemple : le système téléphonique
- Pour la transmission de signaux analogiques ou numériques

La bande passante dépend de l'épaisseur du câble et de la distance à parcourir => plusieurs Mbit/s sur quelques km



© Pearson Education France

Câble coaxial (coax)

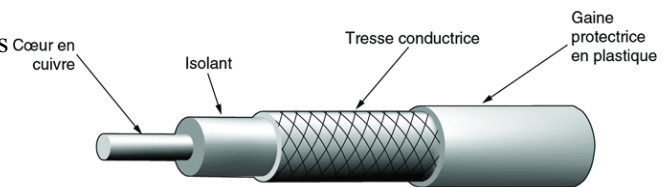
Il se compose d'une âme, un conducteur rigide en cuivre, enfermée dans un matériau isolant, lui-même entouré d'une tresse protectrice. Une gaine plastique protège le tout.

Meilleure protection que la paire torsadée => meilleurs débits

Utilisation :

- Exemple : télévision par câble et réseaux métropolitains
- Principalement pour la transmission numérique

Bande passante proche de 1GHz



© Pearson Education France

Support de transmission guidés : la transmission filaire (2/2)

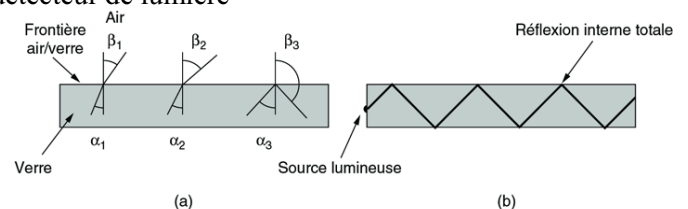
Fibre optique

Evolutions :

- Processeurs 4,77 MHz (1981) -> 2 GHz (aujourd'hui) => facteur de 20/décennie
- Débits 56kbit/s à 1 Gbit/s (ligne optique moderne) => facteur de 125/décennie et réduction du taux d'erreurs de transmission d'un bit de 10^{-5} à presque zéro

Principe :

- Une source de lumière, le support de transmission et le détecteur de lumière
 - Par convention
la présence de lumière = 1
son absence = 0
 - Conversion optique/électrique aux deux extrémités
 - Tout dépend de l'angle du rayon incident et des indices de réfraction
- => fibre multimode et fibre monomode (guide d'ondes)



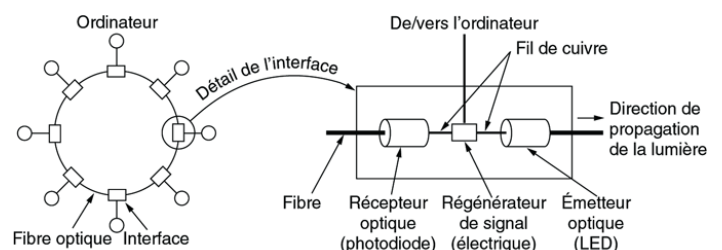
© Pearson Education France

Aujourd'hui limitations dues aux technologies de conversion de signaux électriques et optiques

=> 10 Gbit/s au lieu des 50 Tbit/s « possible »

Exemple de réseau LAN en fibre optique :

- ici un anneau
- Il se utilise des répéteurs actifs
=> ceux purement optiques sont plus performants
- Les réseaux à diffusion sont aussi possibles



© Pearson Education France

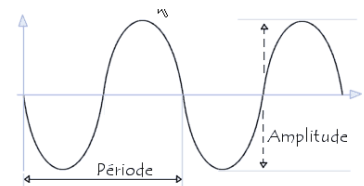
Supports de transmission non guidés : la transmission sans fil (1/2)

Perspectives :

Seuls subsisteront la fibre optique et le sans fil ?

Avantages :

Économique et parfois seule solution possible (exemple Hawaï)



Spectre électromagnétique :

Lorsque des électrons sont en mouvement, ils créent des ondes électromagnétiques qui peuvent se propager dans l'espace (même dans le vide) => principe de l'antenne.

Identifiées et prévues par James Clerk Maxwell en 1865 et observées par Heinrich Hertz en 1887.

Le nombre d'oscillations par seconde d'une onde et appelée **fréquence**, f , et se mesure en Hertz

La distance entre deux maxima (ou minima) d'une onde est appelée **longueur d'onde**, λ .

Dans le vide **toutes les ondes** se propagent à la même vitesse, la **vitesse de la lumière**, c , de 300 000 km/s.

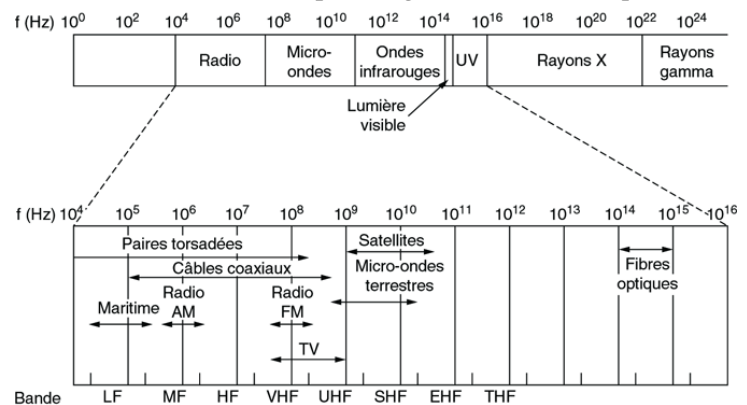
Dans le cuivre ou la fibre optique la vitesse est de 2/3 de celle dans le vide et dépend légèrement de la fréquence

Dans le vide : $\lambda * f = c$

Remarque : ne pas confondre λ et la période $T = 1/f$

Partie du spectre utilisable pour la transmission :

- Entre 10^4 et 10^{16} Hz.
- Au delà dangerosité pour l'homme



© Pearson Education France

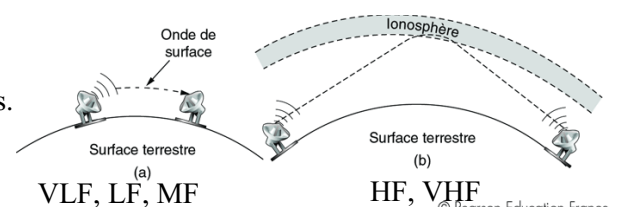
Supports de transmission non guidés : la transmission sans fil (2/2)

Transmission d'ondes radio

Facile à générer avec une antenne.

Elles sont omnidirectionnelles => pas d'alignement des antennes.

Se propagent sur de longues distances et traversent très bien les obstacles. => Très réglementé par les gouvernements



© Pearson Education France

General Motor : Cadillac avec frein antiblocage (1970) => Problèmes dans l'Ohio en présence de la police

Transmission de micro-ondes

Après 100 MHz les ondes se propagent pratiquement en ligne droite et peuvent être étroitement concentrées.

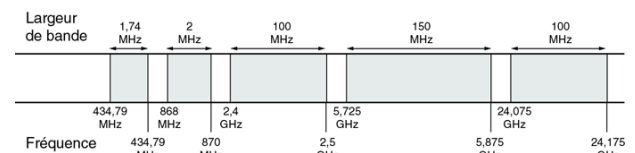
Ces ondes ne traversent pas les murs.

Utilisation : téléphonie mobile, diffusion TV, etc.

Le spectre est très encombré.

Bande ISM (Industrial, Scientific, Medical)

- WiFi, Bluetooth
- Tout le monde peut émettre avec une puissance limitée



© Pearson Education France

Transmission d'ondes infrarouges et millimétriques

Très directif => télécommande

Ne traversent pas les objets solides. (=> pas de licence d'exploitation)

Avantage et inconvénient : pas d'interférence avec le voisin

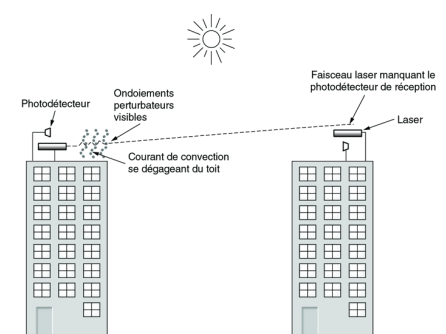
Transmission d'ondes lumineuses

Large bande passante à faible coût.

Pas de licence d'exploitation.

Très directif.

Inconvénient : perturbé par la pluie, par le brouillard, par de fortes chaleurs



© Pearson Education France

Réseau téléphonique public commuté

Réseau téléphonique commuté (RTC)

Objectif : transmettre la parole humaine sous une forme plus ou moins reconnaissable.

Développement de son utilisation pour faire communiquer des ordinateurs sur de longues distances.

- Car moins cher que de faire courir un câble entre les machines ;
- mais il est moins rapide : 56 kbit/s contre 1 Gbit/s avec un LAN => facteur de 20000 (1000 à 2000 avec l'ADSL)

Structure du réseau téléphonique :

1876, Graham Bell dépose un brevet

Au départ téléphones vendus par paires !

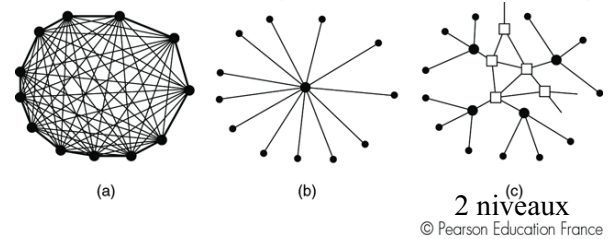
=> toiles d'araignées dans les villes sur les toits, les arbres, ...

1878 Bell Telephone Compagny invente le central téléphonique

Une opératrice faisait les branchements

Développement d'un second niveau de central pour permettre d'interconnecter les villes.

Il y a aujourd'hui 5 niveaux.



Desserte locale au moyen de paire de fils de cuivre torsadés : de 1 à 10 km. Aussi appelée **boucle locale**.

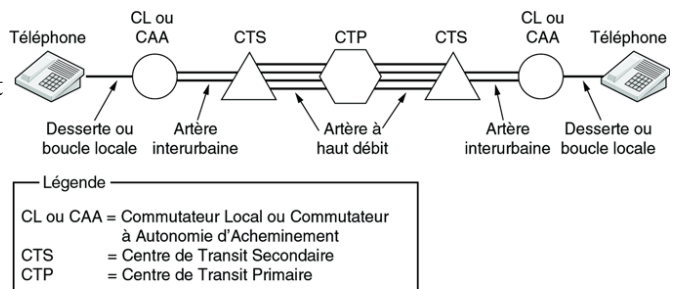
Toutes les boucles locales du monde = 1000 fois la distance terre-lune.

80% de la valeur du capital d'AT&T était sa boucle locale.

Lorsque deux abonnés du même CL se téléphonent ils sont mis en contact directement.

Les commutateurs routent les appels

Possibilité de faire passer plusieurs appels sur les artères interurbaines grâce au multiplexage.



© Pearson Education France



funlok.com



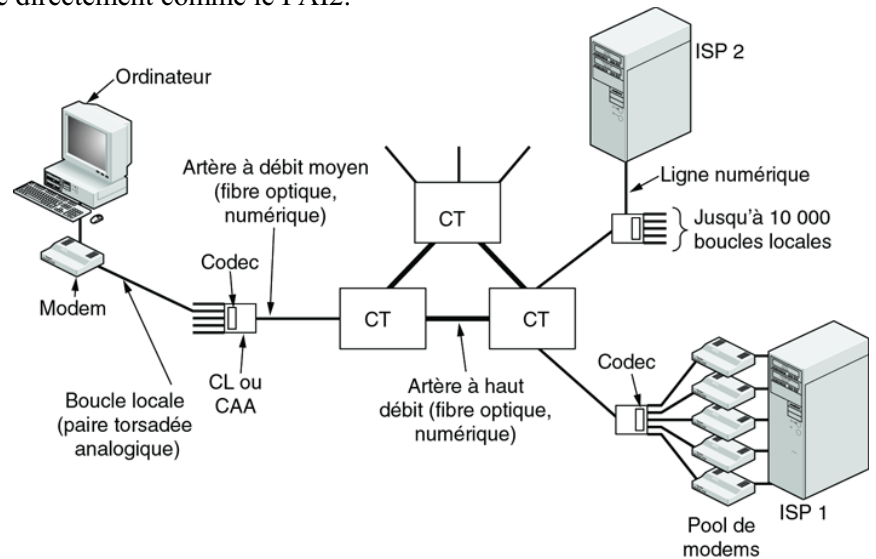
funlok.com

Desserte locale : modems, ADSL et boucle locale radio (BLR)

La desserte locale est analogique depuis plus d'un siècle et le restera sûrement encore longtemps.

Lorsqu'un ordinateur souhaite envoyer des données (numériques) sur une liaison commutée analogique, celles-ci doivent d'abord être converties dans une forme analogique pour être transmises sur la boucle locale. => modem
Dans le central téléphonique ce signal analogique est converti dans une forme numérique par un codec pour transiter sur les artères numériques longue distance.

Le FAI (ISP = Internet Service Provider) à l'autre extrémité de la liaison dispose de modems pour faire la conversion inverse (analogique -> numérique). Le FAI1 gère autant de connexion qu'il a de modems.
Maintenant on utilise une ligne numérique directement comme le FAI2.
=> moins de bruit => plus de débit



© Pearson Education France

Modem (Modulateur-démodulateur)

Pour résoudre les difficultés associées à la transmission de signaux numériques sur les lignes téléphoniques, on recourt aux signaux analogiques.

On introduit un signal sinusoïdal : la **porteuse** (entre 1000 et 2000Hz)

On module pour représenter le 0 et le 1 :

- Modulation d'amplitude (AM)
- Modulation de fréquence (FM)
- Modulation de phase (PM) à 180°

Si on module à 45°, 135°, 225°, 315° on peut transmettre 2 bits par intervalle de temps.

Le nombre de modulation par seconde se mesure en **bauds**.

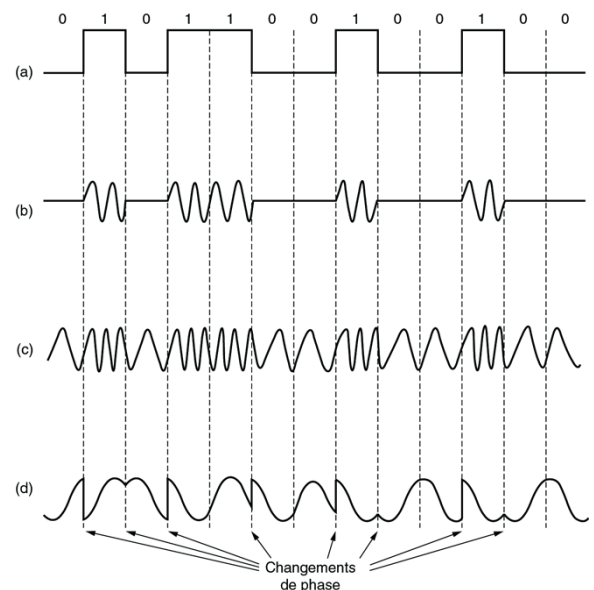
Durant chaque baud, un symbole est envoyé.

2400 bauds => 1 symbole toutes les 416,667 µs.

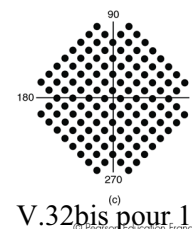
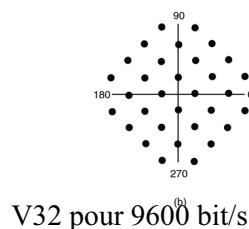
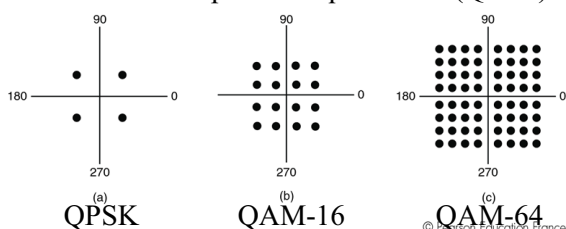
Si on représente le 0 par 0 volt et le 1 par 1 volt le débit binaire est de 2400 bit/s.

Si on utilise 4 tensions (0, 1, 2 et 3 volts) chaque symbole se compose de 2 bits et on a un débit de 4800 bit/s

Modulation de phase en quadrature (QPSK)



© Pearson Education France



DSL

Les opérateurs téléphoniques tentent de concurrencer les câblo-pérateurs et les sociétés de communication via satellite en proposant des services large bande. Ils doivent coexister avec le téléphone.

ADSL (Asymmetric Digital Subscriber Line)

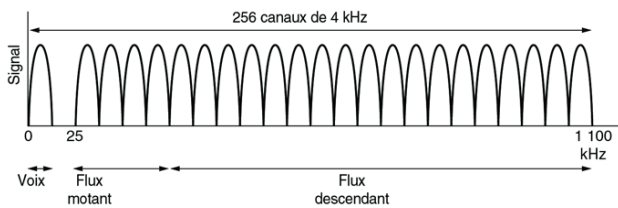
Le réseau téléphonique est optimisé pour la voix. Aussi lorsque la boucle locale arrive au central téléphonique, le câble passe par un filtre qui ne gardent que les fréquences entre 300 Hz et 3400 Hz (coupure à 3dB pour les 2) => bande passante = 3100 Hz

Idée : utiliser le reste de la BP car la bande passante théorique de la ligne est d'environ 1MHz s'il n'y avait pas le filtre (suivant la distance et la qualité du câble) => problème de choix du débit et de l'étendu de l'offre (installation de DSLAM).

Une solution de partage du spectre fréquentiel : le multinomialité discrète (DMT)

Canal 0 pour la voix. Canal 1-5 inutilisé et les 250 autres pour les données (1 pour le contrôle de flux montant et le contrôle de flux descendant) => *Asymmetric* à cause des capacités des flux.

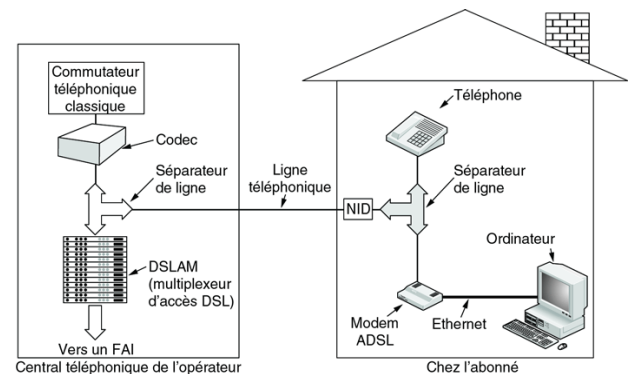
Pour chaque canal une technique de modulation semblable à V.34 est utilisée.



© Pearson Education France

NID (Network Interface Device)

Le séparateur de ligne se remplace maintenant par un filtre passe-bas (à 3400Hz pour le téléphone) et un filtre passe haut (à 26kHz pour le modem) intégré dans la prise.



© Pearson Education France

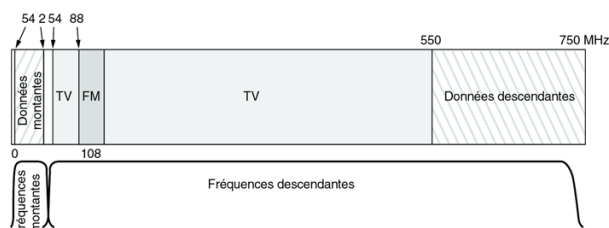
L'internet par le câble

Développement de liaison hybride HFC (Hybrid Fiber Coax) avec à la jonction des convertisseurs électro-optiques (les centres de distributions)

Inconvénient : le même câble est partagé par plusieurs abonnés => problèmes de bande passante

Solution : diviser les longs câbles en segment connecté au centre de distribution (car BP de la tête de réseau est quasiment infinie). Entre 500 et 2000 abonnés par câble.

Avantage : pour la diffusion de programmes TV qu'il y ait 10 ou 10000 téléspectateurs.



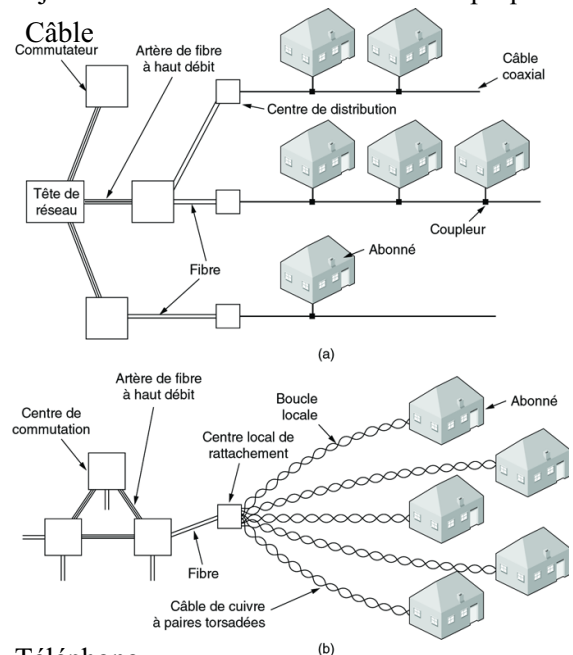
© Pearson Education France

1 canal fait de 6 à 8 MHz

On constate une asymétrie dans les flux montant et descendant.

Comme les signaux TV ne sont que descendant il a fallu employer des amplificateurs opérants dans la plage montante des 5-42 MHz et d'autre opérant uniquement dans la plage descendante au dessus de 54 MHz.

Pour les canaux montant on utilise QPSK => grande asymétrie.



© Pearson Education France

Téléphone

Boucle locale radio (BLR)

MMDS (Multichannel Multipoint Distribution Service)

Utilisation de micro-ondes : portée d'environ 50 km. Traverse relativement bien la végétation et la pluie.

Avantages : technologie bien connue, équipement est disponible

Inconvénient : bande passante totale disponible est limitée et partagée par plusieurs utilisateurs sur une zone géographique assez étendue.

LMDS (Local Multipoint Distribution Service)

Utilisation d'ondes millimétriques avec une largeur de bande de 1,3GHz : très directives. Portée d'environ 2 à 5km.

Sensible à la pluie et à la végétation.

=> il faut de nombreuses tours

=> on augmente la puissance selon les conditions (pluie, ...)

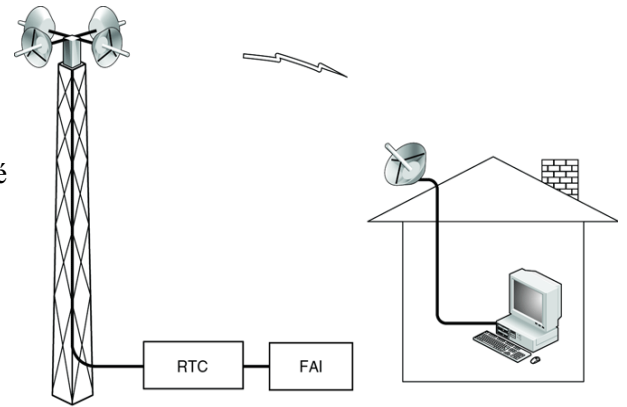
Actuellement : 36Gbit/s en descendant et 1 Mbit/s en montant

1 tour avec 4 antennes => 100000 clients si 1 sur 3 est connecté

A noter :

Ces installations nécessitent l'intervention d'un technicien

Normalisé sous IEEE 802.16 : MAN sans fil (WMAN)



© Pearson Education France

Couche liaison de données

Le contrôle de flux

Lorsqu'un émetteur émet systématiquement plus de trames que le récepteur ne peut en accepter, il se pose un problème.

- quand l'émetteur est sur un ordinateur rapide (ou peu chargé)
 - quand le récepteur est sur une machine lente (ou très chargé)
- => Il faut un mécanisme pour éviter cette situation

Il existe deux approches pour résoudre ce problème :

- un contrôle de flux avec retour d'information (rétroaction) pour contraindre l'émetteur à ne pas envoyer plus de trames que le récepteur peut en accepter.
- un contrôle de flux basé sur le débit : mécanisme intégré au protocole pour limiter le débit de transmission des données sans exploiter de retour d'information (jamais utilisé dans la couche liaison de données)

Il existe de nombreuses variantes de contrôle de flux avec rétroaction.

En général, il est interdit d'envoyer des trames s'il n'y a pas eu auparavant une permission explicite ou implicite du récepteur

- exemple : « Tu peux m'envoyer maintenant n trames, mais après ces n émissions, suspend tes envois jusqu'à ce que je te dise de continuer ».

59

Détection et correction d'erreurs

Selon leur nature les supports de transmission sont sujet à l'apparition d'erreurs dans les messages transportés

Elles peuvent intervenir par rafales ou de façon isolées (dépend de la nature du support)

=> il faut donc mettre en place des mécanismes pour détecter ces erreurs, voir les corriger

- **code correcteur d'erreurs** : inclure dans les blocs de données suffisamment de redondance pour que le récepteur soit capable de restituer les données originales
- **code détecteur d'erreurs** : ajouter juste assez de redondance dans les données à transmettre pour que le récepteur puisse détecter les erreurs et redemander la transmission.

L'utilisation de ces codes dépend du canal de transmission

- fiable (exemple : la fibre optique) : le code détecteur d'erreurs est moins lourd. On retransmettra seulement l'éventuel bloc défectueux.
- non fiable (exemple : réseau sans fil) : il est préférable d'ajouter suffisamment de redondance à chaque bloc pour permettre au récepteur de trouver le bloc d'origine, au lieu de se baser sur la retransmission, qui peut également être erronée

Code détecteur d'erreurs simple : le **contrôle de parité**

- On ajoute aux bits de données **un bit de parité**.
- Celui-ci est choisi de façon que le nombre de bits 1 dans le mot de code soit pair (ou impair).
- exemple : pour envoyer 1011010 en parité paire, on ajoute un bit à la fin pour obtenir 10110100. En parité impaire, 1011010 devient 10110101.
- Il permet de détecter UNE erreur simple.

Il y a des codes détecteurs d'erreur bien plus puissants.

60

PPP (le protocole point-à-point)

L'essentiel de l'architecture de l'Internet repose sur des liaisons louées point-à-point.

- par exemple entre les routeurs de différents backbones (LAN fédérateur d'un FAI).

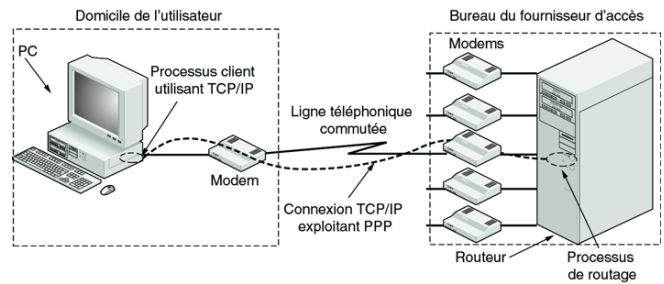
On retrouve les connections point-à-point pour les millions d'utilisateurs qui accèdent à l'internet en utilisant les liaisons téléphoniques et des modems.

PPP est donc nécessaire pour :

- le trafic routeur routeur
- le trafic domestique à un fournisseur d'accès

Il gère la détection d'erreurs

Il permet la négociation d'adresses IP à la connexion



© Pearson Education France

PPP fournit trois choses :

- une méthode qui délimite sans ambiguïté la fin de trame et le début de la suivante. Le format de trame permet également la détection des erreurs.
- un protocole de contrôle de la liaison qui active la ligne, la teste, négocie les options et la désactive proprement lorsqu'on n'en a plus besoin.
- un moyen de négocier les options de la couche réseau indépendamment du protocole de couche réseau à utiliser.

Une trame PPP :

Octets	1	1	1	1 ou 2	Variable	2 ou 4	1
	Fanion 01111110	Adresse 11111111	Contrôle 00000011	Protocole	Charge utile	Total de contrôle	Fanion 01111110

© Pearson Education France

61

Ethernet (1/3)

Protocole utilisé dans les réseaux à diffusion (LAN)

1970 : ALOHANET

Dans un archipel hawaïen ne disposant pas d'un système téléphonique Norman Abramson tente de relier à l'ordinateur central de l'université (Honolulu) des utilisateurs d'îles éloignées.

- impossible de tirer des câbles (trop cher)
- => utilisation d'onde radio de faible portée

Chaque terminal disposait d'un dispositif radio à 2 fréquences : une montante (vers l'ordinateur central) et une descendante.

Quand un utilisateur voulait contacter le central il transmettait simplement le paquet de données sur le canal montant. Si personne ne transmettait en même temps le paquet était acheminé vers sa destination et acquitté par voie descendante. Lorsque un conflit se produisait, il n'y avait pas d'acquiescement et le terminal essayait d'émettre à nouveau.

Il ne pouvait pas y avoir de collision sur le canal descendant car seule l'ordinateur central émettait.

Le système fonctionnait assez bien lorsqu'il y avait de faible fréquentation

- Bob Metcalfe après son doctorat à Harvard va travailler avec Abramson pendant les vacances puis il est embauché au centre de recherches de Palo Alto (PARC) de Xerox. Il conçoit un système pour les ordinateurs personnels basé sur ALOHANET et le nomme Ethernet (éther lumineux). Il fonde 3Com (plus de 100 millions de cartes vendues)

La trame Ethernet :

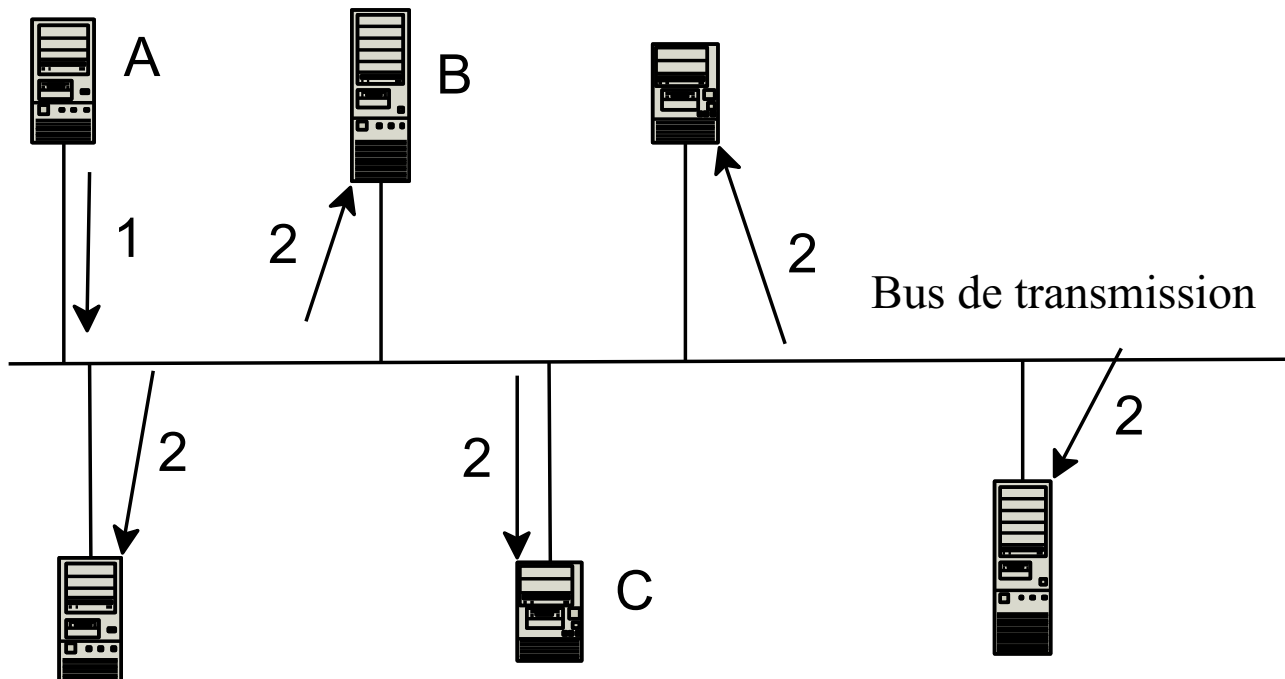
Octets	8	6	26		0-1500	0-46	4
(a)	Préambule	Adresse de destination	Adresse source	Type	Données	Remplissage	Total de contrôle

Ethernet (2/3)

La transmission de l'information

A veut communiquer avec B :

- elle transmet en (1) son message sur le bus de transmission ;
- en (2), toutes les machines connectées au bus reçoivent le message (B comme C) !



63

Ethernet (3/3)

Comment se passe la communication dans un réseau à diffusion ?

CSMA/CD

- Carrier Sense (Détection de porteuse);
- Multiple Access (accès multiple);
- with Collision Detection (avec détection de collision).

Les ordinateurs peuvent transmettre lorsqu'ils le désirent :

- si deux paquets (ou plus) entrent en **collision**, chaque ordinateur attend un temps aléatoire et réémet son paquet.

64

L'adressage dans Ethernet

Chaque carte réseau possède une adresse matérielle appelée adresse MAC (*Medium Access Control*).

Cette adresse est unique par rapport à toutes les cartes réseaux existantes !

Elle est exprimée sur 48 bits ou **6 octets**.

Syntaxe : 08:22:EF:E3:D0:FF

Adresse de Broadcast : FF:FF:FF:FF:FF:FF

Des tranches d'adresses sont affectées aux différents constructeurs :

00:00:0C:XX:XX:XX **Cisco**

08:00:20:XX:XX:XX **Sun**

08:00:09:XX:XX:XX **HP**

Avantage : impossible de trouver deux fois la même adresse dans un même réseau.

65

Bilan : adressage du réseau et communication avec une machine distante

Nous avons vu que :

pour pouvoir communiquer avec une machine distante celle-ci doit avoir une adresse

On sait que :

Ethernet est déployé partout ou presque.
chaque machine possède une adresse MAC via sa carte réseau
Ethernet fonctionne par diffusion

Problème 1 :

Dans des gros réseaux on ne peut pas diffuser un message sur la totalité car il y aurait beaucoup trop de collisions et il serait impossible d'utiliser le réseau.

Solution 1 :

Il faudrait faire du point à point entre le sous réseau de la machine source et celui de la machine cible.

Problème 2 :

Ethernet ne permet pas de localiser une machine dans un sous-réseau.
– L'adresse MAC ne donne aucune information sur la **localisation** d'une machine
(dans quel réseau est la machine avec qui je veux parler ?)

Solution 2 :

Mettre une couche supplémentaire pour assurer le routage point à point (**c'est le travail de la couche réseau**) puis diffuser une fois le sous réseau atteint.

Une des solutions inventées et utilisées sur l'Internet est le **protocole IP** !

66

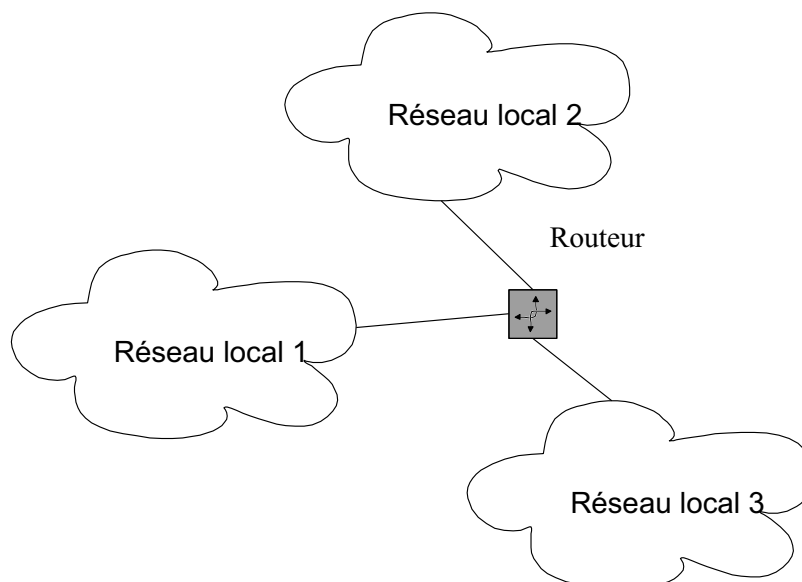
Couche réseau

67

Principe d'interconnexion de réseaux (1/2)

Synthèse

- des réseaux locaux à diffusion ;
- quand les distances augmentent il faut utiliser du point à point ;
- les machines doivent disposer d'un adressage pour pouvoir être jointe ;
- cet adressage doit être commun entre tous les réseaux ;
- il n'est pas nécessaire d'utiliser le même adressage à l'intérieur d'un réseau.

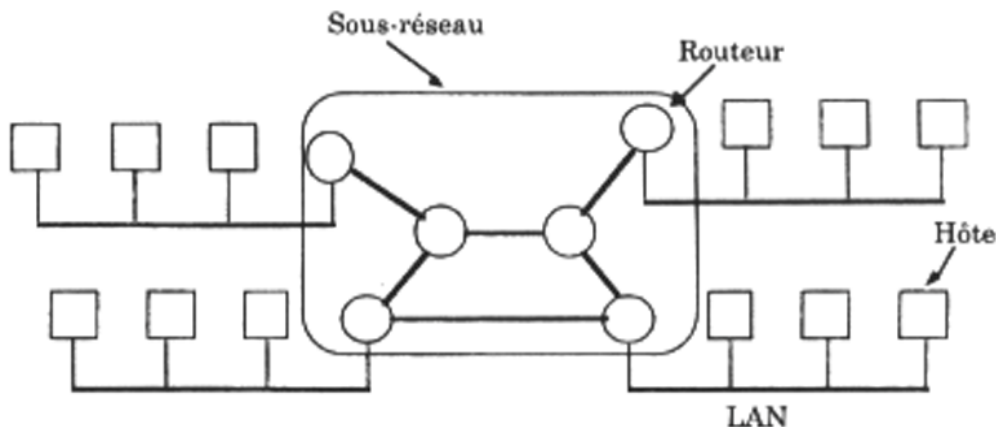


68

Principe d'interconnexion de réseaux (2/2)

Autre schéma

Ici il y a un sous réseau d'inter-connexion.



Exemple : Renater

69

L'acheminement des paquets

Commutation et routage

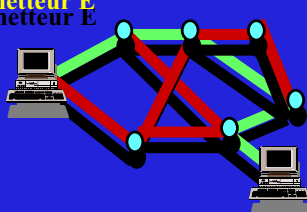
Il existe deux techniques principales d'acheminement

1^{ère} technique : Commutation

Les informations d'un même client suivent toujours un chemin déterminé à l'avance

Emetteur E

1 2 3



Recepteur R

1 2 3

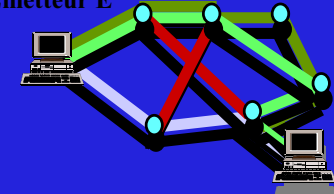
- > 1 info contient 1 référence décrivant le « circuit virtuel »
- > Technique utilisée pour ATM

2^{ème} technique : Routage

Les informations d'un même client peuvent prendre des chemins différents

Emetteur E

1 2 3



Recepteur R

1 3 2

- > 1 info contient 1'adresse complète de R
- > Gestion d'une table de routage
- > Technique utilisée pour Internet

70

Adresse IP

Adresse IP : <adresse réseau>.<adresse machine>

L'adresse IP est décomposée en deux parties :

- un identifiant de réseau
- un identifiant d'ordinateur dans ce réseau

Chaque ordinateur et chaque routeur du réseau Internet possède une **adresse IP**.

Chaque adresse IP est **unique**.

Elle est codée sur 32 bits.

Elle est représentée par commodité sous forme de 4 entiers variant entre 0 et 255 séparés par des points.

Exemple : 164 . 81 . 60 . 43 *une machine dans le bâtiment Jidé*

Un organisme officiel, le "NIC" (*Network Information Center*) est seul habilité à délivrer des numéros d'identification des réseaux.

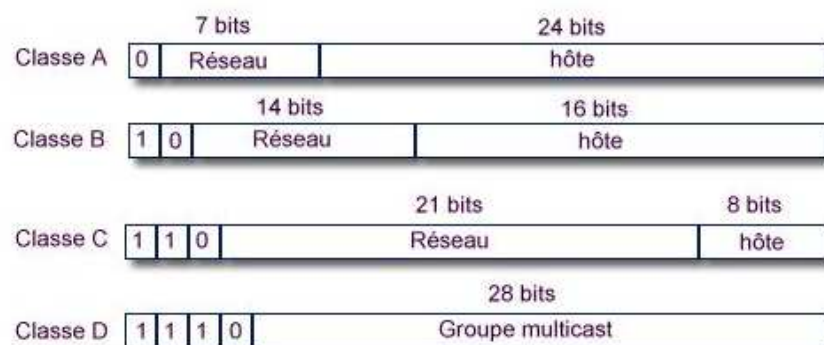
Dans le cas d'un routeur interconnectant 2 réseaux différents, il possède une adresse IP pour chacun des réseaux.

Il existe différentes répartitions des 32 bits entre identifiant réseau et identifiant machine.

Ces différentes répartitions définissent un ensemble de **classes de réseaux**.

71

Les classes de réseaux



Nom de la classe	Numéros TCP/IP	Nombre max de réseaux pour la classe	Nombre maxi de machines par réseau
Classe A	0.x.x.x 127.x.x.x	127	16 777 216
Classe B	128.x.x.x 191.x.x.x	16383	65534
Classe C	192.x.x.x 223.x.x.x	2 031 616	254
Classe D	224.x.x.x 239.x.x.x	N.A	N.A
Classe E	240.x.x.x 247.x.x.x	N.A	N.A

72

Adresses IP réservées

Des adresses particulières

Ces adresses permettent d'effectuer :

- des envois de messages multi-destinataires
- désigner la machine courante
- désigner le réseau courant.

Tout à zéro		L'ordinateur lui-même
Tout à zéro	id. de machine	Un ordinateur sur le réseau lui-même
Tout à 1		Diffusion limitée au réseau lui-même
Id. de réseau	Tout à 1	Diffusion dirigée vers ce réseau
127	Nombre quelconque	Boucle

L'adresse de boucle (127.X.Y.Z) permet d'effectuer :

- des communications inter-programme sur la même machine
- des tests de logiciels réseaux.

Dans ces cas là, les paquets ne sont pas réellement émis sur le réseau.

- 0.0.0.0 est utilisé par une machine pour connaître sa propre adresse IP lors d'un processus d'amorçage. *Elle devra se procurer une adresse IP par l'intermédiaire d'une autre machine.*
- 255.255.255.255 est une adresse de diffusion locale car elle désigne toutes les machines du réseau auquel appartient l'ordinateur qui utilise cette adresse. *pas de connaissance du réseau.*
- Les adresses de classe A de 10.0.0.0 à 10.255.255.255, de classe B de 172.16.0.0 à 172.31.255.255 et de classe C de 192.168.0.0 à 192.168.255.255 sont réservées à la constitution de réseaux privés appelés **intranet**.

73

La notion de sous-réseau

Partition d'un réseau en différents sous-réseaux.

Avantages :

Éviter d'avoir recours à plusieurs numéros de réseaux (classe A, B, ou C) pour regrouper différentes machines au sein d'une même entité (l'université de Limoges par exemple avec les machines du site de Jidé, du campus de Vanteaux, du campus de La Borie...).

L'ensemble des sous-réseaux est vu de l'extérieur comme un unique réseau (gestion du courrier...).

La mise en œuvre est logicielle :

- Définition de sous-réseaux en découpant l'identificateur machine en deux parties :
<id. de réseaux sur 16 bits>.<id. de sous-réseau sur 8 bits>.<id. de machine sur 8 bits>.

Le découpage autour du point facilite le travail des routeurs.

Une machine connecté à un sous-réseau doit connaître :

- son adresse IP,
- le nombre de bits attribués à l'identificateur du sous-réseau et à celui de la machine.

Masque de sous-réseau (*subnet mask*) :

c'est un mot de 32 bits contenant :

- des bits à 1 à la place de l'identificateur de réseau et de sous-réseau,
- des bits à zéro au lieu et place de l'identificateur de machine.

Ainsi, 255.255.255.0 indique que les premiers 24 bits désignent le sous-réseau.

De cette manière à partir de l'adresse d'un datagramme et de son masque de sous-réseau une machine peut déterminer si le datagramme est destiné à une machine sur son propre sous-réseau ou à une machine extérieure.

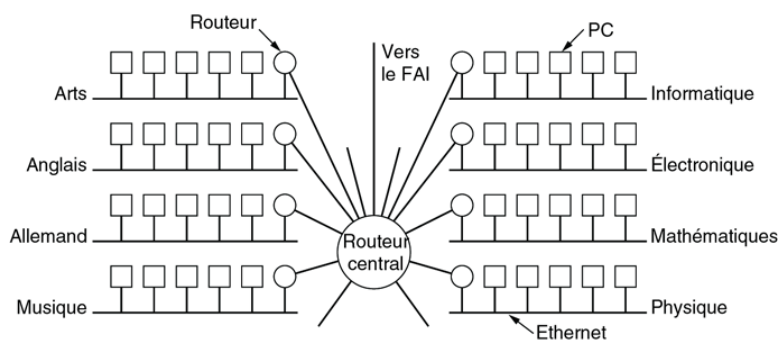
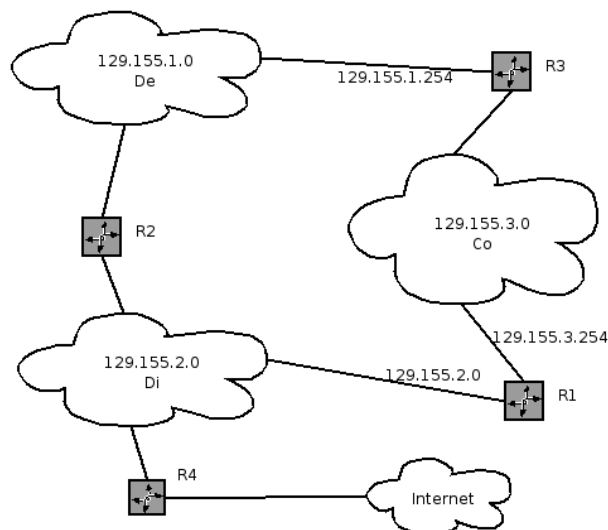
74

Exemple de réseaux et notion de routage

On remarque :

- 3 sous réseaux
- le réseau internet
- 4 routeurs avec chacun 2 IP !
- plusieurs routages possibles

On peut localiser une machine dans les sous-réseaux



© Pearson Education France

75

Création d'un réseau

Il faut :

- choisir une classe de réseau en fonction du nombre de machines à connecter en prenant en compte les besoin actuels et futurs ;
- choisir une adresse de réseau dans la classe choisie.
Exemple : 192.168.12.0 pour un réseau intranet
- affecter une adresse IP unique à chaque machine connectée au réseau :
Exemple : <192.168.12>.<1> la machine de Paul
<192.168.12>.<2> la machine de Nathalie
<192.168.12>.<20>
...
<192.168.12>.<29> 10 adresses réservées pour les postes des élèves
- noter chaque adresse et la machine à laquelle elle est affectée.
Cela facilite le travail de l'administrateur du réseau !

76

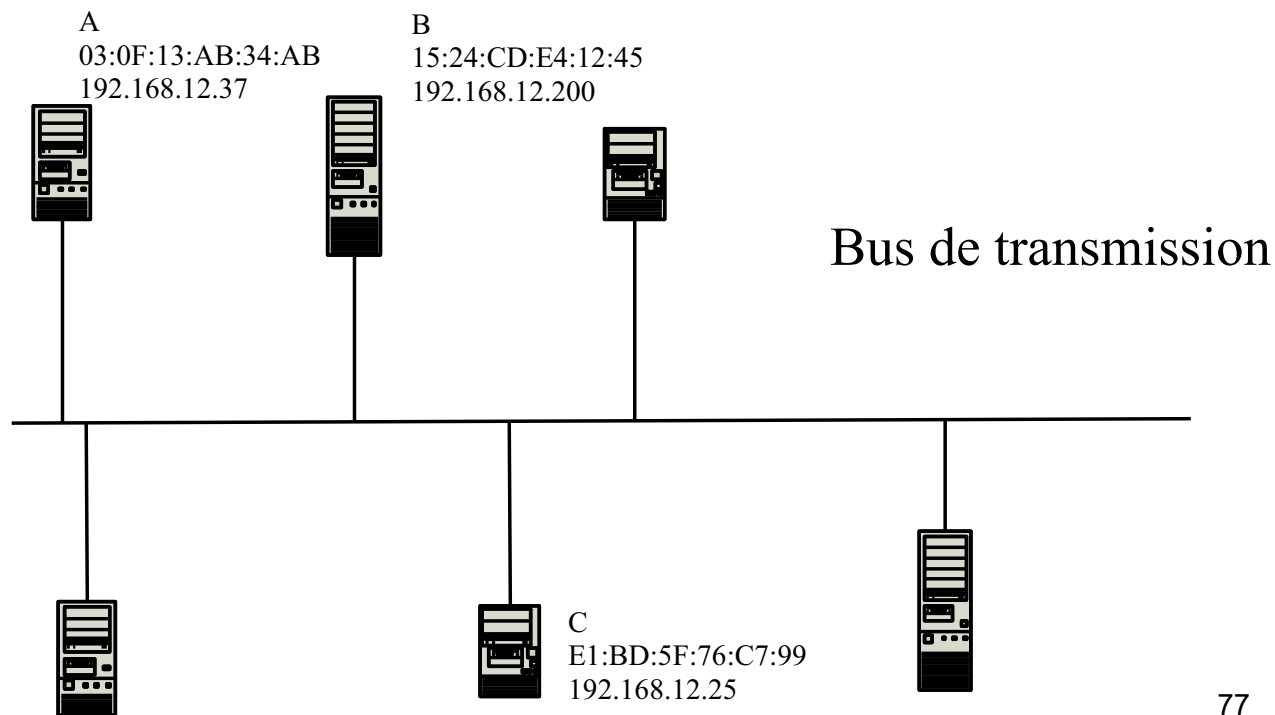
Dialogue dans un réseau local

Comment échanger réellement sur un réseau local à diffusion ?

Les machines ont chacune une carte réseau ;

Chaque carte a une adresse **MAC unique** donnée par le constructeur ;

Chaque machine dispose d'une **adresse IP** donnée par l'administrateur du réseau.



77

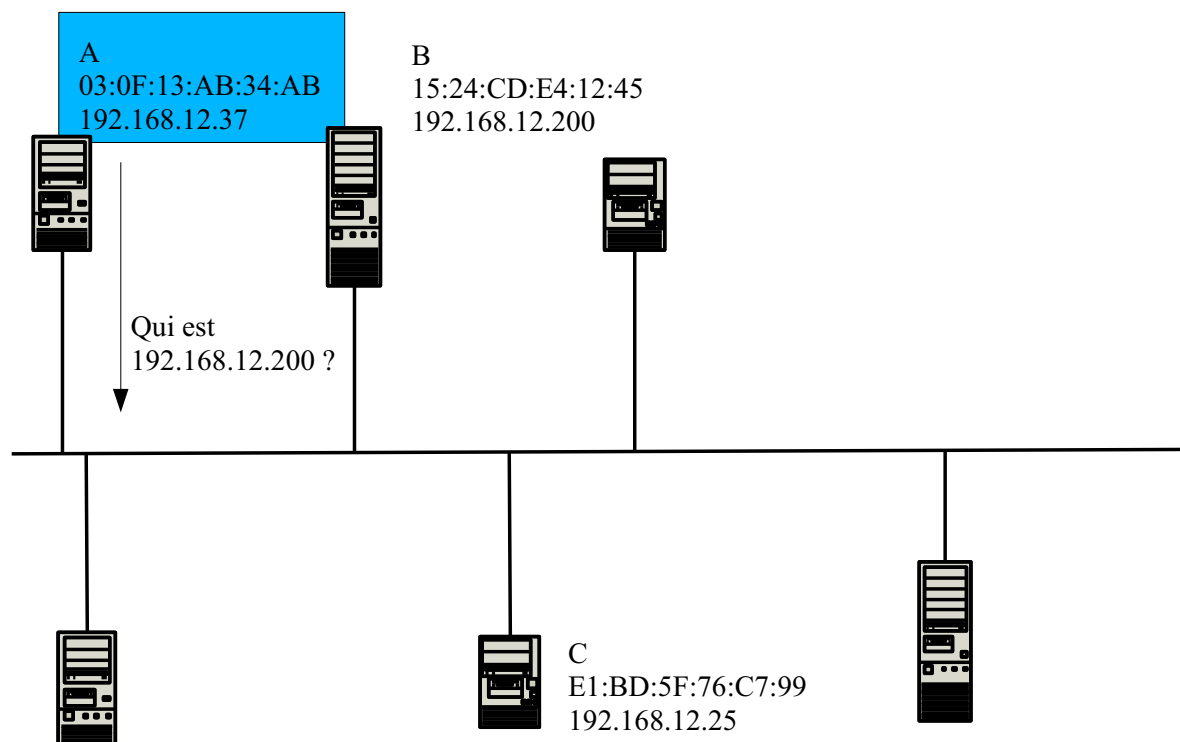
Dialogue dans un réseau local

Comment faire le lien adresse IP et adresse MAC ?

Si A veut communiquer avec B elle ne peut le faire qu'avec l'adresse MAC de B.

Comment obtenir l'adresse MAC de B ?

Pourquoi ne pas la demander ? **Facile ! On est dans un réseau à diffusion !**



78

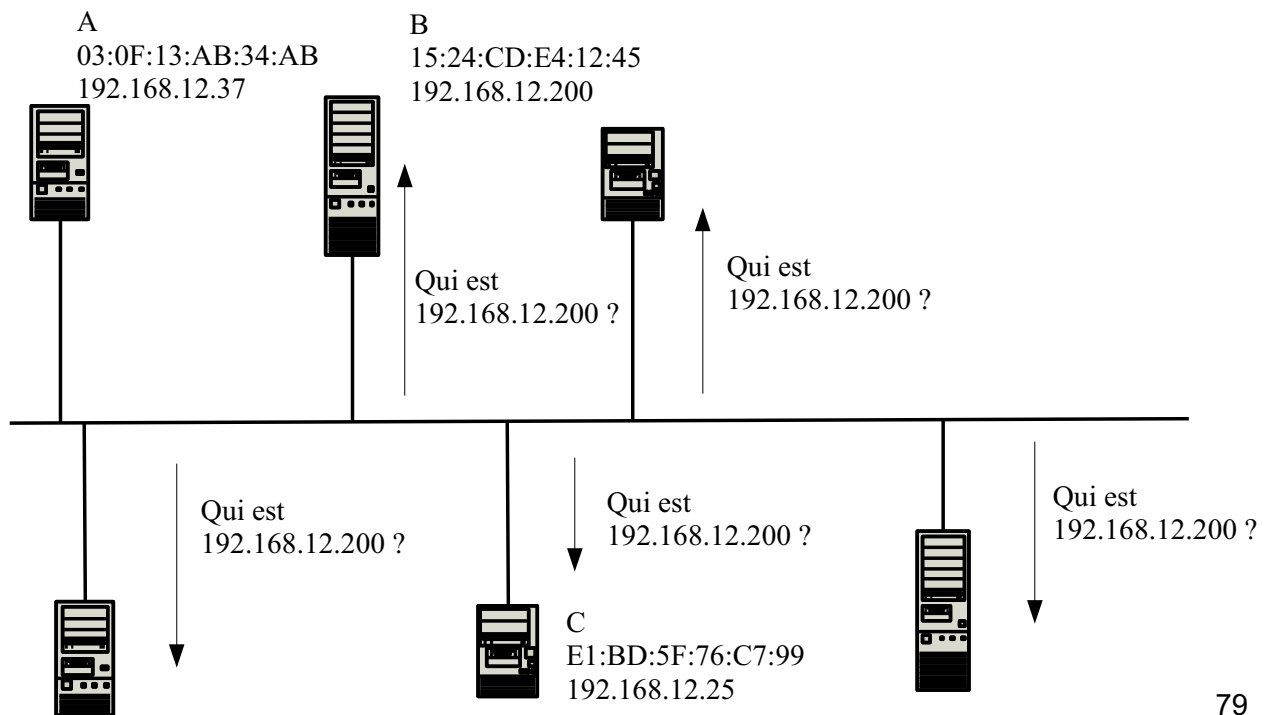
Dialogue dans un réseau local : trouver le destinataire

Comment faire le lien adresse IP et adresse MAC ?

Si A veut communiquer avec B elle ne peut le faire qu'avec l'adresse MAC de B.

Comment obtenir l'adresse MAC de B ?

Pourquoi ne pas la demander ? **Facile ! On est dans un réseau à diffusion !**



79

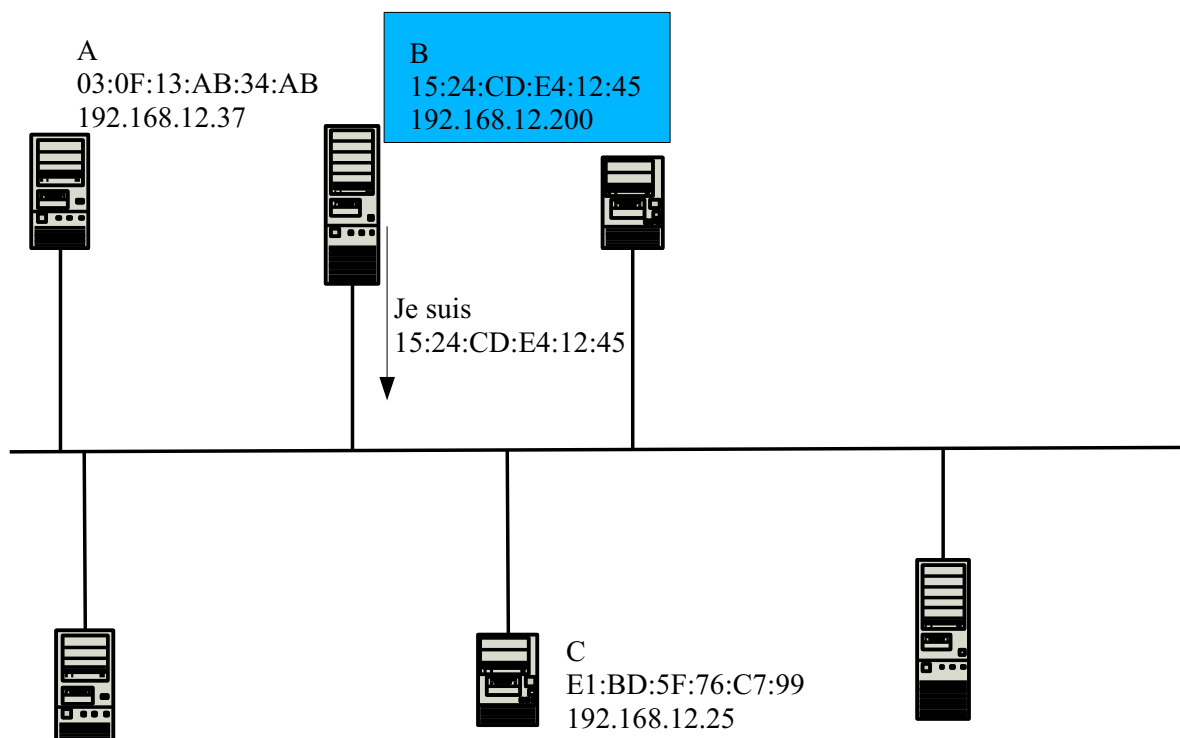
Dialogue dans un réseau local : trouver le destinataire

Comment faire le lien adresse IP et adresse MAC ?

Si A veut communiquer avec B elle ne peut le faire qu'avec l'adresse MAC de B.

Comment obtenir l'adresse MAC de B ?

Pourquoi ne pas la demander ? **Facile ! On est dans un réseau à diffusion !**



80

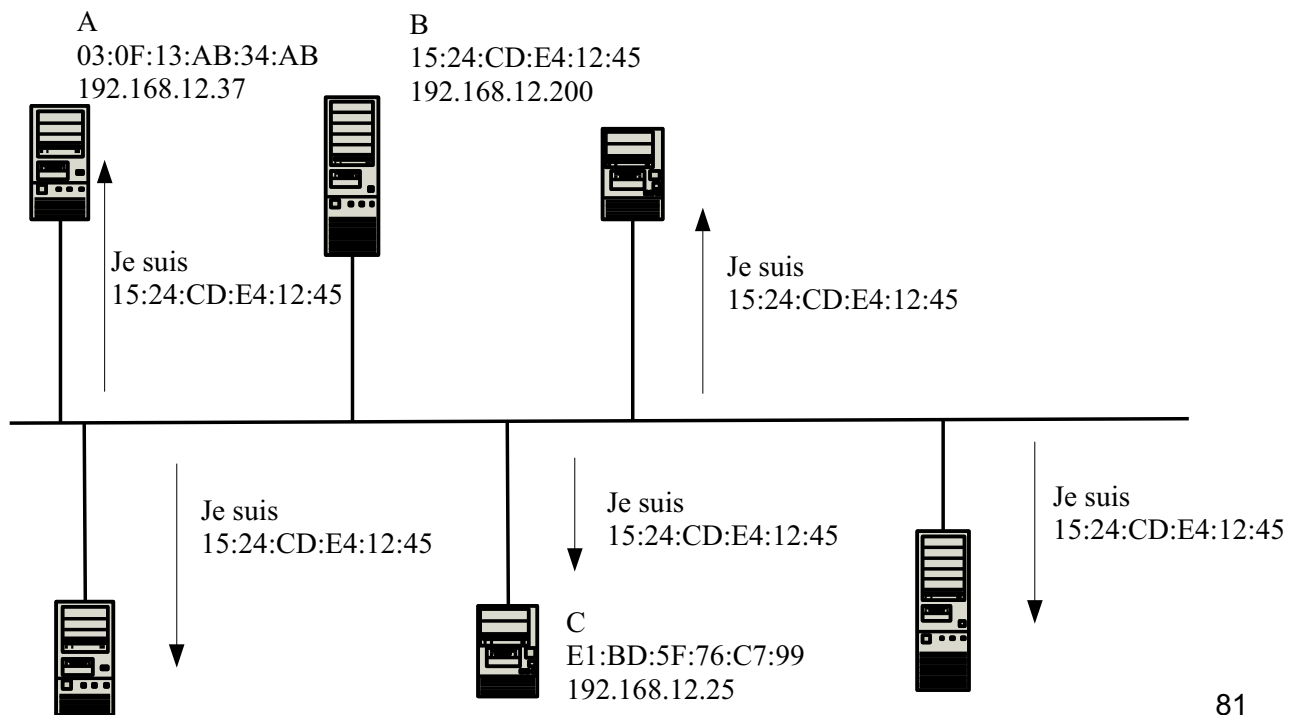
Dialogue dans un réseau local : trouver le destinataire

Comment faire le lien adresse IP et adresse MAC ?

Si A veut communiquer avec B elle ne peut le faire qu'avec l'adresse MAC de B.

Comment obtenir l'adresse MAC de B ?

Pourquoi ne pas la demander ? **Facile ! On est dans un réseau à diffusion !**



Dialogue dans un réseau local : trouver le destinataire

A connaît maintenant l'adresse MAC de B elle peut communiquer avec B.

Les autres machines ont également reçu le message de B, elles peuvent le conserver au cas où elles ont auraient besoin !

Correspondance entre adresses physiques MAC et adresses IP

Le protocole **ARP** "Address Resolution Protocol" :

il fournit une correspondance dynamique entre une adresse IP connue et l'adresse matérielle lui correspondant.

On parle de requête ARP pour la demande envoyée par une machine.

Le protocole **RARP** "Reverse Address Resolution Protocol" :

Il réalise l'opération inverse : une machine sans adresse IP connue peut envoyer une requête RARP pour demander son adresse IP.

Une machine particulière (un serveur gérant le réseau) lui répond et lui affecte son adresse IP.

Cette machine dispose d'une table de correspondance : (adresse physique, adresse IP).

Le protocole RARP est utile pour amorcer une station sans disque ou un Terminal X-Window.

Routage

Algorithme de routage par sauts successifs “next hop routing”

L'entité réseau (ordinateur ou routeur) doit déterminer l'adresse de prochain saut, c-à-d. la première étape du chemin d'acheminement du paquet à transmettre.

Un saut correspond à la transmission d'un paquet à un routeur ou à la machine destinataire.

Deux possibilités :

- le routage direct : Si la destination se trouve sur le même réseau, l'adresse de prochain saut est l'adresse IP simplement.
- le routage indirect : Sinon l'adresse de prochain saut doit être un routeur, c-à-d. qu'au moins un routeur sépare l'expéditeur initial et le destinataire final.

Localisation de la machine destinataire

Chaque ordinateur connecté au réseau Internet dispose d'une adresse IP et d'un masque de sous-réseau (indiquant la répartition des 32 bits d'adresse IP entre l'identification du réseau ou sous-réseau auquel il appartient et son identification au sein de ce réseau).

Lors de l'envoi d'un paquet à destination d'une machine D, l'algorithme de routage est le suivant :

- comparaison de l'adresse de D avec le masque de sous-réseau et le sous-réseau
- si égalité alors la destination est sur le même réseau physique

Utilisation de la diffusion pour assurer le transfert direct

- sinon c'est un **routage indirect** : on diffuse jusqu'au routeur par défaut (car il appartient au réseau local) et c'est lui routera ensuite le paquet vers le bon sous réseau en fonction ses tables de routage
- => On est sorti de son sous-réseau grâce au routeur !

83

Le paquet IP (1/2)

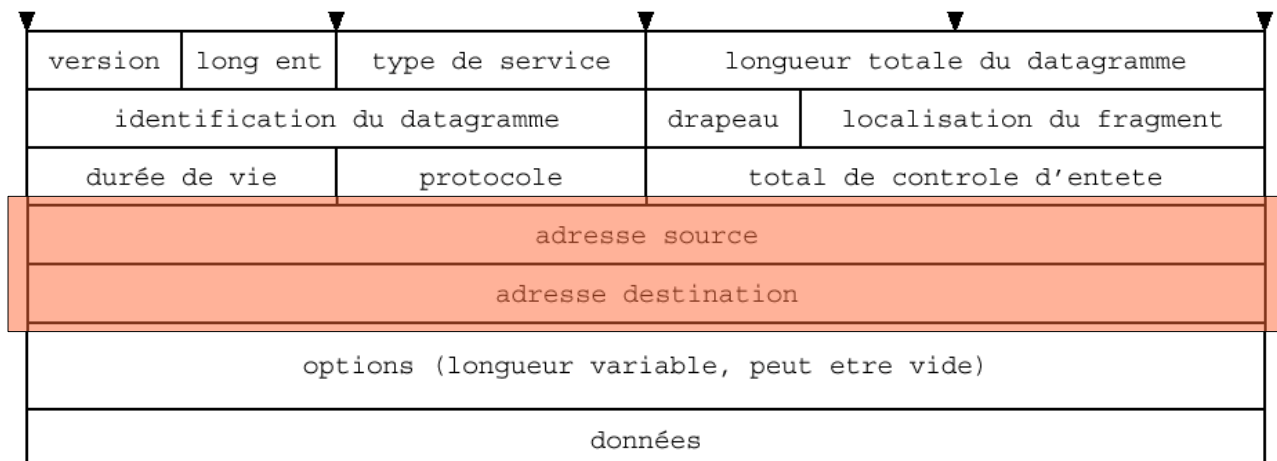
Le paquet ou datagramme IP

Il contient :

- l'adresse IP de la machine qui a envoyé le paquet ;
- l'adresse IP de la machine cible.

Munis de ces informations le paquet devient un datagramme.

Il est autonome et peut être « router », c-à-d. acheminer à travers le réseau.



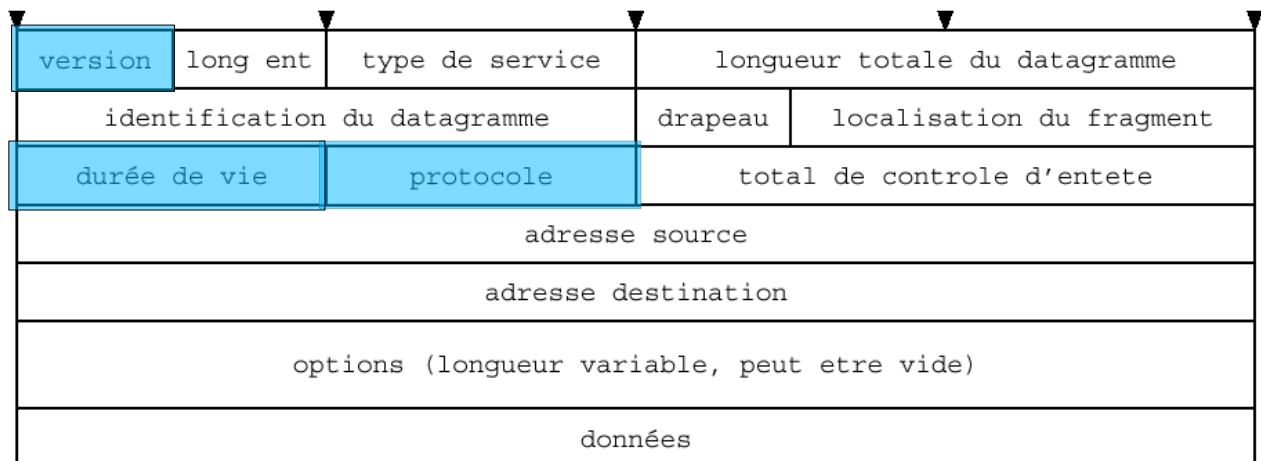
84

Le paquet IP (2/2)

Le paquet ou datagramme IP

Le datagramme contient également :

- un **numéro de version** : actuellement on est à la version 4 ;
- une **durée de vie** : le paquet est détruit s'il reste trop longtemps dans le réseau :
la destination n'est pas accessible ;
le routage a été mal fait...
Cela permet de ne pas saturer le réseau !
- le **type de protocole** : cela correspond à la forme du dialogue (mode connecté ou non – *cf plus loin*).



ICMP (1/2)

Le protocole ICMP (Internet Control Message Protocol) :

Il permet de gérer les informations relatives aux erreurs aux machines connectées.

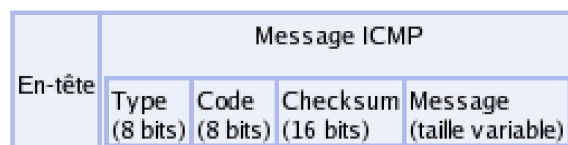
Étant donné le peu de contrôles que le protocole IP réalise, il permet non pas de corriger ces erreurs mais de faire part de ces erreurs aux protocoles des couches voisines. Ainsi, le protocole ICMP est utilisé par tous les routeurs, qui l'utilisent pour signaler une erreur (appelé Delivery Problem).

Les messages ICMP sont encapsulés

Les messages d'erreur ICMP sont transportés sur le réseau sous forme de datagramme, comme n'importe quelle donnée. Ainsi, les messages d'erreur peuvent eux-mêmes être sujet d'erreurs.

Toutefois, en cas d'erreur sur un datagramme transportant un message ICMP, aucun message d'erreur n'est délivré pour éviter un effet "**boule de neige**" en cas d'incident sur le réseau.

Voici à quoi ressemble un message ICMP encapsulé dans un datagramme IP:



ICMP (2/2)

Signification des messages ICMP

Type	Code	Message	Signification du message
8	0	Demande d'ECHO	Ce message est utilisé lorsqu'on utilise la commande <i>PING</i> . Cette commande, permettant de tester le réseau, envoie un datagramme à un destinataire et lui demande de le restituer
3	0	destinataire inaccessible	Le réseau n'est pas accessible
3	1	destinataire inaccessible	La machine n'est pas accessible
3	2	destinataire inaccessible	Le protocole n'est pas accessible
3	3	destinataire inaccessible	Le port n'est pas accessible
3	4	destinataire inaccessible	Fragmentation nécessaire mais impossible à cause du drapeau (flag) DF
3	5	destinataire inaccessible	Le routage a échoué
3	6	destinataire inaccessible	Réseau inconnu
3	7	destinataire inaccessible	Machine inconnue
3	8	destinataire inaccessible	Machine non connectée au réseau (inutilisé)
3	9	destinataire inaccessible	Communication avec le réseau interdite
3	10	destinataire inaccessible	Communication avec la machine interdite
3	11	destinataire inaccessible	Réseau inaccessible pour ce service
3	12	destinataire inaccessible	Machine inaccessible pour ce service
3	11	destinataire inaccessible	Communication interdite (filtrage)
4	0	Source Quench	Le volume de données envoyé est trop important, le routeur envoie ce message pour prévenir qu'il sature afin de demander de réduire la vitesse de transmission
5	0	Redirection pour un hôte	Le routeur remarque que la route d'un ordinateur n'est pas optimale et envoie l'adresse du routeur à rajouter dans la table de routage de l'ordinateur
5	1	Redirection pour un hôte et un service donné	Le routeur remarque que la route d'un ordinateur n'est pas optimale pour un service donné et envoie l'adresse du routeur à rajouter dans la table de routage de l'ordinateur
5	2	Redirection pour un réseau	Le routeur remarque que la route d'un réseau entier n'est pas optimale et envoie l'adresse du routeur à rajouter dans la table de routage des ordinateurs du réseau
5	3	Redirection pour un réseau et un service donné	Le routeur remarque que la route d'un réseau entier n'est pas optimale pour un service donné et envoie l'adresse du routeur à rajouter dans la table de routage des ordinateurs du réseau
11	0	Temps dépassé	Ce message est envoyé lorsque le temps de vie d'un datagramme est dépassé. L'en-tête du datagramme est renvoyé pour que l'utilisateur sache quel datagramme a été détruit
11	1	Temps de ré-assemblage de fragment dépassé	Ce message est envoyé lorsque le temps de ré-assemblage des fragments d'un datagramme est dépassé.
12	0	en-tête erroné	Ce message est envoyé lorsqu'un champ d'un en-tête est erroné. La position de l'erreur est retournée
13	0	Timestamp request	Une machine demande à une autre son heure et sa date système (universelle)
14	0	Timestamp reply	La machine réceptrice donne son heure et sa date système afin que la machine émettrice puisse déterminer le temps de transfert des données
15	0	Demande d'adresse réseau	Ce message permet de demander au réseau une adresse IP
16	0	réponse d'adresse réseau	Ce message répond au message précédent
17	0	Demande de masque de sous-réseau	Ce message permet de demander au réseau un masque de sous-réseau
18	0	réponse de masque de sous-réseau	Ce message répond au message précédent
17	0	Timestamp reply	La machine réceptrice donne son heure et sa date système afin que la machine émettrice puisse déterminer le temps de transfert des données

87

DHCP (1/2)

DHCP signifie Dynamic Host Configuration Protocol.

C'est un protocole qui permet à un ordinateur qui se connecte sur un réseau d'**obtenir dynamiquement sa configuration** (principalement, sa configuration réseau).

=> l'ordinateur trouve tout seul une adresse IP par DHCP.

Le but principal étant la simplification de l'administration d'un réseau.

Il sert principalement à distribuer des adresses IP sur un réseau.

Au départ, il a été conçu comme complément au protocole BOOTP (Bootstrap Protocol) qui est utilisé, par exemple, lorsque l'on installe une machine à travers un réseau.

Par ailleurs, BOOTP est utilisé en étroite collaboration avec un serveur TFTP sur lequel le client va trouver les fichiers à charger et à copier sur le disque dur.

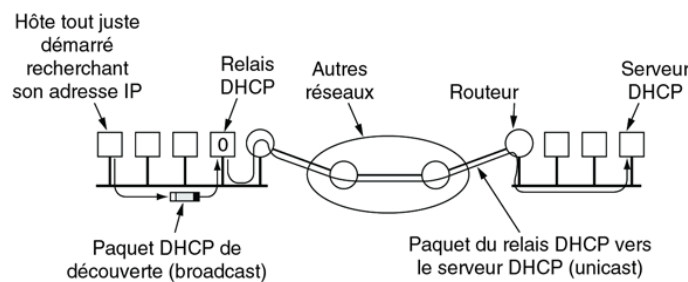
Un serveur DHCP peut renvoyer des paramètres BOOTP ou de configuration propres à un hôte donné.

DHCP (2/2)

Fonctionnement du protocole DHCP

- un **serveur DHCP qui distribue des adresses IP**. Dans un réseau, on peut donc n'avoir qu'une seule machine avec adresse IP fixe, le serveur DHCP.
- Le mécanisme de base de la communication est BOOTP (avec trame UDP). Quand une machine est démarrée, elle n'a aucune information sur sa configuration réseau, et surtout, l'utilisateur ne doit rien faire de particulier pour trouver une adresse IP.
- => 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 (n'oubliez pas que le **client** n'a pas forcément son adresse IP et que donc il n'est pas joignable directement) contenant toutes les informations requises pour le client.
- notion de **baux** ! (libération des ressources)

On a ici un fonctionnement client/serveur pour la distribution des IP dans un réseau.



© Pearson Education France

89

NAT (Network Address Translation) (1/2)

Principe du NAT : mécanisme de translation d'adresses

Objectif : répondre à la pénurie d'adresses IP avec le protocole Ipv4.

Le principe du NAT consiste donc à utiliser une ou plusieurs adresses IP routables pour connecter l'ensemble des machines du réseau en réalisant, au niveau de la passerelle de connexion à internet, une translation entre l'adresse interne (non routable) de la machine souhaitant se connecter et l'adresse IP de la passerelle.

NAT statique :

Le principe du NAT statique consiste à associer une adresse IP publique à une adresse IP privée interne au réseau. Le routeur permet donc d'associer à une adresse IP privée une adresse IP publique routable sur Internet et de faire la traduction, dans un sens comme dans l'autre, en modifiant l'adresse dans le paquet IP.

Avantage : permet ainsi de connecter des machines du réseau interne à internet de manière transparente ;

Inconvénient : ne résout pas le problème de la pénurie d'adresse dans la mesure où n adresses IP routables sont nécessaires pour connecter n machines du réseau interne.

90

NAT (Network Address Translation) (2/2)

NAT dynamique

Il permet de partager une adresse IP routable entre plusieurs machines en adressage privé. Ainsi toutes les machines du réseau interne possèdent virtuellement, vu de l'extérieur, la même adresse IP.
=> "mascarade IP" (en anglais IP masquerading) pour désigner le mécanisme de NAT.

Afin de pouvoir multiplexer les différentes adresses IP sur une ou plusieurs adresses IP routables le NAT dynamique utilise la **translation de port (PAT - Port Address Translation)**.

Cela consiste à affecter un port source différent à chaque requête de telle manière à pouvoir maintenir une correspondance entre les requêtes provenant du réseau interne et les réponses des machines sur Internet, toutes adressées à l'adresse IP du routeur.

La couche transport

Modèle client/serveur

Principe

Une machine dispose de ressources : fichiers, puissance de traitement, *etc.*

Cette machine a un rôle particulier dans le réseau : elle donne accès à ses ressources.

*Elle est appelée **serveur**.*

Lorsqu'une autre machine veut accéder à ces ressources elle doit passer par cette machine.

*Cette machine est **cliente** de la première.*

Le partage des ressources avec des clients est appelé **service**.

En général, le serveur est une machine très puissante en terme de capacités d'entrée-sortie.

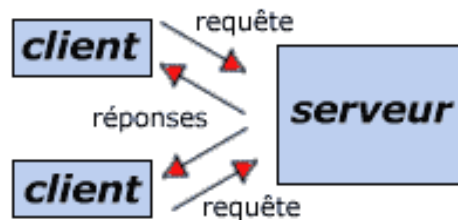
Un serveur fournit plusieurs services (l'heure, des fichiers, une connexion, impression, ...).

Chacun de ces services est supporté par un programme qui s'exécute sur le serveur.

L'accès au service est assuré par un programme chez le client.

Pour accéder à un service dans le réseau, il suffit de connaître la machine qui le propose.

C'est le mode de fonctionnement de nombreuses applications dans un réseau.



93

L'architecture client/serveur

Avantages de l'architecture client/serveur

- des ressources centralisées : étant donné que le serveur est au centre du réseau, il peut gérer des ressources communes à tous les utilisateurs, comme par exemple une base de données centralisée, afin d'éviter les problèmes de redondance et d'intégrité (annuaire LDAP) ;
- une meilleure sécurité : car le nombre de points d'entrée permettant l'accès aux données est moins important ;
- une administration au niveau serveur : les clients ayant moins d'importance dans ce modèle, ils ont moins besoin d'être administrés : les « gros » logiciels s'exécutent sur le serveur, les clients exécutent un programme léger (Serveur Web et Navigateur Web par exemple);
- un réseau évolutif : grâce à cette architecture il est possible de supprimer ou de rajouter des clients sans perturber le fonctionnement du réseau et sans modifications majeures. Il est également possible de rajouter des serveurs proposant les mêmes services pour améliorer les performances.

Inconvénients du modèle client/serveur

- un coût élevé dû à la puissance nécessaire par le serveur. Toutes les machines ne font pas des bons serveurs.
- le problème des pannes de serveur !

94

La notion de port

Comment joindre un service particulier offert sur un serveur ?

Chaque service est associé à un programme qui tourne sur le serveur.

Globalement, tous les programmes communiquent par la même ligne de transmission.

Or, il faut pouvoir désigner de l'extérieur le programme ou service avec lequel on veut communiquer.

Comment différencier différentes communications entre deux machines ?

Il faut les numéroté :

- du côté de l'émetteur ;
- du côté du récepteur ;

Le **numéro de port** est un numéro associé à chaque communication.

Souvent si une communication sert à offrir un service, elle est associée à un seul programme

Exemple : La machine A 192.168.10.30 communique avec la machine B 195.50.185.45.

Elle veut joindre le service de transfert de fichiers proposé par B.

Elle se connecte sur le port 21 associé au programme de gestion de transfert de fichier !

Les numéros de ports sont normalisés

FTP	21
SMTP	25
Web	80
IRC	6667
...	

95

Multiplexage : mélanger les communications

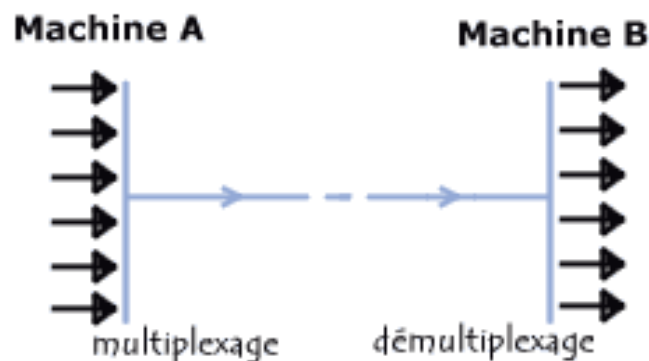
Le multiplexage

Il sert à mettre plusieurs communications ensemble sur une même ligne de transmission.

Exemple : une personne sur la même machine peut :

- relever son courrier ;
- surfer sur le Web ;
- chatter avec un ami ;
- récupérer une bande-annonce d'un film ;
- ...

Toutes ces communications passent par le même câble de sortie !



96

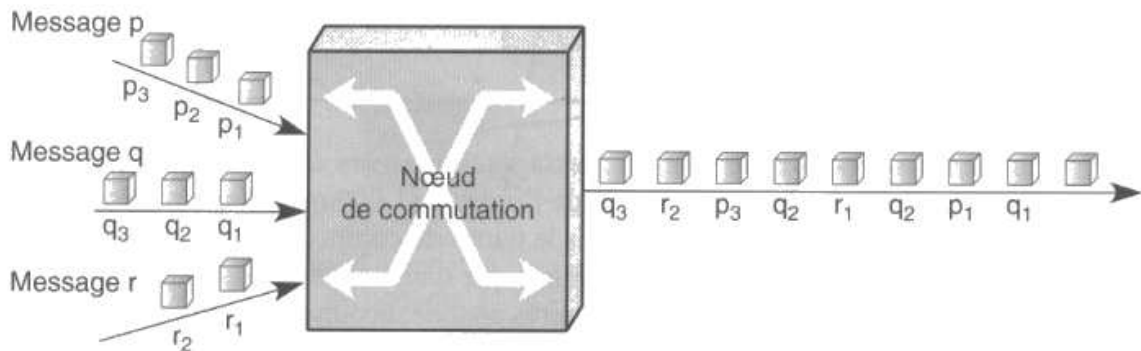
Le multiplexage

Comment ça marche ?

Chaque message envoyé est décomposé en « paquets ».

Chacun de ces paquets est envoyé à la suite du précédent.

Sur la même ligne de transmission des paquets de **différentes communications** peuvent circuler.



Sur la même ligne de de transmission des paquets de **différents ordinateurs** peuvent circuler !

97

Précision : mode connecté ou non connecté

Le réseau informatique marche uniquement en mode non connecté

Chaque paquet est indépendant.

Il correspond à une seule information échangée à la fois.

Il faut que l'information tienne dans le paquet.

Les paquets sont :

- envoyés dans le réseau ;
- le chemin qu'ils empruntent dépend de l'état du réseau ;
- l'expéditeur ne sait pas s'il est arrivé chez le destinataire ;
- il faut demander un accusé de réception si nécessaire au destinataire ;
- et si l'accusé de réception se perd ?

Par dessus un mode non connecté, on « simule » un mode connecté

un échange entre deux machines correspond à une taille variable de données.

Ces données sont découpées en paquet.

Chaque paquet est numéroté.

Chaque paquet transmis donne lieu à un accusé de réception.

Sans accusé de réception on retransmet le paquet.

Si on toujours pas d'accusé de réception alors on dit que le récepteur est inaccessible.

À la réception les paquets sont réordonnés et regroupés pour retrouver le message initial.

98

TCP (1/2)

Le protocole TCP « Transmission Control Protocol »

Il correspond au **mode connecté** (c'est-à-dire qu'il permet à deux machines qui communiquent de contrôler l'état de la transmission)

Les caractéristiques principales du protocole TCP sont les suivantes :

- TCP permet de **remettre en ordre** les datagrammes en provenance du protocole IP
- TCP permet de **vérifier le flot** de données afin d'éviter une saturation du réseau
- TCP permet de formater les données en segments de longueur variable afin de les "remettre" au protocole IP
- TCP permet de **multiplexer** les données, c'est-à-dire de faire circuler simultanément des informations provenant de sources (applications par exemple) distinctes sur une même ligne
- TCP permet enfin l'initialisation et la fin d'une communication de manière courtoise

TCP permet de communiquer de façon fiable.

Remarque : les routeurs (qui travaillent sur le niveau IP) ont pour seul rôle l'acheminement des données sous forme de datagrammes, sans se préoccuper du contrôle des données.

Associé à IP c'est le protocole de communication le plus utilisé sur Internet : TCP/IP

99

TCP (2/2)

Port Source (16 bits): Port relatif à l'application en cours sur la machine source

Port Destination (16 bits): Port relatif à l'application en cours sur la machine de destination

Numéro d'ordre (32 bits):

- Lorsque le drapeau SYN est à 0, le numéro d'ordre est celui du premier mot du segment en cours.
- Lorsque SYN est à 1, le numéro d'ordre est égal au numéro d'ordre initial utilisé pour synchroniser les numéros de séquence (ISN)

Numéro d'accusé de réception (32 bits): Le numéro d'accusé de réception également appelé numéro d'acquiescement correspond au numéro (d'ordre) du prochain segment attendu, et non le numéro du dernier segment reçu.

Somme de contrôle (Checksum ou CRC): La somme de contrôle est réalisée en faisant la somme des champs de données de l'en-tête, afin de pouvoir vérifier l'intégrité de l'en-tête

Le segment TCP :

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Port Source																Port destination															
Numéro d'ordre																															
Numéro d'accusé de réception																															
Décalage données		réservée				URG		ACK		PSH		RST		SYN		FIN		Fenêtre													
Somme de contrôle																Pointeur d'urgence															
Options																						Remplissage									
Données																															

100

UDP

Le protocole UDP « User Datagram Protocol »

Il correspond au **mode non connecté**

Port Source : il s'agit du numéro de port correspondant à l'application émettrice du segment UDP. Ce champ représente une adresse de réponse pour le destinataire. Ainsi, ce champ est optionnel, cela signifie que si l'on ne précise pas le port source, les 16 bits de ce champ seront mis à zéro, auquel cas le destinataire ne pourra pas répondre => messages unidirectionnels.

Port Destination : Ce champ contient le port correspondant à l'application de la machine destinataire à laquelle on s'adresse.

Longueur : Ce champ précise la longueur totale du segment, en-tête comprise, or l'en-tête a une longueur de 4 x 16 bits donc le champ longueur est nécessairement supérieur ou égal à 8 octets.

Somme de contrôle : Il s'agit d'une somme de contrôle réalisée de telle façon à pouvoir contrôler l'intégrité du segment.

Port Source (16 bits)	Port Destination (16 bits)
Longueur (16 bits)	Somme de contrôle (16 bits)
Données (longueur variable)	

101

La couche application

102

DNS (Domain Name System) (1/3)

Il était difficile de se référer aux hôtes, aux serveurs de messagerie ou autres ressources au moyen de leur adresse de réseau.

toto@193.50.185.1 => problème si l'entreprise Toto veut changer la messagerie de machine !
=> introduction des noms en ASCII : toto@alphainfo.unilim.fr

=> il faut un mécanisme de correspondance entre les noms de machine et les adresses

À l'époque d'ARPAnet, on utilisait un fichier hosts.txt centralisé sur un serveur et qui contenait toutes les correspondances entre adresses IP et nom d'hôtes. Ce fichier était téléchargé toutes les nuits par les diverses machines du réseau.

Avec l'augmentation de la taille du réseau la solution n'était plus viable et on a inventé **le système DNS (Domain Name System)**.

Au cœur du système DNS il y a un schéma de nommage hiérarchique fondé sur la notion de domaine et une base de données répartie qui implémente ce schéma de nommage.

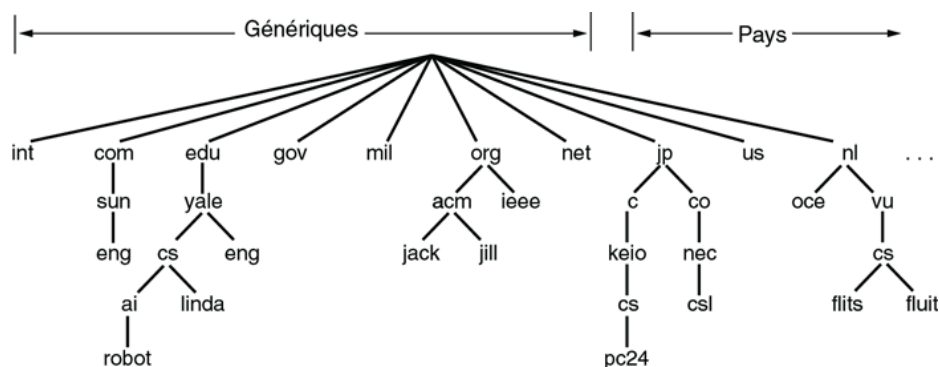
La fonction principale de DNS est de mettre en correspondance les noms d'hôtes ou des serveurs de messagerie et leur adresse IP.

103

DNS (Domain Name System) (2/3)

On a une analogie dans l'organisation avec celle du système postal
(pays/province/ville/rue/numéro/bâtiment/étage/appartement/nom/prénom)

De par sa conception le DNS est réparti en 200 domaines de premier niveau (TLD – Top Level Domain) et ils sont de deux types : génériques et nationaux



© Pearson Education France

Problématique de vérification dans l'attribution du domaine

Par exemple : .biz, .info, .name, .pro

Qui est un professionnel ? Un médecin ? Un avocat ? Un coiffeur ? Un dealer ?

Il existe des domaines plus spécialisé :

Par exemple: .aero (aérospatiales), .coop (coopératives), .museum (musées)

104

DNS (Domain Name System) (3/3)

Notion de domaine :

On peut acheter un domaine de second niveau en payant l'opérateur gérant le TLD : exemple .com pour toto.com

Un nom de domaine se compose de plusieurs composants séparés par un point, en progressant vers la racine (non nommée).

Les noms de domaines absolus se terminent par un point : exemple eng.sun.com.

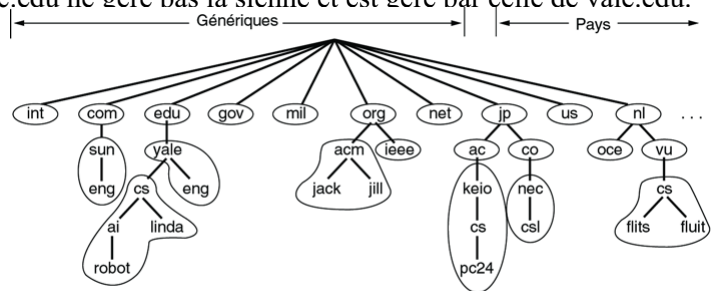
Les noms de domaine relatifs sont interprétés par rapport au contexte.

On a une ou plusieurs machines DNS par domaine qui gère la base donnée relative aux hôtes qu'il héberge dans une zone.

On note que cs.yale.edu gère sa zone alors que eng.yale.edu ne gère pas la sienne et est géré par celle de yale.edu.

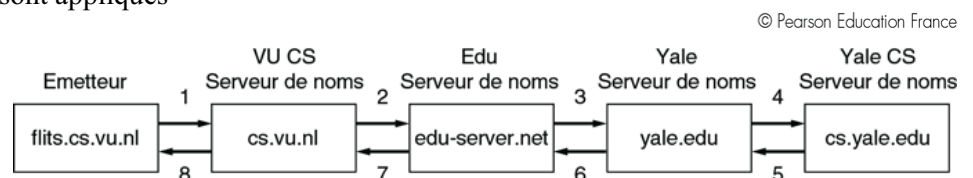
Il existe des serveurs racines au nombre d'une dizaine pour gérer les TLD.

=> attention au DDOS



Recherche DNS

- Recherche récursive : cf ci-dessous.
 - Recherche par nom de serveur auquel s'adresser.
- Il y a des techniques de cache qui sont appliqués



© Pearson Education France

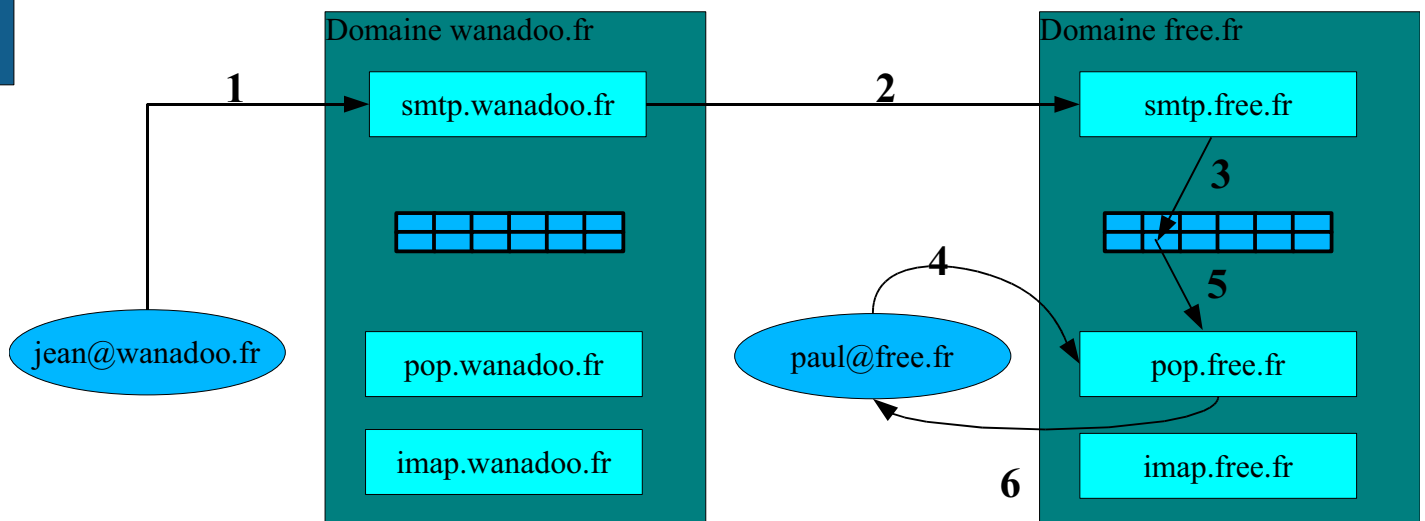
© Pearson Education France

SMTP

MUA (Mail User Agent)

MTA (Mail Transfert Agent)

MDA (Mail Delivery Agent)



Exemple de mail

Return-Path: <prenom.nom@etu.unilim.fr>

Received: from limdns2.unilim.fr (limdns2.unilim.fr [164.81.1.5])
by limrec.unilim.fr (8.9.3/jtpda-5.3.2) with ESMTP id QAA231747
for <sauveron@limrec.unilim.fr>; Fri, 10 Dec 2004 16:14:20 +0100 (MET)

Received: from etu.unilim.fr (etu.unilim.fr [164.81.1.20])
by limdns2.unilim.fr (8.12.6-20030917/jtpda-5.4) with ESMTP id iBAFEJLL019269
for <damien.sauveron@unilim.fr>; Fri, 10 Dec 2004 16:14:19 +0100

Received: from 164.81.170.33
(SquirrelMail authenticated user nom01);
by etu.unilim.fr with HTTP;
Fri, 10 Dec 2004 16:15:24 +0100 (CET)

Message-ID: <1366.164.81.170.33.1102691724.squirrel@164.81.170.33>

Date: Fri, 10 Dec 2004 16:15:24 +0100 (CET)

Subject: TD2

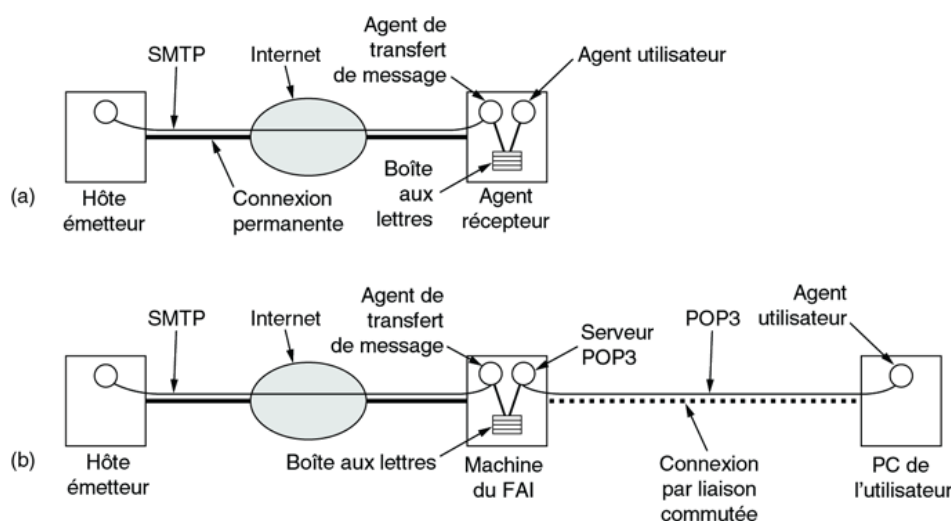
From: "Prénom NOM" <prenom.nom@etu.unilim.fr>

To: damien.sauveron@unilim.fr

1	Texte complet du message
2	Texte complet du message
3	Texte complet du message
4	Texte complet du message
5	Texte complet du message
6	Texte complet du message
⋮	
N	Texte complet du message

107

SMTP (suite)



© Pearson Education France

108

Entête d'un mail

Return-Path: <prenom.nom@etu.unilim.fr>
Received: from limdns2.unilim.fr (limdns2.unilim.fr [164.81.1.5])
by limrec.unilim.fr (8.9.3/jtpda-5.3.2) with ESMTP id QAA231747
for <sauveron@limrec.unilim.fr>; Fri, 10 Dec 2004 16:14:20 +0100 (MET)
Received: from etu.unilim.fr (etu.unilim.fr [164.81.1.20])
by limdns2.unilim.fr (8.12.6-20030917/jtpda-5.4) with ESMTP id iBAFEJLL019269
for <damien.sauveron@unilim.fr>; Fri, 10 Dec 2004 16:14:19 +0100
Received: from 164.81.170.33
(SquirrelMail authenticated user nom01);
by etu.unilim.fr with HTTP;
Fri, 10 Dec 2004 16:15:24 +0100 (CET)
Message-ID: <1366.164.81.170.33.1102691724.squirrel@164.81.170.33>
Date: Fri, 10 Dec 2004 16:15:24 +0100 (CET)|
Subject: TD2
From: "Prénom NOM" <prenom.nom@etu.unilim.fr>
To: damien.sauveron@unilim.fr

109

POP

Commande	Fonction
USER	Il s'agit de l'identifiant du titulaire du compte. En règle générale la partie à gauche du @ dans l'adresse électronique.
PASS	Le mot de passe fourni par le FAI
STAT	Donne le nombre de messages présents dans la file d'attente, ainsi que le volume total des messages en octets.
LIST	Donne la liste des messages en attente, avec pour chaque message: ♦ Son numéro d'ordre dans la file ♦ Sa taille en octets
UIDL	Analogue à LIST, mis à part qu'elle retourne non pas la taille du message mais un identificateur unique
RETR n	Permet de récupérer la totalité du message "n" dans la file d'attente.
DELE n	Détruit le message "n" dans la file d'attente. le numéro d'ordre des messages suivants demeure inchangé jusqu'à la fin de la session.
TOP n x	Permet de récupérer les x premières lignes du message "n". Les ligne d'en-tête ne sont pas comptabilisées. Cette commande est le plus souvent utilisée pour récupérer l'en-tête complet et la première ligne du message, x ne pouvant être égal à 0.
LAST	Permet de connaître le numéro d'ordre du dernier message auquel on a accédé. (Utile avec une session TELNET).
RSET	Cette commande permet d'annuler toutes les commandes de destruction de messages envoyées pendant la session. En fait, les commandes DELE ne sont rendues effectives que si la session a proprement été fermée (commande QUIT acceptée). Cette méthode permet donc d'annuler les opérations d'effacement dans la session en cours.
NOOP	Cette commande sert à ne rien faire.
QUIT	Clôture la session en cours. Le serveur ferme alors la session TCP et "fait le ménage" dans la file d'attente, en fonction des ordres DELE qui ont été donnés.

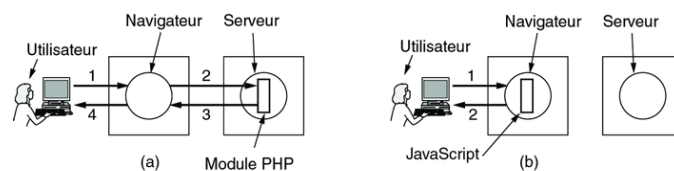
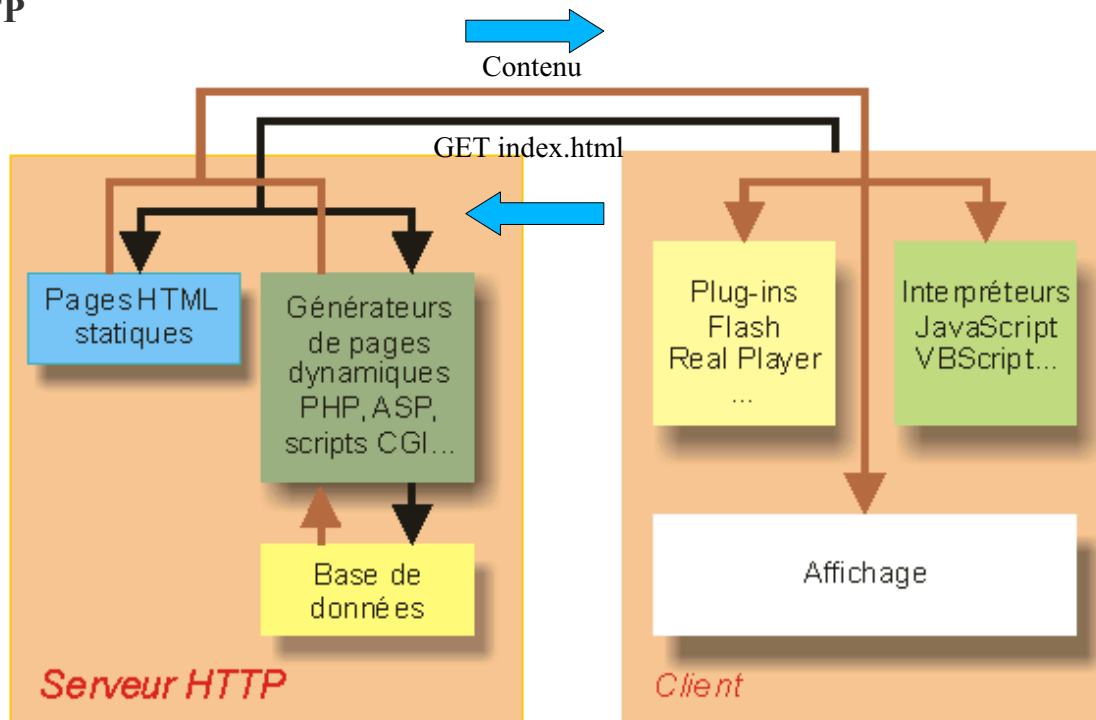
IMAP

Le protocole IMAP (Internet Message Access Protocol) est un protocole alternatif au protocole POP3 mais offrant beaucoup plus de possibilités :

- * IMAP permet de gérer plusieurs accès simultanés
- * IMAP permet de gérer plusieurs boîtes aux lettres
- * IMAP permet de trier le courrier selon plus de critères

111

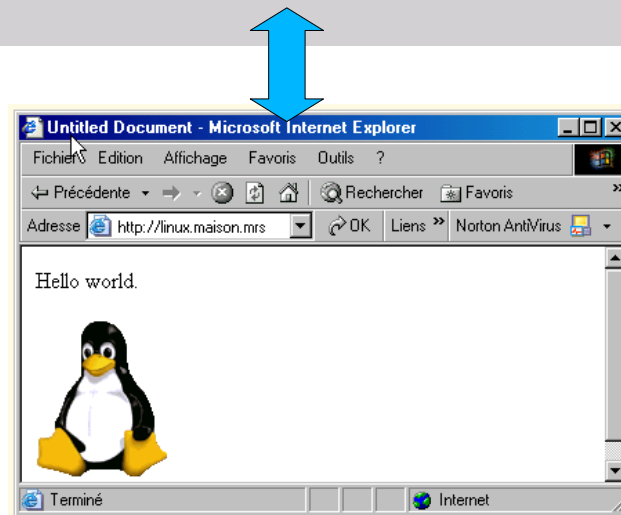
HTTP



Le langage HTML

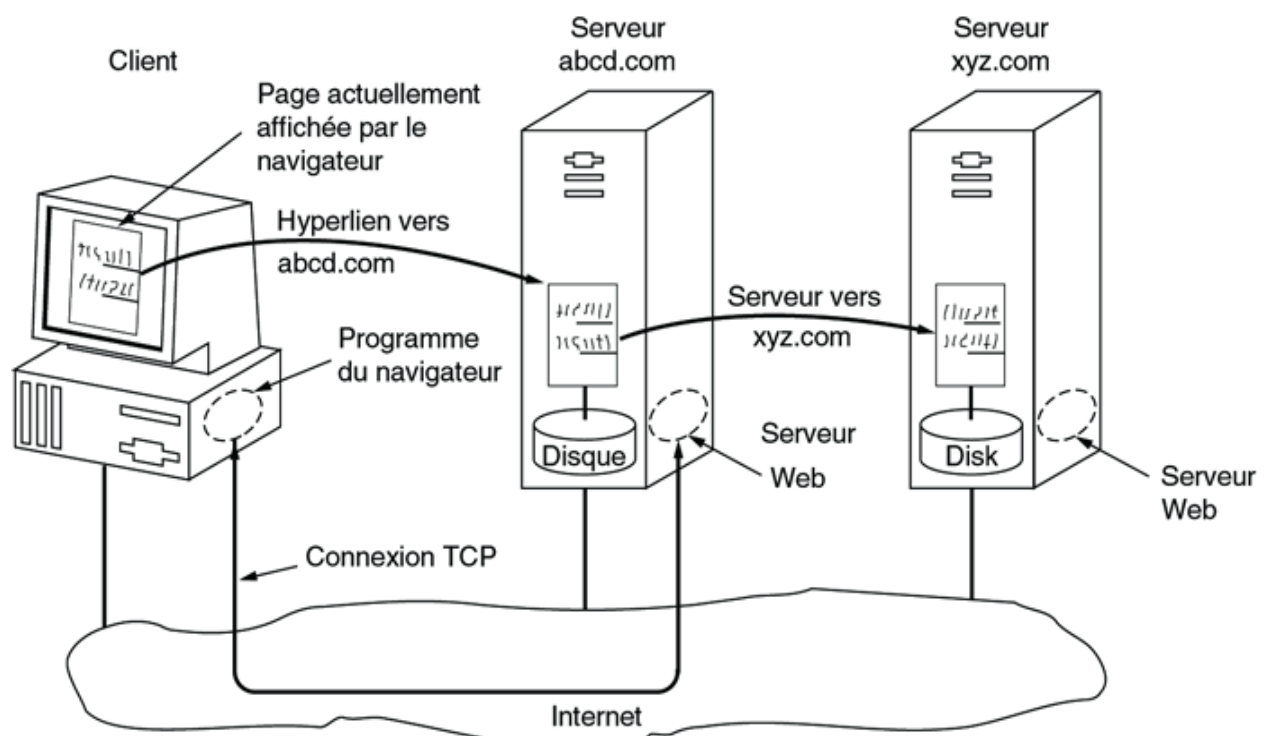
```
<html>
<head>
<title>Untitled Document</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
</head>

<body bgcolor="#FFFFFF" text="#000000">
<p>Hello world.
</p>
<p>
</p>
</body>
</html>
```



113

Hyperlien



• Le réseau Internet

115

Le réseau Internet

Historique

Le réseau Internet signifie « INTERconnection NETwork ».

Il a été créé en 1969 dans le cadre du projet de l'ARPA, « Advanced Research Projects Agency ».

Il part d'une idée du DoD des États-Unis (Department of Defence) :

- créer un réseau informatique capable d'interconnecter différents centres de communication et de fonctionner en cas de cataclysme, une guerre nucléaire par exemple ;
- en cas de destruction partielle du réseau, le reste du système doit rester opérationnel.

Création de l'ARPANET

En 1985, la fondation NSF, « National Science Foundation », crée le NSFNET,

à partir des technologies d'ARPANET, qui est un ensemble de réseaux pour la communication scientifique et universitaire.

Création d'une « épine dorsale » nationale, *BackBone*, réseau fédérateur de super-ordinateurs accessible gratuitement aux organismes scientifiques et universitaires américains.

Création de réseaux régionaux pour connecter chaque institution à « l'épine dorsale » nationale.

Développement rapide du NSFNET :

- plus de personnes connectées ;
- plus de services nouveaux proposés (applications logicielles).



116

Le réseau Internet

Les technologies

Internet repose sur l'utilisation du modèle logiciel de réseau TCP/IP.

Il doit son nom à deux protocoles : TCP et IP définis entre 1977 et 1980.

Le but est de permettre :

- une interconnexion de réseaux ;
- une indépendance vis-à-vis des technologies réseaux utilisées logicielles et matérielles ;
- une indépendance vis-à-vis du nombre et de la position géographique des matériels ;
- un adressage commun à tous ces matériels.



La connexion d'un réseau à Internet

- L'obtention d'une adresse Internet

InterNIC, chargé d'enregistrer toutes les adresses sur Internet.

NIC : Network Information Center

AFNIC, *Association Française pour le Nommage Internet en Coopération* : gère les .fr rt .re (Île de la Réunion).

- disposer des protocoles TCP/IP.

Ils sont disponibles gratuitement, mais les logiciels qui les mettent en œuvre peuvent être payants.

Au départ, uniquement disponible sur Unix, puis intégrable à Windows et MacOS.

Actuellement, ils sont intégrés à tous les systèmes d'exploitation (de l'ordinateur de bureau au PDA !).

Une croissance exceptionnelle

- >100 000 réseaux interconnectés ;
- 800 millions d'utilisateurs

117

Le réseau Internet

Un réseau auto-géré

- pas d'organe centralisateur ;
Tous les utilisateurs connectés peuvent y placer des informations : particuliers, associations, institutions, entreprises, collectivités, organes de presse etc
- une absence de localisation géographique précise des matériels connectés.
Il n'y a pas toujours de rapport entre une adresse internet et un emplacement géographique ;
- des lois qui ont du mal à être appliquées : elles sont nationales et ne peuvent s'appliquer en dehors d'un pays alors que les informations peuvent arriver de l'extérieur ;
- mise en place de l'ICANN « Internet Corporation for Assigned Names and Numbers » qui sert de coordination technique d'Internet pour ses évolutions et proposent des méthodes de résolution de conflit dans l'attribution d'adresses Internet (idée de Gouvernance d'Internet) ;
- nombre exponentiel d'utilisateurs.

Les risques d'une machine connectée

- virus ;
- chevaux de troie ;
- spywares ;
- spams ;
- contenus illicites ;
- usurpation d'identité ;
- ...

118

La connexion à Internet

Les précautions indispensables

Au niveau des usages :

- rester vigilant sur la fiabilité de l'information récoltée (origine et mise à jour), ;
- savoir la sélectionner selon le type de renseignements recherchés (ex : un site «.gouv.fr» donne des informations officielles comme des textes de lois) ;
- faire attention au contenu des courriers que l'on reçoit ;
- faire attention au site Web que l'on consulte ;
- ne pas exécuter n'importe quel logiciel ;
- s'informer sur les nouveaux risques ;
- comprendre et connaître le fonctionnement d'Internet pour ne pas croire tout ce qui est dit et pour savoir ce que l'on risque !
- ...

Au niveau des matériels :

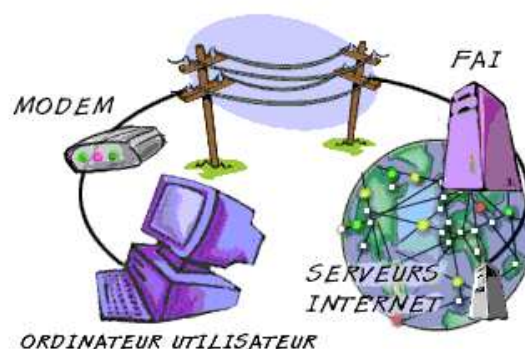
- faire les mises à jour proposées par le constructeur ;
- installer des pare-feux logiciels et/ou matériel ;
- mettre à jour les systèmes d'exploitations sinon les isoler ;
- ne pas installer tout mais seulement ce dont on a besoin ;
- faire des sauvegardes !
- ...

119

La connexion à Internet

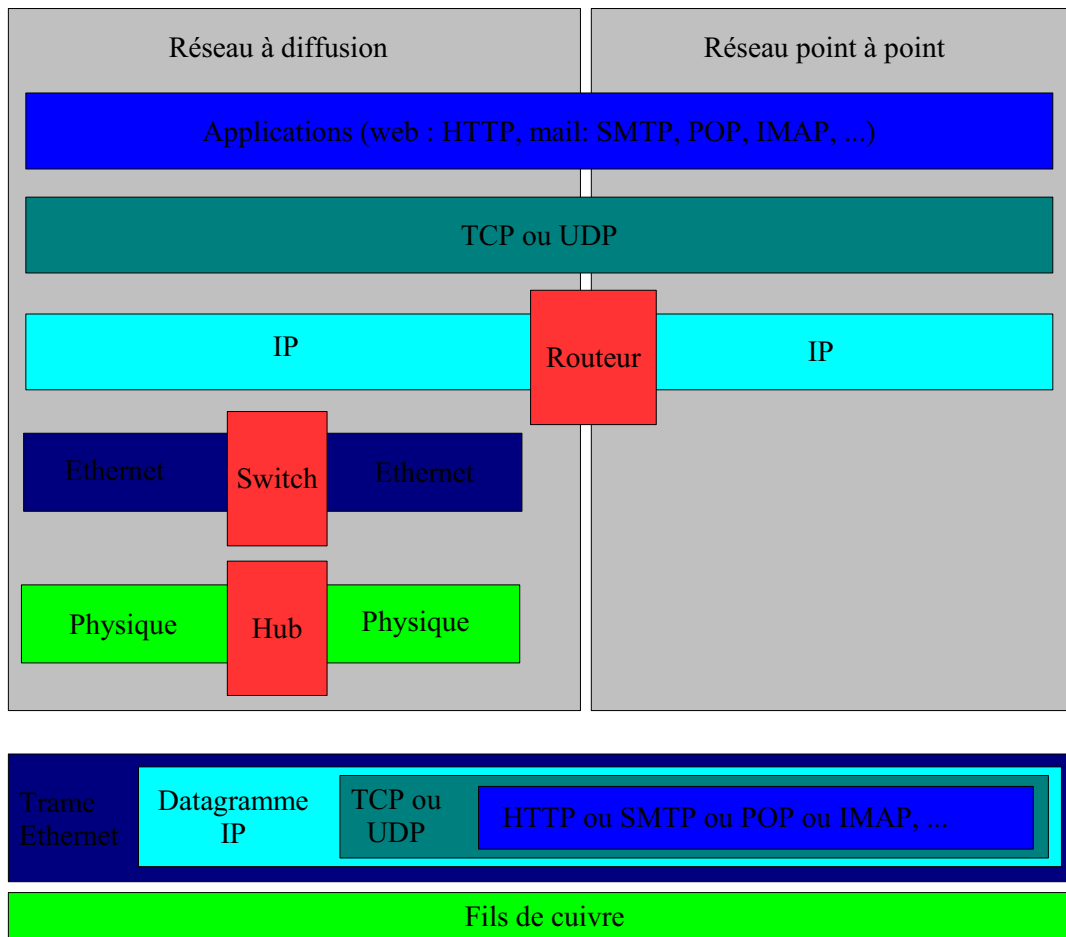
La connexion personnelle

L'ordinateur est connecté à un modem (câble, ADSL, analogique) qui le relie à un FAI, « Fournisseur d'Accès Internet ».



120

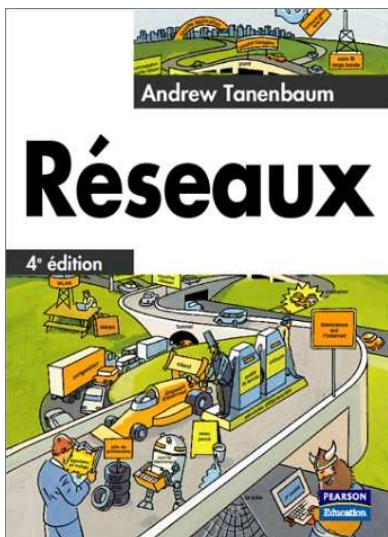
Résumé



121

Bibliographie

ISBN : 2744070017



122