ASR - M1 Crypto

Introduction

Adlen Ksentini
adlen.ksentini@univ-rennes1.fr

Bibliographie

- Computer Networking « a Top-Down Approach », James F. Kurose et Keith W. Ross.

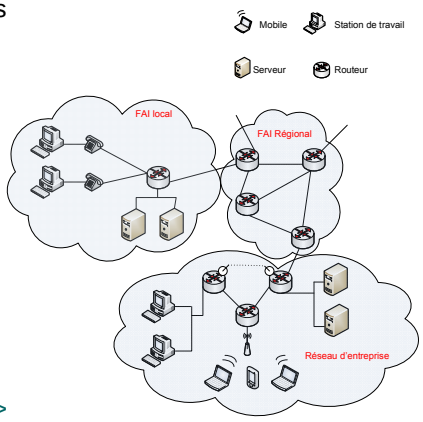
Introduction

- But :
  - Apprendre et connaitre la terminologie réseau
- Approche
  - Le réseau Internet comme exemple

- Plan
  - Internet ?
  - Protocole ?
  - En bordure du réseau
  - Réseaux d'accès
  - Le cœur du réseau
  - Structure d'Internet/FAI
  - Performance : taux de perte, délai, … débit
  - Couches protocolaires et services

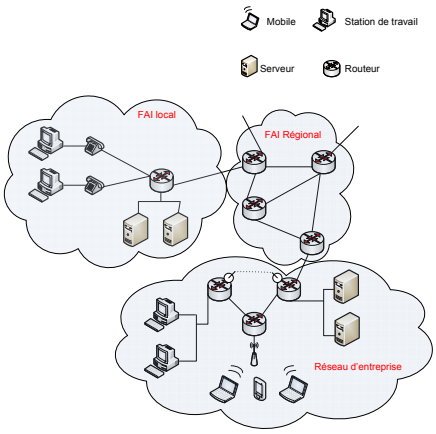
Internet ? – vue composant

- Des millions de machines interconnectées :
  - PC, stations de travail, serveurs
  - Tablettes, téléphones, compteurs électriques, machine à laver !
  - Exécutent des applications réparties
  - 2 milliards d'utilisateurs en 2012
- *Liens de communication*
  - Fibre optique, cuivre, radio, satellite
  - Débit de transmission (Bande passante)
- *Interconnexion : routeur/commutateur =>* transfèrent les paquets de données dans le réseau



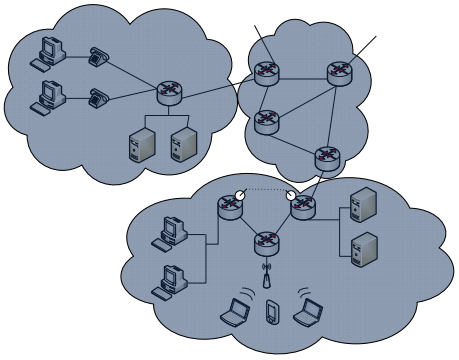
Internet ? – vue composant

- *Protocoles* : définissent l'émission, la réception des messages, les actions
  - Ex., TCP, IP, HTTP, FTP, SMTP
- *Internet :* "un réseau de réseaux"
  - Hiérarchique : réseaux d'accès, FAI (ou ISP)
  - Connecte des réseaux privés et publiques
- Normes d'Internet
  - RFC : *Request for comments*
  - IETF : *Internet Engineering Task Force*



Internet ? – vue service

- *Une infrastructure de communication qui rend possible les applications réparties*
  - Web, email, jeux en réseau, partage de fichiers, e-commerce, connexion à distance
  - Utilisent une *Application Programming Interface* (API) pour communiquer sur Internet ("socket")
- *Des services de communication*
  - Avec connexion => garantie la livraison et l'ordre des données
  - Sans connexion => sans garantie



C'est quoi un protocole ?

Protocole humain:

- "Quelle heure est-il?"
- "J'ai une question…"
- … Messages spécifiques émis
- … Actions spécifiques accomplies quand des messages (ou des requêtes de service) sont reçus

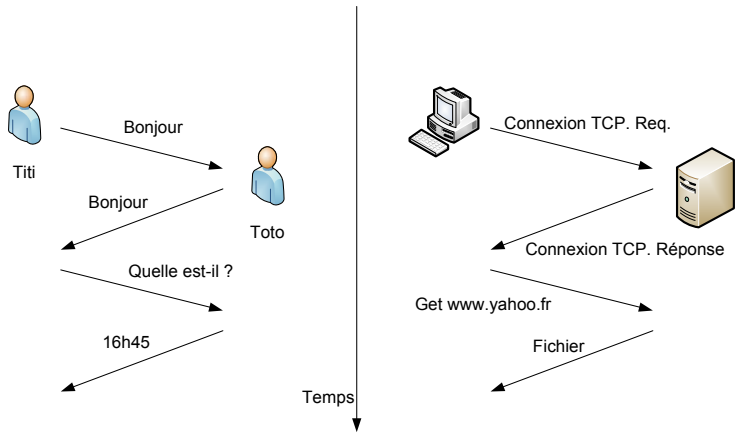
Protocole de communication :

- Permet la communication entre machines
- Toutes les communications sur Internet sont gouvernées par des protocoles

Les protocoles définissent le format, l'ordre des messages émis et reçus entre les entités réparties, ainsi que les actions à exécuter lors de la réception de ces messages (requêtes de service)

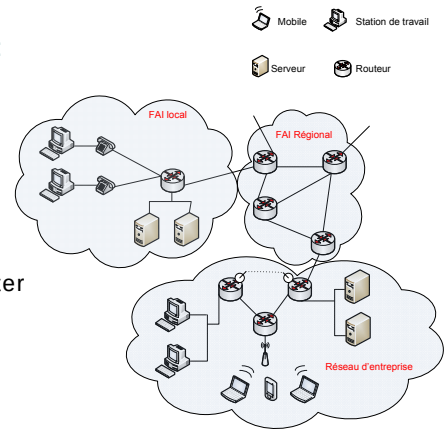
C'est quoi un protocole ?

Un protocole humain et un protocole réseau :



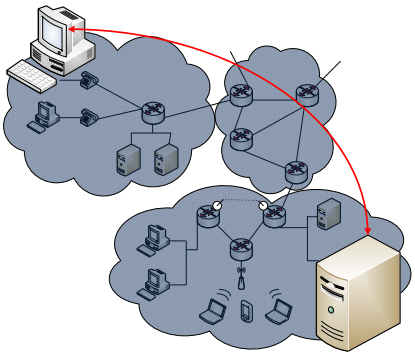
L'architecture du réseau

- En bordure du réseau :
  - Applications, hôtes
- Le cœur du réseau :
  - Routeurs
  - Réseau de réseaux
- Réseau d'accès, liens physiques
  - Moyens de se connecter au réseau



En bordure du réseau

- Systèmes terminaux (hôtes):
  - Exécutent des programmes (applications)
  - Par ex. : WWW, email, etc.
  - En bordure du réseau
  - Ex. PC, Smartphone, tablette, voiture, compteur électrique
- Modèle client/serveur
  - Le client demande un service, le serveur assure un service
  - Par ex., client web (navigateur)/ serveur web; client email/serveur
- Modèle pair-à-pair (*per-to-peer*):
  - Pas (ou peu) d'utilisation de serveurs spécifiques
  - Ex: KaZaA, Bitorrent



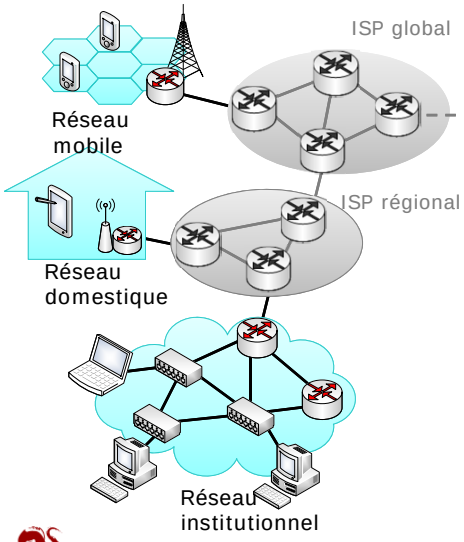
Réseaux d'accès et les médias physique

Comment connecter les terminaux au routeur de bordure ?

- Accès résidentiel
- Accès institutionnel
- Accès sans fil

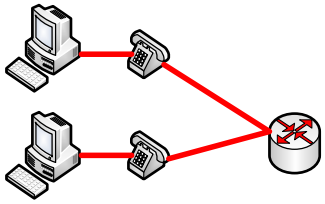
A prendre en compte pour le réseau d'accès :

- Bande passante (bits par seconde, bit/s) ?
- Accès partagé ou dédié ?



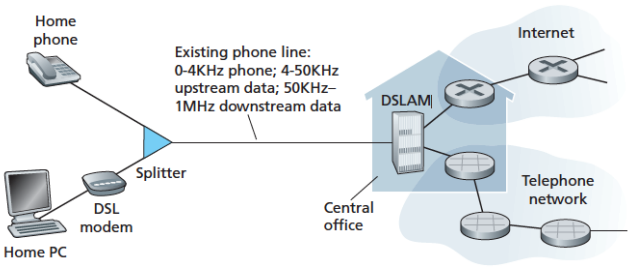
Accès résidentiel : accès point à point

- Accès par la ligne téléphonique via un modem
  - Jusqu'à 56 Kbit/s
  - Pas de communication téléphonique en parallèle avec la transmission des données
- RNIS (Réseau Numérique à Intégration de Services):
  - Accès numérique : jusqu'à 128 Kbit/s



Accès résidentiel : ADSL

- ADSL: asymmetric digital subscriber line
  - Utilise l'infrastructure téléphonique existante
  - Jusqu'à 1,8 Mbit/s du modem vers le DSLAM (DSL Access Multiplexer (1999), 2,5 Mbit/s (2003)
  - Jusqu'à 12 Mbit/s du DSLAM vers le modem (1999), 24 Mbit/s (2003)
  - Communication téléphonique en parallèle avec la communication des données

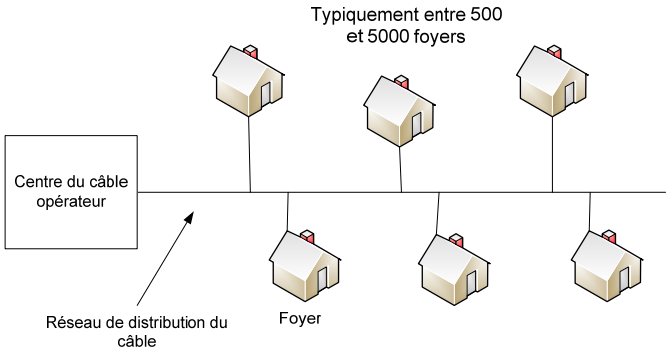


(Source: Computer Networking « a top down approach »)

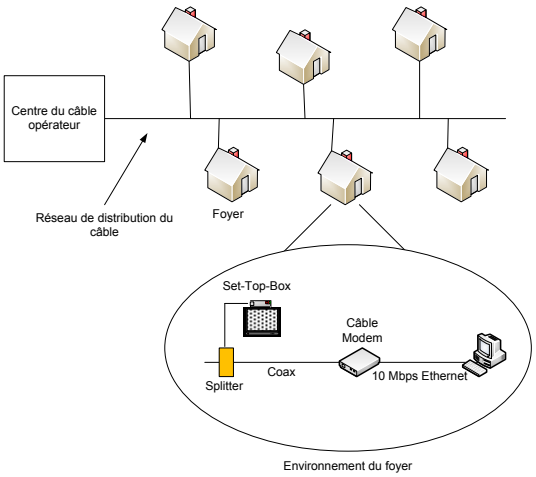
Accès résidentiel : via un câblo-opérateur

- HFC : Hybrid Fiber Coax
  - Asymétrique : jusqu'à 42,8 Mbit/s dans la voie descendante, et jusqu'à 3,7 Mbit/s en voie remontante
- Réseau de câbles (coax.) et de fibres optiques connectant les résidences aux ISPs
  - Le lien remontant est partagé avec tous les autres modems connectés sur ce lien
- Déploiement : disponible via les opérateurs par câble (TV)

Architecture d'un réseau sur câble

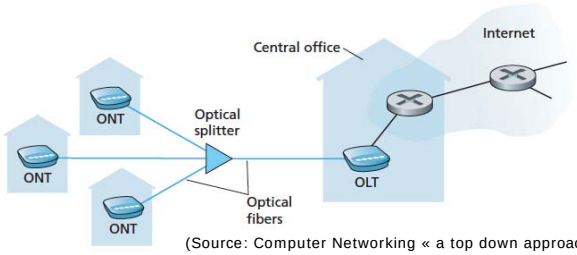


Architecture d'un réseau de câble



Accès résidentiel : FTTH

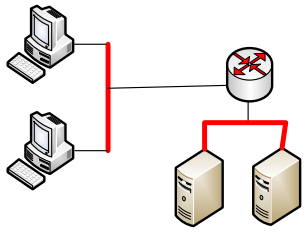
- FTTH (Fiber To Home)
  - Lien optique avec le commutateur du quartier
  - Deux éléments
    - ONT (Optical Network Terminator): extrémité située chez l'usager, conversion opto-électrique.
    - OLT (Optical Line Terminator) : extrémité située chez l'opérateur, conversion opto-électrique
  - Environ 20 Mbit/s



(Source: Computer Networking « a top down approach »)

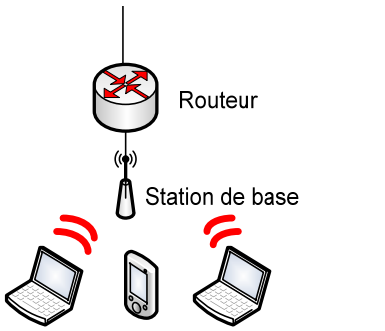
Accès institutionnel : réseau local

- Un réseau local (LAN) connecte les terminaux au routeur de cœur
- Ethernet:
  - Le plus déployé dans les réseaux d'entreprise
  - Il peut nécessiter l'utilisation d' équipements reliant les machines (Commutateur ou "*Switch*")
  - Un lien partagé entre plusieurs machines ou dédié à chaque machine peut être utilisé
  - 10 Mbit/s, 100 Mbit/s, Gigabit Ethernet



Réseaux d'accès sans fil

- Un accès partagé *sans fil* connecte les terminaux au cœur de réseau
- LAN sans fil :
  - Bande de fréquence à accès libre
  - WiFi : 802.11b (11 Mbit/s), 802.11g (54 Mbit/s), 802.11n (100 Mbit/s), 802.11ac (1 Gbit/s).
- Réseaux cellulaires :
  - Bande de fréquence régulée et attribué à des opérateurs
  - 3G, 3G+ (3,84 Mbit/s), LTE-4G (10 Mbit/s)

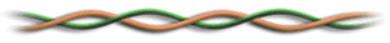


Lien de communication

- Les bits se propagent sur le lien après codage et modulation
- Lien : Relie un ou plusieurs terminaux
  - Avec support physique:
    - Les signaux se propagent sur le support physique : cuivre, fibre
  - Sans support physique:
    - Les signaux se propagent grâce aux ondes électro-magnétiques

Paires torsadées

- Paires de fils de cuivre
  - Catégorie 3: fils téléphoniques classiques, Ethernet 10 Mbit/s
  - Catégorie 5 : Ethernet 100 Mbit/s



Média physique

Cable coaxial :

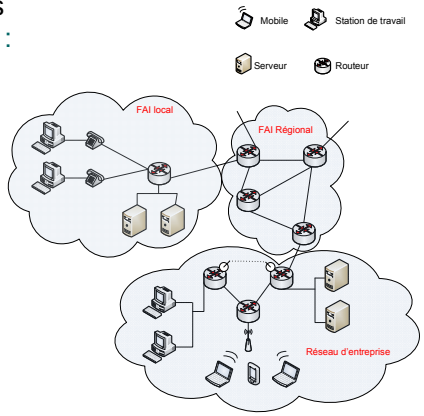
- Conducteurs concentriques à l'intérieur d'une gaine (isolation électro-magnétique, protection mécanique)
  - En bande de base: un seul canal fréquentiel sur le câble
  - A large bande: plusieurs canaux fréquentiels sur le câble
- Bidirectionnel
- Application
  - 10 Mbit/s Ethernet
  - Câble résidentiel

Fibre optique :

- Fibre de silicium transmettant des impulsions optiques
- Haut débit :
  - 1 Gbit/s Ethernet
  - Transmission point-à-point HD (par ex., 5 Gbit/s)
- Très faible taux d'erreur

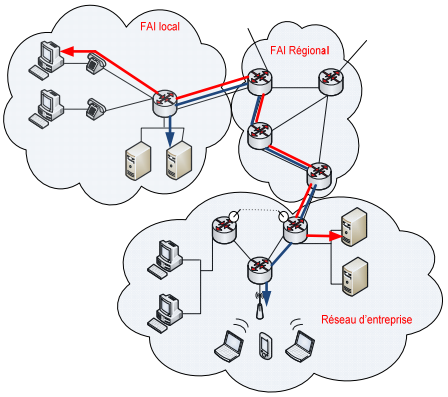
Le cœur du réseau

- Un maillage de routeurs
- Question fondamentale : comment les données sont-elles propagées dans le réseau ?
  - Commutation par circuits : Un circuit (connexion) dédié par communication
    - Réservation de ressources
    - Par ex. le téléphone (ancien)
  - Commutation par paquets: Les données sont envoyées par paquets sur le réseau
    - Utilisation des ressources à la demande



Cœur de réseau : Commutation par circuits

- Réservation de ressources de bout-en-bout pour chaque appel
  - Bande passante du lien, capacité du lien
  - Ressources dédiées : sans partage
  - Performance garantie
  - Nécessite l'établissement de la connexion

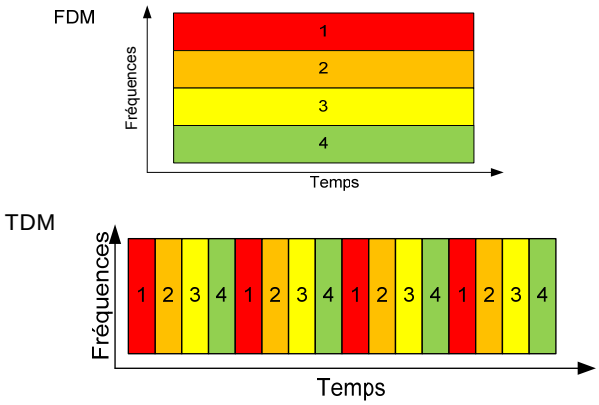


Cœur de réseau : Commutation par circuits

- Ressources réseau (Ex., bande passante) partitionnées en « *morceaux* »
  - allouées à chaque appel
- Ressources considérées comme « *inutiles* » si elles ne sont pas utilisées par l'appel associé à cette ressource *(pas de partage)*
- Division de la bande passante en « *morceaux* »
  - Division fréquentielle => Par ex. canal d'une radio FM
  - Division temporelle => "time slot", trame

Cœur de réseau : Commutation par circuits

Exemple : 4 utilisateurs



Exemple numérique

- Quel est le temps nécessaire pour transmettre un fichier de 640000 bits d'une machine A vers une machine B, sachant que le réseau de cœur est à commutation de circuits ?
  - Chaque lien a un débit de 1,536 Mbit/s (Méga bit par seconde)
  - Chaque lien utilise un partage TDM avec 24 slots
  - 500 ms pour établir la connexion de bout-en-bout
- Réponse : 10,5 s

Cœur de réseau – commutation par paquets

Le flot de données est divisé en *paquets*

- Les paquets des utilisateurs A et B *partagent* les ressources réseaux
- Chaque paquet utilise la bande passante totale
- Les resources sont réutilisées si nécessaires

⃠

Partitionnement de la bande passante (en morceaux)

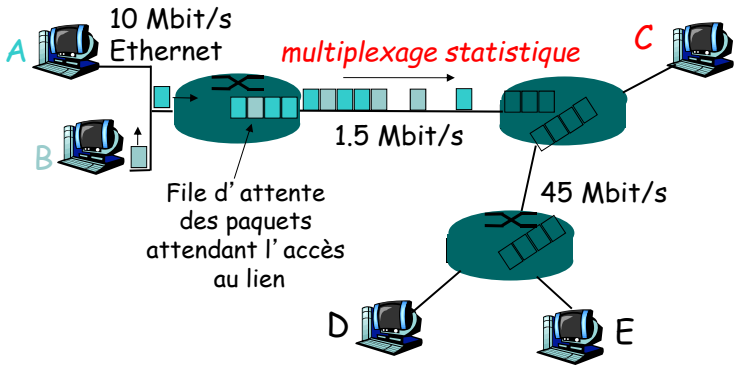
Allocation dédiée à une connexion entre deux stations

Réservation de ressources

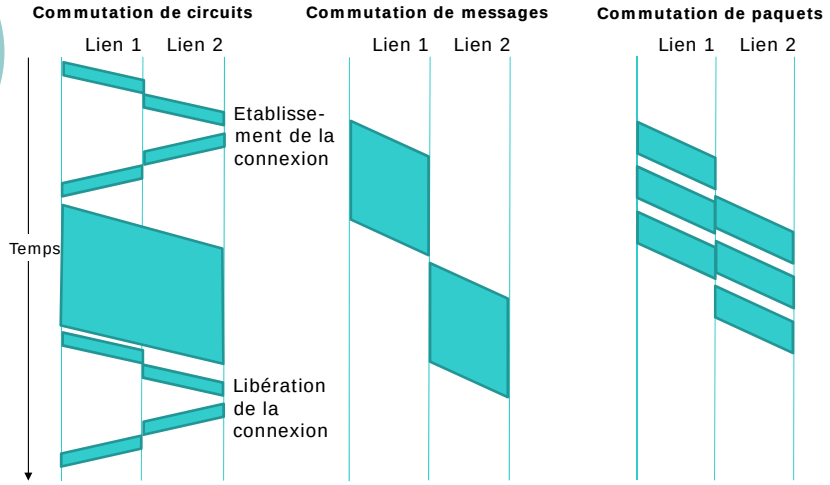
Contention pour l'obtention des ressources:

- Les ressources agrégées peuvent dépasser la capacité d'un lien
- Congestion: Les paquets s'amoncellent dans des files d'attente en attendant l'accès aux ressources
- "store and forward" : Les paquets se déplacent noueds après noeuds
  - Attente de la réception entière du paquet avant de le retransmettre.

Cœur de réseau – commutation par paquets



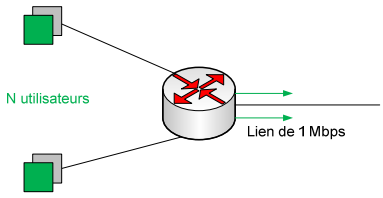
Commutation par paquets – versus commutation par circuits



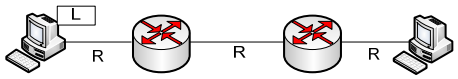
Commutation par paquets versus commutation par circuits

La commutation par paquets optimise l'utilisation de la bande passante => plus d'utilisateurs

- Exemple
  - Un lien de 1 Mbit/s
  - Chaque utilisateur :
    - Émet 100 Kbit/s quand il est actif
    - Est actif que 10% du temps
  - Commutation par circuits :
    - 10 utilisateurs
  - Commutation par paquets
    - 35 utilisateurs, avec Proba(>10 stations actives) est < 0.004



Commutation par paquets : store-and-forward



- L/R seconde pour transmettre un paquet de L bits sur un lien de débit R bit/s
- Attente du paquet entier avant de le transmettre sur le prochain lien : *store-and-forward*
- Délai total : 3L/R (on néglige, ici, le temps de propagation)
- Si R=1,5 Mbit/s, L = 7,5 Mbit alors le délai total est de 15 s.

Commutation par paquets versus commutation par circuits

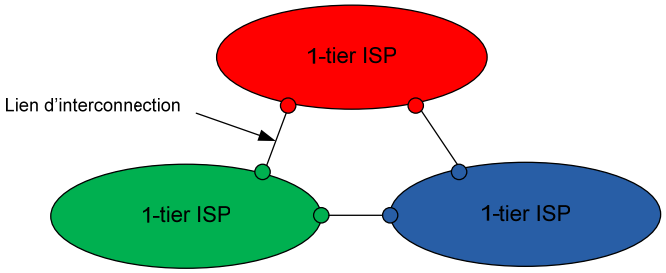
- Commutation par paquets
  - Adaptée au trafic sporadique ("bursty")
  - Partage de ressources (optimisation de la bande passante)
  - Plus simple, pas d'établissement de connexion au préalable
- Cependant : délai d'acheminement et perte des paquets
  - Besoin d'un protocole de contrôle de pertes et de congestion

Commutation par paquets : l'acheminement

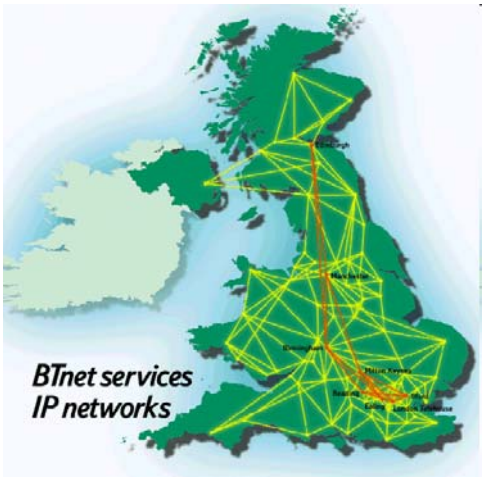
- But : acheminer les paquets le long d'un chemin formés par les routeurs qui relient la source et la destination
- Détermination du prochain saut basée sur
  - l'adresse de destination contenue dans chaque paquet
  - La table de routage présente dans chaque routeur
- Mise à jour de la table de routage …
  - … Algorithme de routage

Structure d'Internet : réseau des réseaux

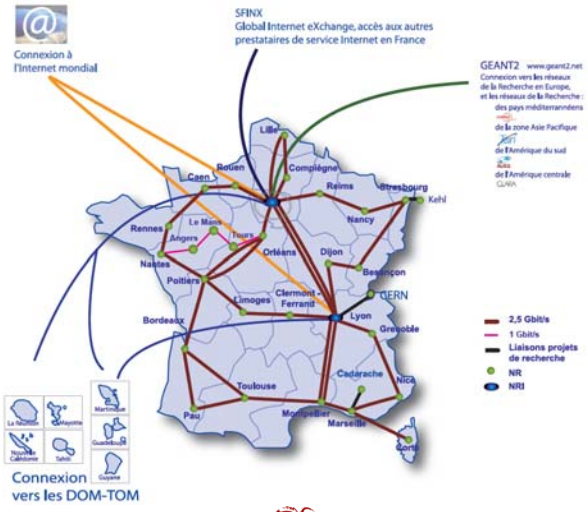
- Hiérarchique
- Au centre : le « 1-tiers » ISP (Internet Service Provider), couverture nationale et internationale



1-tier ISP : exemple British Telecom

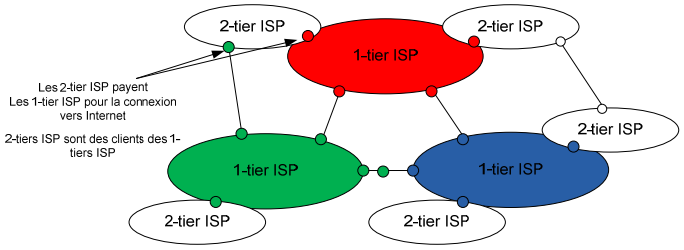


Cœur du réseau universitaire français



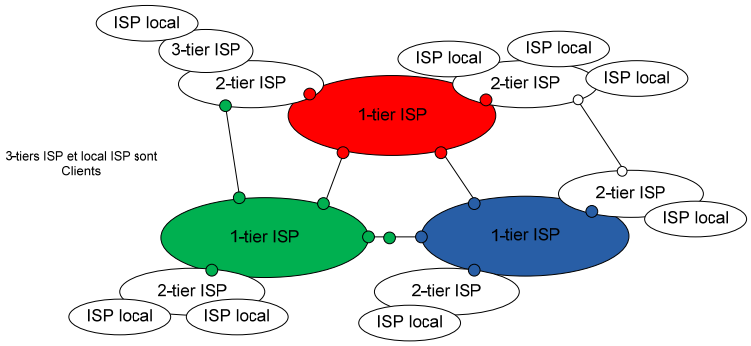
Structure d'Internet : réseau des réseaux

- 2-tier ISPs : plus petit en taille que les 1-tiers ISP (on dit ISP régionale)
  - Connectés à un ou plusieurs 1-tier ISP, ou à d'autres 2-tiers ISP



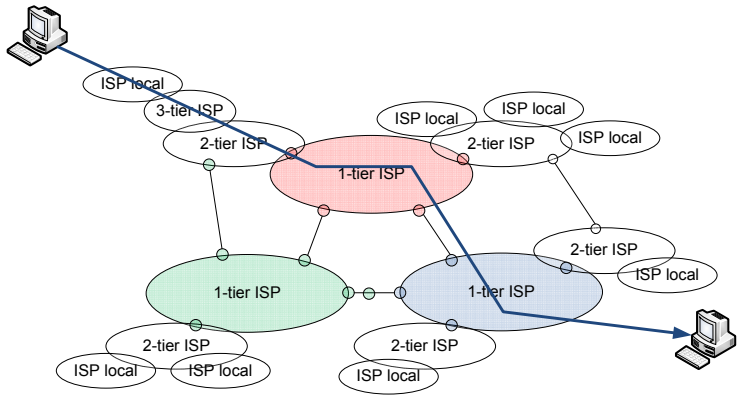
Structure d'Internet : réseau des réseaux

- 3-tiers ISP et ISP locale
  - Dernier maillon de la chaîne, dernier réseau avant le système final

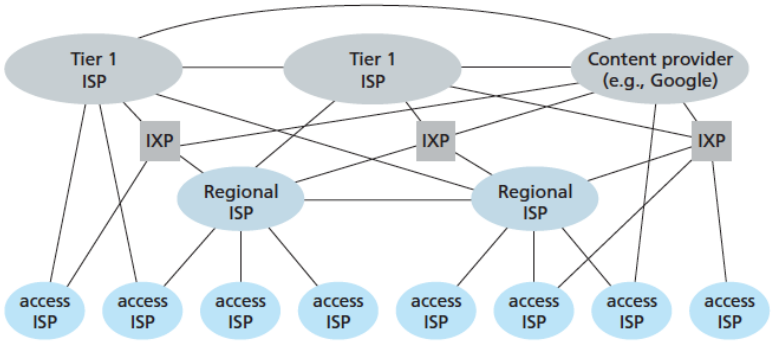


Structure d'Internet : réseau des réseaux

- Un paquet peut passer à travers plusieurs réseaux de plusieurs ISP

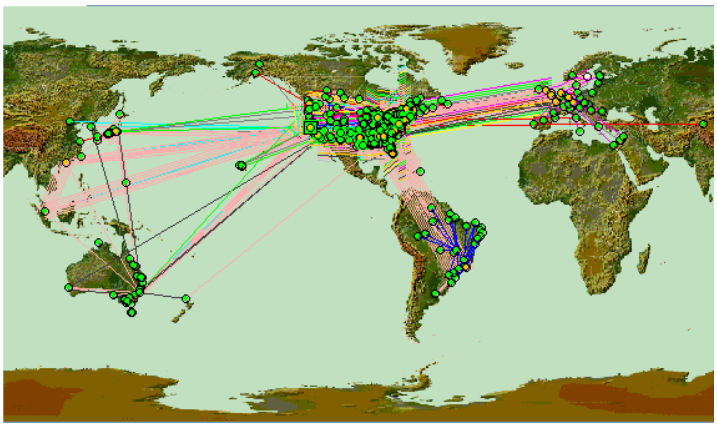


Structure d'Internet : situation en 2012



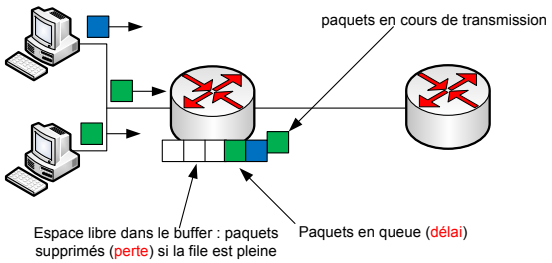
(Source: Computer Networking « a top down approach »)

Interconnexion mondiale (sauf Afrique) des ISPs



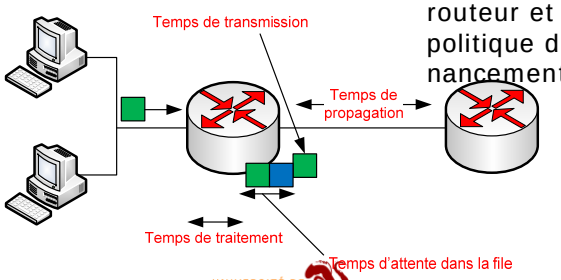
Délai et perte de paquets sur Internet : Pourquoi ?

- Les paquets sont mis en file d'attente au niveau des routeurs
  - Le taux d'arrivée des paquets dépasse la capacité du lien en sortie
  - Les paquets dans la file attendent avant d'être émises



Quatre sources de délai

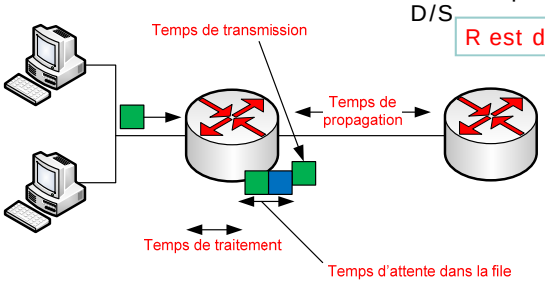
1. Délai de traitement sur le routeur
   - Vérification des erreurs
   - Choix du chemin
2. Délai d'attente dans la file
   - Temps d'attente avant la libération du lien
   - Dépend du niveau de congestion du routeur et de la politique d'ordon-nancement



Quatre sources de délai

3. Délai de transmission
   - R = la bande passante du lien
   - L = Taille des paquets
   - Délai de transmission = L/R
4. Délai de propagation
   - D= longueur du lien physique
   - S = la vitesse de propagation sur le lien (env. $2x10^8$ m/s)
   - Délai de propagation = D/S

R est différent de S



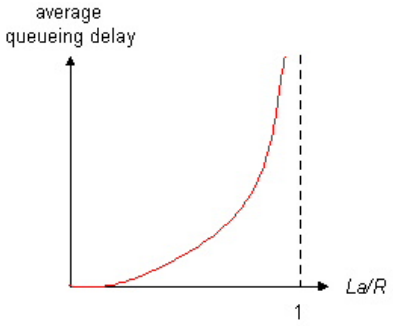
Exemple : La caravane

- Une caravane contient 10 voitures
- Chaque voiture passe 12 secondes à un péage
- La distance entre les péages est de 100 km
- Vitesse constante de 100 km/h
- Donner le temps nécessaire pour que la caravane passe d'un péage à un autre
- Maintenant, on suppose que la vitesse est de 1000 km/h et le temps de passage est de 10 min. Quel est le temps ?

Délais d'attente

- R=Débit (bit/s)
- L=Taille des paquets (bit)
- a=Taux d'arrivée de paquet

Intensité du trafic = L.a/R



- La/R ~ 0: Délai moyen d'attente est faible
- La/R =< 1: Le délai devient important
- La/R > 1: L'arrivée est plus rapide que la sortie, la file est instable

Exemple de délais

```
traceroute: Warning: www.google.fr has multiple addresses; using 173.194.34.31
traceroute to www.google.fr (173.194.34.31), 64 hops max, 52 byte packets
 1  default-gw (131.254.1.1)  1.737 ms  0.293 ms  0.258 ms
 2  renater-gw-128 (131.254.128.9)  0.223 ms  0.225 ms  0.213 ms
 3  * * *
 4  te4-1-caen-rtr-021.noc.renater.fr (193.51.189.54)  7.405 ms  7.349 ms  7.439 ms
 5  te4-1-rouen-rtr-021.noc.renater.fr (193.51.189.46)  7.611 ms  7.360 ms  7.283 ms
 6  te0-0-0-1-paris1-rtr-001.noc.renater.fr (193.51.189.49)  9.231 ms  8.062 ms  9.724 ms
 7  te0-1-0-4-paris2-rtr-001.noc.renater.fr (193.51.189.174)  12.131 ms  11.986 ms  12.905 ms
 8  * * *
 9  193.51.182.197 (193.51.182.197)  7.479 ms  7.704 ms  7.662 ms
10  72.14.238.234 (72.14.238.234)  7.675 ms  7.827 ms  7.928 ms
11  209.85.242.45 (209.85.242.45)  8.158 ms  7.962 ms  8.044 ms
12  par03s02-in-f31.1e100.net (173.194.34.31)  7.736 ms  7.670 ms  7.629 ms
```

3 mesures de délais entre la src et le routeur

Pas de réponse du routeur ou perte

Perte de paquets

- La file d'attente des routeurs a une capacité limitée
- Si la file est pleine, tous les paquets qui arrivent sont supprimés
- Le paquet perdu => retransmission par la source, (ou le nœud précédent) ou rien (pas de retransmission)

Modèle en couche des protocoles

- Les réseaux sont complexes
- Différents acteurs/composants constituent le système
  - Hôtes
  - Routeurs
  - Liens (différents type de médias)
  - Applications
  - Protocoles
  - Hardware/Software
- Comment organiser la structure du réseau ?

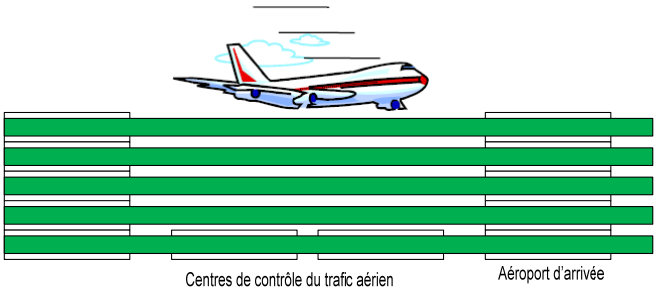
Organisation d'un transporteur aérien

Ticket (achat)	Ticket (plainte)
Bagage (vérification)	Bagage (retrait)
Porte d'accès (chargement)	Porte d'accès (déchargement)
Piste de décollage	Piste d'atterrissage
Plan de vol	Plan de vol

Plan de vol

Une série d'étapes

Les fonctionnalités des couches



- Couches : chaque couche offre un service
  - Construit par ses mécanismes internes
  - En utilisant les services proposés par la couche sous-jacente

Pourquoi le modèle en couches ?

- Traiter des systèmes complexes
- Une structure définie explicitement, permet d'identifier la relation entre les composants le système
- Modularité => facilité de maintenance, facilité de m.-a-j. du système
  - La modification d'un service proposé par une couche n'affecte pas la couche adjacente
  - Ex. : changer la procédure d'embarquement n'affecte pas le reste du système de transport aérien

Les couches protocolaires - Internet

- Application : "supporte" les applications réparties
  - FTP, SMTP, HTTP
- Transport : transporte les messages (flux d'octets) entre les hôtes
  - TCP, UDP
- Réseau: achemine (mondialement) les paquets de données entre la source et la destination
  - IP, protocoles de routage
- Liaison : transfert de trames de données entre éléments voisins d'un réseau local
  - Ethernet, WiFi
- Physique : encodage et modulation d'un train de bits sur un support de communication

application
transport
réseau
Liaison
physique

L'encapsulation