



Introduction Réseau Topologies – Protocoles Architectures en couches (Modèles OSI, IEEE, TCP/IP)

Catherine Bernard
(catherine.bernard@esigetel.fr)

ESIEE – I3FR
2011/2012

Préambule

- ▶ Objectifs du cours
 - Obtenir une culture générale sur l'architecture des réseaux en termes de matériel, interconnexion, topologie et support
 - Comprendre les architectures en couches des modèles réseaux
- ▶ Un certain nombre de technologies abordées ici seront approfondies dans les cours suivants :
 - Couches Physique et Liaison (support, codage, MAC) (semestre 1)
 - Couches Réseau et Transport – Routage – Traffic Management – TCP/IP (semestre 2)
- ▶ Volume horaire : CM 18h – TD 4h – TP 8h



Sommaire

- ▶ Introduction
- ▶ Concepts réseaux
- ▶ Les réseaux d'entreprise/ Les réseaux d'opérateurs
- ▶ Architecture logicielle des réseaux – Structure en couches
- ▶ Le modèle OSI
- ▶ Les réseaux locaux (modèle IEEE)
- ▶ Le modèle TCP/IP
- ▶ Conclusion – Glossaire – Bibliographie

Sommaire

- ▶ Introduction
 - Petit historique
 - Indicateurs pour le secteur Réseau et Télécom
 - Perspectives : Le Cloud ???
- ▶ Concepts réseaux
- ▶ Les réseaux d'entreprise/ Les réseaux d'opérateurs
- ▶ Architecture logicielle des réseaux – Structure en couches
- ▶ Le modèle OSI
- ▶ Les réseaux locaux (modèle IEEE)
- ▶ Le modèle TCP/IP
- ▶ Conclusion – Glossaire – Bibliographie



Introduction – Petit historique

- ▶ L'histoire des télécommunications démarre en 1832 avec le physicien américain Morse (1792–1872)
 - ☺ Première liaison officielle en 1844
 - ☹ Première liaison transocéanique en 1858 (elle ne fonctionne qu'un mois à cause d'un défaut d'isolement du câble immergé !)
- ▶ 1865 : Union Internationale des Télécommunications
- ▶ 1876 : En parallèle, développement de la téléphonie : dépôt d'un brevet par Graham Bell (1847–1922).
- ▶ 1899 : Première liaison hertzienne avec Marconi (1874–1937)
- ▶ 1931 : Télévision (principes)
 - 1953 : Première transmission d'images TV par faisceaux hertziens
- ▶ Invention du transistor : une nouvelle voie aux communications...
 - 1956 : 1^{er} câble téléphonique transocéanique avec 15 répéteurs immergés
 - 1962 : 1^{ière} liaison de télévision transocéanique avec le satellite Telstar 1
- ▶ 1961 : Invention du Laser – 1975 : première liaison sur fibre



Introduction – Petit historique

- ▶ 1969 : Début de l'Internet
- ▶ 1970 : Réseaux locaux – Ethernet qui ne cessera d'évoluer... (1995 : Fast Ethernet, 1998 : Gigabit Ethernet, aujourd'hui 10Gigabit Ethernet, demain 100 Gigabit)
- ▶ 1978 : Premier réseau mondial de transmission de données par paquets –X25– ouvert au public – France : Transpac).
- ▶ 1981 : Expérience de Velizy qui concrétise l'explosion de la télématique, le Minitel !!!
- ▶ 1981 : Modèle OSI (Open System Interconnection)
- ▶ 1988 : RNIS (Réseau Numérique à Intégration de Services)
- ▶ 1995 : ATM (Asynchronous Transfer Mode)
- ▶ 1998 : Ouverture des services de téléphonie à la concurrence
- ▶ Les années 2000 avec la démocratisation de la Téléphonie mobile (GSM, GPRS, UMTS...), les accès Internet Haut débit (ADSL, FTTx...), le Tbit/s dans les backbones
- ▶ Le début du 21ème siècle : Web 2.0, les réseaux sociaux, la virtualisation et demain tous dans le nuage! (Cloud Computing)



La vague Internet



- ▶ **Internet**, son ancêtre : ARPANET, conçu dans les années 1960 par le DARPA
- ▶ But : Concevoir une architecture de réseau dans laquelle la rupture d'une liaison n'interrompt pas brutalement les conversations
- ▶ Principe : les données sont découpées en « paquets » de bits, chaque paquet peut emprunter un chemin différent pour atteindre sa destination => **réseau à commutation de paquets**
- ▶ Connexion des centres du DoD à l'ARPANET dans les années 1970, puis des centres de recherche et des universités
- ▶ Fin des années 1980 : connexion des entreprises privées => naissance de l'Internet – Standardisation de IPv4 en 1981 (RFC 791)
- ▶ Tous ces réseaux fonctionnent selon les **protocoles de routage et de transport TCP/IP**
- ▶ 1.5 milliard d'internautes soit 22% de la population mondiale connectés en 2011 (source : Juniper Research) (1980, quelques dizaines d'hôtes – 1996, 12 millions de machines réparties en 500 000 réseaux). Croissance nourrie par 4 pays : Brésil, Russie, Inde, Chine

Quelques indicateurs pour le secteur Réseaux & Télécoms...

- ▶ Explosion du marché des Télécoms
 - Volume des transmissions de données qui double tous les ans
 - La vague Internet
 - 21.3 millions d'abonnements à Internet à haut débit fin 2010 (soit un accroissement de 7.5% en un an – Réf. : <http://www.arcep.fr/>)
- ▶ Place de plus en plus importante dans les économies nationales
- ▶ Revenus des opérateurs de communications électroniques sur le marché des clients finaux : 11.5 milliards d'euros au 3ème trimestre 2010 – Réf. : <http://www.arcep.fr/>
- ▶ Trois composantes majeures du marché (téléphonie fixe, Internet et téléphonie mobile) : 8.8 milliards d'euros au 3ème trimestre 2010 (Services fixes 3.9Md, services mobiles 4.9Md)
- ▶ Déréglementation – Arrivée de nouveaux opérateurs sur le marché
 - 1000 opérateurs déclarés auprès de l'ARCEP (juillet 2010)
- ▶ Les acteurs du monde Réseaux & Télécom
 - Les constructeurs : Cisco, Alcatel-Lucent, Ericsson, Huawei, Nokia-Siemens...
 - Les opérateurs : Orange, AT&T (US), Verizon (US), Telefonica (Spain), China Mobile (CH), NTT (Japon), British Telecom (UK)...

Perspectives : Le Cloud ??



- ▶ Définition du Cloud

- Selon le Burton Group, le Cloud Computing regroupe « l'ensemble des disciplines, technologies et modèles d'entreprise utilisés pour fournir des capacités informatiques (logiciels, plates-formes, matériels) à la manière d'un service à la demande, évolutif et élastique »

- ▶ Caractéristiques du Cloud (NIST, National Institute of Standards Technology)

- Libre-service à la demande
- Accès étendu au réseau
- Mutualisation des ressources
- Elasticité/mise à l'échelle rapide
- Service mesuré



- ▶ Microsoft TechDays (février 2011) – Etude menée par Brocade

- 60 % des entreprises envisagent une migration vers le Cloud Computing d'ici 2012
 - Pour quelles raisons ??? Réduction des coûts, gain en agilité et flexibilité
- Marché du Cloud entre 2009 et 2013, une croissance continue : + 20%

Les modèles de service du Cloud

- ▶ Software as a Service
 - Concerne les applications d'entreprise : CRM, outils collaboratifs, messagerie, ERP....
- ▶ Platform as a Service
 - Concerne les environnements middleware, de développement, de test
- ▶ Infrastructure as a Service
 - Concerne les serveurs, moyens de stockage, réseau... Techniques de **Virtualisation**
- ▶ Un modèle économique novateur
 - Plus de coûts de licence, plus de coûts d'infrastructure, plus de coûts de maintenance et d'exploitation
 - ... mais un coût unique à l'utilisation
- ▶ Et demain ??? De nouveaux défis...
 - De nouvelles régulations (internationales, locales) ??
Domaine de responsabilité ??
 - Quelle sécurité ?? Une solution Green???



Sommaire

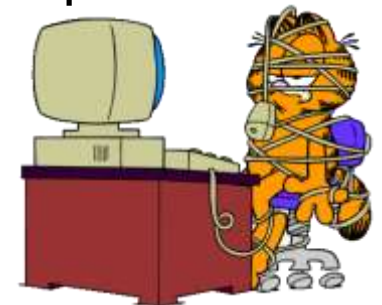
- ▶ Introduction
- ▶ **Concepts réseaux**
 - Notion de Réseau – Classification des réseaux
 - Le transport de l'information
 - Les modes de communication
- ▶ Architecture logicielle des réseaux – Structure en couches
- ▶ Le modèle OSI
- ▶ Les réseaux locaux (modèle IEEE)
- ▶ Le modèle TCP/IP
- ▶ Conclusion – Glossaire – Bibliographie

Notion de réseau

- ▶ Réseau :
 - Étymologie : du latin « reticulum », petit filet, diminutif de « retis »
 - Définition : maillage constitué de nœuds et de fils les reliant les uns aux autres

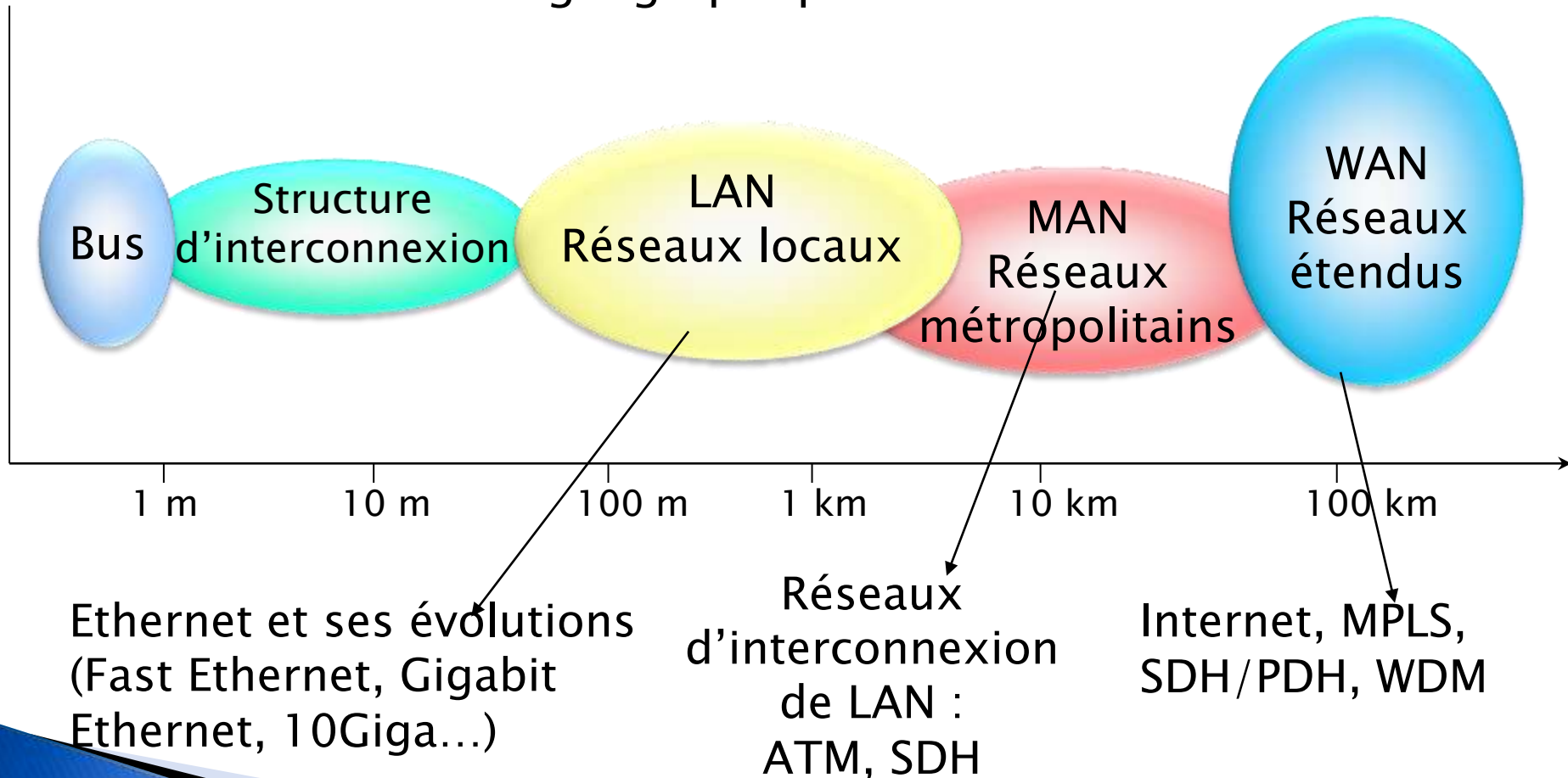
Réseau = résultat de la connexion de plusieurs machines entre elles

- ▶ Pourquoi constituer un réseau ???
 - Partage de logiciels, de fichiers
 - Mise en commun d'applications
 - Partage de ressources : imprimantes, espace disque
 - Augmenter les performances
 - Diminution des coûts
 - Fiabilité des équipements, Sécurité



Classification des réseaux

- ▶ Critères de choix d'un réseau :
 - La couverture géographique



Classification des réseaux

- ▶ Critères de choix d'un réseau :
 - Le type d'environnement
 - Bureautique : Réseaux Locaux d'Entreprises (RLE)
 - Industriel : Réseaux Locaux Industriels (RLI) : CAN, BITBUS, FIP...
 - Le débit
 - Le type d'architecture physique (filaire ou radio)
 - Au niveau des LAN : Ethernet défini sur paires torsadées, fibre optique – Réseaux 802.11 /Wi-Fi
 - La qualité de service (QOS) : garantie de bande passante, taux d'erreurs...
 - Contrainte différente suivant le type d'application, de trafic
 - Transport de la voix, vidéo – Transport de données
 - La sécurité : disponibilité, confidentialité, authentification...
 - Le coût

Sommaire

- ▶ Introduction
- ▶ **Concepts réseaux**
 - Notion de Réseau – Classification des réseaux
 - **Le transport de l'information**
 - Signal analogique/numérique
 - Les supports de transmission
 - Paires Torsadées, Coaxiaux, Fibre optique
 - Support à Propagation libre
 - Les techniques de transmission
 - Transmission Bande de Base
 - Transmission large bande – Modulations
 - Les modes de communication
- ▶ Les réseaux d'entreprise/Les réseaux d'opérateurs
- ▶ Architecture logicielle des réseaux – Le modèle OSI
- ▶ Les Réseaux Locaux
- ▶ L'architecture TCP/IP
- ▶ Conclusion – Glossaire – Bibliographie

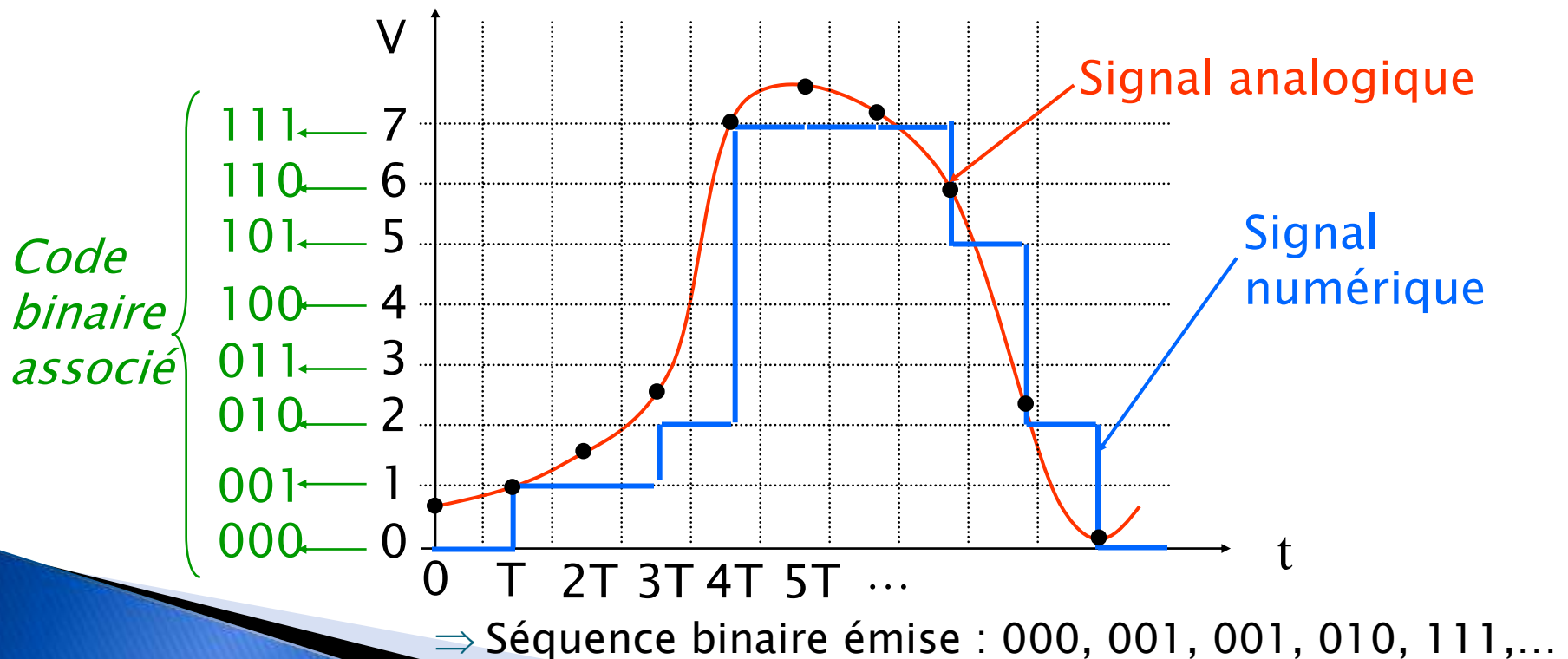
Signaux analogiques – numériques



- ▶ Quelle tendance ??
 - « Communiquer plus vite et plus loin »
- ▶ Plusieurs types de signaux à transmettre : voix, vidéo, images, données \Rightarrow signaux **analogiques** ou **numériques**
- ▶ Analogique ?
 - Les données analogiques = signaux de type continu
 - Signaux se présentant comme des variations de grandeurs physiques pouvant prendre n'importe quelle valeur de façon continue entre deux intervalles de temps
 - Propriétés d'un signal : fréquence et l'amplitude
 - Typiquement la voix, le son...
- ▶ Numérique ?
 - Signal ayant des états discrets
 - Données, les 0, 1 codés en un signal physique (par exemple 0 par une tension positive $+V$ et 1 par une tension négative $-V$)

Signaux analogiques/numériques

- ▶ Pour traiter des données de nature analogique par un ordinateur, il faut les numériser. Ex: CD audio = le son est « enregistré » sous forme de données numériques, remises sous forme analogique à l'entrée du haut-parleur.
- ▶ Principe : Echantillonnage + Codage de chaque échantillon sur n bits



Signaux analogiques / numériques

▶ Numérisation de la voix



$$f_{\max} = 4 \text{ kHz}$$

$$f_{\text{ech}} = 2 \times 4 \text{ kHz} = 8 \text{ kHz}$$

$$\text{échantillonnage} = 125 \mu\text{s}$$

$$\text{débit} = 64 \text{ kbit/s} \text{ (échantillonnage sur 8 bits)}$$



$$f_{\max} = 20 \text{ kHz}$$

$$\text{débit} = 640 \text{ kbit/s}$$

$$\text{(échantillonnage sur 16 bits)}$$

▶ Numérisation de la vidéo

- Signal vidéo caractérisé par ses trois composantes RGB (exprimées en composante de luminance (Y) et chrominance (UV)) échantillonné et numérisé pour former des pixels.
- Vidéo standard : 720 pixels x 576 lignes à 25 Hz (frame rate), chaque pixel Y, U et V codé sur 8 bits
 - Débit résultant : $720 \times 576 \times 25 \times 8 + 360 \times 576 \times 25 \times (8 + 8) = 166 \text{ Mbit/s}$ (sous-échantillonnage horizontal de la chrominance)
 - Technique de compression permettant de réduire ce débit : standards MPEG (Motion Picture Experts Group) - taux de compression 100:1

Signaux analogiques / numériques

▶ Le numérique roi : pourquoi ???



- Plus simple de transporter une représentation binaire d'un signal (2 niveaux 0 ou 1) que les variations de ce signal ⇒ possibilité d'utiliser des lignes de transmission de moins bonne qualité
- Un même réseau quelque soit le type de signal transmis : voix, vidéo, données
- Possibilité d'utiliser les outils de contrôle d'erreurs, compression, cryptage

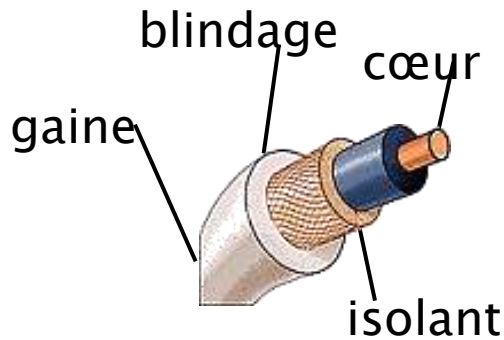
Les supports de transmission

- ▶ Les supports de transmission ????
 - Signaux convertis en signaux électriques, en lumière, en ondes électromagnétiques pour passer sur le support de transmission : un câble de cuivre, l'« air »...
- ▶ Caractéristiques des supports de transmission
 - Bande Passante W (Hz)
 - Caractérise tout support de transmission, bande de fréquence dans laquelle les signaux sont correctement reçus
$$W = F_{\max} - F_{\min}$$
 - Exemples :
 - l'atmosphère élimine les UV
 - l'oreille humaine est sensible dans la bande 15-15000 Hz
 - Débit Binaire (Bit/s) caractérisant une liaison
 - C'est la quantité maximale d'information transmissible sur une voie



Les supports de transmission

► Supports à propagation guidée



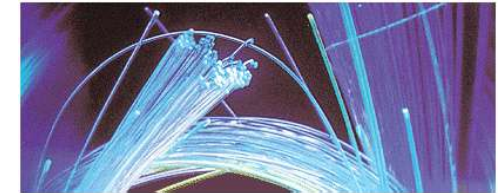
Câble coaxial
Câble antenne



Paires torsadées : brins de
cuivre torsadés pour se
protéger des perturbations
extérieures
Câble téléphonique

Signaux électriques

Signaux optiques



Fibre optique
Guide d'onde en verre de
très haute performance
(très haut débit, longue
distance)

► Supports à propagation libre

- Liaisons radios, satellites.... Définies selon la bande de fréquence utilisée

Les techniques de transmission

- ▶ **Transmissions de données et Bande passante**
 - Le spectre du signal à transmettre doit être compris dans la bande passante du support physique.
 - La transmission d'un signal à spectre étroit sur un support à large bande passante \Rightarrow mauvaise utilisation du support de transmission
 - Techniques de **Modulation** et **Multiplexage** pour pallier à ces problèmes
 - adapter les signaux au support
 - rentabiliser l'utilisation du support

- ▶ **Techniques de transmission**
 - **Transmission numérique bande de base**
 - **Transmission bande transposée**
 - Modulation d'amplitude, fréquence, phase



Les techniques de transmission

- ▶ Transmission bande de base
 - Pas de transposition en fréquence (ETCD simple codeur)
 - Codes en lignes consistant à associer à chaque élément binaire ou suite d'éléments binaires un signal cadencé par une horloge (exemple : code NRZ, 0 codé par une tension $+V$, 1 par une tension $-V$)
 - Utilisable uniquement sur les supports n'introduisant pas de décalage en fréquence (le signal occupe toute la bande passante disponible)

- ▶ Transmission bande transposée – Modulation
 - Utilisation d'une fréquence porteuse adaptée au support de transmission
 - Effets de la modulation :
 - **transposition** dans un domaine de fréquences adapté au support de transmission
 - meilleure **protection** du signal contre le bruit
 - **transmission simultanée** de plusieurs messages dans les bandes de fréquences adjacentes : meilleure utilisation du support

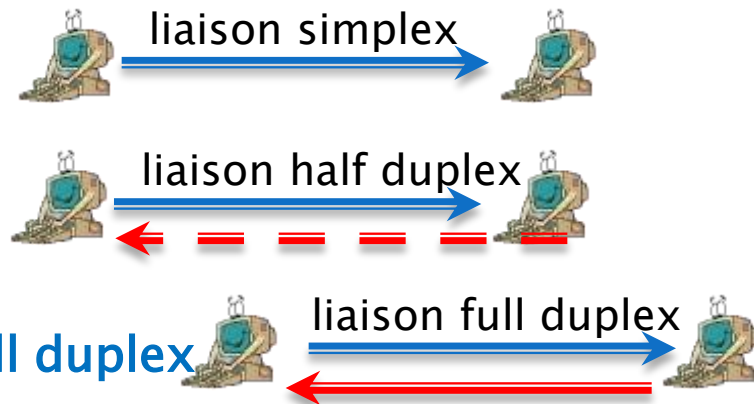
Sommaire

- ▶ Introduction
- ▶ **Concepts réseaux**
 - Notion de Réseau – Classification des réseaux
 - Le transport de l'information
 - **Les modes de communication**
 - Les modes de transmission (full-duplex, half duplex)
 - Transmission synchrone/asynchrone
 - Les types de commutation
 - Commutation de circuits
 - Commutation de paquets
 - Les modes de connexion (connecté, non connecté)
- ▶ Les réseaux d'entreprise/Les réseaux d'opérateurs
- ▶ Architecture logicielle des réseaux – Structure en couches
- ▶ Le modèle OSI
- ▶ Les réseaux locaux (modèle IEEE)
- ▶ Le modèle TCP/IP
- ▶ Conclusion – Glossaire – Bibliographie

Les modes de transmission

▶ Les sens de transmission

- liaison unidirectionnelle ou **simplex**
- liaison à l'alternat ou **half duplex**
- liaison bidirectionnelle intégrale ou **full duplex**



▶ Transmission parallèle/série

▶ Transmission synchrone/asynchrone

- Transmission **synchrone** : Émetteur, récepteur synchronisés sur la même horloge de référence (horloge transportée par le signal, séquence de synchronisation au départ)
- Transmission **asynchrone** : La source produit des caractères à des instants aléatoires, indépendamment les uns des autres. L'horloge d'émission n'est pas transmise.

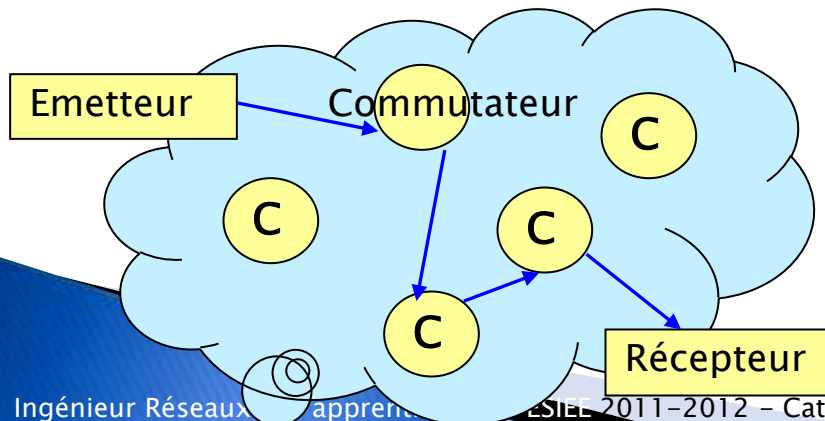
Commutation de circuits/paquets

- ▶ **Commutation** : aiguillage d'une communication d'un port d'entrée vers un port de sortie

- **Commutation de circuits**

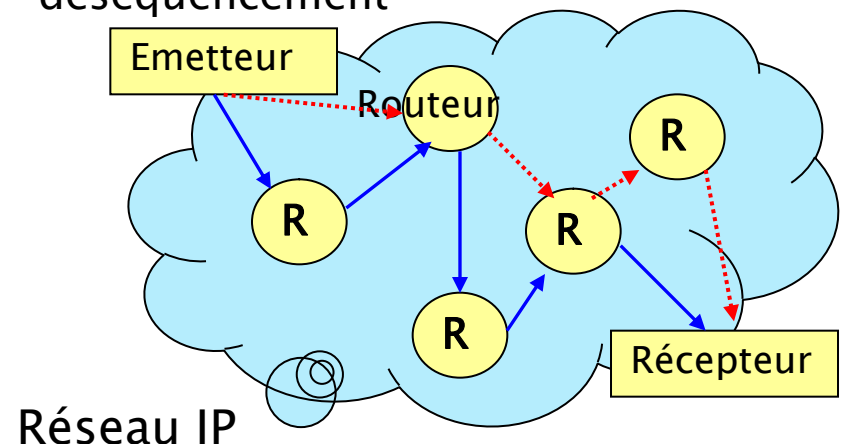
- Circuit : itinéraire physique permanent au canal de communication
- Circuit établi au préalable, ressources allouées pour la durée de vie du circuit
- Information transférée en un flux continu et constant
- Mauvaise utilisation des ressources

Réseau Téléphonique



- **Commutation de paquets**

- Info transférée par bloc de taille donnée
- Acheminement des paquets dans le réseau indépendamment du précédent
- Partage des ressources entre les communicants afin d'optimiser les liens
- Files d'attente dans les commutateurs
- Efficace pour des échanges variables ou sporadiques,
- Risque de congestion, délai variable, déséquilibrage



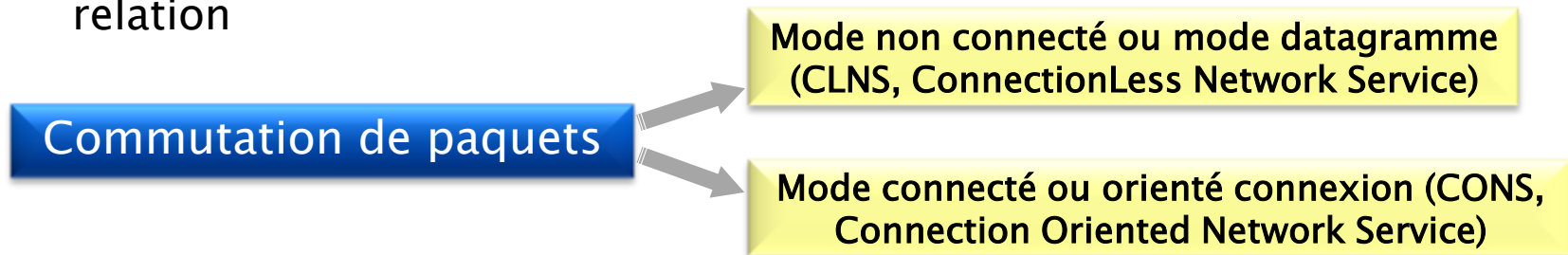
—▶ paquet1
- - -▶ paquet2

Les types de commutation – Comparaison

Critères	Commutation de circuits	Commutation de paquets
Mémorisation des informations	Impossible (flux continu de données entre émetteur et récepteur)	Chaque nœud mémorise les paquets en attente d'acquittement (mémoire vive)
Conversion de format et de débit	Impossible	Conversion de débit et (ou) de taille des blocs effectuée par le réseau
Choix d'un circuit parmi n	Oui à l'établissement	Oui, à l'établissement en mode connecté (Transpac paquet d'appel), ou à chaque paquet en mode non connecté (datagramme)
Partage du circuit entre plusieurs	Non, cependant un utilisateur peut multiplexer des liaisons sur un même circuit	Oui, plusieurs paquets, d'applications différentes, peuvent se succéder sur un même circuit
Bonne utilisation des circuits	Non, la ligne est attribuée durant toute la relation	Optimale surtout en mode non connecté
Diffusion	Non	Non
Facturation	Temps de connexion	Essentiellement au volume
Garantie de délais	Oui	Non
Réseau type	RTC	IP
Applications	Parole, transfert de fichiers	Transactionnel

Les modes de connexion

- ▶ Commutation de paquets qui se décline selon deux modes de mise en relation



- ▶ **Mode non connecté ou datagramme (best effort)** = Les paquets de données sont acheminés dans le réseau indépendamment les uns des autres
 - Possibilité de pertes de données, déséquilibrage
 - Bloc de données contenant l'adresse du destinataire
 - Aucune réservation de ressources
 - ▶ **Mode connecté ou orienté connexion** = Une connexion est établie avant la transmission des données puis relâchée (liaison virtuelle)
 - Phase d'établissement de connexion avec réservation de ressources (buffer, voies..)
 - Un paquet d'appel marque le chemin jusqu'au destinataire
 - Le destinataire confirme l'acceptation de l'appel
 - La station appelante envoie les données qui suivent le chemin marqué
- Liaison permanente (PVC, Permanent Virtual Circuit) ou établie appel par appel (SVC, Switched Virtual Circuit)

Comparaison mode connecté/non connecté

Critères	Mode non connecté	Mode orienté connexion
Mise en relation nécessaire	Non	Oui
Délai de connexion (déconnexion)	Non, pas de connexion	Oui, pouvant être important
Routage	Adaptatif, le chemin est calculé par les routeurs instantanément	Déterministe : chemin unique durant la communication (circuit virtuel)
Adresses	Chaque paquet comporte des adresses source et destination	Simplifié, label attribué à la connexion
Ressources	Pas de réservation	Réservation du chemin pendant la durée de la communication
Acquittement	Pas d'acquittements	Les nœuds intermédiaires échangent des acquittements
Fiabilité	Transmission non fiable : perte de paquets	Transmission fiable
Contrôle des congestions	Aucun contrôle n'est effectué	Contrôle par échange de crédits entre nœuds
Interconnexion des réseaux	Simple et naturelle	Complexe
Résumé	Réseau « stupide », robuste, universel. Système terminal « intelligent »	Système terminal « stupide ». Réseau « intelligent », fiable.

Sommaire

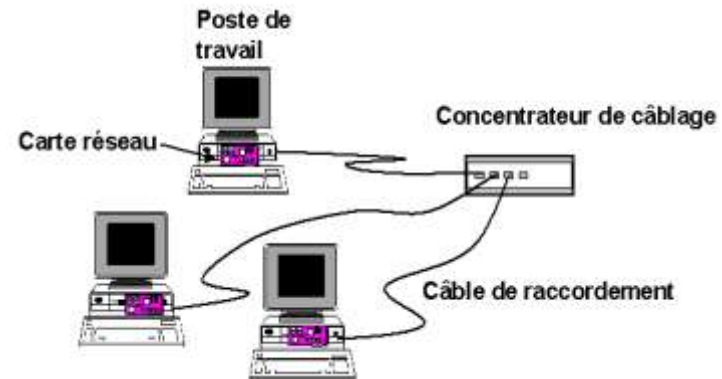
- ▶ Introduction
- ▶ Concepts réseaux
- ▶ **Les réseaux d'entreprise/ Les réseaux d'opérateurs**
 - Les réseaux d'entreprise : Définition/Structure
 - Les réseaux d'opérateurs
 - Définitions
 - Exemples de réseaux d'opérateurs : Le Réseau Téléphonique Commuté, Les technologies du réseau d'accès (ADSL, FTTx...), MPLS, Internet...
- ▶ Architecture logicielle des réseaux – Le modèle OSI
- ▶ Les Réseaux Locaux
- ▶ L'architecture TCP/IP
- ▶ Conclusion – Glossaire – Bibliographie

Définition et structure d'un réseau d'entreprise

- ▶ Réseau d'entreprise = réseau qui interconnecte les équipements informatiques d'une entreprise ⇒ LAN (**ETHERNET**) ou MAN

Topologie : manière dont les équipements sont reliés entre eux par le support physique de communication

⇒ bus, étoile, anneau, maillée



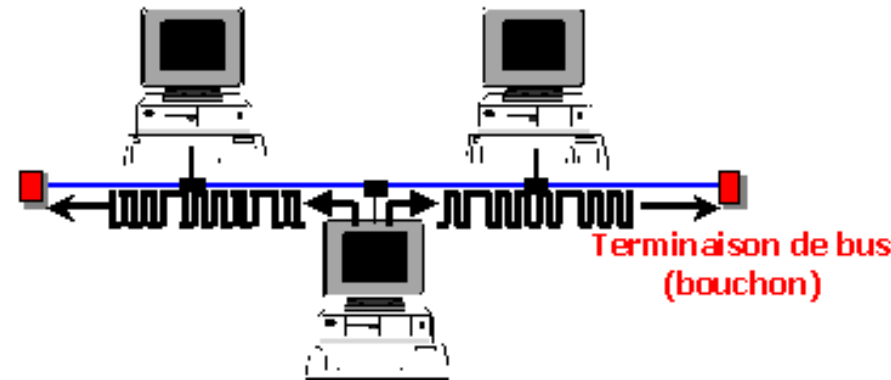
- ▶ La carte réseau
 - Attribue une identité à la machine sur le réseau, grâce à un numéro unique = **l'adresse physique (adresse MAC)**
 - Assure toutes les fonctionnalités permettant la communication avec les autres machines du réseau
- ▶ Les machines communiquent via un support : câbles électriques (paire torsadée, câble coaxial), ondes hertziennes, fibre optique... Le support est caractérisé par le débit binaire maximum qu'il peut transporter (bande passante)
- ▶ Modèle client serveur (apparu dans les années 80)

Topologies des réseaux – Définition

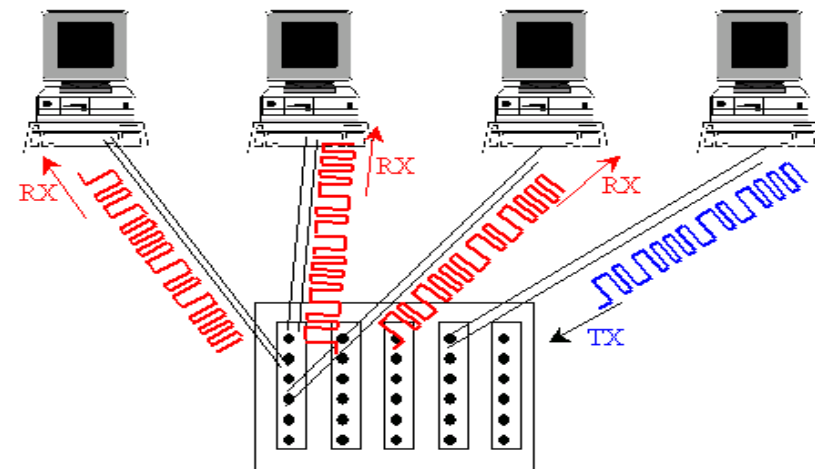
- ▶ **Topologie Physique d'un réseau** = manière dont les équipements sont reliés entre eux par le support physique de communication.
- ▶ Le choix du support influence le choix de la topologie, dans la mesure où certaines normes sont incompatibles avec certaines architectures. Ex. : Ethernet \Rightarrow Bus, Token Ring \Rightarrow Anneau
- ▶ Les trois topologies de réseaux locaux sont l'étoile, le bus et l'anneau.
- ▶ La topologie d'un réseau détermine la difficulté de maintenance par l'administrateur :
- ▶ Rajout d'une station, Existence d'un point critique, Détection des pannes, Nombre de câbles...
- ▶ **Topologie Logique** : manière dont se font les échanges de données

Exemple : Architecture physique d'Ethernet

- ▶ Deux types de topologie physique pour Ethernet
- ▶ Bus (obsolète)
 - ▶ Câble coaxial, connexion des stations « en parallèle »
 - ▶ Diffusion des trames par propagation bidirectionnelle



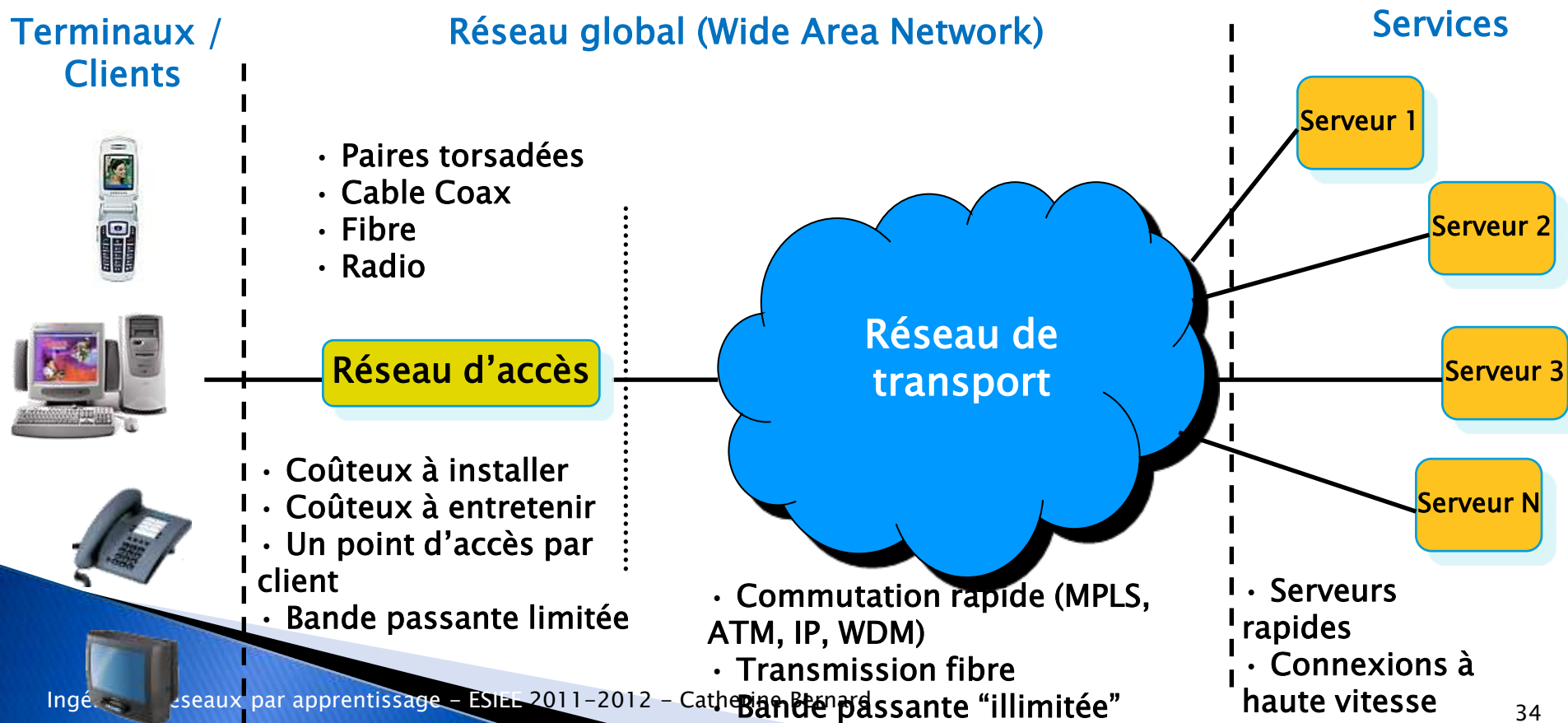
- ▶ Etoile (très courant)
 - ▶ Equipement d'interconnexion (hub, switch) avec deux paires torsadées (Tx et Rx).
 - ▶ Une trame reçue sur une ligne est diffusée sur toutes les autres
 - ▶ 😊 : souplesse d'installation
 - ▶ ☹️ : augmentation du nombre de câbles nécessaires
 - ▶ **Topologie Physique en étoile – Topologie logique en bus**



Les réseaux d'opérateurs

Réseaux d'opérateurs = réseaux qui interconnectent les réseaux privés appartenant à des sites éloignés et qui se chargent du transport des informations d'un point du réseau à un autre. **Topologie maillée.**

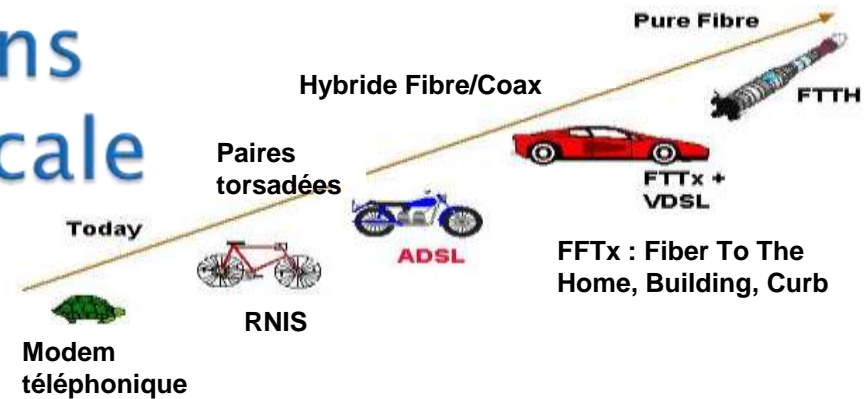
► De l'accès au cœur du réseau



RTC et Boucle Locale

- ▶ RTC (Réseau Téléphonique Commuté), PSTN (Public Switched Telephone Network)
 - Architecture hiérarchique – Commutation de circuits
 - Signalisation véhiculée dans un réseau séparé : réseau sémaphore à commutation de paquets (SS7)
- ▶ Le RNIS (Réseau Numérique à Intégration de Services) parfois appelé RNIS bande étroite (64Kbits/s à 2Mbits/s) ou NISDN pour Narrow ISDN en opposition au RNIS large bande (réseau ATM) ou B-ISDN pour Broadband ISDN.
 - Basé sur les technologies du RTC, numérisation jusqu'à l'abonné
 - Mécanismes de commutation de circuits établis pour la durée de la communication (remplacés par des liaisons DSL)
- ▶ Boucle Locale : « Ensemble des liens filaires ou radioélectriques existants entre le poste de l'abonné et le commutateur d'abonnés auquel il est rattaché »
 - En France => exclusivité historique de France Telecom
 - Nécessité d'ouvrir la boucle locale à la concurrence dans le cadre de la déréglementation => Dégroupage (effectif depuis 2002)
 - 7.7 millions de lignes totalement dégroupées (T4 2010, ARCEP)

Panorama des solutions d'accès à la boucle locale

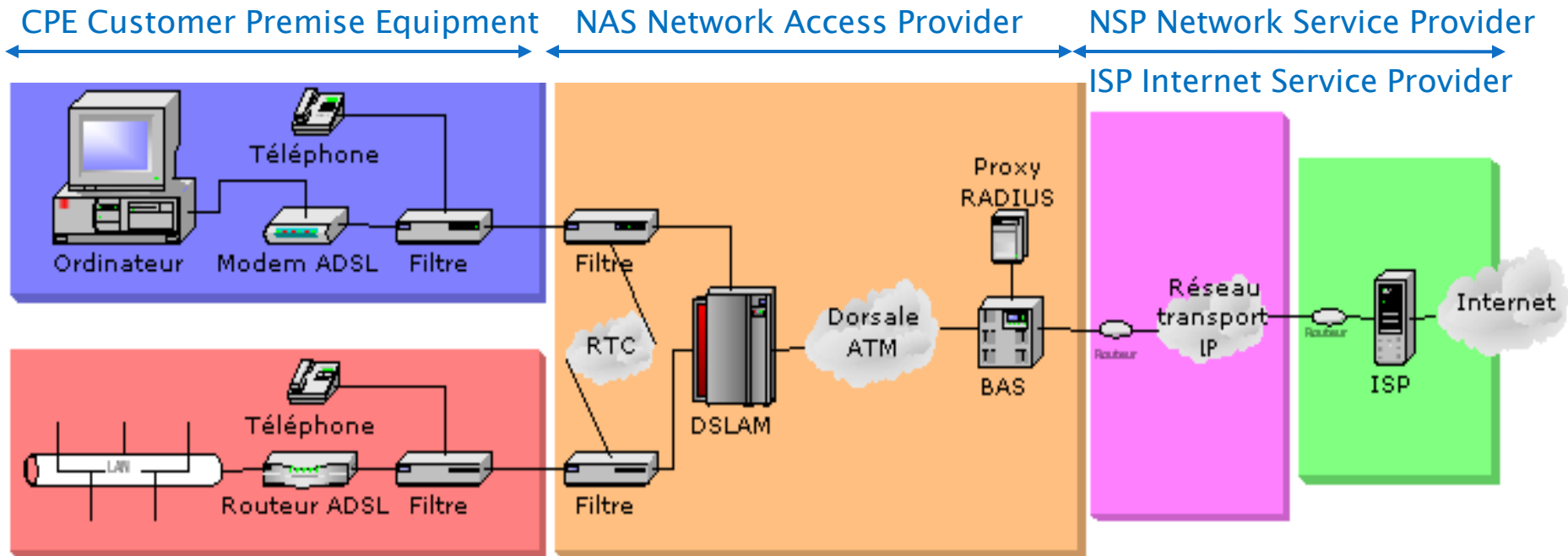


- ▶ Solutions « standards »
 - Boucle locale cuivre : ADSL
 - Les réseaux câblés HFC (Hybrid Fiber Coax)
- ▶ Les solutions optiques, FITL (Fiber In the Loop) : FTTB (Fiber To The Building), FTTH (Fiber To The Home), ...
- ▶ Solutions alternatives :
 - Sans fil : WITL (Wireless In The Loop), WiMax (IEEE 802.16)
 - Satellite
 - Courants porteurs en ligne, utilisant la partie basse tension de l'infrastructure d'un réseau de distribution d'énergie : PLC (Power Line Communication)

ADSL (Asymmetric Digital Subscriber Line)

- ▶ Ce n'est pas « un réseau » mais une méthode d'accès à Internet !
- ▶ La voix, les données informatiques haut débit, la télévision transmises simultanément en conservant le support téléphonique du RTC
 - Diversification des services : Voix sur IP, forfaits téléphoniques et ADSL illimités, diffusion audiovisuelle, visiophonie, haut débit à plus de 10 Mbit/s avec la technologie ADSL 2+
- ▶ Technologie ADSL basée sur l'utilisation de modulations évoluées (utilisation de bandes de fréquences différentes par services)
- ▶ A cause des pertes sur le câble téléphonique, les débits accessibles dépendent de la distance séparant l'abonné du central téléphonique : 1.5 Mbit/s pour 5.5 km, 51.8 Mbit/s pour 300m...
 - Pour une distance inférieure à 1.5 km, débit de l'ADSL2+ variant de 16 à 25 Mbit/s (contre 8 Mbit/s en ADSL) – Débit montant : 1 Mbit/s max.
 - Variantes : SDSL (Symetric DSL), VDSL (Very high speed DSL), ...

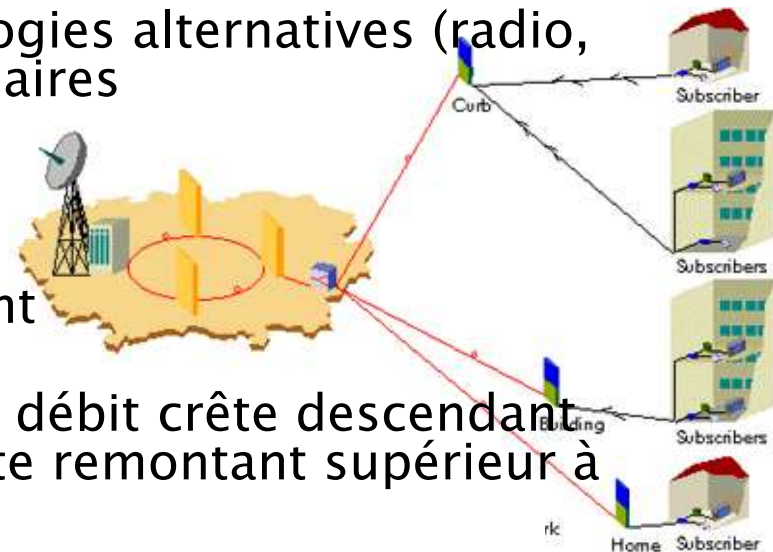
Architecture ADSL



- ▶ DSLAM (DSL Access Multiplexer) : série de modems situés en vis à vis des modems ADSL utilisateurs
 - Frontière entre la boucle locale et le réseau de transport proprement dit
 - Aiguille les basses fréquences vers le réseau téléphonique, les hautes fréquences vers le réseau de données tout en assurant le multiplexage
- ▶ Serveur RADIUS permettant l'authentification des utilisateurs (Authentication, Autorisation and Accounting)

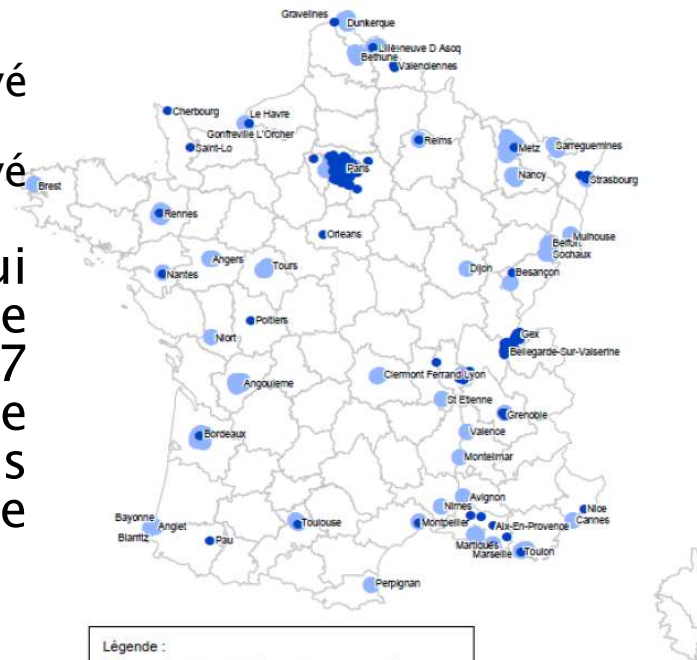
Vers des architectures FTTH

- ▶ Augmentation des besoins utilisateurs
 - Besoins des entreprises en communications symétriques en croissance régulière (de 1 à 10 puis 100 Mbit/s voir 1 Gbit/s à terme)
 - Besoins des usagers résidentiels (plusieurs canaux TV HD, téléchargements, Internet, Visiophonie...)
- ▶ Convergence des applications et des terminaux, favorisée par l'utilisation du protocole IP \Rightarrow utilisation d'un média large bande et transparent
- ▶ Technologies cuivre traditionnelles qui ont atteint leurs limites liées aux lois de la physique, technologies alternatives (radio, satellite, CPL) des solutions intermédiaires
- ▶ Vers un réseau fibre optique jusqu'à l'utilisateur assurant la pérennité
- ▶ Mais aspects économiques ralentissant son déploiement
- ▶ Offre d'accès très haut débit (avec un débit crête descendant supérieur à 50 Mbit/s et un débit crête remontant supérieur à 5 Mbit/s)



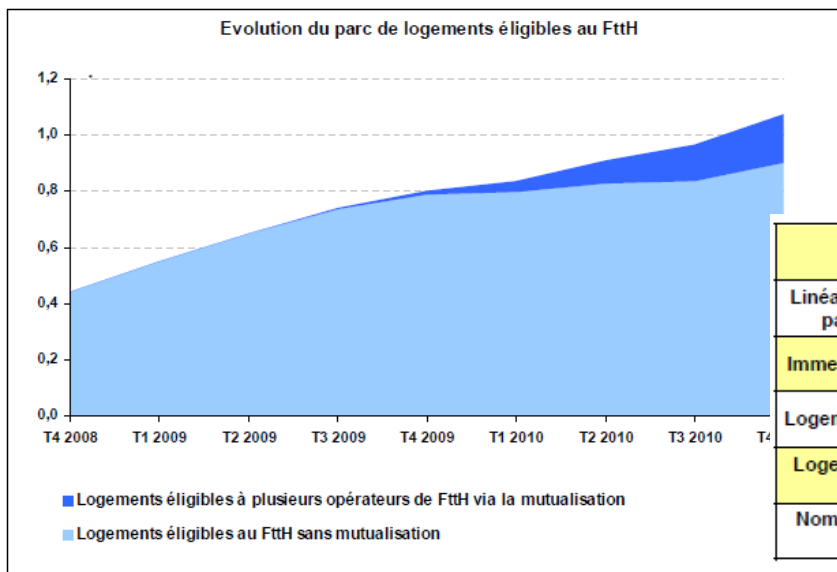
Le très haut débit en France

- ▶ Deux approches
 - FTTH : Fiber To The Home (déployé notamment par FT, SFR et Free)
 - FTTLA : Fiber To The Last Amplifier (déployé par Numericable)
- ▶ Mutualisation des infrastructures qui accélère les déploiements (décision de l'ARCEP, publiée au Journal Officiel du 17 janvier 2010, relative aux modalités de l'accès aux lignes de communications électroniques à très haut débit en fibre optique)



Légende :
 ● Agglomérations avec des réseaux FTTH en cours de déploiement
 ● Agglomérations avec des réseaux FTTLA en cours de déploiement

Source : <http://www.arcep.fr>



	31 décembre 2009	31 mars 2010	30 juin 2010	30 septembre 2010	31 décembre 2010	Évolution annuelle
Linéaire de génie civil loué par France Télécom	560	910	1 320	2 030	2 690	+ 380 %
Immeubles équipés en FttH	29 300	33 800	38 700	44 000	46 500	+ 58,7 %
Logements éligibles au FttH	800 000	840 000	910 000	967 000	1 075 000	+ 34,4 %
Logements éligibles via la mutualisation	10 000	40 000	83 000	130 000	175 000	+ 1650 %
Nombre d'abonnés via la mutualisation	350	450	850	1 800	3 300	+ 843 %

Les réseaux d'opérateurs – Cœur de réseau

- ▶ **Infrastructure optique**
 - Standards de transmission numérique PDH/SDH sur fibre optique (Plesiochronous Digital Hierarchy / Synchronous Digital Hierarchy)
 - Augmentation des débits grâce aux techniques WDM (Wavelength Division Multiplexing)
- ▶ **Les solutions Internet**
 - Evolutions d'Internet vers le haut débit et la qualité de service
 - Interconnexion sécurisée via VPN IP (Virtual Private Network)
 - Aujourd'hui forte intégration des technologies Ethernet dans le WAN : Services « Ethernet de classe opérateur » étudiés par le Metro Ethernet Forum, l'IEEE, l'IETF
- ▶ **MPLS (Multi Protocol Label Switching)**
 - Commutation de labels (Opérations de commutation et routage découplées)
 - Remplace les mécanismes de commutation de trames (Frame Relay), commutation de cellules (ATM)
- ▶ **IP : Clef de voute des interconnexions réseau**

En résumé... Concepts Réseaux

- ▶ Un réseau est constitué d'un ensemble d'ordinateurs et de périphériques interconnectés, capables d'échanger des données relativement rapidement.
- ▶ Equipements réseau : **commutateur** (switch), **routeur**,...
- ▶ Chaque nœud possède une **adresse**
- ▶ Les données qui transitent sur le réseau sont fragmentées en paquets (paquets identifiés par les adresses source et destination). Notion de commutation.
- ▶ Les différents éléments d'un réseau communiquent grâce à des **protocoles** c'est-à-dire l'ensemble des règles portant sur la constitution des adresses, des paquets, etc.
- ▶ Deux modes de fonctionnement
 - **Mode non connecté** (datagramme IP) : Vision data, Internet. Simple et économique, mais aucune garantie
 - **Mode connecté** : Vision voix, téléphonie. Réservation de ressources, établissement de connexion, mécanismes de signalisation

En résumé... Caractéristiques des Réseaux

- ▶ **Débit possible** : quel type de lien ??
- ▶ **Bande passante**
 - Partagée ou dédiée
 - Partagée : garantie ou pas ??
- ▶ Temps écoulé entre l'envoi et la réception d'un message, **temps de latence**, temps de transit. On le désire minimum et/ou constant. Dépend de
 - la distance : temps de propagation
 - la rapidité des éléments actifs sur le chemin
 - la charge (file d'attente)
- ▶ Variation du temps de latence : jitter ou **gigue**
- ▶ **Taux de pertes ou d'erreurs**
 - Dépendant de la qualité du média de transmission
 - Débordement des buffers
 - Attention au découpage/assemblage qui peut augmenter le taux d'erreurs
- ▶ **Contrôle de flux** (Régulation du trafic) – Contrôle de congestion
- ▶ Débit utile
- ▶ Capacité à différencier les trafics (notion de **priorité**)

Synthèse

- ▶ Exemple : Architecture du réseau Internet
 - source : http://www.navigators.com/internet_architecture.html)



PC utilisateur multimédia
(image, son, vidéo,
données - Internet...)

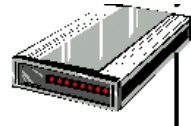
A domicile



En entreprise



Ethernet



Modem ADSL,
câble, fibre...



LAN



Services
utilisateur:
DNS, Email...

Equipements réseau :
hub, switch, routeur

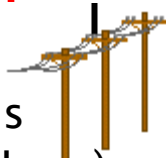
Equipements de
communication
utilisateur

Sécurité
(firewall)



Boucle locale

RTC (liaisons
louées, xDSL, ...)



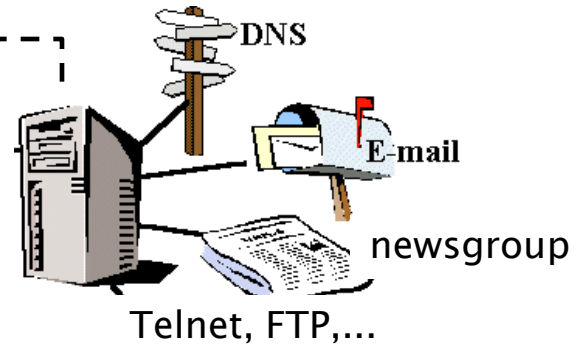
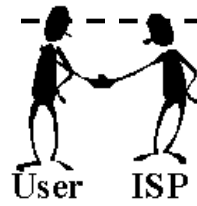
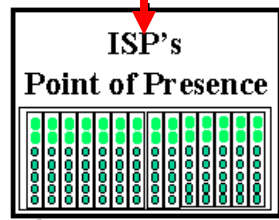
Cable



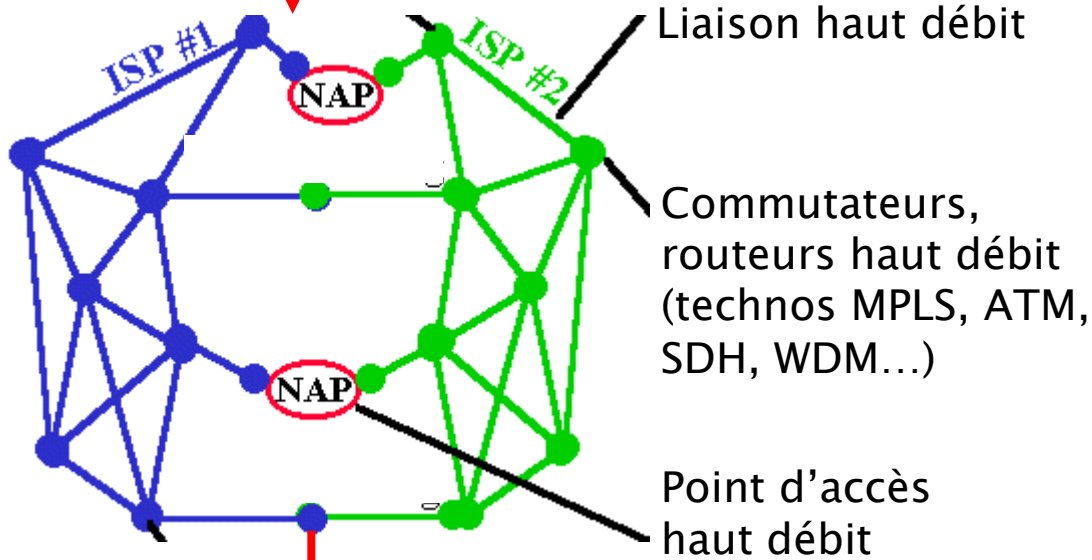
Réseaux
radios

Vers ISP (Internet Service Provider)

Point de présence
du fournisseur
d'accès Internet



Backbone
Internet



Sites Internet

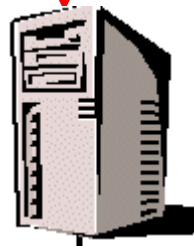


Plate-forme hôte
(web, audio, vidéo)

Sommaire

- ▶ Introduction
- ▶ Concepts réseaux
- ▶ Les réseaux d'entreprise/ Les réseaux d'opérateurs
- ▶ **Architecture logicielle des réseaux**
 - Réseaux et Normalisation
 - Concepts de base de la structuration en couches
 - Définitions : Protocoles, Primitives de services, Unités de données
- ▶ Le modèle OSI
- ▶ Les réseaux locaux (modèle IEEE)
- ▶ Le modèle TCP/IP
- ▶ Conclusion – Glossaire – Bibliographie

Réseaux et Normalisation

- ▶ Pourquoi normaliser ?
 - Faciliter l'interconnexion et la communication entre différents utilisateurs
 - Assurer l'interopérabilité des différents équipements
- ▶ Organismes de normalisation pour les réseaux informatiques :
 - l'ISO (International Standardization Organisation)
 - l'UIT-T (Union Internationale des Télécommunications)
 - l'IEEE (Institute of Electronic and Electricity Engineers)
- ▶ Définition du **modèle OSI** proposé par l'ISO (1983)
- ▶ En pratique, **modèle TCP/IP** devenu le standard

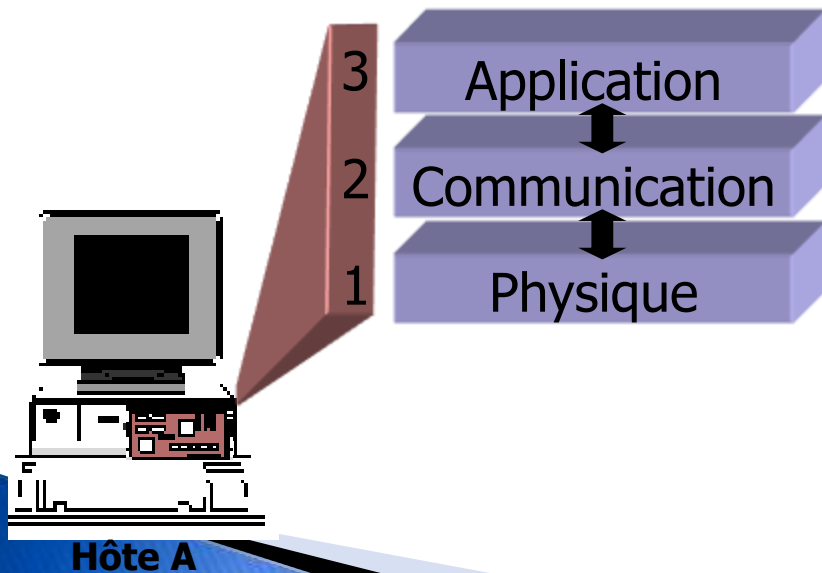


Que doit-on normaliser ??

- ▶ Les caractéristiques des réseaux touchent des domaines très divers, de la représentation physique des signaux aux protocoles de communication entre les machines.
 - Le type de support de transmission : Paires torsadées ? Fibre optique ? Liaison satellite ?
 - La représentation physique des signaux (niveaux de tension, modulation, débit...)
 - L'établissement de la liaison entre les équipements : ouverture préalable de connexion ou envoi direct des données ?
 - Route entre les machines pré-établie (commutation) ou non (routage) ?
 - Mode fiable ou non (=acquittements/retransmission ou non) ?
 - Adressage : Format ? Fonctions ? (différents types d'adresse : unicast, multicast ou broadcast)
 - Codage des bits ? Etc. ...
- ▶ Pour structurer la normalisation, définition d'un **modèle en couches**

Concepts de base de la structuration en couches

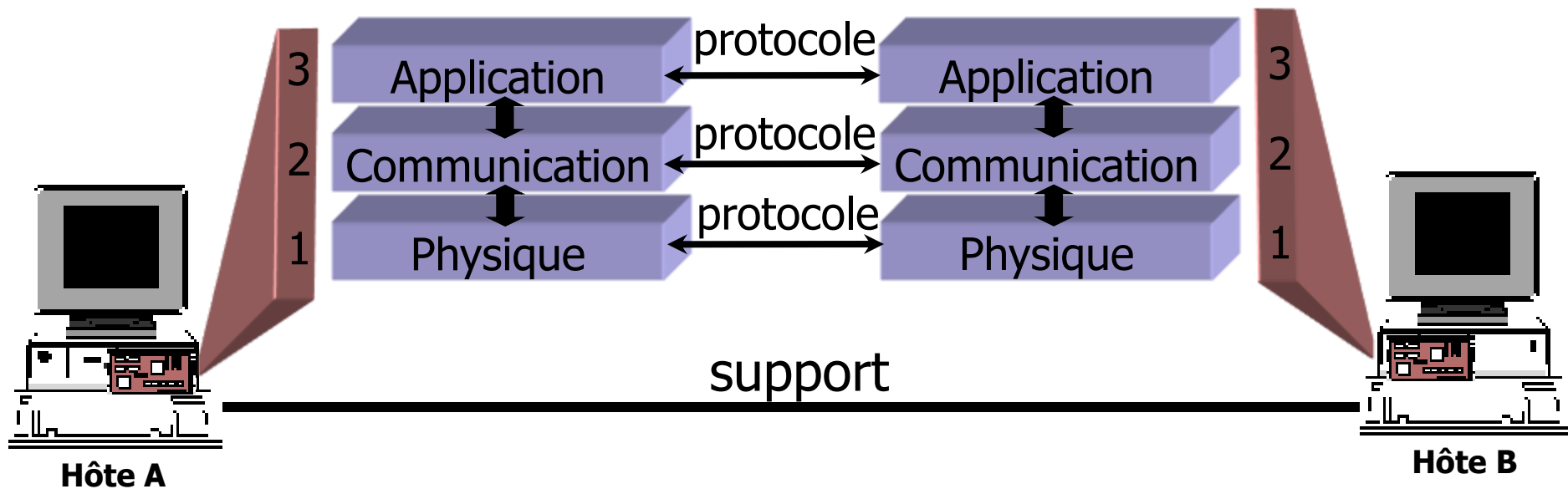
- ▶ Idée : regrouper dans une même « couche » (layer) toutes les fonctions touchant à un même domaine.
 - Ex. : une couche pour les aspects physiques du signal, une couche pour l'aspect « ouverture de la connexion », une couche pour l'aspect « fiabilité de la communication », etc
 - Exemple simplifié, purement théorique



- Application : transfert de fichier, mail, web, etc
- Communication : ouverture/fermeture de connexion ? mode fiable ?
- Physique : support utilisé, niveaux de tension, débit

Concepts de base de la structuration en couches

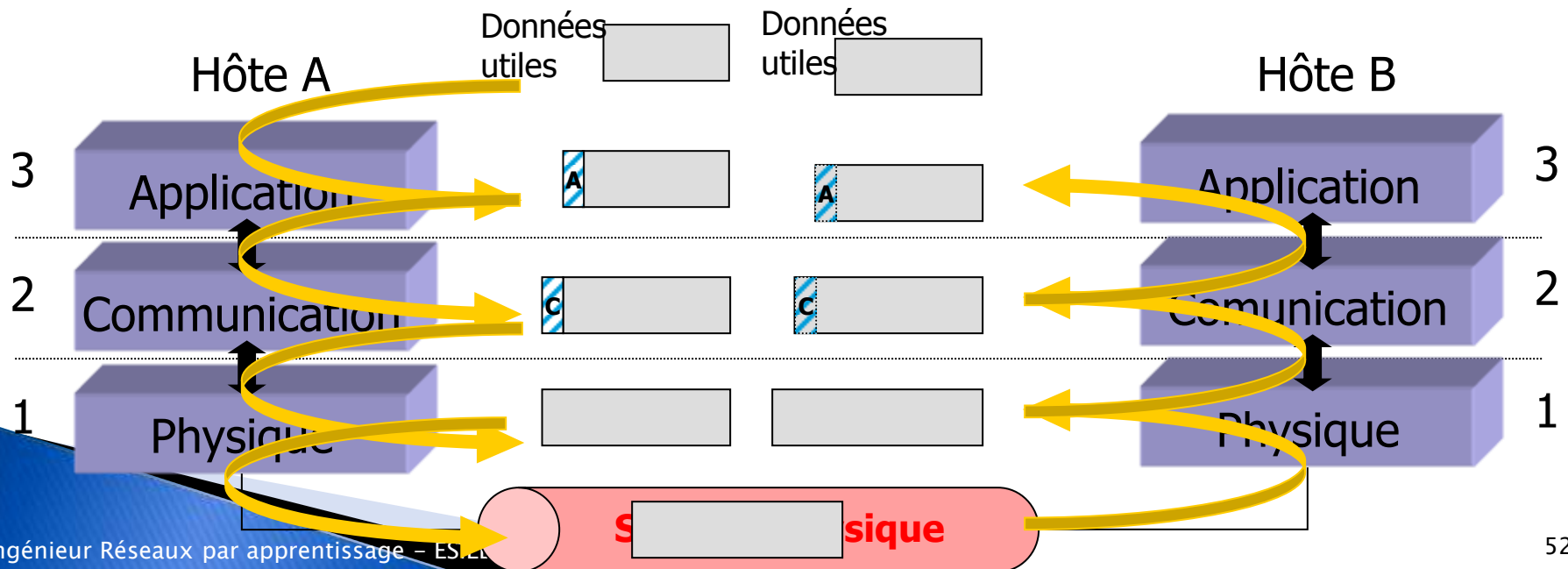
- ▶ Pour pouvoir communiquer, les deux machines doivent avoir la **même architecture en couches**



- ▶ Les couches de même niveau de chaque machine correspondent entre elles suivant un protocole.
 - Physique : câble paires torsadées, niveaux $\pm 15V$, 100Mbit/s
 - Communication : protocole spécifiant le mode connecté et fiable
 - Application : protocole d'échange de données sur le web, HTTP

Concepts de base de la structuration en couches

- ▶ A l'émission, **encapsulation** : chaque couche rajoute aux données de la couche supérieure des bits de contrôle dans une entête ou un suffixe
 - Ils sont utilisés par la couche distante de même niveau pour le traitement du paquet **suivant le protocole**
 - Les couches inférieures ignorent le contenu de l'entête
- ▶ A la réception, **désencapsulation** : les entêtes sont enlevées progressivement par chaque couche.
 - Ex. d'entête : adresse, bits de détection d'erreur, n° de paquet, etc. ...



Concepts de base de la structuration en couches

- ▶ Comment définit-on un modèle en couches ?
 - Chaque couche assure un ensemble de fonctions spécifiques.
 - Le choix des frontières entre chaque couche doit limiter le flux de données échangées.
 - Le nombre de couches doit être suffisant pour éviter de faire cohabiter dans une même couche des fonctions trop différentes.
 - Chaque couche utilise les services de la couche immédiatement inférieure pour rendre à son tour un service à la couche immédiatement supérieure.
 - Chaque couche est constituée d'éléments matériels et logiciels.

Concepts de base de la structuration en couches

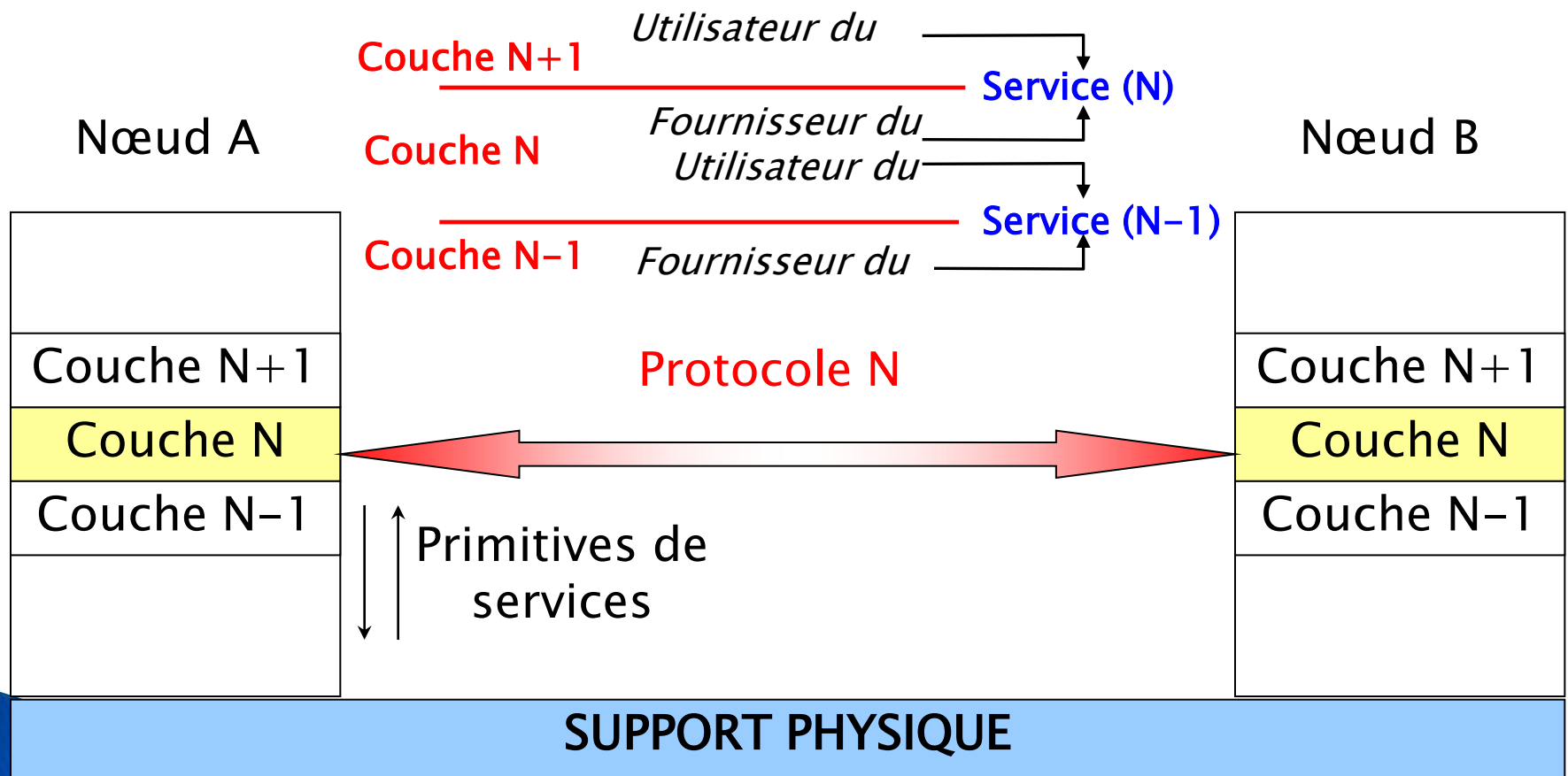
- ▶ Fonctionnalités des couches :
 - mécanismes d'identification des émetteurs et récepteurs
 - conception qui doit prendre en compte les règles de transfert de données
 - contrôle d'erreurs
 - possibilité de remettre les paquets dans le bon ordre
 - contrôle de flux
 - mécanismes de désassemblage, transmission et réassemblage
 - possibilité de multiplexage
 - choix d'une route quand il existe plusieurs chemins

Concepts de base de la structuration en couches

- ▶ Réseaux organisés en couches pour réduire la complexité, chacune des couches étant construite sur la précédente.
- ▶ Définition d'une couche : Une couche permet de définir des niveaux de compatibilité entre réseaux. La source et le destinataire doivent impérativement implémenter les mêmes couches pour communiquer.
 - Demandes de services des couches hautes vers les couches basses
 - Etablissements des services des couches basses vers les couches hautes
 - Service de niveau N : service qui doit être rendu au niveau N pour la couche N+1
- ▶ Les couches de même niveau des deux machines communiquent suivant un protocole qui définit toutes les règles de communication
 - Protocole de niveau N, ensemble de règles de communication pour le niveau N

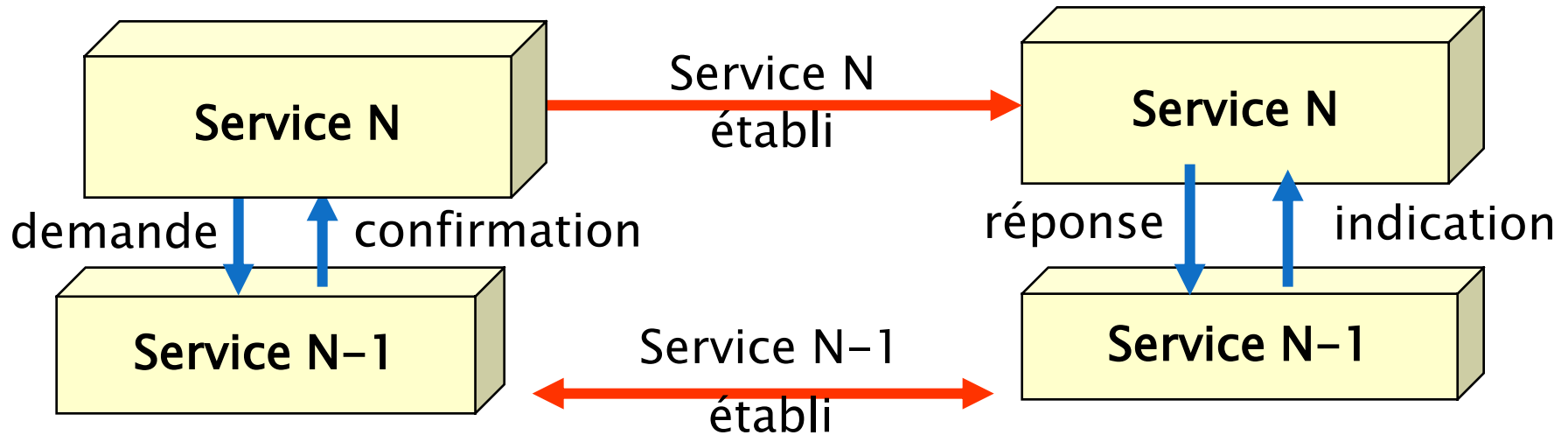
Concepts de base de la structuration en couches

► Modèle de services en couches



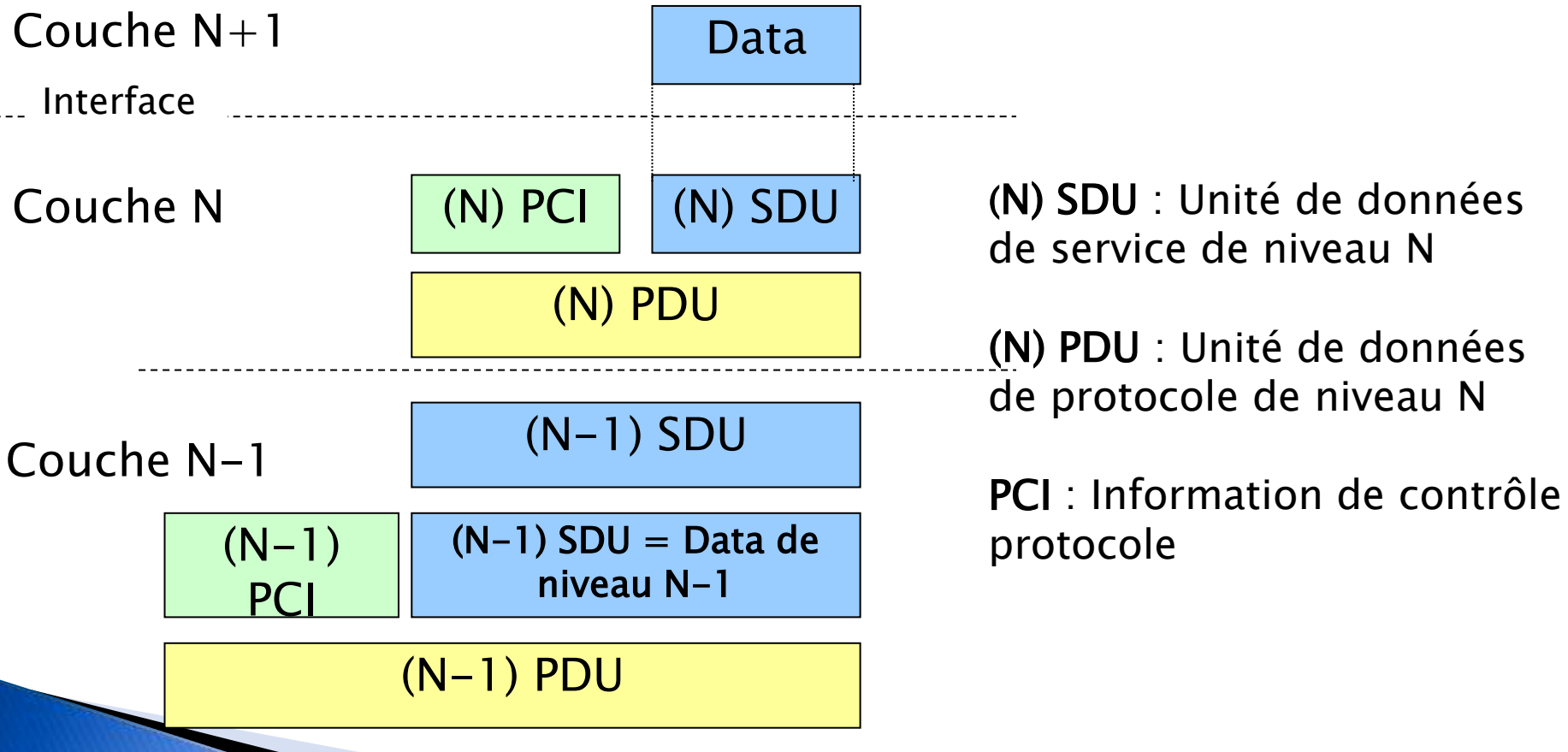
Concepts de base de la structuration en couches

- ▶ Les primitives de services :
 - Services offerts par la couche (N) invoqués par la couche (N+1) à l'aide de primitives de service (échanges verticaux dans le modèle OSI)
 - En mode connecté, 4 primitives de services utilisées pour offrir un service



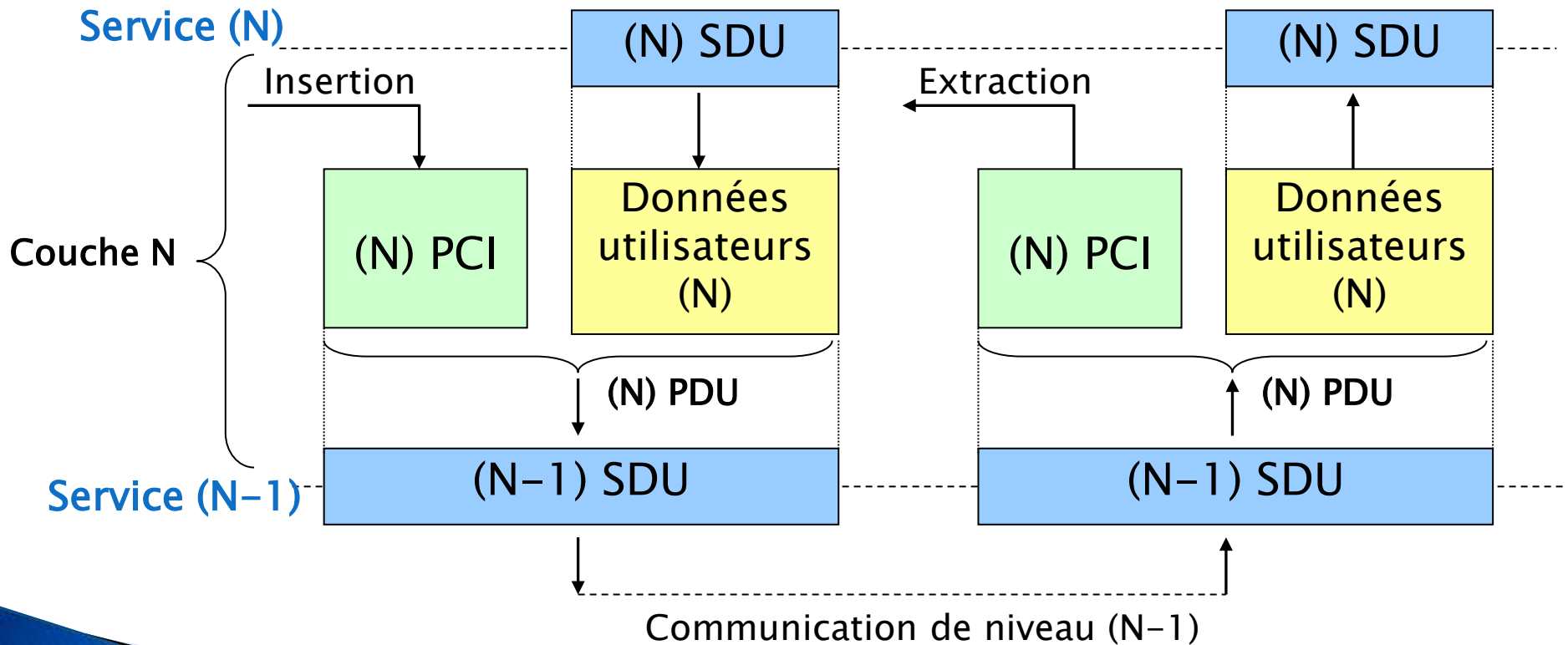
Concepts de base de la structuration en couches

▸ Les unités de données



Concepts de base de la structuration en couches

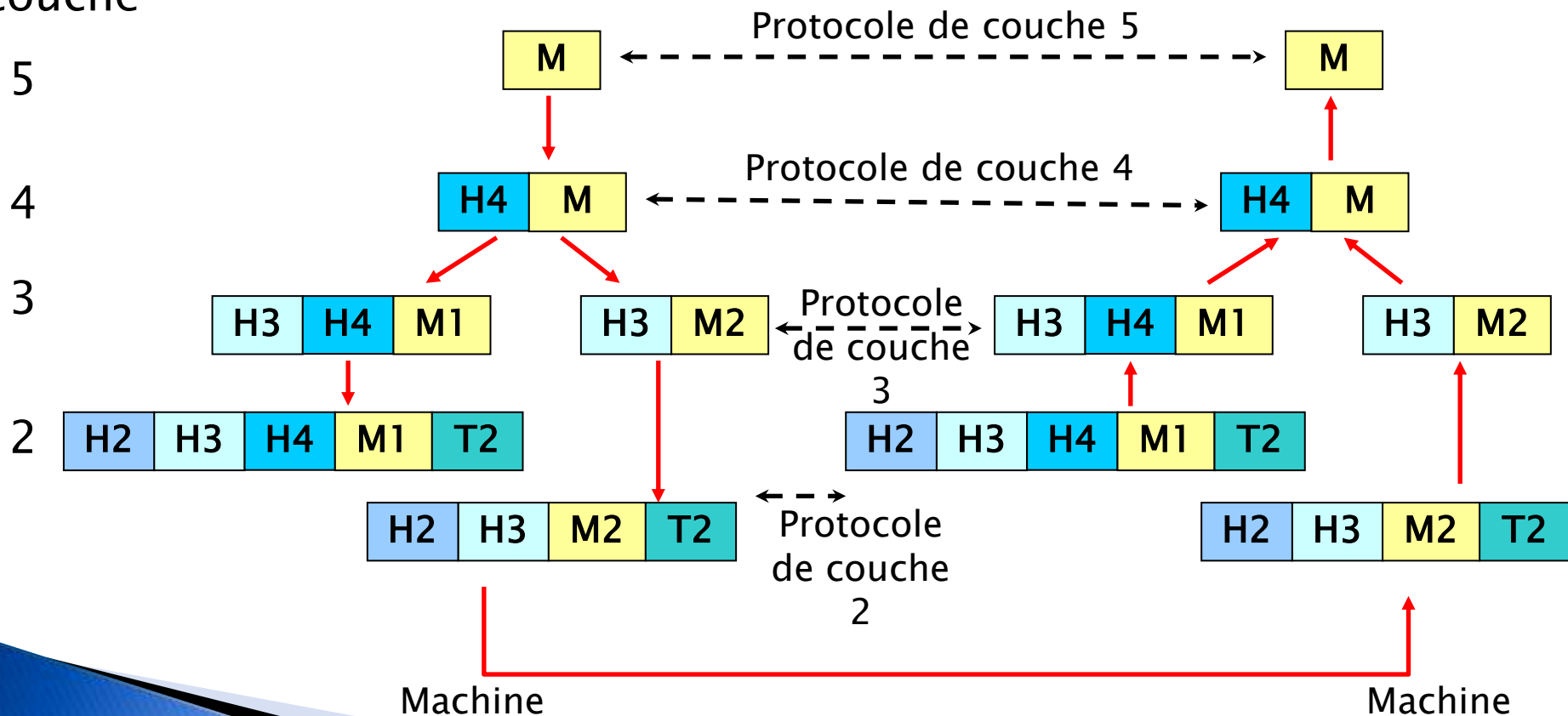
- ▶ Les unités de données : mécanismes d'encapsulation



Concepts de base de la structuration en couches

- ▶ Exemple : Flot d'informations supportant une communication virtuelle de niveau 5

couche



En résumé

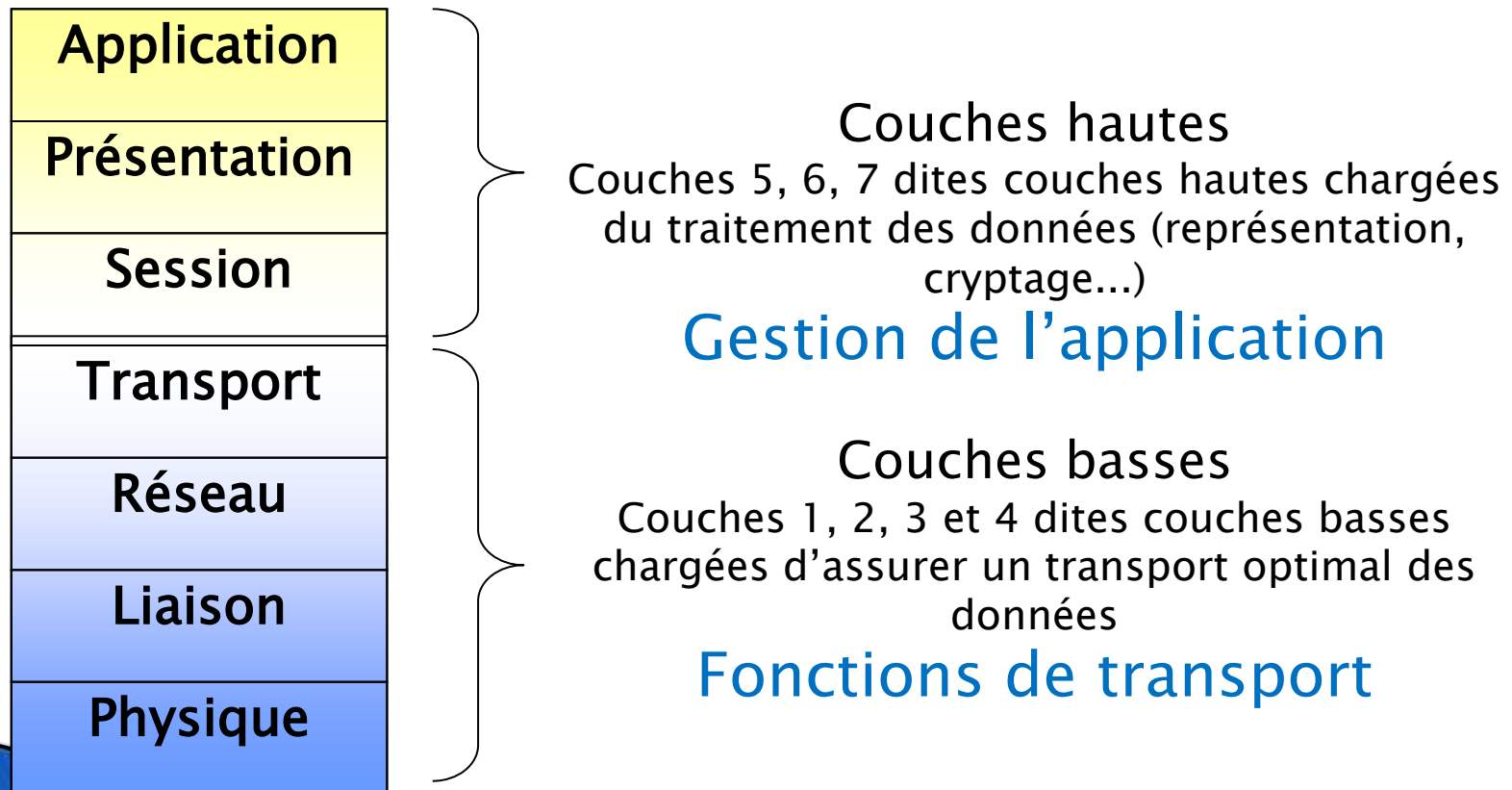
- ▶ Les protocoles normalisent l'échange des informations entre deux couches de même niveau.
- ▶ Une couche demande un service à la couche qui lui est inférieure.
- ▶ L'établissement d'un service est effectué d'une couche vers la couche qui lui est supérieure.
- ▶ Une fois le service rendu, deux couches de même niveau appartenant à deux systèmes différents échangent des informations selon un **protocole**, comme si les couches qui leur sont inférieures étaient transparentes.
- ▶ Entre deux couches adjacentes se trouve l'interface qui définit les opérations et les services que la couche inférieure offre à la couche supérieure.
- ▶ **Architecture d'un réseau** = ensemble des couches et des protocoles qui le constitue

Sommaire

- ▶ Introduction
- ▶ Concepts réseaux
- ▶ Les réseaux d'entreprise/ Les réseaux d'opérateurs
- ▶ Architecture logicielle des réseaux
- ▶ Le modèle OSI
 - Architecture du modèle OSI
 - Définition des sept couches du modèle OSI
 - Le modèle OSI et les systèmes d'interconnexion
 - Limites et critiques du modèle OSI
- ▶ Les réseaux locaux (modèle IEEE)
- ▶ Le modèle TCP/IP
- ▶ Conclusion – Glossaire – Bibliographie

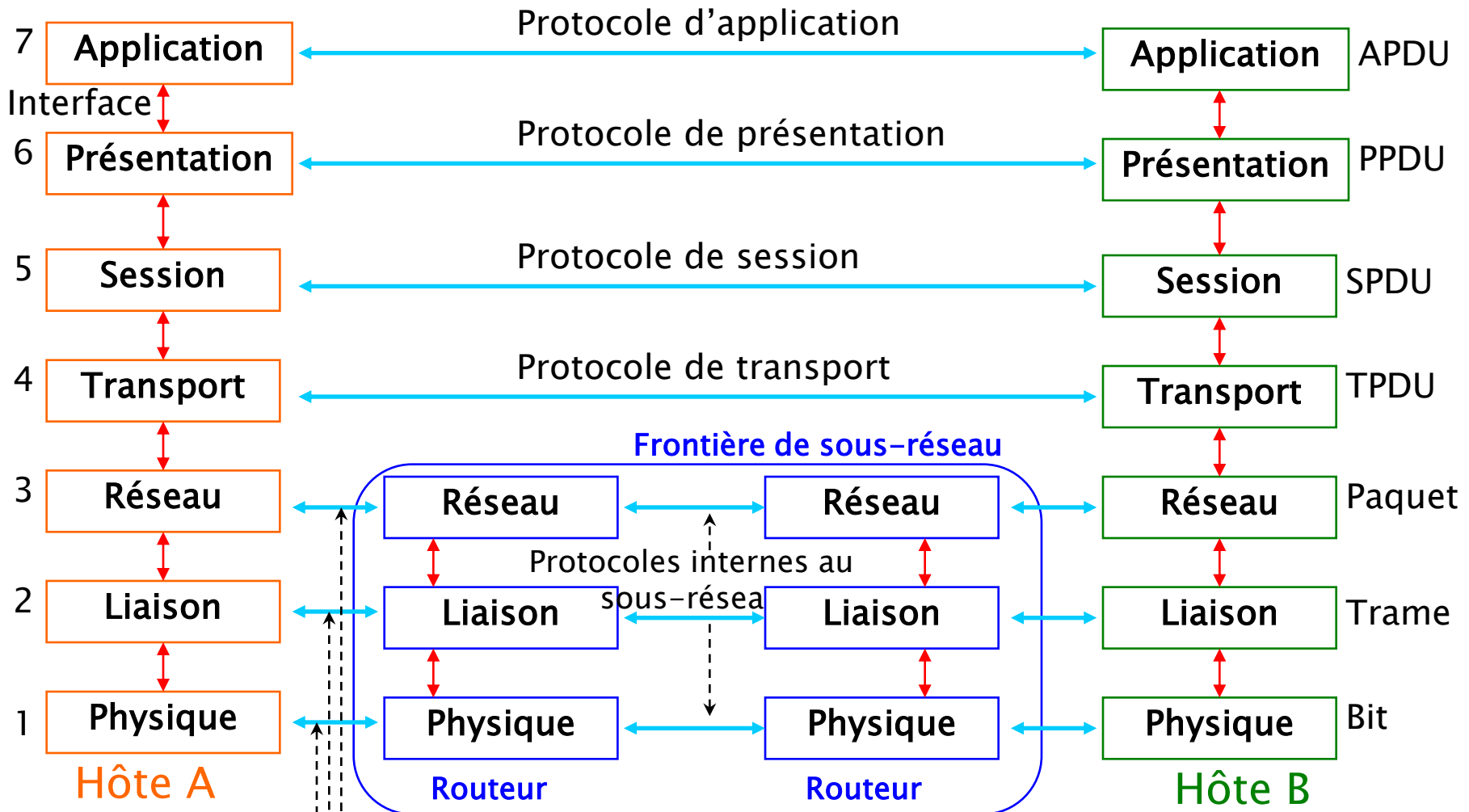
Le Modèle OSI

- ▶ Le modèle de référence OSI (Open Systems Interconnection) a été proposé par l'ISO dans les années 1980 dans le but de tendre vers une normalisation des différents protocoles de communication.



Le modèle de référence OSI

Couches



- Protocole de couche 3 entre l'hôte et le routeur
- Protocole de couche 2 entre l'hôte et le routeur
- Protocole de couche 1 entre l'hôte et le routeur

Le Modèle OSI

▶ Couche Physique

- Transfert des données sur le canal physique
- Définition des supports et moyens d'y accéder

▶ Couche Liaison de données

- Transfert de blocs de données (trames) en assurant le contrôle, l'établissement, le maintien et la libération du lien logique entre les entités
- Détection et correction d'erreur. Adressage physique

▶ Couche Réseau

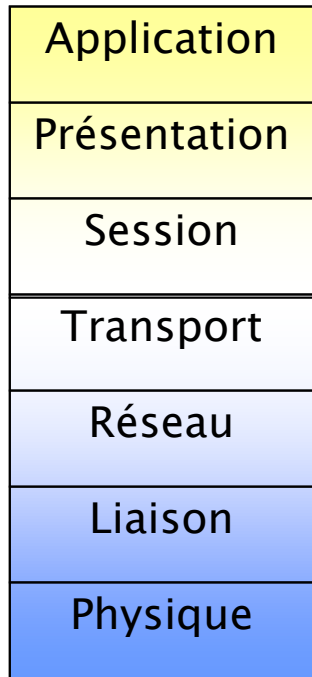
- Responsable de l'adressage, de la traduction des adresses en noms logiques. Définit le routage des paquets
- Gère les problèmes de trafic, commutation de paquets, encombrement

▶ Couche Transport

- Assure le contrôle de bout en bout des informations (messages).
- Assure aux couches supérieures un transfert fiable quelque soit le sous-réseau de transport utilisé.

Application
Présentation
Session
Transport
Réseau
Liaison
Physique

Le Modèle OSI



▶ Couche Session

- Gère l'échange de données entre applications distantes.
- Synchronise les échanges et autorise les points de reprise.

▶ Couche Présentation

- Transforme les données dans un format reconnu par les applications.
- Responsable de la conversion des protocoles, l'encodage des données et la compression.

▶ Couche Application

- Gère l'accès des applications (transfert de fichier, courrier électronique...) au service du réseau.

Couche Physique

Application
Présentation
Session
Transport
Réseau
Liaison
Physique

- ▶ La couche Physique
 - Transmission des bits sur un circuit de communication
 - Mode de représentation des données (bits) ou codage
 - Spécifications mécaniques et électriques (ou optiques)
 - Synchronisation
 - Éléments de la couche physique
 - support physique
 - codeur, modulateur
 - multiplexeur, concentrateur, répéteur

Couche Liaison de données

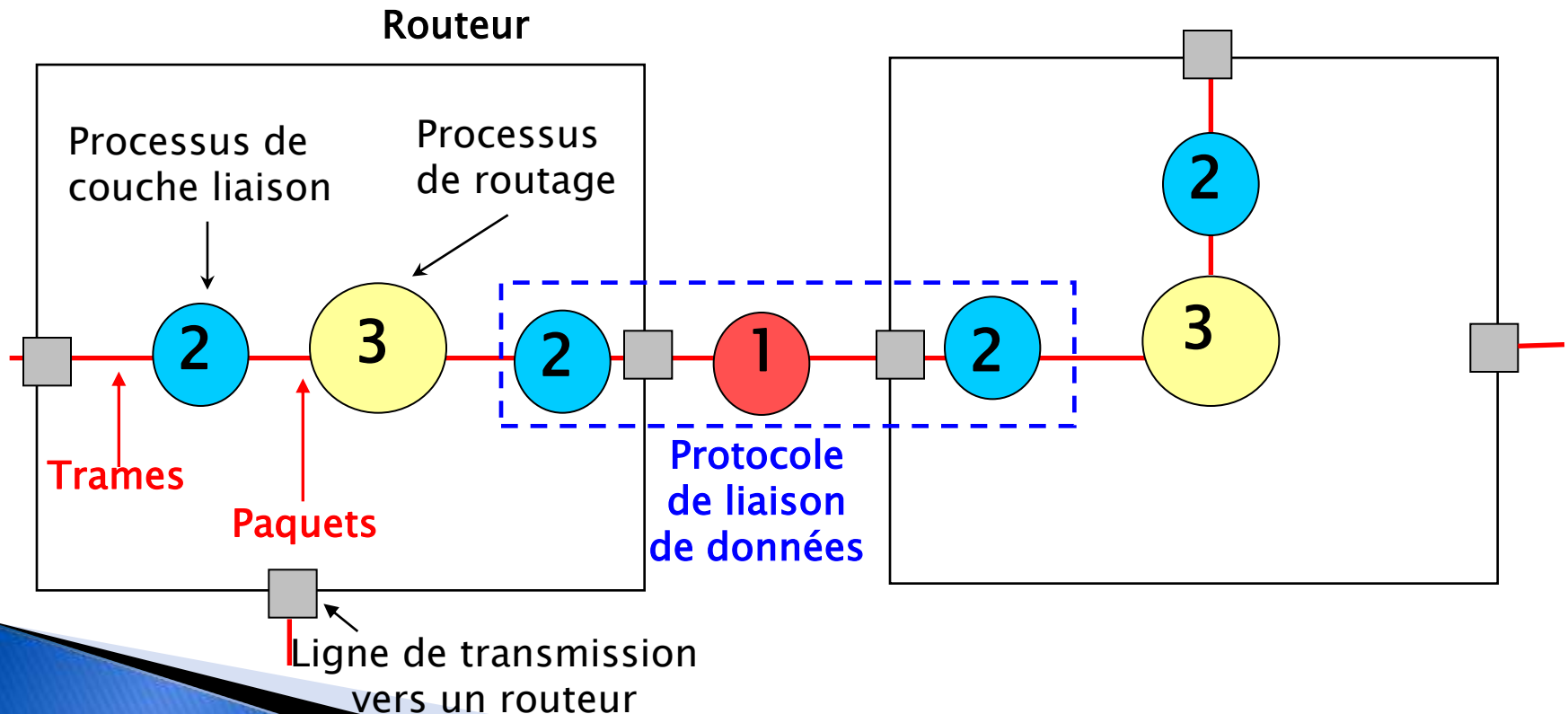
► La couche Liaison de données

- Création de la trame
- Permet d'établir et de libérer les connexions sur les liaisons physiques, gérer l'attribution de la connexion physique
- Détection, Correction et reprise sur erreur
- (régulation du trafic, gestion des erreurs)
- Gestion des adresses physiques
- Gestion de la liaison de données
 - données de l'émetteur en trames de données
 - transmission des trames en séquences
 - gestion des trames d'acquittement
 - reconnaissance des frontières de trames envoyées par la couche physique
- Procédures de transmission (HDLC, LLC, BSC...)



Couche Liaison de données

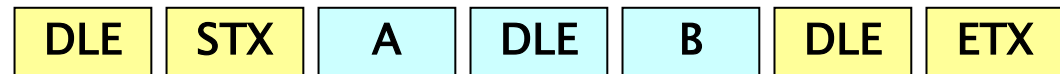
- ▶ Positionnement du protocole liaison de données
 - Rôle de la couche liaison de données (qui apparaît dans le rectangle en pointillés) : donner l'illusion au logiciel de routage que la liaison même peu fiable est parfaite ou en tout cas correcte. Propriété importante pour les liaisons sans fil peu fiables.



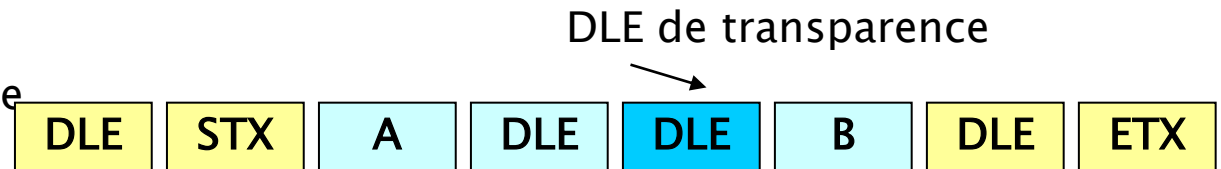
Couche Liaison de données

- ▶ Méthodes de découpage des trains de bits en trame
 - compter les caractères
 - avoir des caractères de début de trame, de fin de trame et de transparence

Données envoyées
par la couche réseau



Ajout de caractère de
transparence par la couche
liaison de données

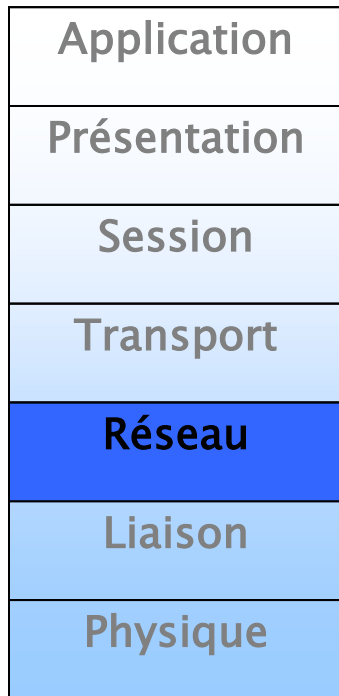


Données remises à la
couche réseau
destination



- utiliser des fanions de début et de fin de trame avec des bits de transparence
- violer le codage utilisé au niveau physique (représentation physique des 0 et 1)

Couche Réseau



▶ La couche Réseau

- Doit permettre l'interconnexion de réseaux hétérogènes, acheminement des paquets de la source vers le destinataire
- Nécessite l'adaptation du format et de la taille des données en fonction de chaque sous-réseau
 - Eventuellement conversion d'adresse
 - Adaptation de la taille des paquets de données
 - Adaptation des débits
 - Choix des modes connecté ou non connecté
- Fonctionnalités principales
 - Routage
 - Adressage logique
 - Contrôle de flux – Gestion de la congestion dans le réseau – gestion des erreurs

Couche Transport

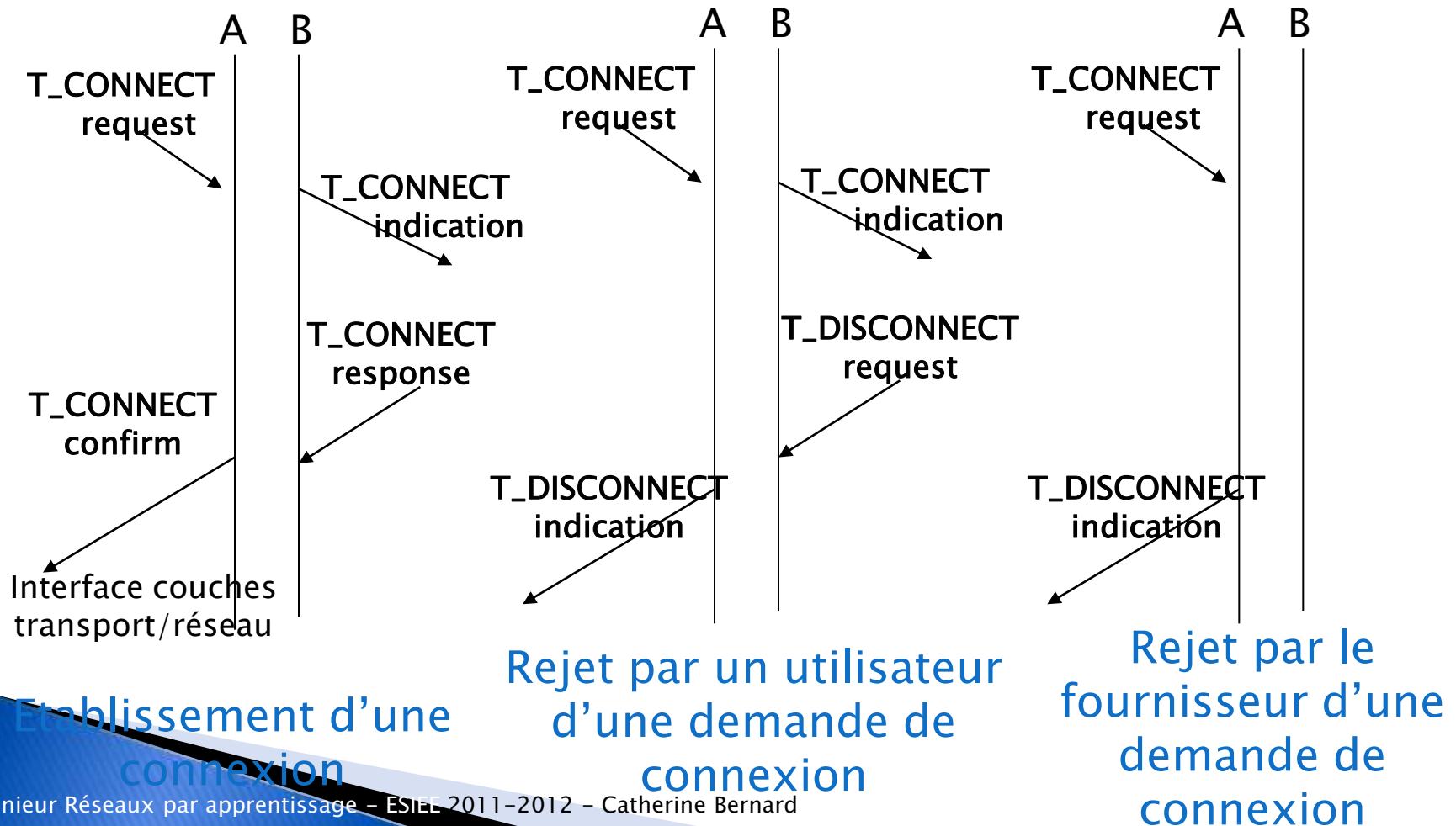
Application
Présentation
Session
Transport
Réseau
Liaison
Physique

► La couche Transport

- Indépendance des réseaux sous-jacents
 - permet de transmettre les données indépendamment de leur format, leur codage...
- Accepte les données de la couche session
 - les découpe éventuellement, s'assure de l'ordonnancement
- Optimiser les ressources réseau
- Ses fonctions sont :
 - la segmentation et le réassemblage des messages pour adapter la taille des tampons aux tampons de la couche 3
 - le contrôle de flux (de la couche 4 à la couche 3) pour éviter la saturation de la mémoire
 - la gestion des erreurs
 - le multiplexage
 - l'adressage
 - le choix du mode connecté/non connecté
- Assurer la qualité de service

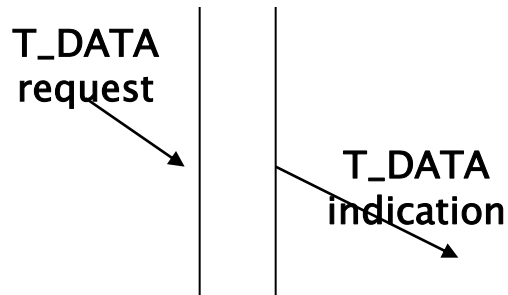
Couche Transport

- ▶ Exemple de mise en œuvre des primitives de services : enchaînements de primitives en mode connecté

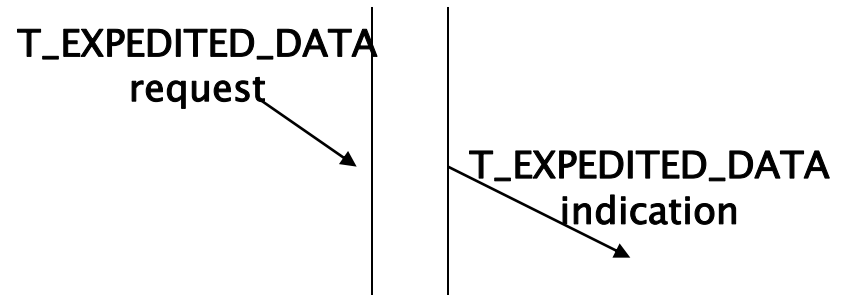


Couche Transport

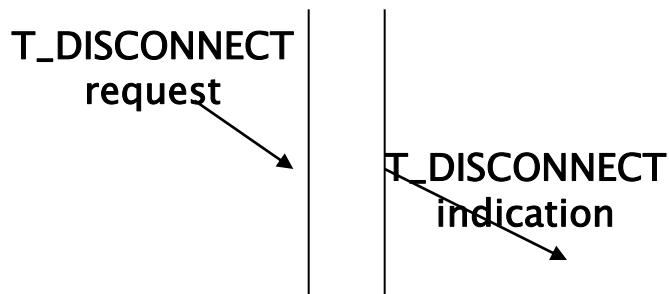
- ▶ Enchaînements de primitives en mode connecté



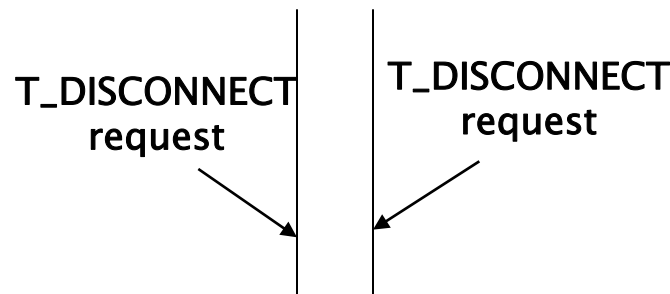
Transfert de données normales



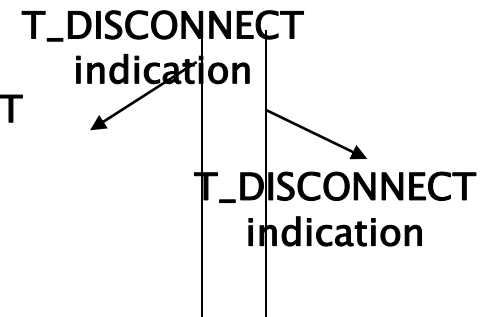
Transfert de données exprès



Libération sur initiative d'un utilisateur



Libération sur initiative des deux utilisateurs



Libération provoquée par le fournisseur

Couche Session

► La couche Session

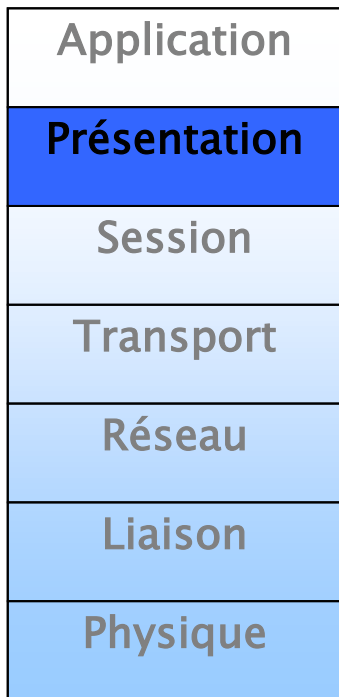
- Responsable de la synchronisation
- Utilisation de jetons de synchronisation permettant de délimiter des unités d'activité
- Fonctions de type :
 - La mise en contact de deux utilisateurs :
 - choix de la route (quelle route prendre ?)
 - négociation des paramètres de session (qui parle en premier ?)
 - contrôle des autorisations de dialogue (qui peut parler avec qui ?)
 - Gestion du dialogue (bi-uni directionnel)
 - Points de reprise
 - Retour en arrière
- Gestion des transactions



Couche Présentation

► La couche Présentation

- S'intéresse à la syntaxe et à la sémantique des informations
 - Transforme les données dans un format reconnu par les applications, conversion de code
 - Eventuellement fonctions de cryptage et compression de données
- Mise à disposition des utilisateurs d'un langage commun
 - L'ISO a défini une norme appelée ASN 1 (Abstract Syntax Notation 1, syntaxe abstraite numéro 1) permettant de définir une sorte de langage commun (syntaxe de transfert) dans laquelle toutes les applications présentent leurs données avant de les transmettre.



Couche Application

▶ La couche Application

- Offre aux processus d'application le moyen d'accéder à l'environnement OSI
- Définition d'ASE (Application Service Element), service normalisé communiquant avec l'ASE homologue distant par un protocole normalisé
- Fournit tous les services directement utilisables par l'application
 - le transfert d'informations
 - l'allocation de ressources
 - l'intégrité et la cohérence des données accédées
 - la synchronisation des applications coopérant

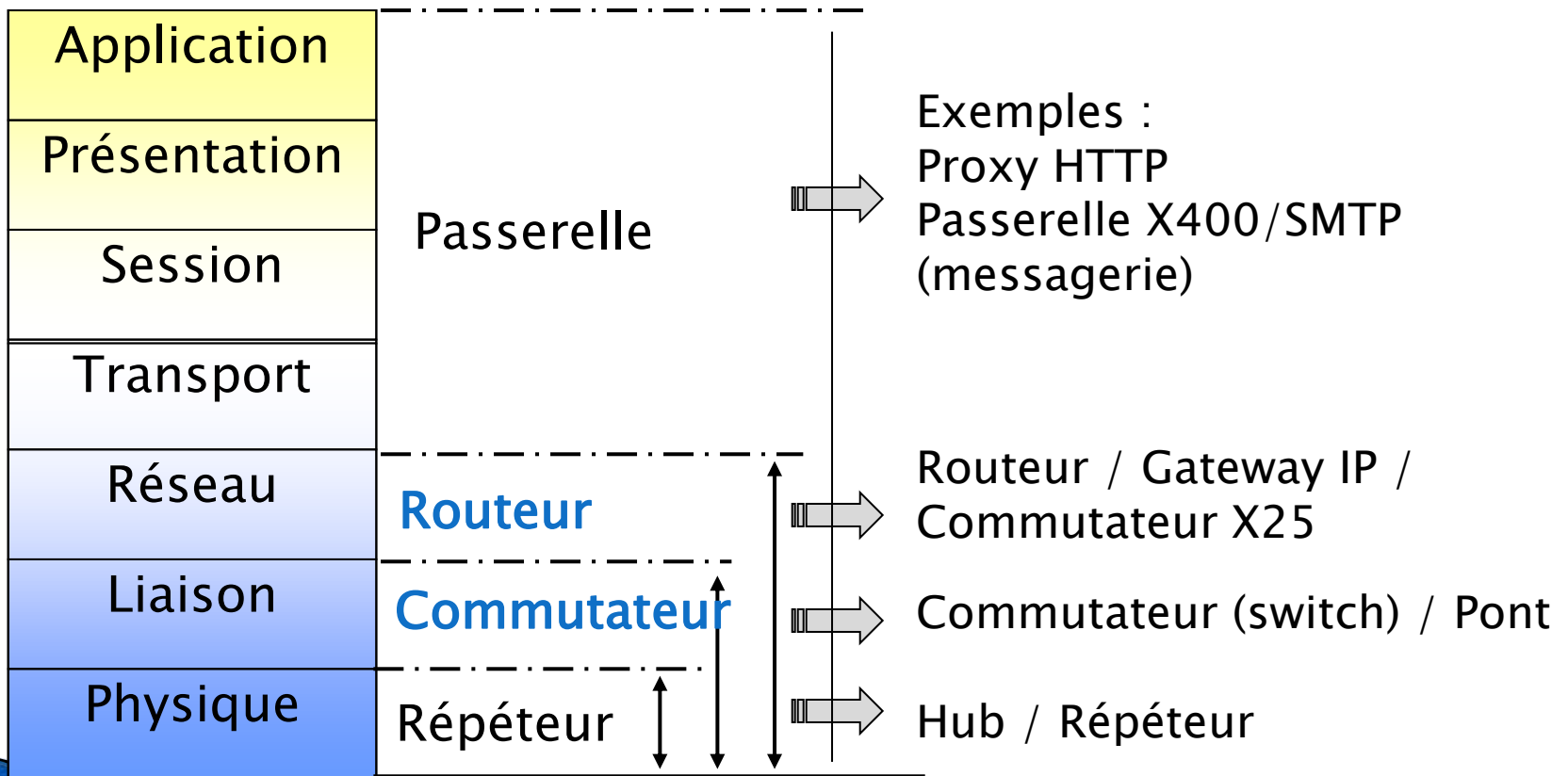
Application
Présentation
Session
Transport
Réseau
Liaison
Physique

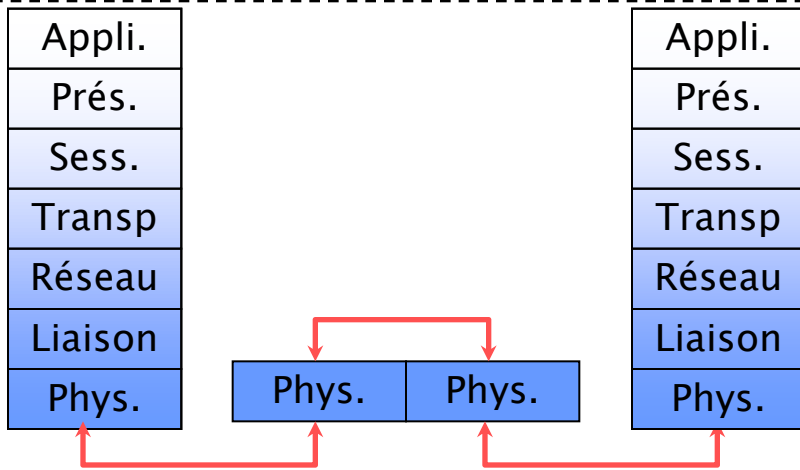
Le Modèle OSI et les systèmes d'interconnexion

- ▶ Initiatives importantes de l'ISO dans le domaine de l'interconnexion
 - Définition des fonctionnalités des équipements couches basses
 - Classification utile des diverses opérations de chaque système d'interconnexion
- ▶ Deux techniques pour construire une interconnexion réseau
 - Concaténation de réseau, mise bout à bout de segments de réseau
 - Techniques d'encapsulation
- ▶ Niveau d'interconnexion défini par la couche commune permettant de relier les différents réseaux (la couche IP joue souvent ce rôle)

Le Modèle OSI et les systèmes d'interconnexion

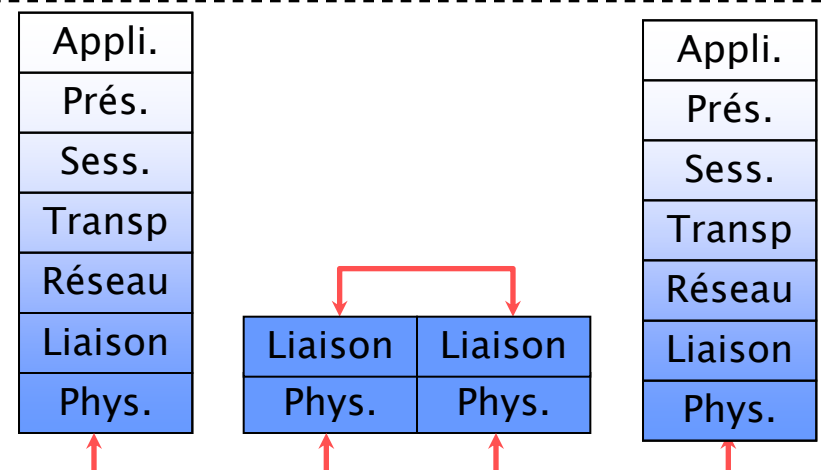
- ▶ Les équipements d'interconnexion et le modèle OSI





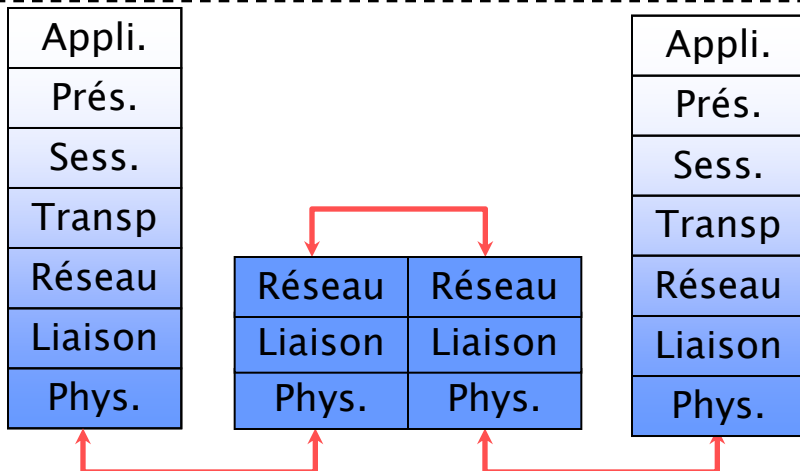
Répéteur ou Hub

- Amplification du signal pour augmenter la taille du réseau éventuellement conversion
- Répétition du signal vers N ports



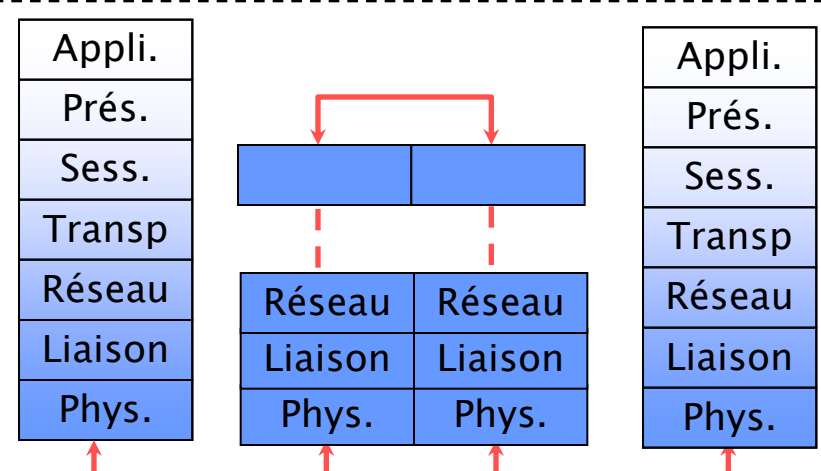
Commutateur (Switch) – Pont (*Bridge*)

Conversion de format des trames (couche 2) – @niveau 2 (@MAC)



Routeur (*Router* ou *Gateway IP*)

- Conversion de format des paquets et @niveau 3 (@IP) – **Routage** des paquets



Passerelle ("*Gateway*")

- Conversion de format de messages d'une des couches supérieures (4 à 7)

Critiques du modèle OSI

- ▶ Le modèle OSI ne s'est jamais réellement imposé car à l'époque de son élaboration, le modèle TCP/IP était déjà implanté.
- ▶ Modèle OSI doit servir de modèle de référence...
- ▶ Parmi les 7 couches proposées, plusieurs ne sont pas vraiment utiles ni utilisées.
 - Exemple : couches session et présentation presque vides
- ▶ Il existe une certaine redondance entre les couches.
 - Exemple : Le contrôle de flux et le contrôle d'erreurs sont réalisés dans les couches 2, 3 et 4.

Sommaire

- ▶ Introduction
- ▶ Concepts réseaux
- ▶ Les réseaux d'entreprise/ Les réseaux d'opérateurs
- ▶ Architecture logicielle des réseaux
- ▶ Le modèle OSI
- ▶ **Les réseaux locaux (modèle IEEE)**
 - Architecture des Réseaux Locaux
 - Le protocole CSMA/CD
 - Les adresses MAC
 - Format des trames IEEE802.3/Ethernet
 - Les équipements d'interconnexion du LAN
 - Le WiFi
- ▶ L'architecture TCP/IP
- ▶ Conclusion – Glossaire – Bibliographie

Architecture des Réseaux Locaux

- ▶ Objectif : développer un standard permettant la transmission de trames d'information entre deux systèmes informatiques de conception courante, à travers un **support partagé** entre ces systèmes, ceci quelque soit l'architecture.

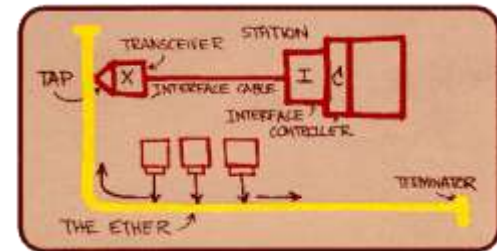
A pour origine le protocole Aloha développé pour interconnecter les îles Hawaï...

⇒ CSMA/CD ⇒ **Ethernet... Norme 802.3**



Plan de Metcafe du futur réseau Ethernet

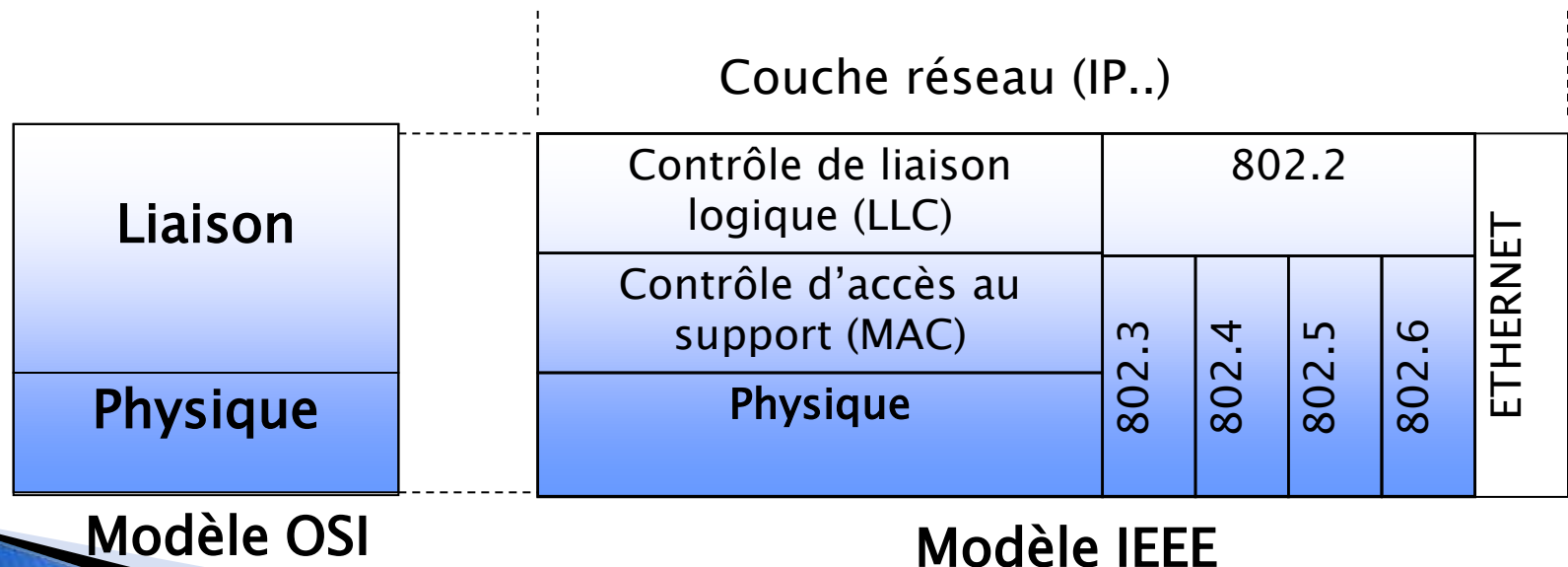
Configuration originale : réseau en bus sur câble coaxial à 10 Mbit/s.



- ▶ Réseau local le plus répandu (proposé initialement par Xerox, Digital et Intel et normalisé ensuite par l'IEEE et ISO)

L'architecture IEEE

- ▶ Correspond à la normalisation des couches 1 & 2 du modèle OSI
- ▶ Architecture IEEE divisant la couche 2 en deux sous-couches
 - Sous-couche MAC (Medium Access Control)
 - Rôle : assurer le partage du support entre tous les utilisateurs
 - Gestion des adresses physiques (adresses MAC)
 - Sous-couche LLC (Logical Link Control)
 - Rôle : gestion des communications, liaisons logiques, entre stations
 - Interface avec les couches supérieures



Architecture physique d'Ethernet

- ▶ Par ordre chronologique d'apparition
 - 10BASE5 : 10Mbit/s en bande de base (sur câble coaxial épais) avec des segments de 500m maximum
 - 10BASE2 : 10Mbit/s en bande de base (sur câble coaxial fin) avec des segments de 200m maximum (185m en réalité)
 - 10BASE-T : 10Mbit/s en bande de base sur câble à paires torsadées
 - 10BASEF : 10Mbit/s en bande de base sur fibre optique
 - 100BASE-TX : 100Mbit/s en bande de base, sur câble à paires torsadées (RX et TX)
 - 100BASE-FX : 100Mbit/s en bande de base sur fibre optique
 - 1000BASE... pour le Gigabit Ethernet. Quatre standards basés sur l'utilisation des câbles à paires torsadées ou fibre
 - 10GBase... : spécifications du 10 Gigabit/s (standard ratifié en juin 2002)
 - Extension de l'utilisation de la technologie Ethernet dans le MAN, WAN
 - Ethernet en route vers les 100 Gbit/s
 - Objectif du groupe de travail High Speed Study Group (HSSG) de l'IEEE formé en juillet 2006. Norme IEEE802.3ba désignée pour les spécifications à 100Gbit/s en décembre 2007

Le protocole CSMA/CD

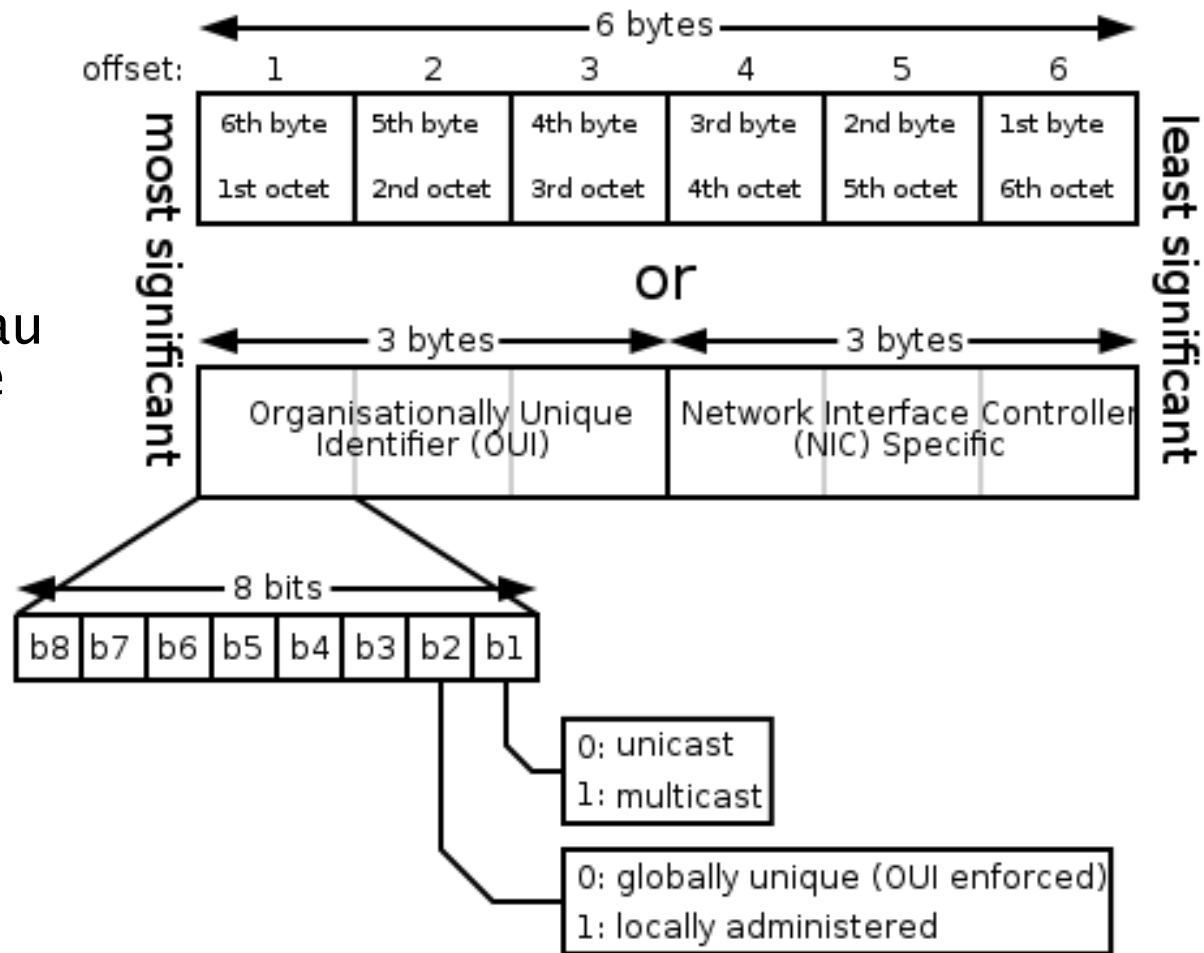
- ▶ Protocole CSMA/CD (Carrier Sense Multiple Access with Collision Detection) : Accès multiple par écoute de la porteuse et détection des collisions) : très utilisé dans les réseaux locaux et localisé dans la sous-couche MAC
- ▶ Méthode d'accès utilisée dans les réseaux locaux de type Ethernet pour contrôler l'accès au support physique. Repose sur la **diffusion** des trames dans le réseau.
- ▶ Principe :
 - Ecouter si le canal de transmission est libre
 - Si canal occupé, attendre
 - Si le canal de transmission est disponible commencer à transmettre
 - Si une collision se produit pendant la transmission, arrêter et attendre un moment avant de recommencer à transmettre
 - Emetteur et destinataire identifiés par leur adresse : adresse MAC

Adresse MAC

- ▶ Adresse MAC : identifie de manière unique une adresse dans le monde (adresse physique liée au matériel). Adresse régie par l'IEEE

- Adresse sur 6 octets

- ▶ Adresse Broadcast : FF:FF:FF:FF:FF:FF



Source : http://en.wikipedia.org/wiki/File:MAC-48_Address.svg

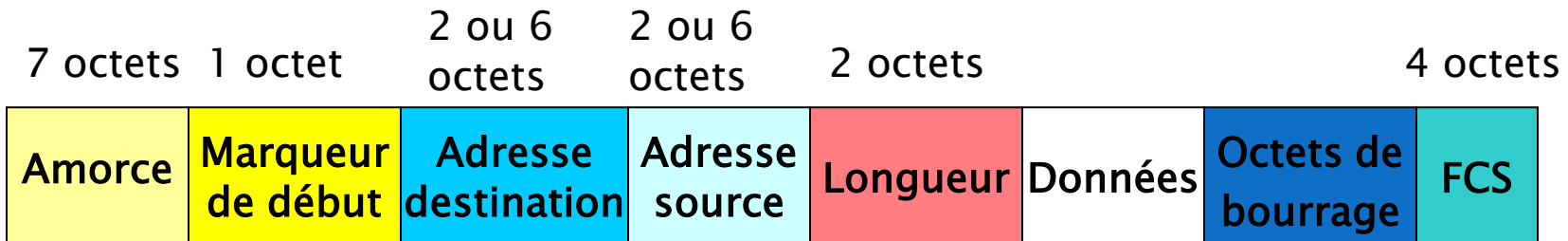
Adresse MAC / Adresse IP ???

- ▶ Attention à la confusion courante Adresse MAC/Adresse IP!!! Aucun lien entre les adresses MAC et IP.
- ▶ L'adresse MAC est le « nom de famille » de la carte réseau: elle « naît et meurt » avec !
- ▶ Comme dans la vie courante, le nom de famille ne suffit pas à localiser une personne dans le monde ; sur Internet, on attribue donc une « adresse postale » aux machines pour les localiser : l'adresse IP.
 - L'adresse IP a une structure logique qui permet de la localiser sur le réseau Internet, tout comme une adresse postale est structurée de manière à localiser le pays, la ville, la rue, la maison, l'étage, etc. ...
 - Si l'ordinateur change de réseau, son adresse IP change.
- ▶ **L'adresse IP a une portée globale** (elle localise la machine dans le monde) ; **l'adresse MAC a une portée locale** (une fois la machine localisée, on l'identifie par « son nom »).

Format des trames Ethernet/IEEE 802.3

- ▶ Sur un bus, toutes les stations voient toutes les trames ⇒ chaque trame contient @source et @destinataire
- ▶ Chaque carte Ethernet ou interface d'un équipement est identifiée par son adresse MAC
- ▶ Deux standards : trame Ethernet issue des travaux de Xerox et trame IEEE 802.3
 - Trames IEEE 802.3 : encapsulation LLC nécessaire pour rendre service à la couche réseau
 - Trame Ethernet : champ type dans la trame permettant de passer les données directement à la couche réseau
 - Format de trame le plus utilisé
 - **Longueur des trames Ethernet : 64 oct. < taille < 1518 oct.**

Format des trames IEEE 802.3



Présente en début de trame 7 octets initialisés à 10101010 (permet de synchroniser les horloges des stations réceptrices)

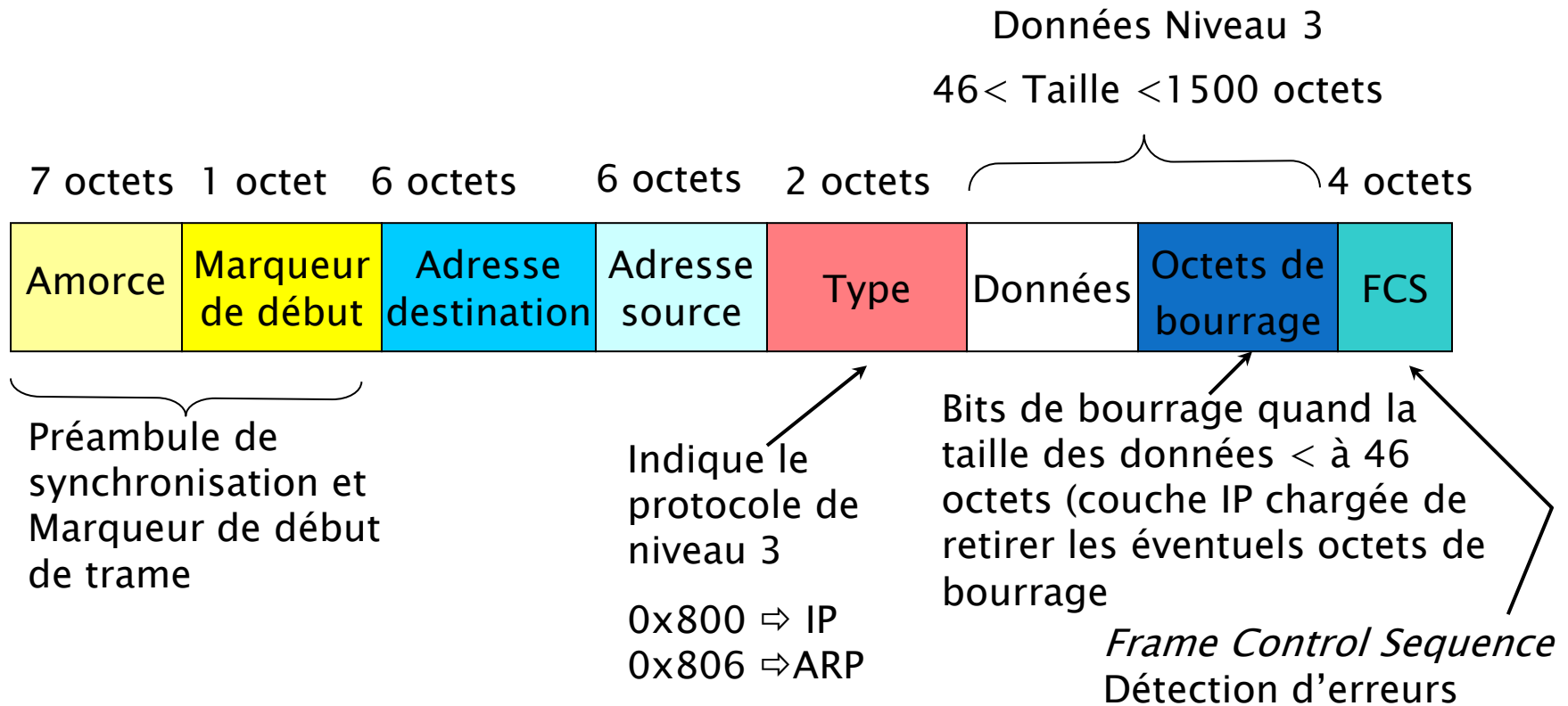
Marqueur de début de trame (*Start Frame Delimiter*) octet à la valeur 10101011 (permet la synchronisation par caractère)

2 ou 6 octets pour une @ locale ou non

Indique la longueur effective des données (entre 0 et 1500) permet de distinguer les données d'éventuels bits de bourrage

Bits de bourrage quand la taille des données < à 46 octets
Frame Control Sequence
Détection d'erreurs

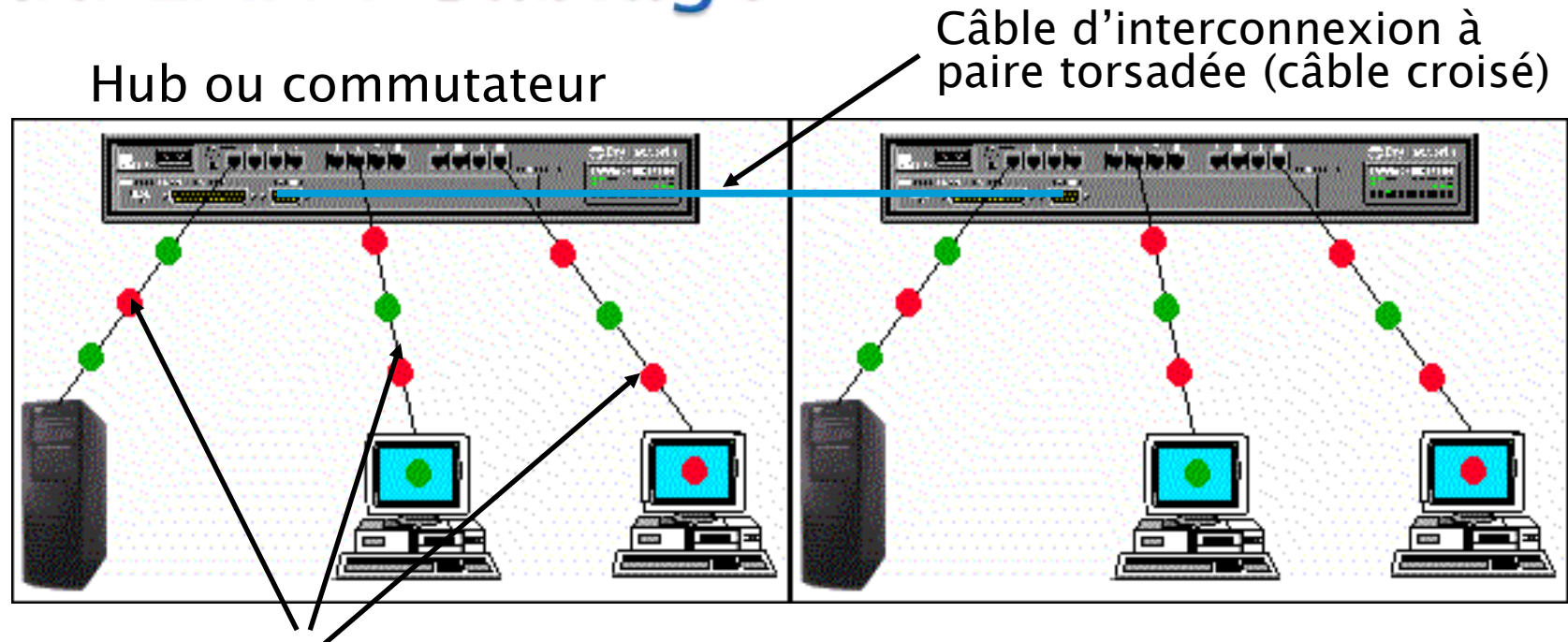
Format des trames Ethernet



Les équipements d'interconnexion du LAN

- ▶ Equipements d'interconnexion au niveau du LAN qui vont agir sur les couches 1 et 2
 - Répéteur, Hub : niveau 1
 - Pont (bridge), Commutateur (switch) : niveau 2
- ▶ Routeur : équipement de niveau 3
 - Permet l'interconnexion de LAN, interface entre le réseau local et les autres réseaux
 - Filtre et transmet des paquets entrants en se basant sur l'adresse destination du paquet (adresse IP) et sa table de routage
- ▶ **Domaine de collision** : segment de réseau dans lequel toutes les machines partagent la même bande passante (plus il y a de stations, plus il y a de collisions)
 - Equipement de niveau 2 utilisé pour séparer les domaines de collision (analyse des adresses MAC qui évite la propagation des collisions)
- ▶ **Domaine de broadcast** : ensemble des éléments du réseau recevant le trafic de diffusion
 - Equipement de niveau 3, routeur qui bloque les broadcasts

Les équipements d'interconnexion du LAN : Câblage



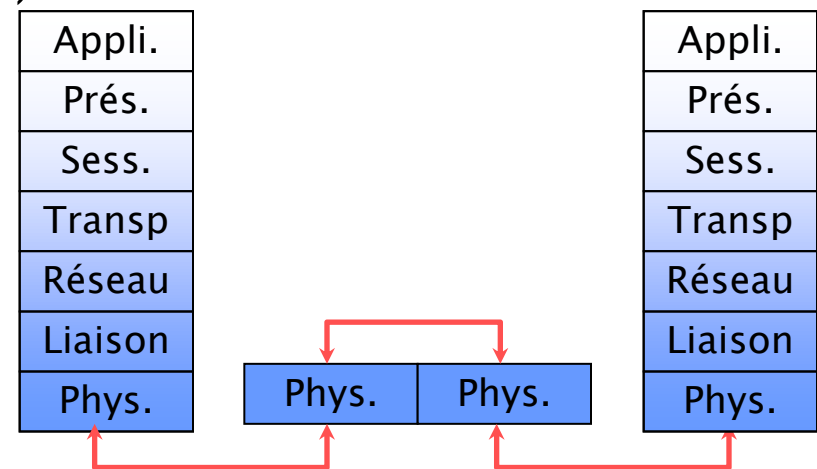
Paires torsadées :

- câble 4 paires catégorie 5 ($f_{\max} = 100$ MHz) de 100m maximum (paires 1-2, 3-6 utilisées) - Câble droit
- connecteurs RJ45

Aujourd'hui, port capable de détecter si câble droit ou torsadé (adapte alors son fonctionnement), la vitesse : port autosense

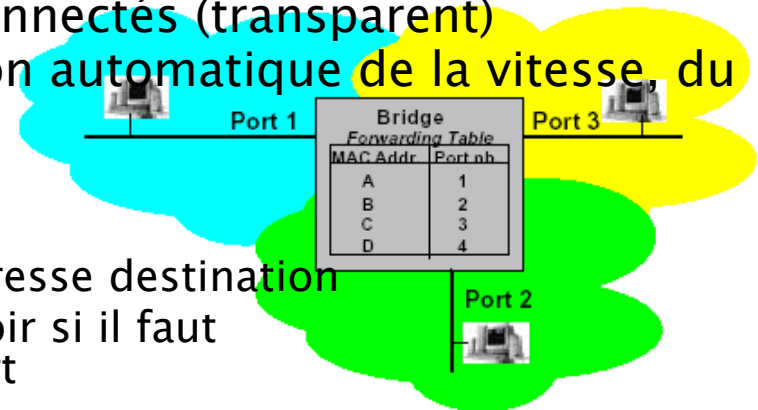
Répéteur / Hub

- ▶ Répéteur : permet d'étendre le réseau plus loin que les limitations dues au câble
- ▶ Hub : répéteur multiport
 - Pour les supports à base de paires torsadées : stations raccordées au Hub, équipement de niveau physique qui joue le rôle de diffusion du bus passif
 - Agit au niveau physique (répète les bits reçus sur un port sur tous les autres ports)
 - Limitations : un unique domaine de collisions, trafic diffusé sur tout le réseau (sécurité ???)
 - Plus utilisé



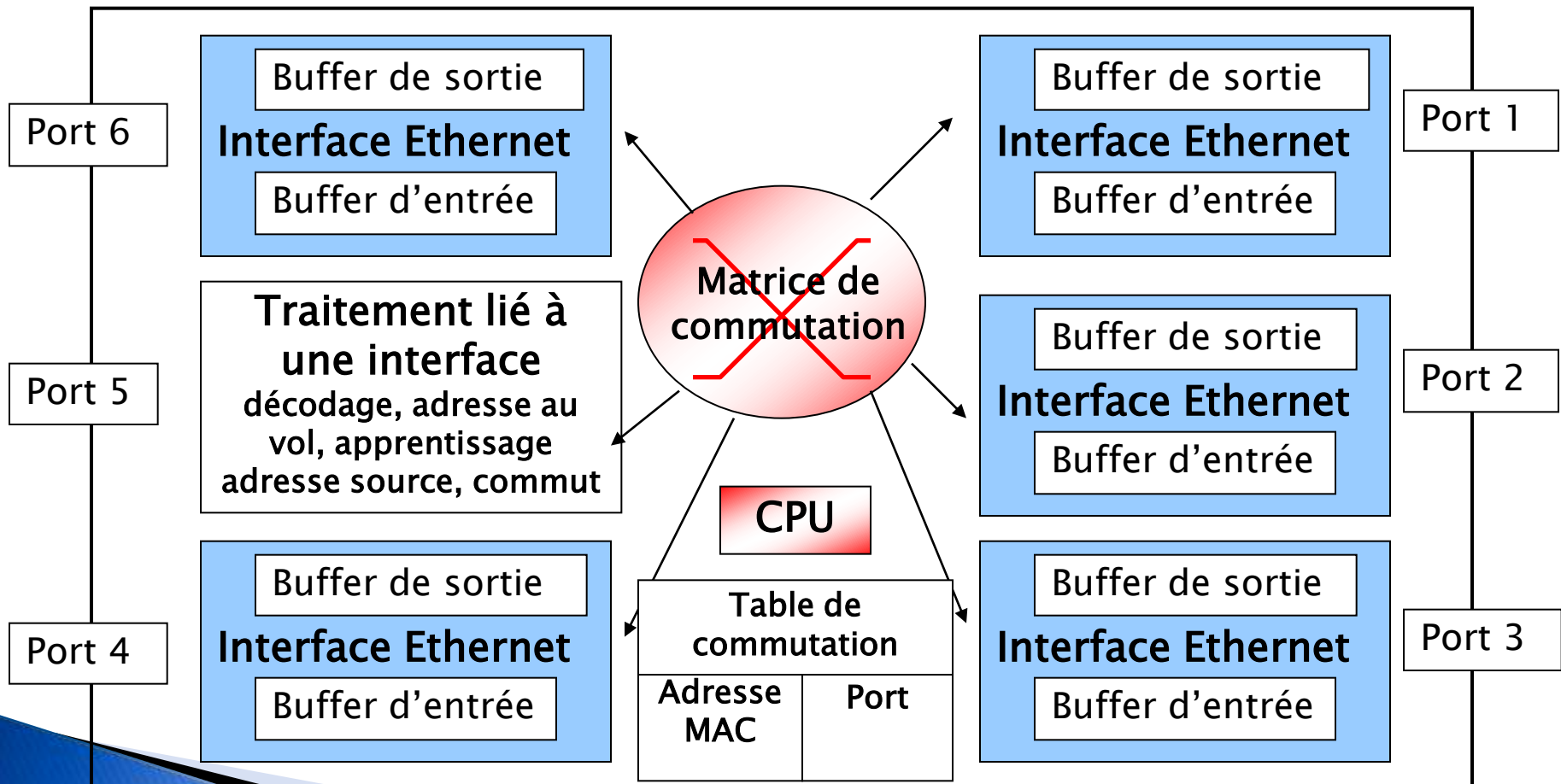
Commutateur

- ▶ Niveau 2 du modèle OSI
- ▶ Ils séparent les domaines de collisions : plusieurs trames peuvent être transmises en parallèle sur un réseau LAN commuté
- ▶ Commutateur filtrant auto-apprenant
 - Réduction des collisions en évitant grâce à des buffers que deux trames soient émises en même temps (aucune si full-duplex)
 - Aucune modification des systèmes connectés (transparent)
 - Très souvent port autosense (détection automatique de la vitesse, du mode transfert...)
 - Fonctionnement
 - reçoit les trames sur ses ports
 - à l'arrivée d'une trame, examen de l'adresse destination
 - consulter la table port/adresses pour voir si il faut retransmettre la trame sur un autre port
 - Si oui, transmettre la trame
 - Si non, trame déjà été émise sur le LAN où la destination se trouve
- ▶ Aujourd'hui équipement utilisé majoritairement dans le LAN



Interconnexion par commutateur

► Architecture interne d'un commutateur



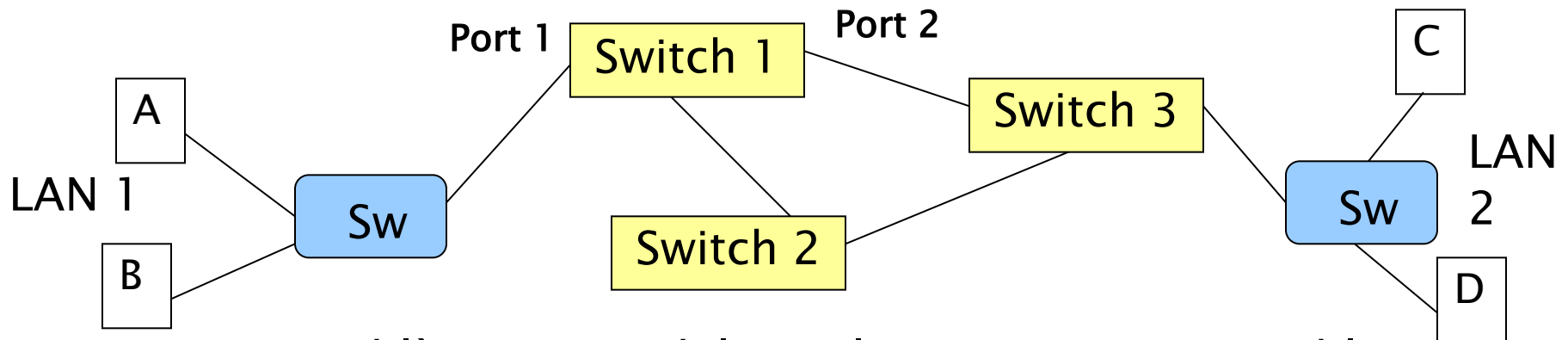
Interconnexion par commutateur

- ▶ Deux techniques de commutation :
 - **commutation à la volée** (cut through)
 - accepte la trame et commence à détecter l'adresse destination pour la transmettre directement sur le port sortant
 - pas de contrôle ⇒ peut transmettre des trames erronées
 - doit bufferiser si le port est occupé
 - **commutation store and forward**
 - accepte la trame entrante, la stocke temporairement, la vérifie, la retransmet sur le port sortant
- ▶ ☹ Problème de congestion du réseau – Pas de contrôle de flux.
- ▶ Nombreuses fonctionnalités : création de groupes selon différentes règles (VLAN, Virtual LAN), possibilité de redonder des liens (utilisation de l'algorithme de Spanning Tree)....

Problématique : Fiabilité du réseau

► Fiabilité du réseau

- Si un pont ou un hub tombe en panne, le réseau peut être coupé en deux
- Comment améliorer la tolérance aux pannes ?
 - Idée : introduire des liaisons redondantes

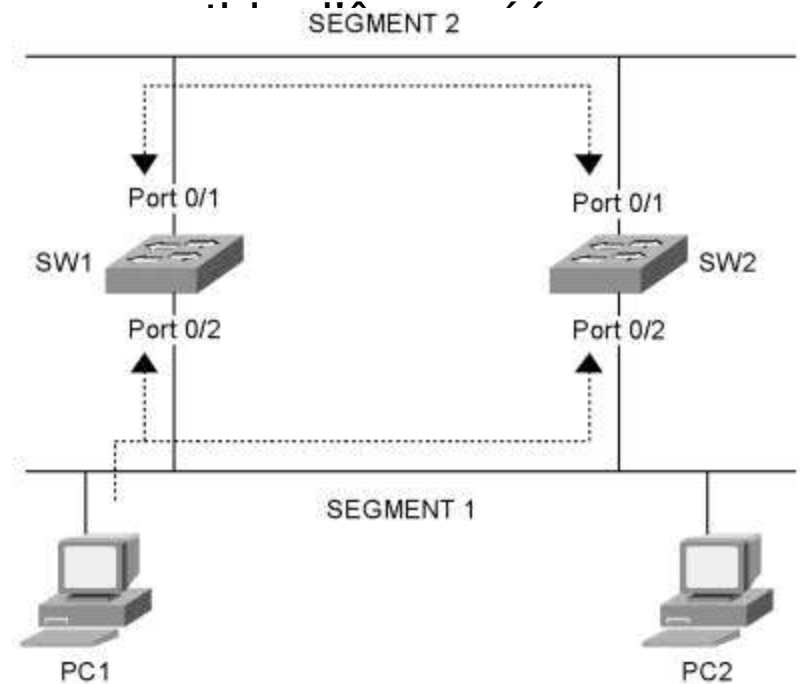
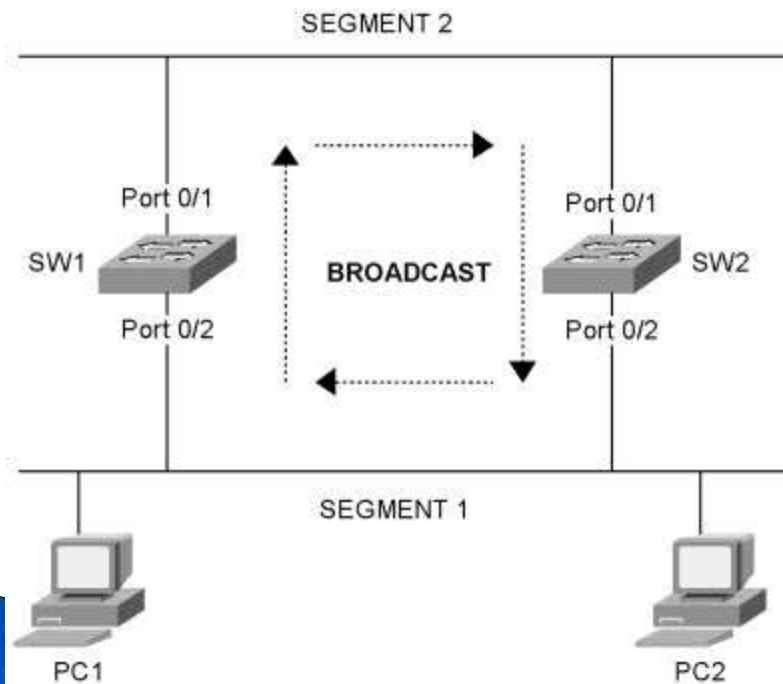


Problème : quand il y a plusieurs routes possibles sur le réseau, recopies multiples de trames et inondation du réseau

Boucles dans le LAN : Problématique

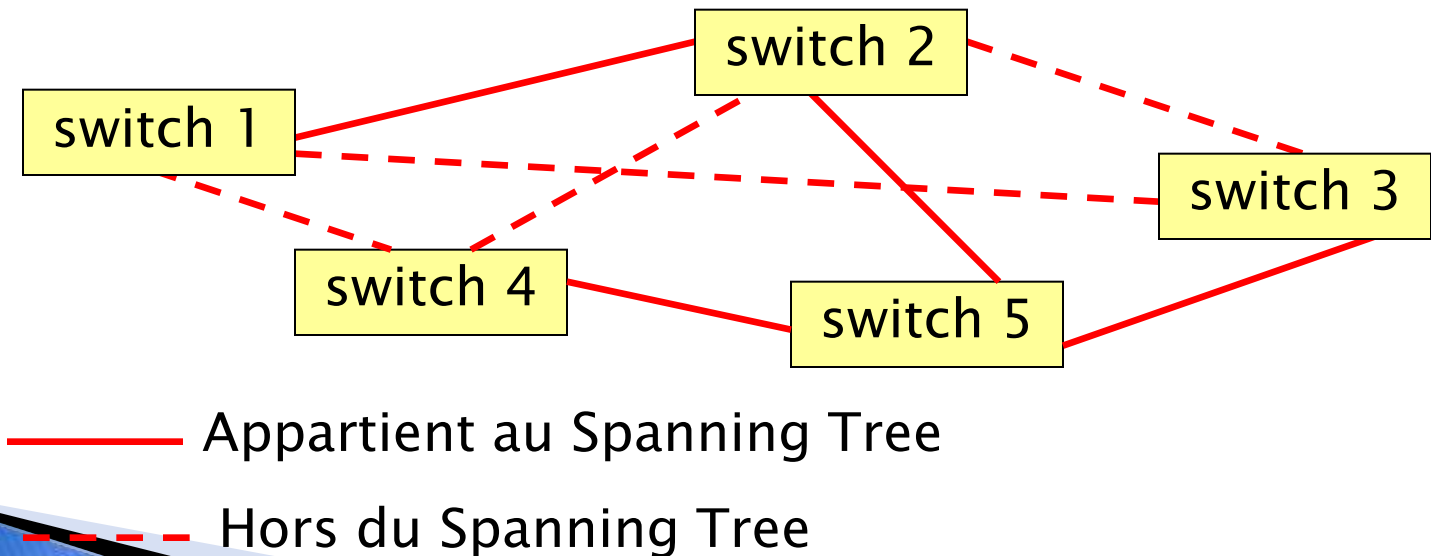
Des tempêtes de broadcast : lorsque des trames de broadcast sont envoyées (FF-FF-FF-FF-FF-FF en destination), les switchs les renvoient par tous les ports. Les trames circulent en boucles et sont multipliées (pas de TTL)

Instabilité des tables de commutation : quand une trame, même unicast, parvient aux switchs connectés en redondance, le port du switch associé à l'origine risque d'être erroné. Une boucle est



Algorithme du Spanning Tree – Principe

- ▶ Fonction de l'Algorithme de Spanning Tree : s'assurer qu'il n'y a pas de boucles dans un contexte de liaisons redondantes entre des matériels de couche 2
 - STP détecte et désactive des boucles de réseau et fournit un mécanisme de liens de backup
 - Peut-être mis en œuvre sur des ponts ou commutateurs
 - Spécifications du Spanning Tree (SPT) définies dans la norme 802.1D



Algorithme du Spanning Tree – Principe

- ▶ Fonctionnement basé sur la sélection d'un bridge Root et de calculs des chemins les plus courts vers ce bridge
- ▶ Etats des ports bridges
 - "Blocking" qui ne transfère pas de trames de donnée
 - "Forwarding" qui transfère les trames de donnée
- ▶ Création d'un chemin la plus court, chemin établi en fonction de la somme des coûts de liens entre switches (coût basé sur la vitesse d'un port)

- ▶ Les commutateurs vont s'échanger des messages contenant :
 - l'identificateur supposé de la racine par le commutateur émetteur,
 - le coût de la liaison entre le commutateur et la racine supposée
 - l'identificateur du commutateur émetteur,
 - le numéro du port sur lequel le message est émis.
- ▶ ⇒ Envoi de trames BPDU (Bridge Protocol Data Unit)

Algorithme du Spanning Tree – Principe

- ▶ Sélection du switch Root
 - Point central de l'arbre STP
 - Switch racine ayant l'ID la plus faible
 - ID du switch composé de deux parties : la priorité (2 octets) + adresse MAC (6 octets)
 - Priorité par défaut 32768 (8000 Hex), soit pour une adresse MAC 00 :A0 :C5:12:34:56, un ID de 8000:00A0 :C512:3456 (valeur de priorité qui peut être modifiée)
 - Sur le switch racine, tous les ports sont en état forwarding
- ▶ Sélection d'un port Root pour les switch non-root

- Sélection d'un port Root qui aura le chemin le plus court vers le switch Root.
- **Port Root en état « forwarding »**

Vitesse du Lien	Coût	Plage de coût recommandé
4 Mbps	250	100 à 1000
10 Mbps	100	50 à 600
16 Mbps	62	40 à 400
100 Mbps	19	10 à 60
1 Gbps	4	3 à 10
10 Gbps	2	1 à 5

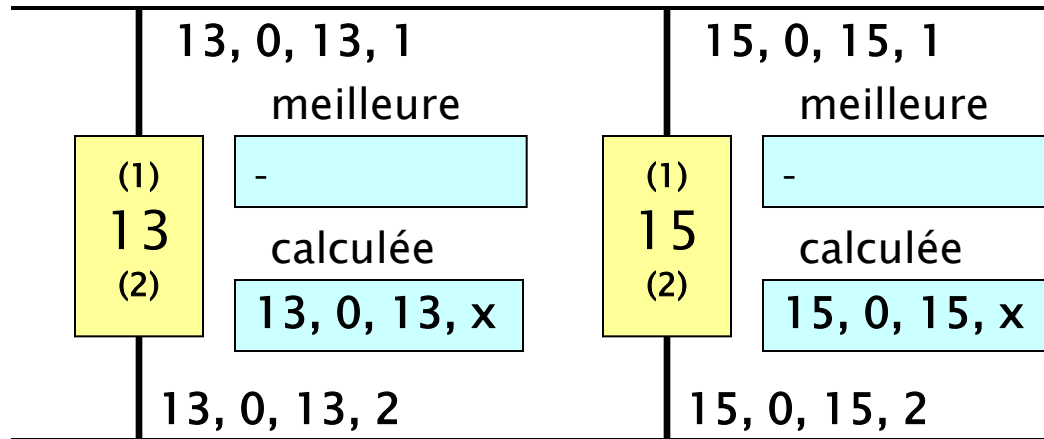
Algorithme du Spanning Tree – Principe

- ▶ Sélection d'un port désigné pour chaque segment
 - ▶ Pour chaque segment d'un LAN (domaine de collision), il y a un port désigné
 - ▶ Port désigné : celui ayant le chemin le plus court vers le Switch Root
 - ▶ Port désigné en état « forwarding »
 - ▶ Si plus d'un port sur un même segment a le même coût vers le switch Root, le port du switch qui a l'ID la plus faible est choisi

En résumé

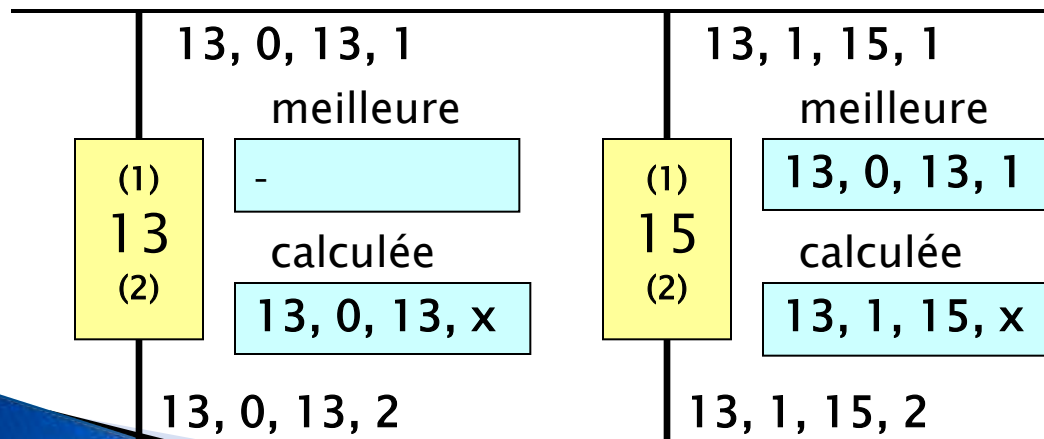
- ▶ 1 switch Root par réseau dont tous les ports sont désignés
- ▶ 1 port Root par switch non-root
- ▶ 1 port désigné par domaine de collision
- ▶ tous les autres ports sont non-désignés

Algorithme du Spanning Tree – Switch en parallèle



Chaque commutateur se considère comme racine, message émis <id du pont racine, 0, id du pont, n° du port>

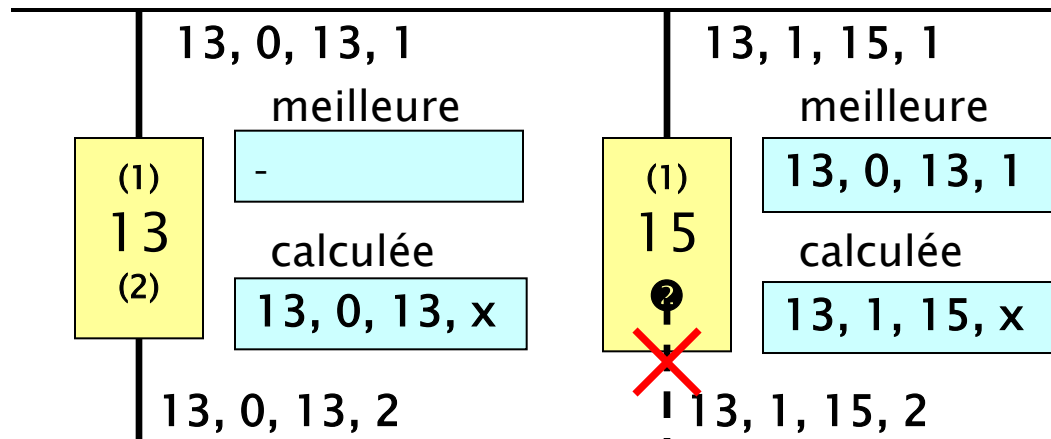
*terminologie utilisant le terme de bridge même pour des commutateurs



Commutateur avec Id à 13 inchangé (il a reçu 2 messages de configuration avec des id plus grands <15, 0, 15, 1> <15, 0, 15, 2>

Pour le commutateur Id à 15, il reçoit des messages avec une meilleure configuration, message sur le port 1 meilleur \Rightarrow port 1 vers racine

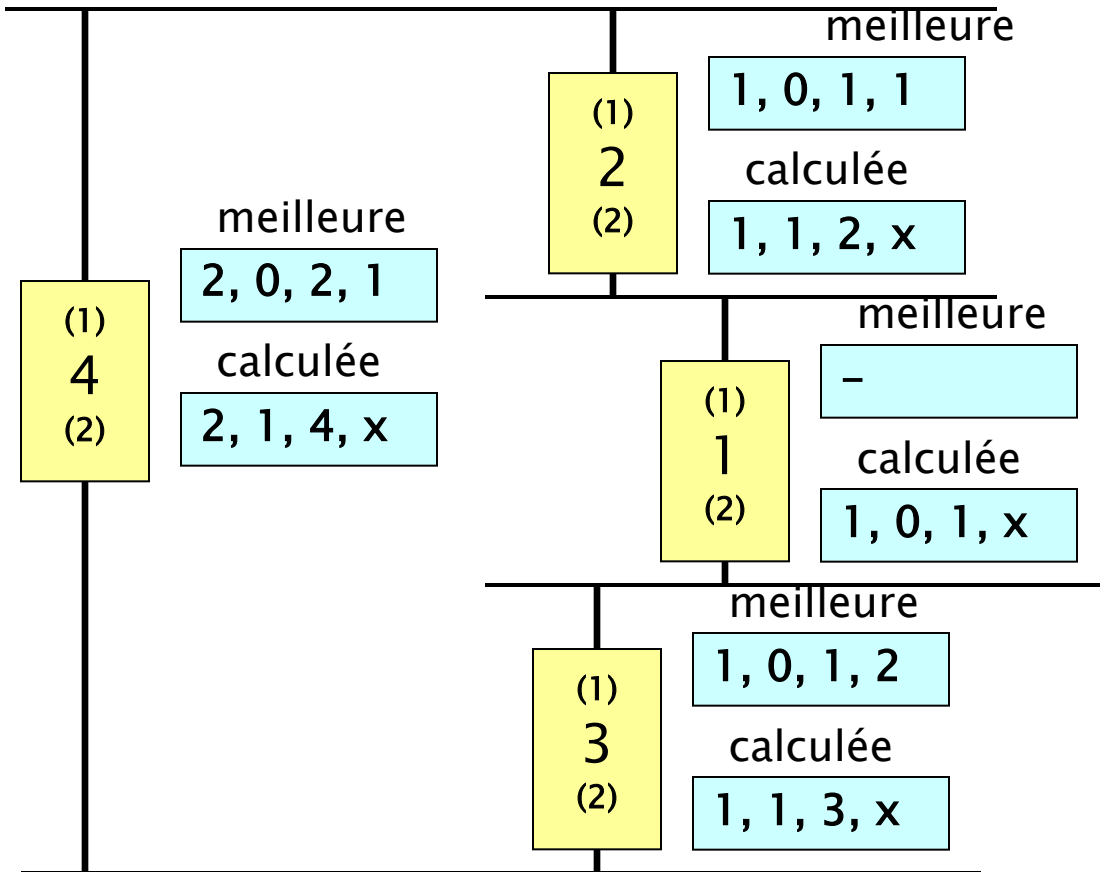
Algorithme du Spanning Tree – Switch en parallèle



Message reçu sur le port 2 du commutateur 15 $\langle 13, 0, 13, 2 \rangle$ plus grand que la meilleure configuration reçue par le commutateur $\langle 13, 0, 13, 1 \rangle$ mais plus petit que la configuration calculée par le commutateur $\langle 13, 1, 15, x \rangle$
 \Rightarrow port 2 inhibé

Il n'y a plus de boucle sur le réseau, puisque le commutateur 2 ne peut plus recopier des messages d'un commutateur sur l'autre.

Algorithme du SPT – Interconnexion de 4 sous-réseaux



Commutateurs qui se supposent initialement tous racine

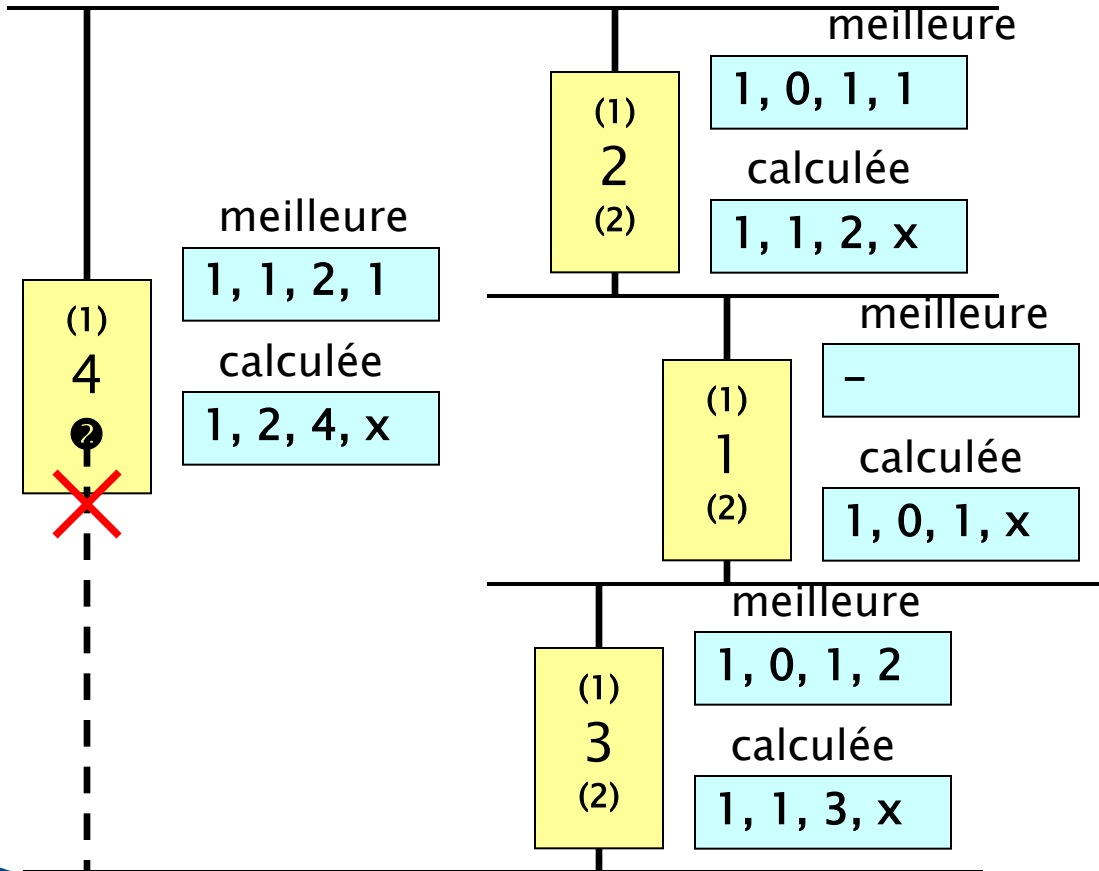
Commutateur 1 qui n'a reçu aucun message avec une meilleure configuration

Commutateur 2 reçoit par le port 2 $\langle 1, 0, 1, 1 \rangle$ meilleure que $\langle 2, 0, 2, x \rangle$, port 2 port vers la racine. Sur le port 1 configuration qui n'est pas meilleure $\langle 4, 0, 4, 1 \rangle$ que la configuration calculée $\langle 1, 1, 2, x \rangle \Rightarrow$ port 2 qui reste actif

Idem pour le commutateur 3, port 2 qui reste actif

Commutateur 4 a reçu deux messages $\langle 2, 0, 2, 1 \rangle$ $\langle 3, 0, 3, 2 \rangle$ qui contiennent une meilleure configuration que la sienne \Rightarrow port 1 devient racine. Configuration calculée $\langle 2, 1, 4, x \rangle$ supérieure à la configuration reçue sur le port 2 $\langle 3, 0, 3, 2 \rangle \Rightarrow$ le port 2 est pas inhibé

Algorithme du SPT – Interconnexion de 4 sous-réseaux



Commutateurs qui continuent d'émettre leur configuration

Commutateurs 2 et 3 qui reçoivent les mêmes messages du commutateur 1, ne changent pas leur configuration.

Commutateur 4 reçoit $\langle 1, 1, 2, 1 \rangle$ sur le port 1 et $\langle 1, 1, 3, 2 \rangle$ sur le port 2. Meilleure configuration toujours sur le port 1 \Rightarrow reste port racine.

Configuration calculée qui devient $\langle 1, 2, 4, x \rangle$. Message reçu sur le port 2 $\langle 1, 1, 3, 2 \rangle$ plus petit que la configuration calculée \Rightarrow port 2 inhibé, plus de boucle.

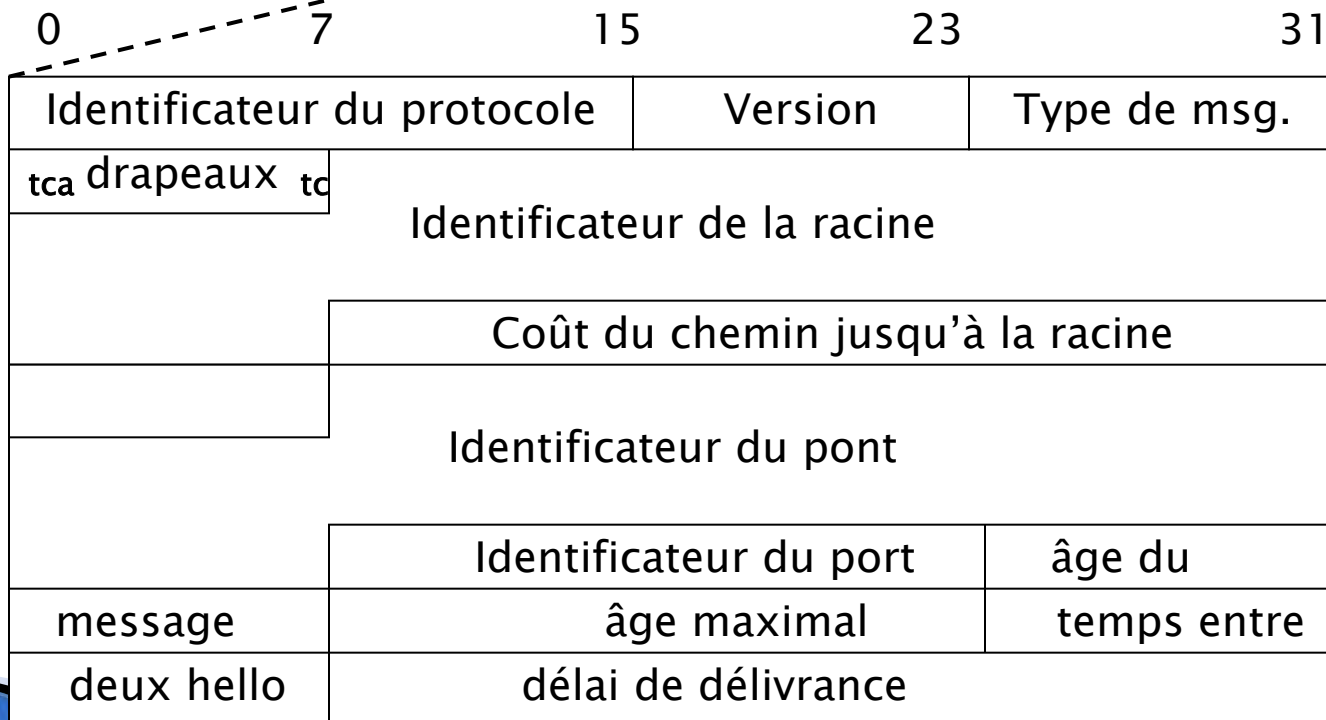
Format de la trame de Spanning Tree

@ destination

@ source

01:80:C2:00:00:00	@ MAC du pont	0x4	0x4	0x0	Données : trame de Spanning Tree
-------------------	---------------	-----	-----	-----	----------------------------------

@ réservée, @ de groupe, 1er bit à 1 N°SAP pour le pont-0x42 sur le 802.3



VLAN : Ethernet 802.1p, 802.1Q

- ▶ Mise en œuvre des VLAN dans un contexte d'Ethernet commuté : bonne solution pour constituer différents domaines de broadcast (+ sécurité en isolant des groupes d'utilisateurs)
- ▶ Interconnexion de VLAN - fonction de routage
- ▶ VLAN permettant de regrouper des stations partageant les mêmes caractéristiques ⇒ moyen efficace pour affecter une QoS à chaque VLAN
- ▶ Au niveau des commutateurs, IEEE 802.1Q et p
 - Marquage des VLAN (Q) + priorisation (p)
 - Gestion de la contention sur les liens de sortie
 - Insertion d'un « tag » dans la trame
 - 8 niveaux de priorité, 7 utilisés

Fonctionnalités des commutateurs

- ▶ Large évolution des technologies Ethernet
 - Compatibilité 10Mbit/s, 100 Mbit/s, Gbit/s voire 10 Gbit/s
 - 802.3u : version 100 Mbit/s 100BaseT
 - 802.3z : Gigabit Ethernet, 1000BaseSX, 1000BaseLX
 - 802.3ab : Gigabit Ethernet, 1000BaseT
 - 802.3ae : 10 Gigabit Ethernet
 - 802.3x : Ethernet full-duplex
 - 802.1p : Classe de service (Qualité de service)
 - 802.3q : VLAN (Virtual LAN) Tagging – VLAN : création de groupe dans le LAN permettant de limiter les domaines de broadcast.
 - 802.3ad : agrégation de liens (trunking)
 - 802.1x : Authentification port par port
 - 802.3af : transmission des signaux d'alimentation sur des câblages 10BaseT, 100BaseT et 1000BaseT

Architecture Ethernet, quelles évolutions ??

- ▶ Normalisation en perpétuelle évolution... place des technologies Ethernet de plus en plus importante
- ▶ Problématique
 - Equipements (PC, switchs, ...) : durée de vie approximativement de 3-5 ans
 - Durée de vie du câblage : 10-15 ans (3* celle des équipements!!!)
 - ⇒ Câblage installé aujourd'hui qui devra supporter trois générations d'équipements
- ▶ Structure de câblage qui n'est plus simplement utilisée pour interconnecter des PC
 - Téléphone IP, Point d'accès WiFi, Caméras IP, RFID, Lecteurs de badges/cartes
 - Technologie clef dans cette multiplicité d'applications : Power over Ethernet

Norme 802.11 – WiFi

- ▶ La norme IEEE 802.11 (ISO/IEC 8802–11) est un standard international décrivant les caractéristiques d'un réseau local sans fil. Révisions apportées à la norme originale afin d'optimiser le débit, la sécurité ou l'interopérabilité (802.11a, 802.11b, 802.11g..)

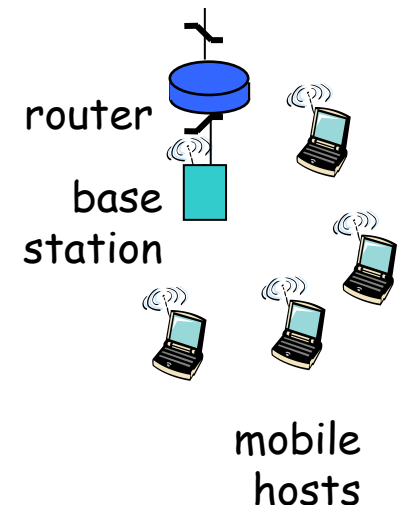
Standard	Vitesses (max/moy) Bandes de fréquences	Spécificités
802.11a (IEEE)	54 Mbps/24 Mbps 5 à 5.8 GHz	Cher et une bande de fréquence contraignante
802.11b (IEEE)	11 Mbps/5.5 Mbps 2.4 GHz	Déjà très répandu Point faible : la sécurité
802.11g (IEEE)	22 Mbps 2.4 GHz	Très attendu pour offrir de meilleurs débits que le 802.11b

- ▶ WiFi ou Wi-Fi : contraction de Wireless Fidelity, correspond initialement au nom donné à la certification délivrée par la WI-FI Alliance, anciennement WECA (Wireless Ethernet Compatibility Alliance).
 - La Wi-Fi Alliance est l'organisme chargé de maintenir l'interopérabilité entre les matériels répondant à la norme 802.11.
 - Le nom de la norme se confond aujourd'hui avec le nom de la certification.



Modes de fonctionnement du WiFi

- ▶ Équipements pour la mise en place d'un réseau WiFi
 - Les adaptateurs sans fils aux cartes d'accès : carte réseau à la norme 802.11 permettant à une machine de se connecter à un réseau sans fil (carte PCI, PCMCIA, adaptateur USB..)
 - Le point d'accès (AP, Access Point) permettant de donner un accès au réseau filaire (auquel il est raccordé) aux différentes stations avoisinantes équipées de cartes WiFi
- Deux modes opératoires dans le standard 802.11
 - **Mode infrastructure** : clients connectés à un point d'accès (mode par défaut des cartes 802.11b)
 - **Mode ad hoc** : clients connectés les uns aux autres sans aucun point d'accès



Architecture en couches du WiFi

- ▶ S'appuie sur les couches 1 et 2 du modèle OSI ⇒ Interopérabilité avec Ethernet
 - Couche Physique : spécifications des caractéristiques radios
 - Couche liaison de données : définition de la méthode d'accès
 - CSMA dans un environnement sans fil ne garantit pas l'absence de collision à la réception (problème de la station cachée)
 - Méthode du CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance), protocole d'accès des réseaux 802.11
 - Avant de transmettre, l'émetteur émet une trame RTS (Request To Send). Attente d'un CTS (Clear To Send) avant d'émettre (éventuellement collision lors de l'envoi du RTS, détection par absence de CTS)
 - Mécanisme d'accusé de réception

WLAN, conclusion...

- ▶ Le WiFi à 100 Mbits/s : la Norme 802.11n
 - Norme visant à remplacer la norme IEEE 802.11g en restant compatible avec 802.11a et 802.11g
 - Doit assurer des débits de 100 Mbits/s et au-delà (on vise les 500 Mbits/s !)
- ▶ La sécurité ??? Quelles solutions ??
 - Une infrastructure adaptée : positionner intelligemment les points d'accès selon la zone à couvrir
 - Éviter les valeurs par défaut (configuration du point d'accès, changement du mot de passe admin, du SSID, désactiver la diffusion du SSID sur le réseau...)
 - Filtrage par adresse MAC (ce qui ne résout pas le problème de la confidentialité des échanges!)
 - Gestion des authentications, autorisations et comptes utilisateurs (AAA, Authentication, Authorization and Accounting) à l'aide d'un serveur RADIUS (Remote Authentication Dial-In User Service, RFC 2865, 2866), système client/serveur permettant de gérer de façon centralisée les comptes des utilisateurs et les droits associés
 - Cryptage des données : Norme 802.11i appelée norme WPA2

Sommaire

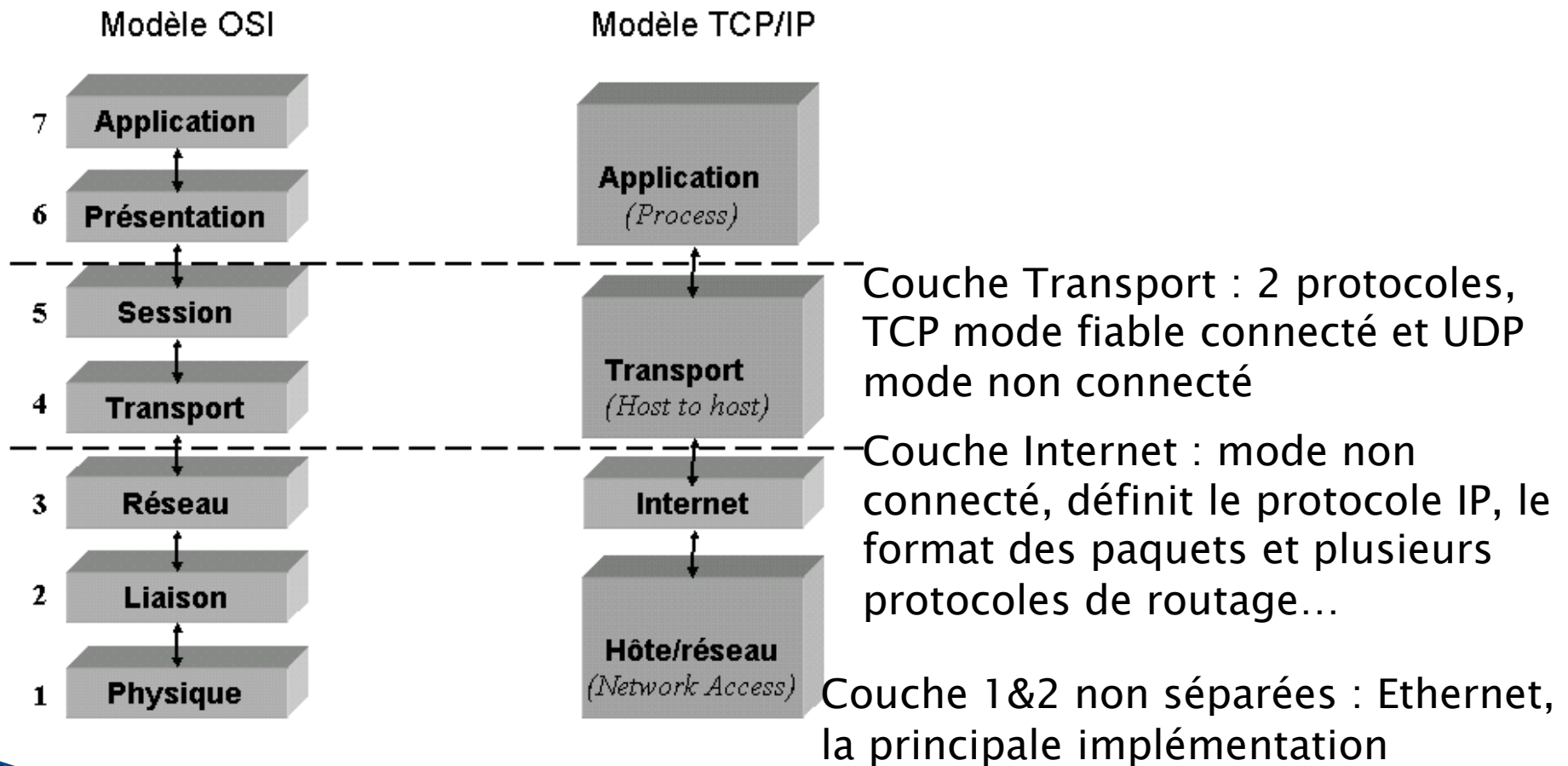
- ▶ Introduction
- ▶ Concepts réseaux
- ▶ Les réseaux d'entreprise/ Les réseaux d'opérateurs
- ▶ Architecture logicielle des réseaux
- ▶ Le modèle OSI
- ▶ Les réseaux locaux (modèle IEEE)
- ▶ **L'architecture TCP/IP**
 - **Caractéristiques de TCP/IP**
 - Les protocoles de la couche transport et la couche Internet
 - Les adresses IP
 - Interconnexion des réseaux IP
 - Les protocoles de TCP/IP
- ▶ Conclusion – Glossaire – Bibliographie

Architecture TCP/IP

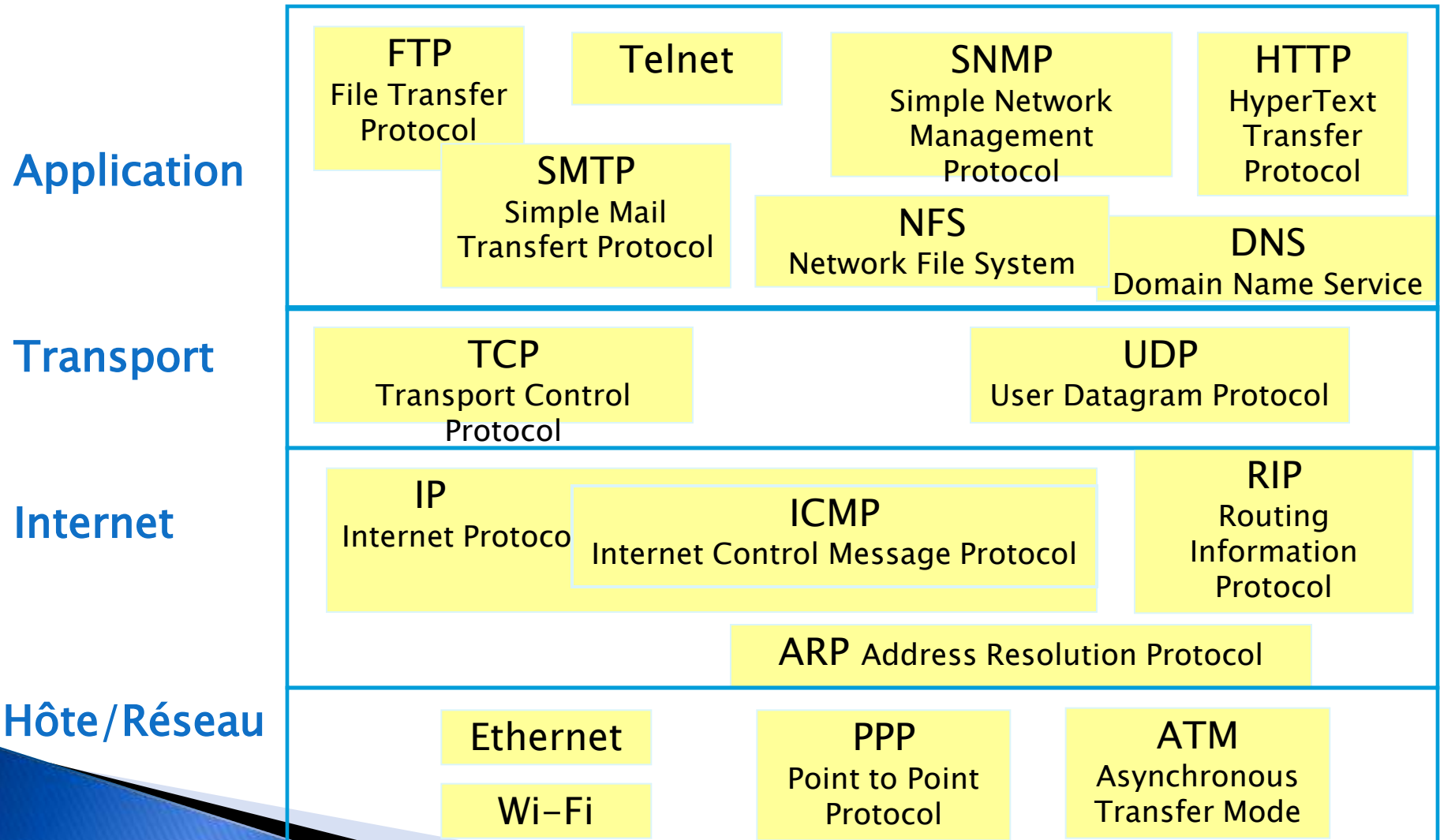
- ▶ Internet caractérisé par ces deux principaux protocoles : TCP/IP (Transport Control Protocol/Internet Protocol)
 - Protocole ouvert
 - Sources disponibles gratuitement et développées indépendamment d'une architecture particulière, d'un système d'exploitation particulier, d'une structure commerciale propriétaire
- ▶ Protocole indépendant du support physique du réseau
 - véhiculé par des supports et des technologies aussi différents qu'Ethernet, une liaison louée, une liaison radio (satellites, wifi 802.11a/b/g), une liaison xDSL, ATM, MPLS....
- ▶ Mode d'adressage commun à tous les utilisateurs de TCP/IP
- ▶ Standardisation des protocoles de haut niveau

- ▶ **L'IETF (Internet Engineering Task Force)** : groupe international de chercheurs et d'industriels qui collaborent pour produire les standards de l'Internet (www.ietf.org)
- ▶ **RFC (Request For Comment)** : ensemble des spécifications et évolutions des protocoles TCP/IP

Modèle OSI et TCP/IP

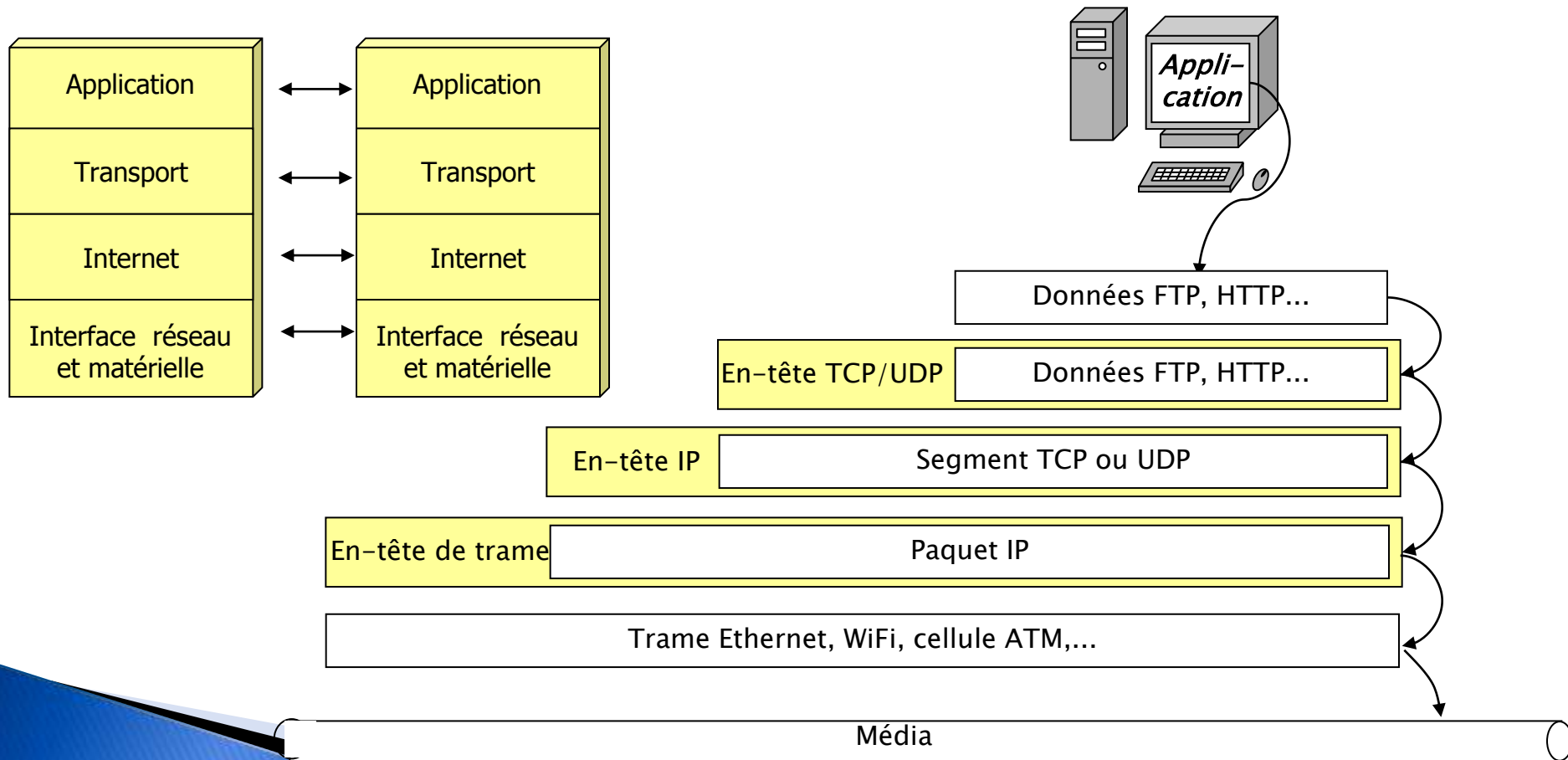


Les protocoles du modèle TCP/IP



Concepts de l'architecture en couches

- Les données issues de l'application sont encapsulées au niveau de la couche transport pour fournir des segments TCP, puis des paquets IP au niveau de la couche réseau (Internet) et enfin des trames délivrées sur le média utilisé



Mise en œuvre des protocoles TCP/IP

- ▶ TCP/IP est basé sur un principe non connecté
 - Mode datagramme ⇒ équipements relativement simples et rapides à l'intérieur du réseau
 - Routage et segmentation des données
- ▶ But du protocole IP : construire un réseau mondial en s'adaptant à tout type de supports physiques ⇒ RFC pour définir les règles d'encapsulation des paquets IP
 - Réseaux Locaux Ethernet : RFC 894
 - Liaisons point à point avec PPP (Point to Point Protocol) : RFC 1661
 - ATM : RFC 1483...
- ▶ ⇒ Interconnexion de réseaux hétérogènes grâce au protocole IP

Sommaire

- ▶ Introduction
- ▶ Concepts réseaux
- ▶ Les réseaux d'entreprise/ Les réseaux d'opérateurs
- ▶ Architecture logicielle des réseaux
- ▶ Le modèle OSI
- ▶ Les réseaux locaux (modèle IEEE)
- ▶ **L'architecture TCP/IP**
 - Caractéristiques de TCP/IP
 - **Les protocoles de la couche transport et la couche Internet**
 - La couche Transport
 - Les numéros de ports – TCP-UDP, Format du segment
 - La couche Internet
 - Rôle de la couche Internet – Format du paquet IP
 - La couche Ethernet
 - Les adresses IP
 - Interconnexion des réseaux IP
 - Les protocoles de TCP/IP

▶ **Conclusion – Glossaire – Bibliographie**

Les protocoles de la couche Transport

- ▶ La couche transport couvre l'implémentation des deux protocoles
 - TCP : Transmission Control Protocol (mode orienté connexion) – RFC 793
 - Majorité du trafic
 - Domaines d'application : Web avec le protocole HTTP, Transfert de fichier avec le protocole FTP, Telnet...
 - UDP : User Datagram Protocol (mode non connecté) – RFC 768
 - Protocole de transport des applications multimédias
- ▶ Principale fonction : réaliser une transmission de bout en bout des messages entre deux stations (End to End Transport Service)
- ▶ Elle met en relation les deux processus communicants qui résident dans les extrémités de la liaison
- ▶ Offre des services indépendamment du type du réseau, elle pallie donc les insuffisances du réseau

TCP, UDP : Les numéros de port

- ▶ Identification d'une application : numéro de port
 - Le port est une destination abstraite utilisée par le protocole
- ▶ Port prédéfini (RFC 1060 « assigned numbers » pour les services (numérotés de 0 à 1023))
 - 23 : Telnet
 - 25 : SMTP
 - 53 : DNS
 - 80 : web HTTP...
- ▶ Tous les équipements TCP/IP respectent cette attribution de ports pré-définis
 - Fichier `/etc/services` sous Unix
- ▶ Mode client serveur
 - Serveur, on parle de démons dans Unix (Linux)
 - Le client se voit attribuer un numéro de port non affecté (>1024) pour éviter toute confusion avec les ports « officiels »

TCP, UDP : Les numéros de port

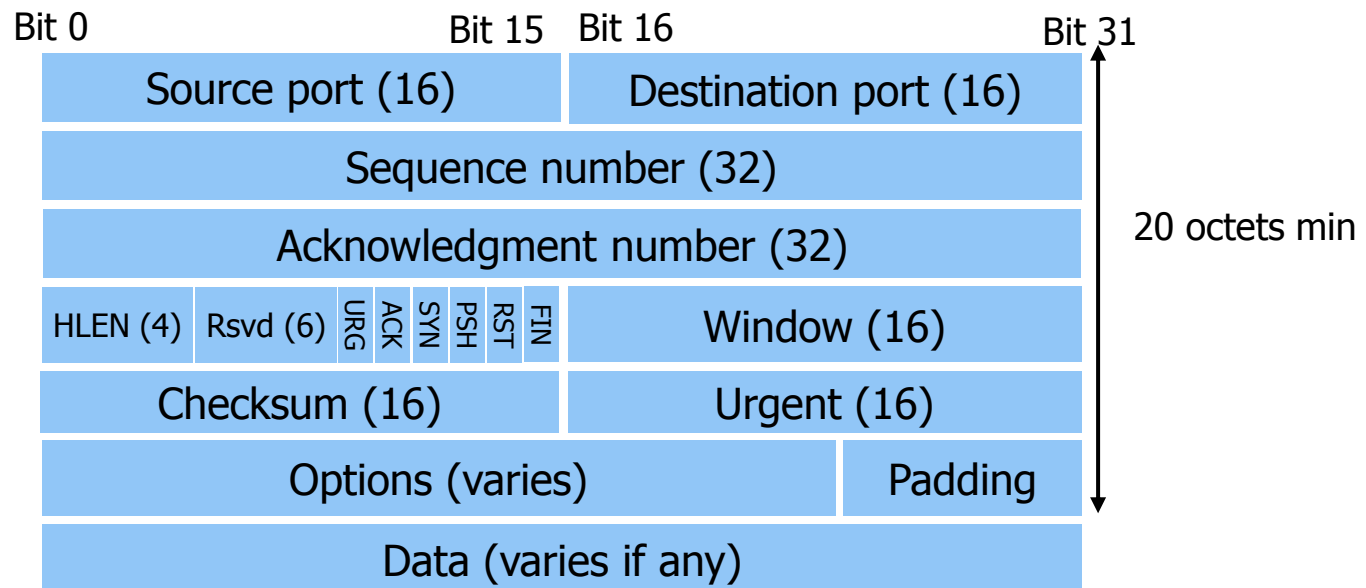
- ▶ Port prédéfini (RFC 1060 « assigned numbers » pour les services (numérotés de 0 à 1023)
 - 20 : FTP transfert de données (File Transfer Protocol)
 - 21 : FTP contrôle
 - 23 : Telnet
 - 25 : SMTP
 - 53 : DNS
 - 69 : TFTP
 - 80 : web HTTP
 - 161 : SNMP
- ▶ Mode client serveur
 - Serveur, on parle de démons dans Unix (Linux)
 - Le client se voit attribuer un numéro de port non affecté (>1024) pour éviter toute confusion avec les ports « officiels »
- ▶ Tous les équipements TCP/IP respectent cette attribution de ports pré-définis
 - Fichier `/etc/services` sous Unix

TCP (RFC 793)

- ▶ Importance dans l'Internet :
 - 90% du trafic, utilisation optimale des ressources réseaux
 - Domaines d'application : Web avec le protocole HTTP, Transfert de fichier avec le protocole FTP, Telnet...
- ▶ TCP ne « tourne » pas dans les routeurs (uniquement aux extrémités)
- ▶ Traite les données venant des couches supérieures comme une suite d'octets
- ▶ Découpe cette suite d'octets en segments (Taille max. 64 koctets)
- ▶ Un segment TCP est contenu dans un datagramme IP (Champ protocole du datagramme IP = 6)
- ▶ Des segments sont échangés pour
 - Ouvrir les connexions
 - Transférer les données
 - Envoyer des acquittements, gérer le contrôle de flux
 - Fermer les connexions

Format du segment TCP

- ▶ Taille minimale de 20 octets
 - (plus 20 octets d'en tête IP ⇒ en tête TCP/IP : 40 octets)



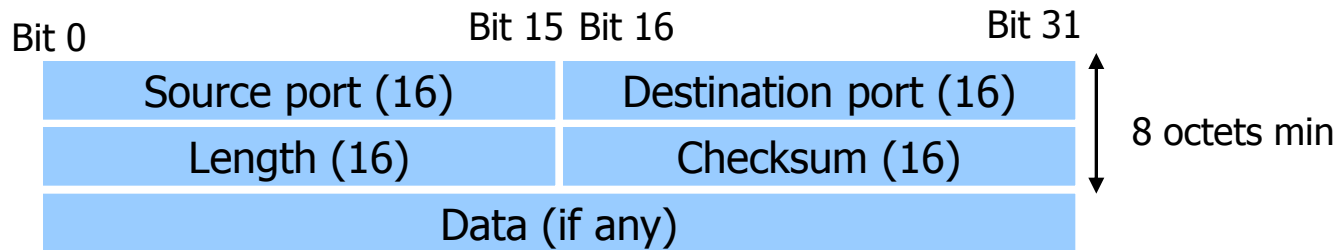
Champs de l'en tête TCP

- ▶ **Source Port, Destination Port** (16 bits) : numéro du port qui identifie l'application du côté émetteur et destinataire
- ▶ **Sequence number** (32 bits), **Acknowledgment number** (32 bits) : Pour le séquence et l'acquittement des données reçues
- ▶ **HLEN** (Header Length, 4 bits) ou **Data Offset** : Longueur de l'entête donnée en multiple de 32 bits (souvent 5)
- ▶ **Rsvd** (Reserved) : Réserve, toujours à 0
- ▶ **Code bits** (6 bits) : Drapeaux (flags) pour l'établissement et la fermeture de la session.
- ▶ **Window** (16 bits) : Taille de la fenêtre coulissante (nombre d'octets qu'on peut recevoir à la fois avant acquittement). Mécanisme de contrôle de flux.
- ▶ **Cheksum** (16 bits) : code pour la détection et la correction d'erreurs sur l'entête et les données
- ▶ **Urgent Pointer** (16 bits) : indique le dernier octet urgent à transmettre si flag URG à 1
- ▶ **Options** : permet d'ajouter des options (options standards décrites dans les RFC, par exemple taille maximale du segment négociée au moment de l'établissement de la connexion)

UDP (RFC 768)

- ▶ User Data Protocol – Protocole de transfert non fiable
 - Caractéristiques :
 - Protocole de transmission de message en mode datagramme
 - Pas de connexion, Pas de séquençement, Pas de fiabilité
 - Détection d'erreur bit mais pas de retransmission en cas d'erreur
 - Pas de contrôle de flux/congestion (⇒ facile de saturer le réseau et les routeurs)
 - Utilisation de numéros de port pour le multiplexage/démultiplexage
 - Domaines d'utilisation :
 - Transfert de fichier dans un réseau local avec TFTP (Trivial File Transfer Protocol)
 - Résolution de nom de domaine avec DNS (Domain Name Service)
 - Gestion de réseau avec SNMP (Simple Network Management Protocol)
 - Temps réel : flux audio vidéo pour les visioconférences avec RTP (Real-Time Transfer Protocol)
 - Communication de groupes en multicast

Format du datagramme UDP



- ▶ SP, DP : Les Ports source et destination (port source optionnel, identifie un port pour la réponse)
- ▶ Length : Longueur du datagramme (taille max 64 koctets)
- ▶ Cheksum : Un code pour la détection d'erreur

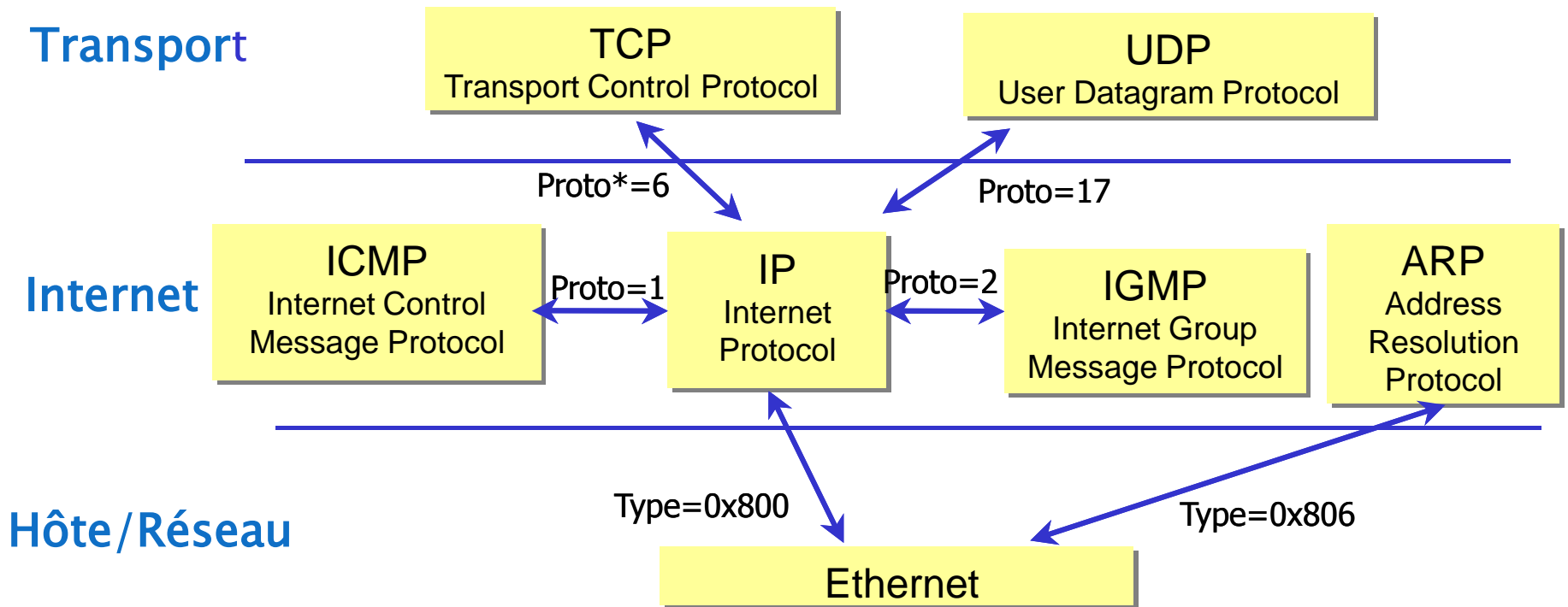
- ▶ Remarques :
 - Le protocole UDP est très simple et utile
 - Ne nécessitant pas les trois étapes de connexion TCP
 - Il ne fait que passer les données au protocole IP pour les acheminer à destination sans aucun contrôle : Risque de congestion du réseau!!!!
 - Risque de perturbation non négligeable des connexions TCP

Rôle de la couche Internet

- ▶ Fonctions principales de cette couche :
 - Adressage et routage
 - L'adressage permet une identification universelle des machines
 - Le routage permet d'atteindre ces machines grâce à leur adresse
 - Interface unique entre les couches hautes et basses
 - Adaptation des données aux couches 1 et 2 utilisées (par exemple segmentation/réassemblage)
- ▶ Les protocoles de la couche Internet :
 - Internet Protocol (IP), RFC 791
 - représente à lui seul toute la couche Internet (les autres protocoles ne font que l'assister dans sa fonction!)
 - Internet Control Message Protocol (ICMP)
 - Internet Group Message Protocol (IGMP)
 - Address Resolution Protocol (ARP)/ Reverse ARP (RARP)

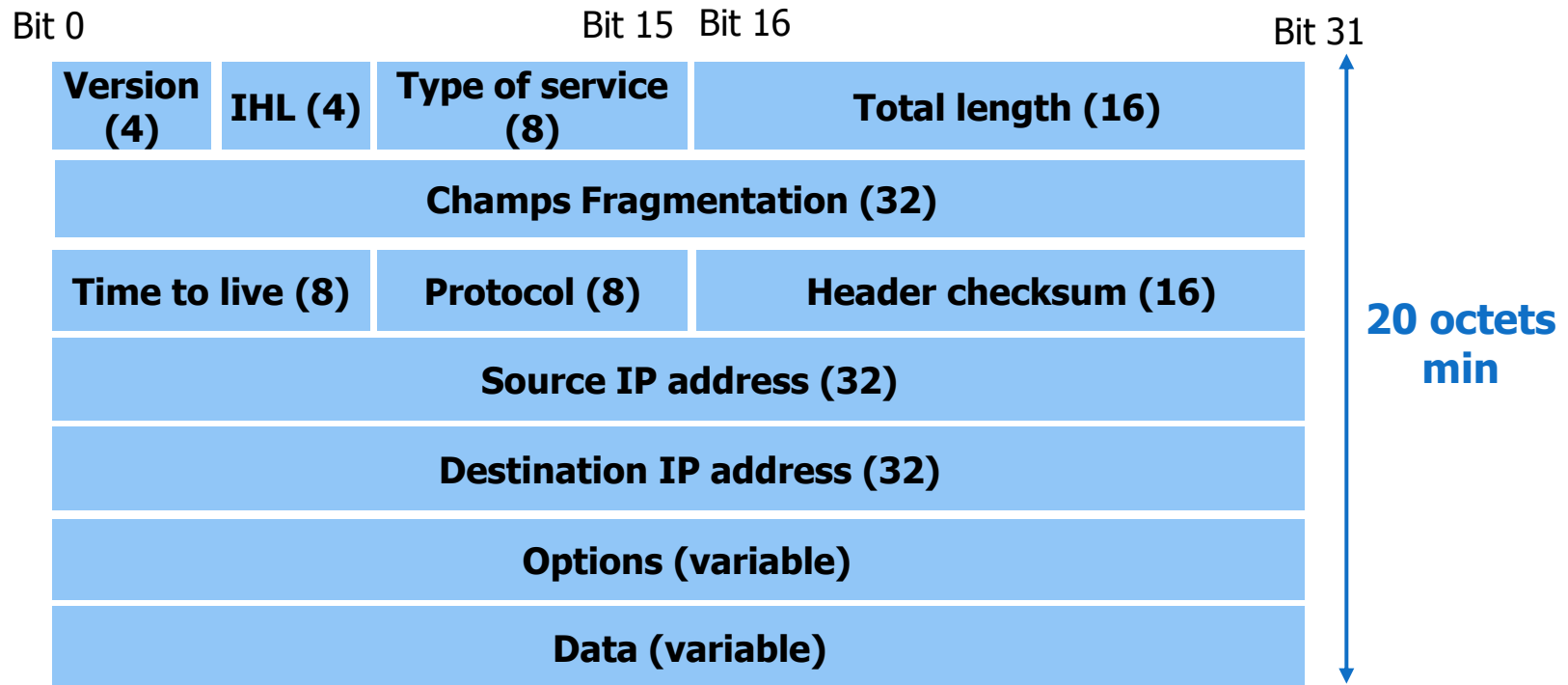
Architecture de la couche IP

- Couche 3 d'une machine IP



* Permet de déterminer le type de message

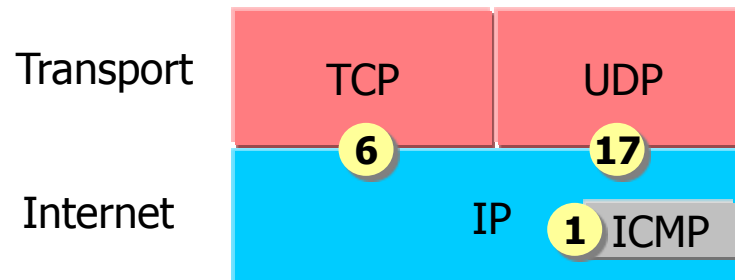
Format du paquet IP



- ▶ **Version** : version du protocole IP (Version courante = 4, 6 pour l'IPv6)
- ▶ **IHL** (IP Header Length) : longueur de l'entête IP (en général 5, taille de l'en-tête = 20 octets sans option)
- ▶ **Type de service** (TOS) : pour routage avec QoS (en terme de débit, délais...)
- ▶ **Total Length** : La longueur totale du paquet IP, entête + data en octets (max 64 koctets)

Format du paquet IP

- ▶ Champs pour la fragmentation/réassemblage
- ▶ **Time To Live (TTL)** :
 - Durée de vie du paquet en seconde
 - TTL décrémenté de 1 à chaque passage d'un routeur
 - Si le TTL atteint 0 le paquet est détruit et un message ICMP est envoyé à l'expéditeur (évite au paquet de circuler éternellement en cas de boucle)
- ▶ **Protocol** : indique le numéro de protocole à qui il faut remettre le paquet



- ▶ **Header Checksum** : Checksum sur l'entête seulement, afin de vérifier son intégrité
- ▶ **Source address, Destination address** : adresse IP des équipements source et destinataire d'extrémité (pas les nœuds intermédiaires)

La couche Ethernet

- ▶ Majorité des réseaux qui s'appuie sur la couche Ethernet
- ▶ Ethernet reposant sur l'utilisation des adresses MAC (adresse physique, spécifique à la carte réseau)
- ▶ Format de la trame Ethernet (RFC 894) :

Adresse de destination	Adresse source	Type	Données	CRC
6 oct.	6 oct.	2 oct.	46-1500 oct.	4 oct.

Type=0x800, données à destination du protocole IP
Type=0x806, données à destination du protocole ARP

Sommaire

- ▶ Introduction
- ▶ Concepts réseaux
- ▶ Les réseaux d'entreprise/ Les réseaux d'opérateurs
- ▶ Architecture logicielle des réseaux
- ▶ Le modèle OSI
- ▶ Les réseaux locaux (modèle IEEE)
- ▶ **L'architecture TCP/IP**
 - Caractéristiques de TCP/IP
 - Les protocoles de la couche transport et la couche Internet
 - Les adresses IP
 - Format des adresses IP
 - Les classe d'adresses
 - Le masque de sous-réseau
 - Configuration des adresses IP (statique, dynamique)
 - Interconnexion des réseaux IP
 - Les protocoles de TCP/IP
- ▶ Conclusion – Glossaire – Bibliographie

Les adresses IP

- ▶ Chaque machine connectée au réseau doit avoir une adresse IP pour pouvoir communiquer en TCP/IP
- ▶ Types d'adresses
 - Adresse unicast : permet d'identifier un équipement IP de façon unique
 - Adresse multicast : adresse de diffusion vers un groupe d'équipements IP
 - Adresse broadcast : adresse de diffusion vers toutes les adresses d'un même sous-réseau
- ▶ Adresse unique associée à chaque interface réseau
 - Configurable de manière statique (commande `ifconfig` sous Linux) ou dynamique (DHCP, Dynamic Host Configuration Protocol, RFC 1451)
- ▶ Adresse IPv4 sur 32 bits (4 octets)
 - Exemple : 192.16.11.89 (notation décimale pointée)
- ▶ Adresse IPv6 sur 128 bits (16 octets)
 - Exemple : 2001:0db8:0:85a3:0:0:ac1f:8001

Les adresses IP

- ▶ Une adresse IP est une valeur de 32 bits (4 octets) composée de 2 parties :
 - NetId : Identifiant du réseau auquel appartient la machine
 - HostId : Identifiant de la machine (attribuée par l'administrateur du réseau)
- ▶ Découpage précis qui dépend de la classe d'adresse
- ▶ L'écriture de l'adresse se fait en « notation décimale pointée » où les octets sont séparés par des points

	32 bits			
Notation pointée	Network		Host	
Maximum	255	255	255	255
Binaire	11111111	11111111	11111111	11111111
Exemple décimal	172	16	122	204
Exemple Binaire	10101100	00010000	0111010	11001100

IP : Les classes d'adresse

- ▶ Il existe 5 classes d'adresse (selon l'importance du réseau)
 - Comment les différentier ? -> Par la valeur du premier octet

Classe	Plage d'adresses	Premier octet en binaire	Nbre de bits de la partie réseau	Nbre de réseaux	Nbre de bits de la partie hôte	Nbre d'hôtes
A	0-127	0 000 0000	7	126	24	16 777 214
B	128-191	10 00 0000	14	16 382	16	65 534
C	192-223	1100 0000	21	2 097 150	8	254
D	224-239	1110 0000	Adresses de Multicast			
E	240-254	1111 0000	Réservé			

Masque de sous-réseau

- ▶ Définition d'un masque de sous réseau (Netmask)
 - Il a la forme d'une adresse IP. Notation :
 - Décimale pointée: 255.255.255.0
 - Abrégé : /N (N est le nombre de bits à 1 dans le masque)
 - Contient une suite continue de 1 (binaire) de longueur variable de la gauche vers la droite
 - Masque utilisé pour faire du subnetting (voir cours suivants)
- ▶ L'adresse réseau résulte d'un ET logique entre l'adresse IP et le masque
 - IP= 180.16.45.21
 - Masque= 255.255.255.0
 - Adresse du réseau = 180.16.45.0

Classe	Masque par défaut	Possibilités	Notation
A	255.0.0.0	255.x.x.x	/8
B	255.255.0.0	255.255.x.x	/16
C	255.255.255.0	255.255.255.x	/24

IP : Adresses Particulières

- ▶ Loopback (localhost) :
 - 127.0.0.1
 - Adresse à usage local affectée par défaut à une interface virtuelle sur une machine locale (permet de tester des programmes sans perturber le réseau)

- ▶ Adresse de Réseau :
 - S'obtient en mettant à 0 la partie HostId (Exemple : 194.16.54.0)
 - Utilisée dans les tables routage pour adresser les réseaux

- ▶ Machine qui ne connaît pas son adresse : 0.0.0.0 (utilisée lors d'une procédure d'initialisation)

- ▶ Adresse de Broadcast (diffusion) :
 - Adresse pour atteindre toutes les machines d'un même réseau (au lieu d'une seule machine)
 - S'obtient en mettant toute la partie HostId de l'adresse IP à 1 binaire (255 en décimal pour chaque octet)
Exemple: 194.16.54.255, adresse toutes les machines du réseau
194.16.54.0

IP : Adresses Privées

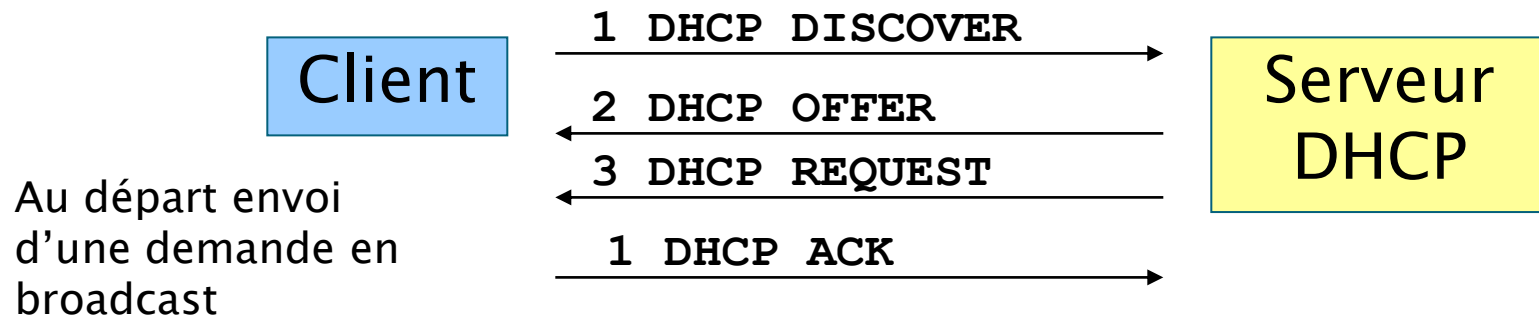
- ▶ La RFC 1918 définit des plages d'adresses réservées à un usage strictement privé
 - Réseau d'entreprise, école ...
- ▶ Ces adresses ne sont pas routables sur Internet
- ▶ Ces adresses peuvent être utilisées si le réseau n'est pas directement connecté à Internet
- ▶ Il peut l'être à travers un proxy
- ▶ Ou un routeur (firewall) qui permet la traduction d'adresse **NAT (Network Address Translation)**
- ▶ Les plages d'adresses privées :
 - Classe A : 10.0.0.1 à 10.255.255.254 (10/8)
 - Classe B : 172.16.0.1 à 172.31.255.254 (172.16/12)
 - Classe C : 192.168.0.1 à 192.168.255.254 (192.168/16)

Affectation des adresses IP

- ▶ L'affectation des adresses IP n'est pas aléatoire, elle est gérée par des organismes spécialisés :
 - IANA (Internet Assigned Numbers Authority) délègue au Regional Internet Registries (IR) :
 - INTERNIC : Amérique, Afrique du sud
 - RIPE : Europe, Afrique, Moyen Orient
 - qui allouent les adresses aux Local IRs (LIR)
- ▶ En France l'AFNIC (Association Française pour le Nommage Internet en Coopération) gère les adresses IP (www.afnic.fr) et les affecte aux fournisseurs d'accès à Internet (ISP)
- ▶ Une organisation (ou un particulier) obtient ses adresses IP de son fournisseur d'accès
 - 1 adresse ou plusieurs selon le nombre d'utilisateurs et les moyens financiers!!!
- ▶ Méthode d'allocation des adresses CIDR (Classless Internet Domain Routing, RFC 1466) : apporte une certaine hiérarchisation des adresses

Configuration IP dynamique : DHCP

- ▶ DHCP (Dynamic Host Configuration Protocol, RFC 1451) : affectation automatique des adresses IP
- ▶ Pour chaque poste : adresse IP valide (homogénéité avec le netmask), informations sur les noms de domaines
- ▶ Configuration statique qui peut devenir fastidieuse ⇒ mise en place d'un protocole de configuration distante : DHCP



- ▶ Configuration standard : affecte des adresses IP, un masque de sous-réseau, les paramètres DNS (éventuellement option telle que nom de domaine...)

Sommaire

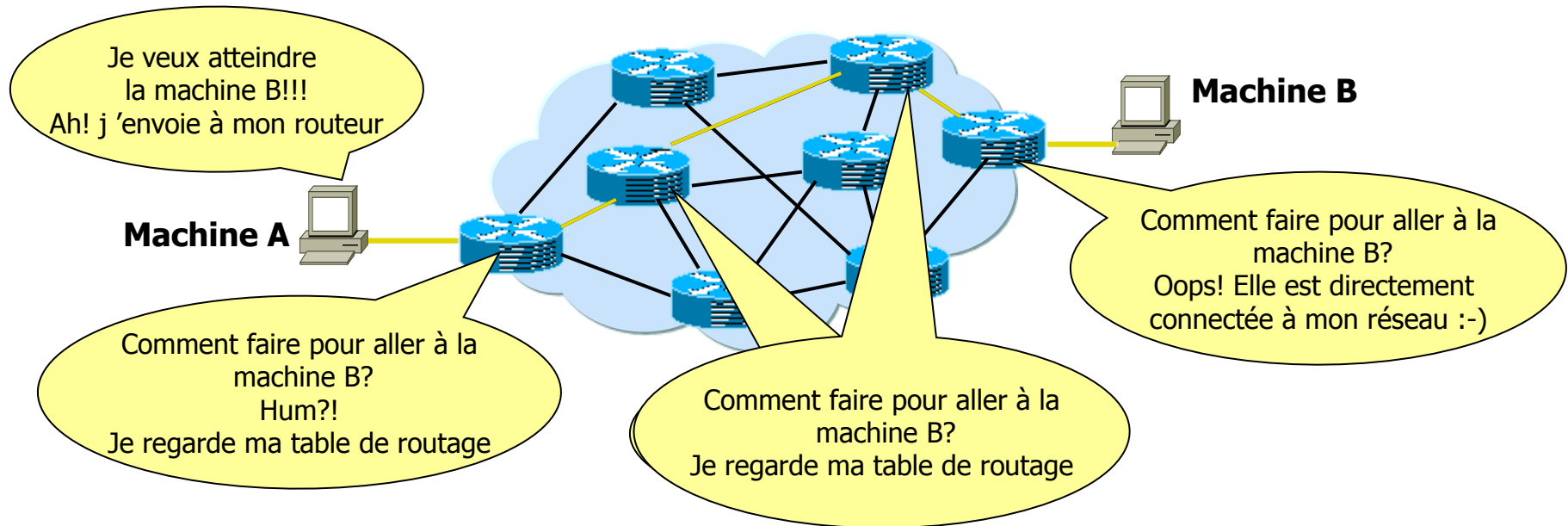
- ▶ Introduction
- ▶ Concepts réseaux
- ▶ Les réseaux d'entreprise/ Les réseaux d'opérateurs
- ▶ Architecture logicielle des réseaux
- ▶ Le modèle OSI
- ▶ Les réseaux locaux (modèle IEEE)
- ▶ **L'architecture TCP/IP**
 - Caractéristiques de TCP/IP
 - Les protocoles de la couche transport et la couche Internet
 - Les adresses IP
 - **Interconnexion des réseaux IP**
 - Les protocoles de TCP/IP
- ▶ Conclusion – Glossaire – Bibliographie

Interconnexion des réseaux IP

- ▶ **Routeur (Gateway IP)**
 - Analyse l'adresse réseau (adresse IP) des paquets pour prendre une décision de routage
 - Gère des tables de routage (adresse réseau, port de sortie) statiques ou dynamiques
- ▶ Chaque poste connaît l'adresse du routeur lui permettant de « sortir » du LAN. Routeur directement accessible par lien physique
- ▶ TTL (Time To Live) : champ du paquet IP donnant le nombre maximal de routeurs à travers lesquels le paquet IP peut passer (décrémenté de 1 à chaque passage par un routeur. Paquet détruit si TTL=0 ⇒ Evite l'encombrement du réseau si paquet perdu
- ▶ Commutateur/Routeur

Commutateur	Routeur
Niveau 2	Niveau 3
Analyse des Adresses MAC	Analyse des Adresses IP
Séparation des domaines de collision	Séparation des domaines de broadcast
Interconnexion au sein du LAN	Interconnexion de LAN, de réseaux hétérogènes

Principe du Routage



- ▶ Pour router, un routeur a besoin de :
 - Connaître l'adresse destination du paquet (adresse IP dans l'entête)
 - Avoir les routes possibles pour tous les réseaux (tables de routage)
 - Avoir la meilleure route pour chaque réseau (protocole de routage)
- ▶ Mécanismes de routage statiques (Sous Linux, `route add...`) ou dynamiques (protocoles de routage dynamiques : RIP, OSPF, BGP...)

Principe du Routage

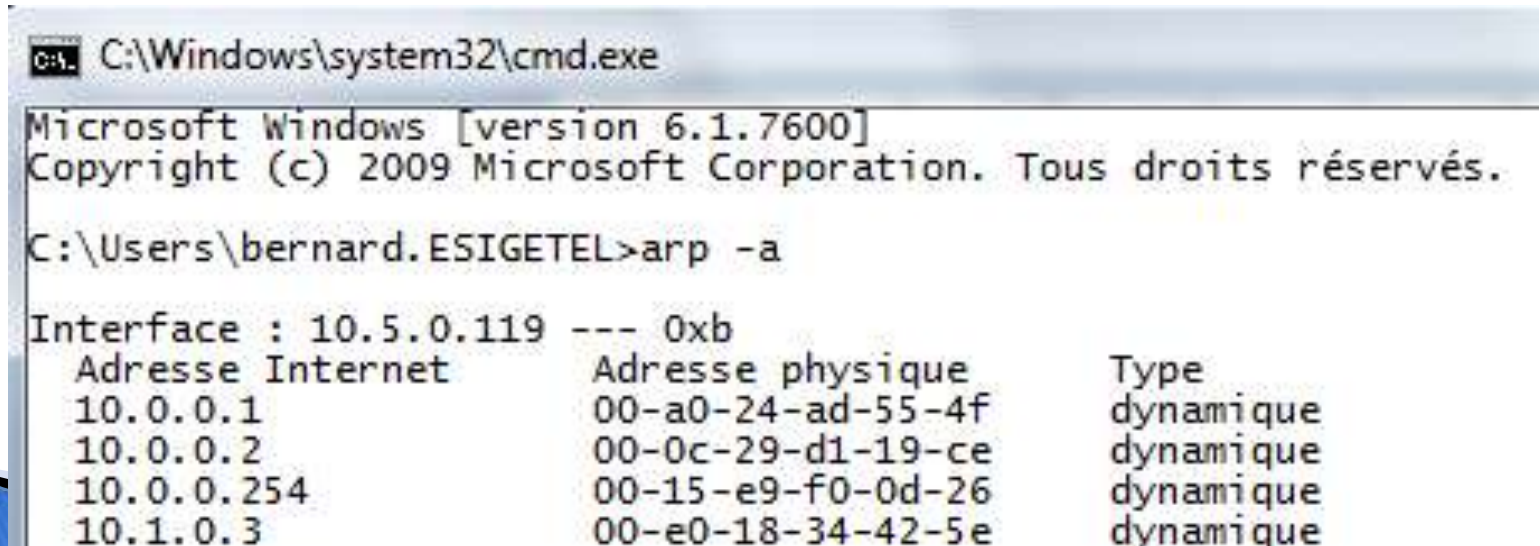
- ▶ Consiste à trouver le chemin à travers les nœuds du réseau pour transférer un paquet d'une unité source à une unité destination
 - Routage direct : Les deux machines sont dans le même réseau
 - Routage indirect : Entre deux machines dans deux réseaux différents
- ▶ Chaque machine dispose d'une table de routage contenant les chemins aux différents réseaux accessibles. Principes :
 - Si le paquet émis par une machine ne trouve pas sa destination dans le réseau ou sous-réseau local, il doit être dirigé vers un routeur qui rapproche le paquet de son objectif (chaque routeur possède une adresse par interface réseau) .
 - La machine source applique le masque de sous-réseau (netmask) pour savoir si le routage est nécessaire.
 - Chaque routeur doit donc connaître l'adresse du routeur suivant, il doit gérer une table de routage de manière statique ou dynamique.
- ▶ Deux types de routage
 - Statique : C'est l'administrateur réseau qui définit manuellement les chemins à prendre dans une table de routage
 - Dynamique : Grâce aux protocoles de routage qui permettent la construction automatique des tables de routage

Sommaire

- ▶ Introduction
- ▶ Concepts réseaux
- ▶ Les réseaux d'entreprise/ Les réseaux d'opérateurs
- ▶ Architecture logicielle des réseaux
- ▶ Le modèle OSI
- ▶ Les réseaux locaux (modèle IEEE)
- ▶ **L'architecture TCP/IP**
 - Caractéristiques de TCP/IP
 - Les protocoles de la couche transport et la couche Internet
 - Les adresses IP
 - Interconnexion des réseaux IP
 - **Les protocoles de TCP/IP**
 - Le protocole ARP
 - Le protocole ICMP
 - Le DNS
 - Quelques Protocoles Applicatifs : messagerie, VoIP, Telnet, SNMP..
- ▶ Conclusion – Glossaire – Bibliographie

ARP (RFC 826)

- ▶ Problème : Trouver une adresse MAC à partir d'une adresse IP ? Adresses IP totalement indépendantes des adresses physiques.
- ▶ **Address Resolution Protocol**
 - Permet de trouver l'adresse physique d'une machine sur le même réseau en donnant uniquement son adresse IP
- ▶ Pour chaque machine, stockage des adresses physiques dans une table ARP (cache). Permet d'optimiser les recherches suivantes.
 - Le cache est remis à jour périodiquement
 - Commande : `arp -a`



```
C:\Windows\system32\cmd.exe
Microsoft Windows [version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. Tous droits réservés.

C:\Users\bernard.ESIGETEL>arp -a

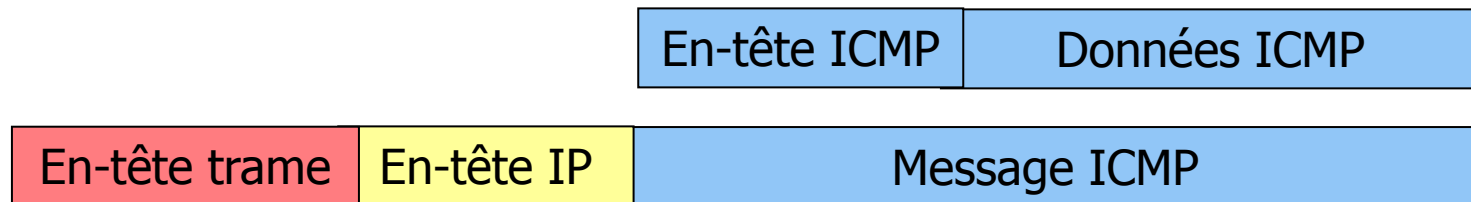
Interface : 10.5.0.119 --- 0xb
  Adresse Internet      Adresse physique      Type
  10.0.0.1              00-a0-24-ad-55-4f    dynamique
  10.0.0.2              00-0c-29-d1-19-ce    dynamique
  10.0.0.254           00-15-e9-f0-0d-26    dynamique
  10.1.0.3              00-e0-18-34-42-5e    dynamique
```

ICMP (RFC 792)

- ▶ **Internet Control Message Protocol**
 - Message ICMP encapsulé dans un paquet IP
 - Protocole de gestion de réseau : mécanisme de rapport d'erreurs
 - Implémenté sur tous les équipements réseau : stations, routeurs
- ▶ Deux types de message ICMP
 - Messages d'indication d'erreur
 - Messages de demande d'information (commande **ping**)
- ▶ Message envoyé par l'équipement destinataire ou un routeur intermédiaire
 - Quand il s'aperçoit d'un problème dans un datagramme
 - Pour avertir l'émetteur qu'il modifie son comportement (Exemple : routeur qui a une mauvaise information de routage)

ICMP

- ▶ Message ICMP contenu dans un datagramme IP
 - Champ version = 4
 - Champ type de service = 0
 - Champ protocole du datagramme IP = 1
- ▶ Format des messages ICMP
 - 3 champs communs
 - TYPE (1 octet) : 22 types définis
 - CODE (1 octet) : plus d'informations sur le champ type
 - CHECKSUM (2 octets) sur le message ICMP



- ▶ Permet de pallier aux manques de service IP

Types d'indication d'un message ICMP

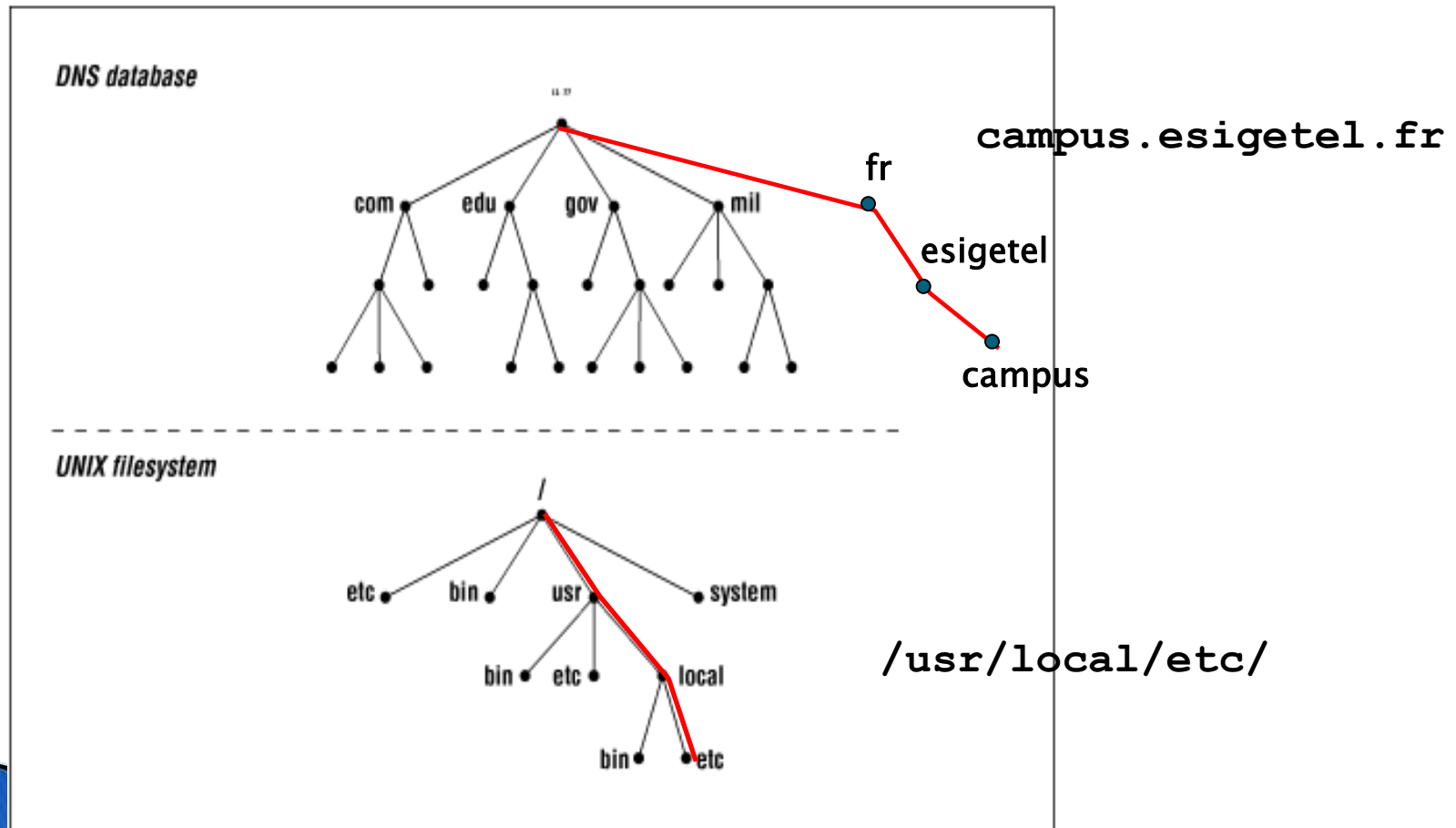
Type	Code	
0	0	Réponse à une demande d'écho (ping)
3		Destination non accessible
	0	Le réseau ne peut être atteint (Network unreachable)
	1	La station ne peut être atteinte (Host unreachable)
	2	Le protocole ne peut être atteint
	3	La fragmentation est nécessaire mais le bit DF=1. Paquet plus grand que la taille maximale admise sur le réseau
	4	Port TCP ou UDP inaccessible
	5	Route proposée en option n'est pas valable
4	0	Réduction du débit d'émission (Source Quench). Obsolète
5	0-3	Indication de redirection
8	0	Demande d'écho (ping)
10	0	Sélection du routeur
11	0-1	Durée de vie à 0 (pendant le transit – pendant le réassemblage)
30		Traceroute

DNS (RFC 1034, RFC 1035)

- ▶ **DNS (Domain Name Service)** : effectue la correspondance entre les adresses IP utilisées par les équipements pour communiquer et des noms plus simples à gérer par les humains
 - Ex : `www.esigetel.fr` = `192.134.106.60`
- ▶ Correspondance inverse (reverse lookup)
 - Ex : `192.134.106.60` = `hesperides.esigetel.fr`
- ▶ DNS contient aussi des informations complémentaires
 - Ex : `mail.esigetel.fr` est le serveur de mail de `esigetel.fr`
- ▶ Espace des noms DNS : schéma de nommage hiérarchique
 - Internet est divisé en plusieurs centaines de domaines de haut niveau, chacun contenant un grand nombre d'hôtes.
 - Les domaines sont divisés en sous-domaines, eux mêmes divisés en sous-domaines, etc. ...
 - Deux types de domaines de haut niveau : les génériques (`.com`, `.gov.`, `.net`, `.org`) et les géographiques (`.fr`, `.uk.`, `.de`, ...).
 - En France AFNIC chargée de l'attribution des domaines `.fr`

L'espace de noms DNS

- ▶ Hiérarchie inspirée du filesystem UNIX :

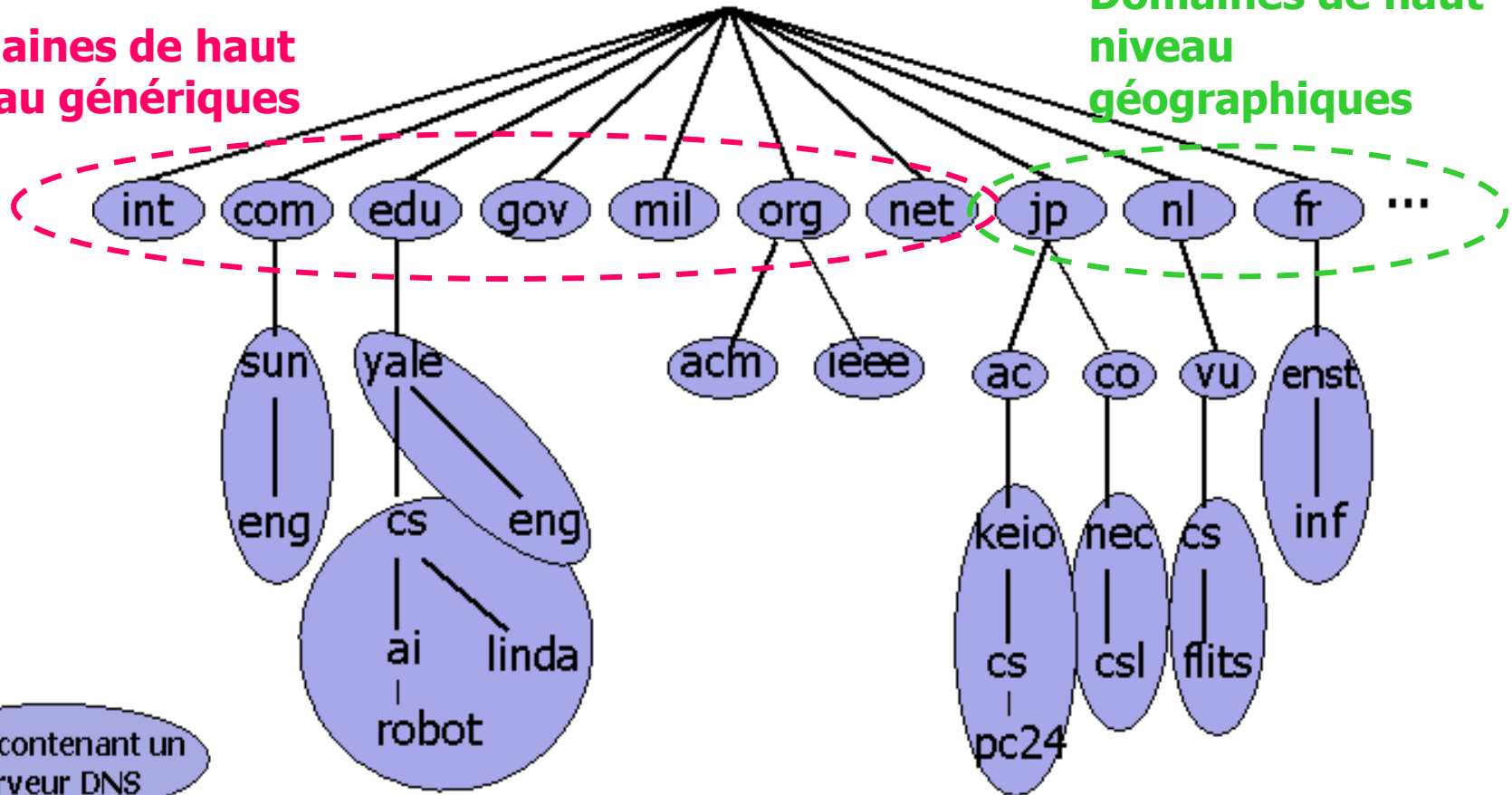


L'espace de noms DNS : exemple

- ▶ Il existe aujourd'hui 13 serveurs de noms racine répartis dans le monde connaissant tous les serveurs de noms de 1er niveau (de a.root-servers.net à m.root-servers.net) - <http://www.root-servers.org/>

Domaines de haut niveau génériques

Domaines de haut niveau géographiques



Fonctionnement du DNS

- ▶ Lorsqu'une application (par exemple la messagerie) a besoin de connaître une adresse IP, elle appelle une procédure appelée solveur (ou resolver) et lui passe le nom en paramètre.
- ▶ Le resolver envoie au DNS local une requête dans un segment UDP sur le port 53 (requête éventuellement retransmise à un plus haut niveau, etc)
- ▶ Le DNS cherche le nom dans sa table locale et renvoie l'adresse IP au solveur, qui la transmet à son tour à l'application.
- ▶ Dans le cas où le domaine du destinataire est distant, le serveur local ne contient pas forcément l'adresse dans sa table. Le serveur transmet alors la requête au serveur de plus haut niveau, qui peut à son tour être amené à passer la requête au niveau supérieur...
- ▶ BIND (Berkeley Internet Name Domain) : Standard de facto pour les implémentations de DNS sur des plates-formes Unix/Linux, Windows (<http://www.isc.org/bind>)

Fonctionnement du DNS

- ▶ Lorsqu'une application (par exemple la messagerie) a besoin de connaître une adresse IP, elle appelle une procédure appelée solveur (ou resolver) et lui passe le nom en paramètre.
 - ▶ Rôles du resolver :
 - Envoyer des requêtes aux NS
 - Interpréter les réponses (RR, erreur, timeout)
 - Retourner la réponse au programme qui a initié la demande
 - Conserver les réponses en cache
 - ▶ Deux méthodes de résolution :
 - La récursivité : interrogation du serveur maître qui répond avec l'information demandée ou avec les messages d'erreur appropriés
 - L'itération : une requête itérative est envoyée à un serveur de noms qui donne l'adresse d'un autre serveur ; le « resolver » interroge alors cet autre serveur (qui peut donner l'adresse d'un autre serveur...)
- Mode utilisé par le resolver des serveurs en général

Principaux types d'enregistrement DNS

- ▶ Espace de nom structuré comme une arborescence
 - Chaque domaine est un nœud de cette arborescence
 - Pour chaque nœud, il existe des enregistrements de ressources ou RR (Ressource Records), chacun conservant une information d'un type spécifique
 - Enregistrement A (Address) : adresse IP associée à un nom
 - Enregistrement NS (Name Server) : serveur de nom ayant autorité pour le domaine
 - Enregistrement SOA (Start Of Authority) : propriétés de base du domaine et de la zone du domaine
 - Enregistrement PTR (Pointer) : nom réel de l'hôte auquel appartient l'adresse IP
 - Enregistrement MX (Mail Exchanger) : serveur de messagerie pour la zone
 - Enregistrement CNAME (Canonical Name) : indique que le nom est un alias vers un autre nom

Structure des enregistrements

- ▶ Un RR est composé de 5 champs :
 - Name : nom du RR
 - TTL : durée de vie dans un cache
 - Class : classe d'appartenance, IN pour Internet
 - RR type : A, A6, MX, NS ...
 - Data

▶ Ex :

Name	TTL	Class	Type	Data
esigetel.fr.	10	IN	MX	mail.esigetel.fr.
mail.esigetel.fr.		IN	A	192.134.106.5
test.esigetel.fr.		IN	CNAME	mail.esigetel.fr.
www.esigetel.fr.		IN	A	192.134.106.60
192.134.106.5		IN	PTR	mail.esigetel.fr.

- ▶ RQ : FQDN (Fully Qualified Domain Name)
 - Ex : mail.esigetel.fr. (= hostname+domain name)
 - Dans les fichiers de configuration, mail.esigetel.fr. signifie que le nom est fqdn



Les protocoles de messagerie

- ▶ Protocole d'envoi des mails
 - Protocole SMTP (Simple Mail Transfer Protocol) : protocole standard permettant de transférer le courrier d'un serveur à un autre en connexion point à point.
 - Spécifications du protocole SMTP définies dans la RFC 821
 - SMTP fonctionne en mode connecté (au-dessus de TCP), encapsulé dans un paquet IP

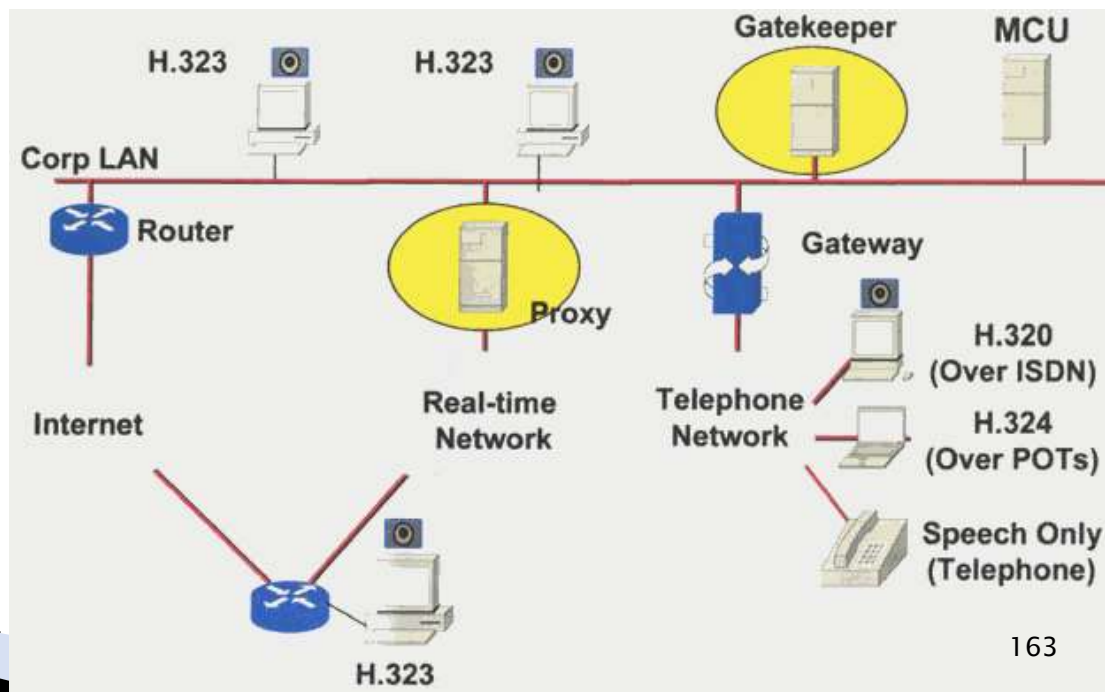
- ▶ Protocoles de réception des mails
 - POP3 (Post Office Protocol version 3) est le plus ancien et le plus utilisé des protocoles de remise finale des messages.
 - Les courriers sont sauvegardés sur le serveur jusqu'à ce que l'utilisateur les télécharge
 - IMAP (Interactive Mail Access Protocol) alternative au protocole POP3
 - Il permet de manipuler les messages (lecture, classement, effacement...) sur le serveur, sans les télécharger

La voix sur IP : Les protocoles associés

- Protocole de transport : **UDP**, mode non connecté \Rightarrow simplicité et rapidité qui rendent le protocole UDP parfait pour faire transiter des paquets de voix le plus rapidement possible quitte à les perdre (pas trop grave pour la voix tant que le taux de perte n'est pas très élevé)
- **RTP: Real-Time Protocol**, protocole temps réel ajouté pour faire transiter des paquets de voix, permet de pallier les lacunes d'UDP
- RTP permet de régénérer le synchronisme du flux de voix
- Protocole de réservation de ressources sur un réseau
 - RSVP (Ressource Reservation Protocol) ou DiffServ pour pallier les défauts du réseau (à savoir la QOS)
- Standardisation des protocoles de signalisation. Deux standards :
 - **H323** : standard issu des travaux de l'UIT et de Microsoft (Netmeeting compatible H323). S'inspire des réseaux télécoms
 - **SIP** (Session Initiation Protocol) standardisé par l'IETF, avec une philosophie réseaux IP

Architecture d'un réseau VoIP

- ▶ Gateway :
 - Equipement de type Passerelle qui permet l'interconnexion entre le réseau IP et le RTC, transforme la signalisation pour passer d'un réseau à un autre
 - Assure diverses fonctions, notamment le codage ou le décodage de la voix, la mise en paquet de la voix, le traitement des télécopies, l'annulation d'écho, etc
- ▶ Gatekeeper (portier)
 - Rôle : convertir les adresses et contrôler l'accès au réseau pour les terminaux, les passerelles et les ponts de conférence
 - D'autres services comme la gestion de largeur de bande passante et la localisation des passerelles
- ▶ Le pont de conférences (MCU, Multipoint Control Unit)
 - Permet à trois terminaux ou plus, et aux passerelles de participer à une conférence multipoint
- ▶ Les terminaux
 - PC, IP phone, ...

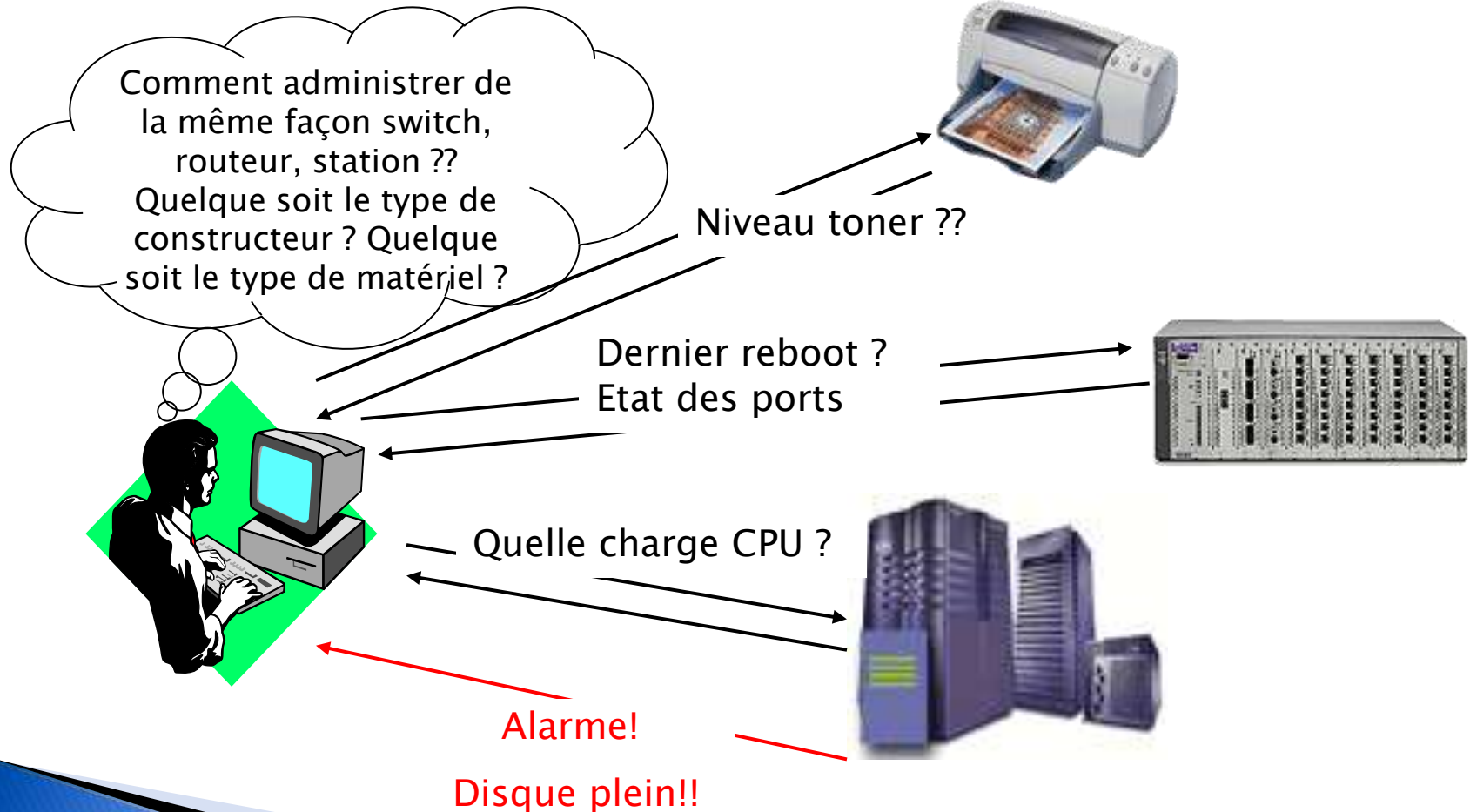


Autres protocoles applicatifs

- ▶ FTP (File transfert Protocol) permet le transfert de fichiers et de répertoires entre un serveur et un client sur un réseau IP (RFC 959)
 - Fonctionne au-dessus du protocole de transport TCP (port 21)
- ▶ Telnet : protocole standard d'Internet permettant l'interfaçage de terminaux et d'applications à travers Internet (RFC 854)
 - S'appuie sur une connexion TCP (port 23) pour envoyer des données au format ASCII codées sur 8 bits entre lesquelles s'intercalent des séquences de contrôle Telnet
- ▶ HyperText Transmission Protocol , RFC 1945
 - Protocole de communication entre le navigateur du client et les serveurs Web, basé sur le principe des liens hypertextes
 - Apache serveur Web open source le plus utilisé sur Internet : 60% – Microsoft IIS : 20% (Source : www.netcraft.com, mars 2001)

Administration Réseau et SNMP

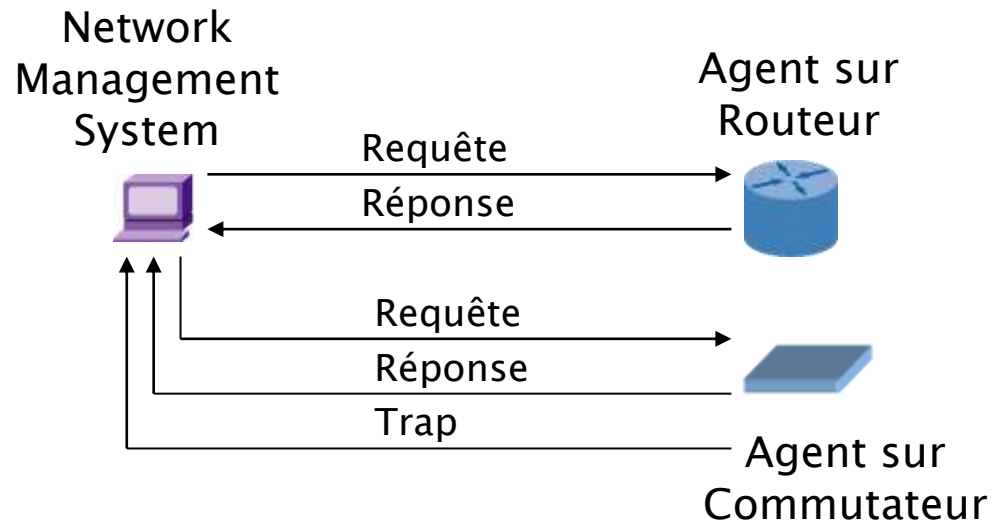
► Problématique



Le protocole SNMP

- ▶ SNMP (Simple Network Management Protocol) : premier protocole d'administration de réseau standardisé. Largement développé et répandu.
- ▶ Trois types d'interaction :

- Interrogations produites par la plate-forme permettant de demander la valeur d'un paramètre
- Mises à jour produites par la plate-forme permettant d'affecter une nouvelle valeur dans les objets gérés par un agent
- Alarmes initiées par l'agent



- ▶ SNMP implémenté avec UDP (ports 161, 162)
 - Simple, en-tête réduite, sans connexion
 - Moins fiable que TCP (récemment introduit comme option dans SNMPv3)

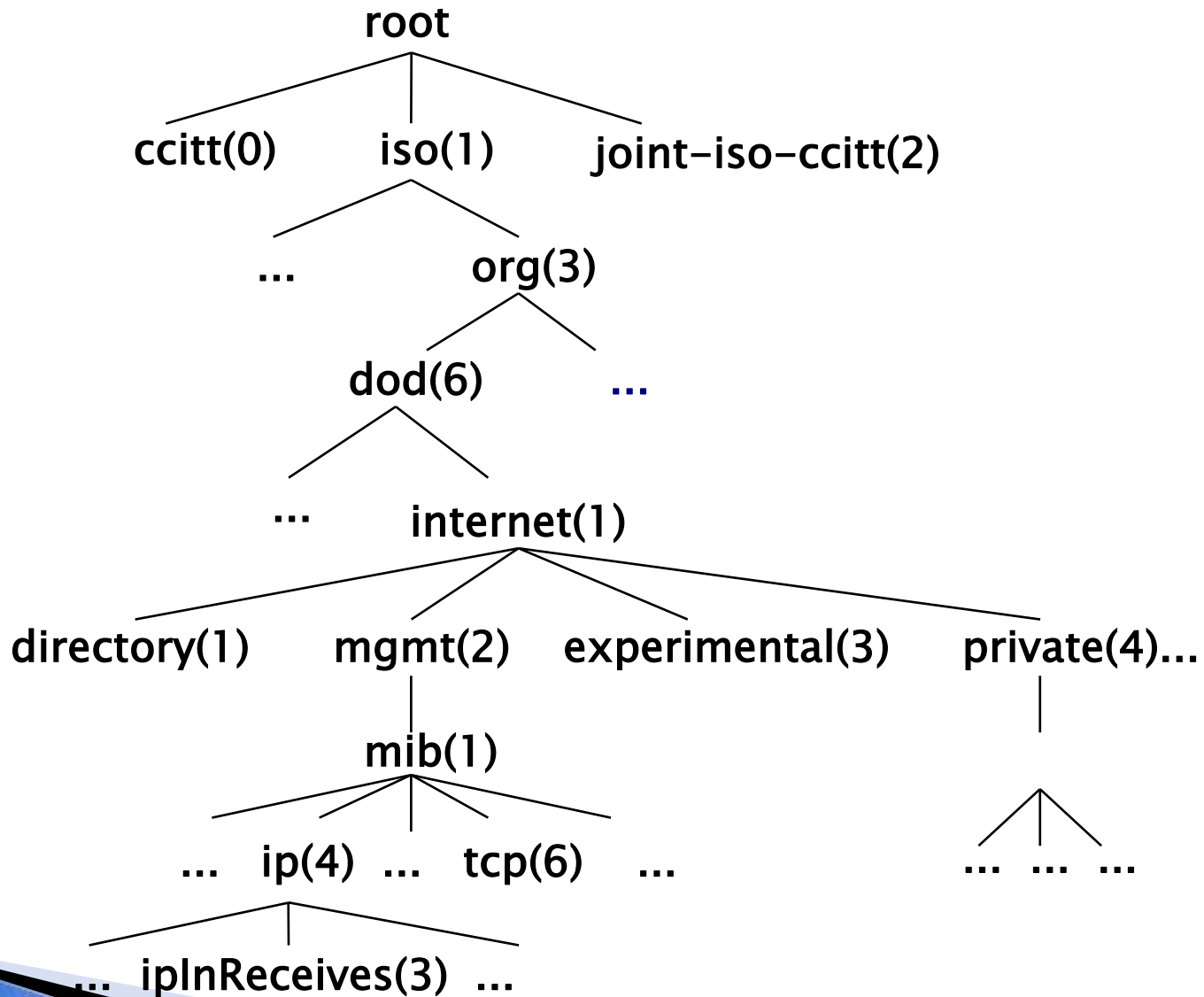
Vocabulaire et Concepts

- ▶ Agent : programme exécuté sur l'équipement à administrer, avec un accès direct aux parties matérielles et logicielles. Interrogé à distance
- ▶ Plate-forme d'administration : logiciel interrogeant via un protocole d'administration propriétaire ou normalisé les agents. Présente les résultats après traitements (moyenne, écart-type...)
- ▶ Informations stockées dans des bases de données
 - Description des objets gérés par les équipements (type, format, taille de ces objets mais pas leurs valeurs). Connue de l'agent et de la plate-forme
 - MIB : Management Information Base
 - Ensemble des infos stockées sur le réseau
- ▶ Proxy : offre d'un côté les fonctions d'un agent et traduit les requêtes venant des plateformes d'administration dans un langage propre au matériel à administrer

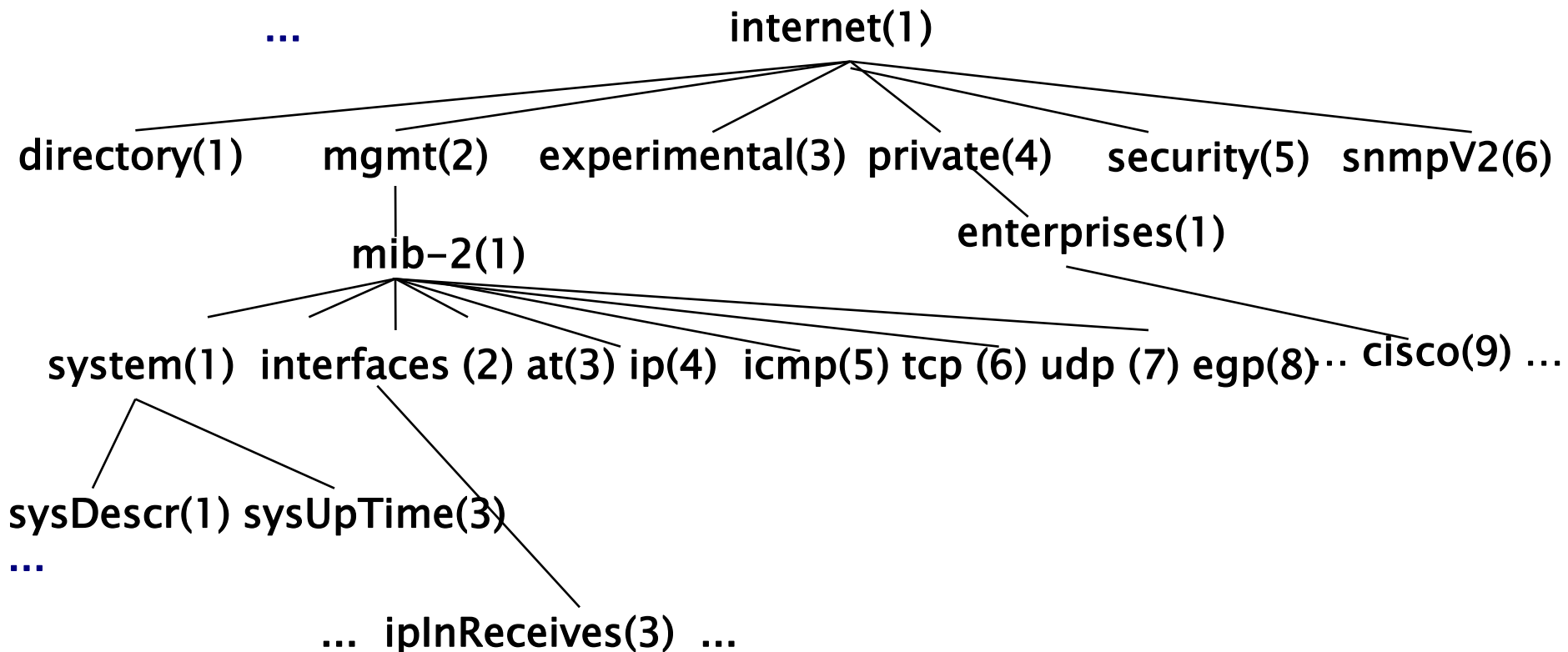
Structure des MIB

- ▶ Organisée hiérarchiquement, de la même façon que l'arborescence des domaines Internet
- ▶ Contient une partie commune à tous les agents SNMP en général, une partie commune à tous les agents SNMP d'un même type de matériel, et une partie spécifique à chaque constructeur
- ▶ Peut contenir
 - Des scalaires (valeur unique)
 - Des tableaux de scalaires
- ▶ Structure normalisée mais également les appellations des diverses rubriques
- ▶ Niveau de la hiérarchie repéré par un index numérique

Espace de nommage de ISO-CCITT



Structure la MIB. Zoom de la branche Internet



Exemple de MIB-Browser – RFC 1213 – MIB-II

The screenshot displays the MG-SOFT MIB Explorer interface. The left pane shows a list of MIB modules, with 'RFC1213-MIB' selected. The central pane shows the tree structure of the MIB-II hierarchy, including 'sysObjectID', 'sysUpTime', 'sysContact', 'sysName', 'sysLocation', 'sysServices', 'interfaces', 'ifNumber', and 'ifTable'. The right pane provides detailed information for the selected module, RFC1213-MIB, including its parent, first child, previous sibling, numerical syntax, base syntax, composed syntax, status, max access, and a list of sequences. The description at the bottom states: 'A list of interface entries. The number of entries is given by the value of ifNumber.'

Module: RFC1213-MIB

Module: (2). ifTable(2)
RFC1213-MIB

Parent: [interfaces](#)
First child: [ifEntry](#)
Previous sibling: [ifNumber](#)

Numerical syntax: Sequence
Base syntax: SEQUENCE OF IfEntry
Composed syntax: SEQUENCE OF IfEntry
Status: mandatory
Max access: not-accessible
Sequences:

- 1: [ifIndex](#) - INTEGER (2 - Integer (32bit))
- 2: [ifDescr](#) - DisplayString (4 - Octets)
- 3: [ifType](#) - INTEGER (2 - Integer (32bit))
- 4: [ifMtu](#) - INTEGER (2 - Integer (32bit))
- 5: [ifSpeed](#) - Gauge (66 - Gauge (32bit))
- 6: [ifPhysAddress](#) - PhysAddress (4 - Octets)
- 7: [ifAdminStatus](#) - INTEGER (2 - Integer (32bit))
- 8: [ifOperStatus](#) - INTEGER (2 - Integer (32bit))
- 9: [ifLastChange](#) - TimeTicks (67 - timeticks)
- 10: [ifInOctets](#) - Counter (65 - cntr32)
- 11: [ifInUcastPkts](#) - Counter (65 - cntr32)
- 12: [ifInNUcastPkts](#) - Counter (65 - cntr32)
- 13: [ifInDiscards](#) - Counter (65 - cntr32)
- 14: [ifInErrors](#) - Counter (65 - cntr32)
- 15: [ifInUnknownProtos](#) - Counter (65 - cntr32)
- 16: [ifOutOctets](#) - Counter (65 - cntr32)
- 17: [ifOutUcastPkts](#) - Counter (65 - cntr32)
- 18: [ifOutNUcastPkts](#) - Counter (65 - cntr32)
- 19: [ifOutDiscards](#) - Counter (65 - cntr32)
- 20: [ifOutErrors](#) - Counter (65 - cntr32)
- 21: [ifOutQLen](#) - Gauge (66 - Gauge (32bit))
- 22: [ifSpecific](#) - OBJECT IDENTIFIER (6 - oid)

Description: A list of interface entries. The number of entries is given by the value of ifNumber.

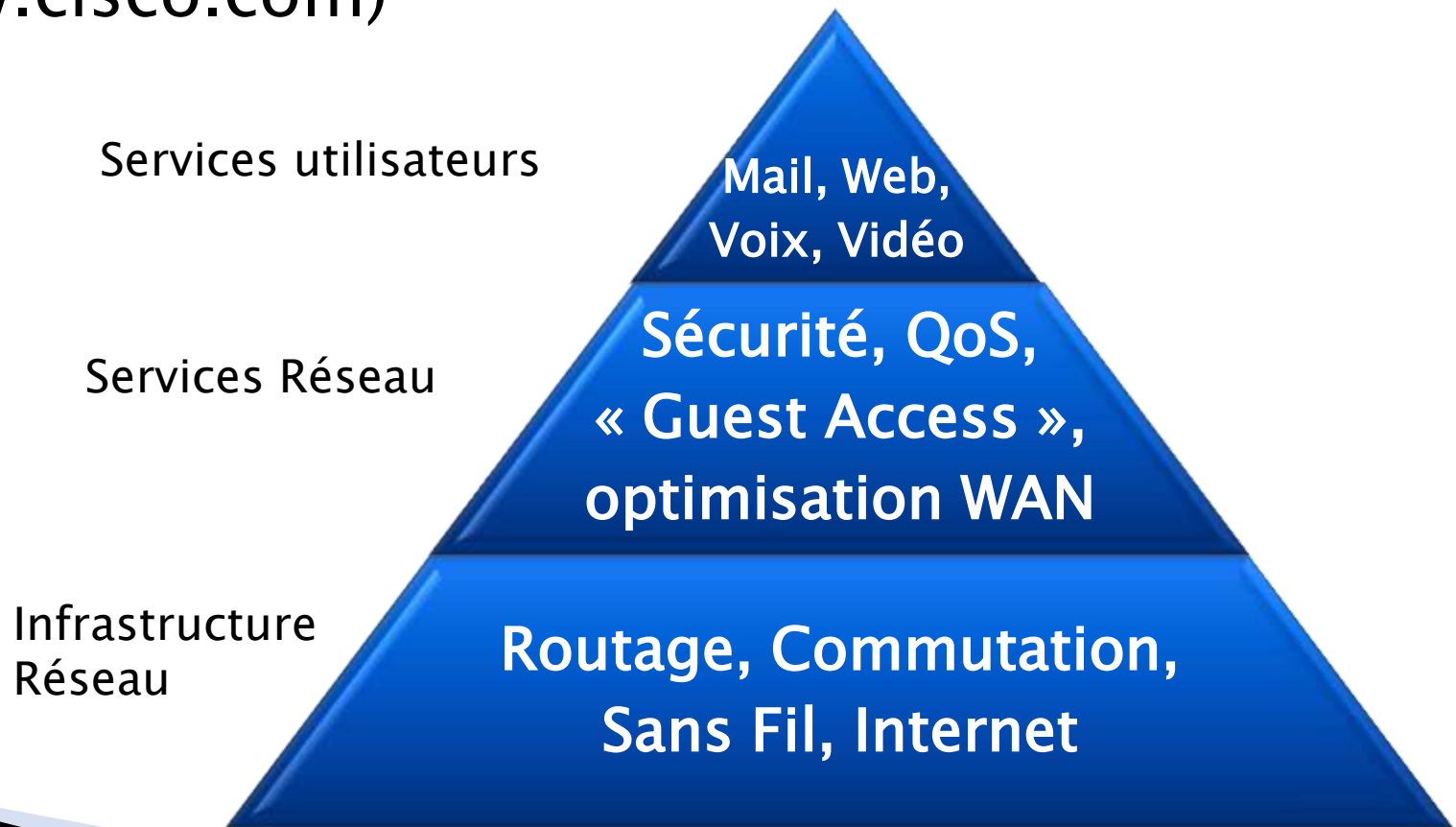
Modules: 98 | Compiled: 97 | Selected: 1

Sommaire

- ▶ Introduction
- ▶ Concepts réseaux
- ▶ Les réseaux d'entreprise/ Les réseaux d'opérateurs
- ▶ Architecture logicielle des réseaux
- ▶ Le modèle OSI
- ▶ Les réseaux locaux (modèle IEEE)
- ▶ L'architecture TCP/IP
- ▶ **Conclusion**
 - Conception du réseau d'entreprise, méthodologie
 - Sécurité, supervision, quelles stratégies ??
- ▶ **Glossaire – Bibliographie**

Architecture Réseau

- ▶ Smart Business Architecture Pyramid (source : www.cisco.com)



Déploiement réseau : quels objectifs ??

- ▶ Facilité de déploiement
- ▶ Flexibilité et « Scalabilité »
- ▶ Disponibilité et Sécurité
- ▶ Facilité de management
- ▶ Architecture évolutive



Conception du réseau d'entreprise

- ▶ Analyse des besoins – Analyse du modèle de trafic réseau
- ▶ Conception de la structure interne du réseau commuté (architecture LAN)
- ▶ Définition de l'architecture physique
- ▶ Définition d'un plan d'adressage IP, choix du protocoles de routage
- ▶ Conception de la ferme de serveurs



Sécurité & Sauvegardes



- ▶ Méthodologie
 - Evaluation des risques, définition des politiques de sécurité. Quelles menaces et quels impacts potentiels ??
 - Quelles solutions ?? Contre-mesures (système de détection d'intrusion, firewall, AAA...)
- ▶ Mise en place de stratégies de sécurité
- ▶ Mise en place de pare-feux (firewalls) pour se protéger des attaques extérieures
- ▶ Installation de systèmes antivirus centralisés ou locaux
- ▶ Planification de sauvegardes quotidiennes
- ▶ Pour les entreprises multisites ou accès nomades : VPN (Virtual Private Network)
 - Tunnel sécurisé avec mécanismes d'authentification

Administration et surveillance du réseau

- ▶ Technologie SIEM (Security Information and Event Management)

Security Information Management	Event Mangement
Collecte de Log, Archivage, Historique, Reporting...	Reporting temps réel, Corrélation d'événements, normalisation, agrégation, collecte de log

- ▶ Outils de supervision de réseau
 - Protocole SNMP (Simple Network Management Protocol)
 - Outils propriétaires (HPOpenView) ou Open Source (Nagios)
- ▶ Outils de gestion de parc informatique

Autres mécanismes

- ▶ Mise en œuvre de la haute disponibilité
 - Définition de haute disponibilité, évaluation et impacts
 - Analyse des éléments de l'architecture
- ▶ Gestion de la Qualité de Service
 - Identification des mécanismes de QOS
 - Quelle architecture ? Composants ??
- ▶ Intégration de services multicast
 - Vidéo

Des Questions ???



Quelques outils de base

- ▶ `Ping` ⇒ Tester le fonctionnement de la pile TCP/IP (protocole IP et ICMP)
- ▶ `ifconfig` (`ipconfig` sous Windows) ⇒ Consultation, configuration des paramètres IP
- ▶ `Traceroute` (`tracert`) ⇒ Détermine le chemin (les adresses de routeurs) traversé par un paquet pour atteindre la destination
- ▶ `Netstat` ⇒ outil permettant de connaître les connexions TCP actives sur la machine sur laquelle la commande est activée et ainsi lister l'ensemble des ports TCP et UDP ouverts sur l'ordinateur
- ▶ `Netstat - r` ou `route print` ⇒ Visualisation des tables de routage
- ▶ `Nslookup`, `Dig` ⇒ Permet d'interroger le serveur DNS pour connaître la correspondance nom de domaine adresse IP
- ▶ `Arp` ⇒ Permet de voir la cache ARP et faire la translation adresse IP / adresse MAC
- ▶ Analyseur de trames : **Wireshark**, `tcpdump`, `iptraf`...

Glossaire

- ▶ **ADSL** Asymmetric Digital Subscriber Line
- ▶ **AFNIC** Association Française pour le Nommage Internet en Coopération
- ▶ **AFNOR** Association Française de NORmalisation
- ▶ **ANSI** American National Standard Institute
- ▶ **ARP** Address Resolution Protocol
- ▶ **ASN 1** Abstrac Syntax Notation 1
- ▶ **ATM** Asynchronous Transfer Mode
- ▶ **CSMA/CD** Carrier Sense Multiple Access with Collision Detection
- ▶ **DHCP** Dynamic Host Configuration Protocol
- ▶ **DNS** Domain Name System
- ▶ **DSLAM** DSL Access Multiplexer, équipement situé à l'autre bout de la ligne téléphonique, reliant tous les modems ADSL reliés à ce central
- ▶ **ETCD** Equipement Terminal de Circuit de Données (Ang. DCE)
- ▶ **ETTD** Equipement Terminal de Traitement de Données (Ang. DTE)
- ▶ **FCS** Frame Control Sequence
- ▶ **FTP** File Transfer Protocol
- ▶ **FTTB** fibre jusqu'à l'immeuble (Fiber To The Building)
- ▶ **FTTC** fibre sur le trottoir (Fiber To The Curb)
- ▶ **FTTD** fibre jusqu'au bureau (Fiber To The Desk)
- ▶ **FTTH** fibre chez l'abonné (Fiber To The Home)
- ▶ **FTTLa** fibre jusqu'au dernier amplificateur (Fiber To The Last Amplifier)

Glossaire

- ▶ **FITL** fibre dans la boucle locale (Fiber In The Loop)
- ▶ **HTTP** HyperText Transfer Protocol
- ▶ **ICMP** Internet Control Message Protocol
- ▶ **IEEE** Institute of Electrical and Electronics Engineers
- ▶ **IGMP** Internet Group Message Protocol
- ▶ **IMAP** Interactive Mail Access Protocol
- ▶ **IOS** Internetwork Operating System (Cisco)
- ▶ **IP** Internet Protocol
- ▶ **ISDN** Integrated Service Digital Network
- ▶ **ISO** International Standardization Organisation
- ▶ **LAN** Local Area Network
- ▶ **LLC** Logical Link Control
- ▶ **MAC** Medium Access Control
- ▶ **MAN** Metropolitan Area Network
- ▶ **MPLS** Multi Protocol Label Switching
- ▶ **MTU** Maximum Transmission Unit
- ▶ **NAT** Network Address Translation
- ▶ **NFS** Network File System
- ▶ **OSI** Open System Interconnection
- ▶ **PDH** Plesiochronous Digital Hierarchy
- ▶ **POP** Post Office Protocol

Glossaire

- ▶ **PPP** Point to Point Protocol
- ▶ **RADIUS** Remote Access Dial-in User Service
- ▶ **RARP** Reverse Address Resolution Protocol
- ▶ **RFC** Request For Comment
- ▶ **RIP** Routing Information Protocol
- ▶ **RNIS** Réseau Numérique à Intégration de Services
- ▶ **RPC** Remote Procedure Call
- ▶ **RTC** Réseau Téléphonique Commuté
- ▶ **SDH** Synchronous Digital Hierarchy
- ▶ **SMTP** Simple Mail Transfer Protocol
- ▶ **SNMP** Simple Network Management Protocol
- ▶ **TCP** Transport Control Protocol/Internet Protocol
- ▶ **UDP** User Datagram Protocol
- ▶ **UIT-T** Union Internationale des Télécommunications ex CCITT
- ▶ **WAN** Wide Area Network
- ▶ **WITL** Wireless In The Loop
- ▶ **xDSL** Terme générique regroupant toutes les technologies DSL

Bibliographie

▶ Les « bibles » réseau

- Les réseaux de Guy Pujolle (Eyrolles)
- Réseaux de Andrew Tannenbaum (Prentice Hall – InterEditions)
- Réseaux et Télécoms de Claude Servin (Dunod)
 - et...
- Les Réseaux – Principes fondamentaux de Pierre Rollin – Gilbert Martineau – Laurent Toutain – Alain Leroy (Réseaux & Télécommunications – Hermes)
- Réseaux Locaux et Internet de Laurent Toutain (Réseaux & Télécommunications – Hermes)
- ...



- ▶ Nombreuses sources Internet...
- ▶ RFC disponibles sur le net