

Protocoles et Internet

M1 option RX

Sondes Kallel

Organisation

- 12 heures de cours (6 séances de 2h)
 - 5 cours de 2h heures
 - Partie 1-2 : Introduction
 - Partie 3 : Algorithmes de routage et protocoles de routage
 - Séance 4 : 1 CC
 - Partie 4 : RIP
 - Partie 5 : OSPF
 - 6 séances de TDs/TPs de 4 heures
 - TD Théorique sur l'adressage et le routage
 - Pratiques sur les routeurs Cisco en salle TP (401/402)
- Contrôle Continue (séance 4 du cours à confirmer)



Organisation

- 6 séances de TDs/TPs de 4 heures
 - TD1 : Théorique sur l'adressage et le routage
 - TD2 : Exercices routage sur Packet tracer
 - TD3 : configuration des paramètres de base d'un routeur
 - TD4 : Interconnexion de réseaux : Routage Statique sur Matériel CISCO
 - TD5 : Routage Dynamique RIP sur CISCO
 - TD6 : Routage Dynamique OSPF sur CISCO

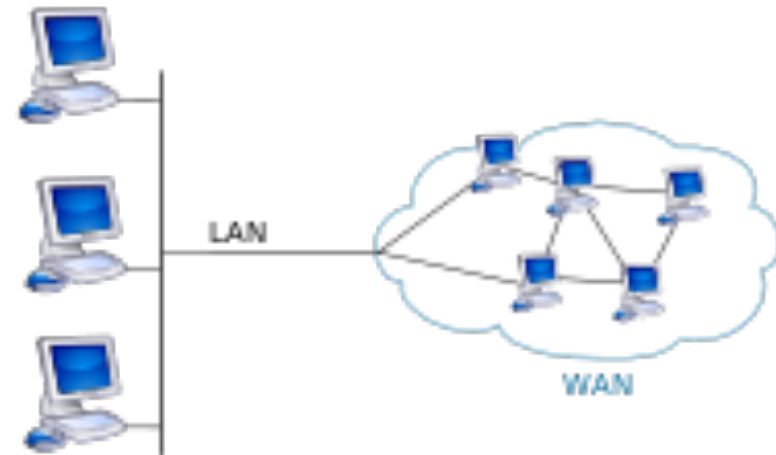


Plan

- Introduction
 - Internet / Modèle OSI
 - Couche réseau et adressage
 - Fonction de routage et table de routage
- Algorithmes de routage et protocoles de routage
 - Classification
 - Routage statique
- Le protocole de routage RIP
- Le protocole de routage OSPF
- Les protocoles de routage BGP/EIGRP

Introduction

- Un réseau étendu, souvent désigné par son acronyme anglais WAN (Wide Area Network), est un réseau informatique couvrant une grande zone géographique, typiquement à l'échelle d'un pays, d'un continent, voire de la planète entière. Le plus grand WAN est le réseau **Internet**.
 - Internet ? Protocole ?





Plan

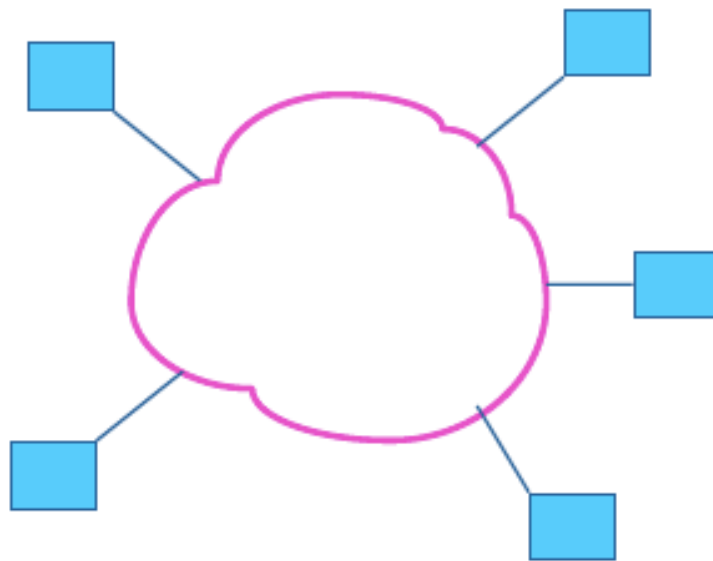
- Bordure du réseau
 - Applications
 - Terminaux
 - Protocoles de transport de bout-en-bout
- Cœur du réseau
 - Routeurs
 - Liens physiques



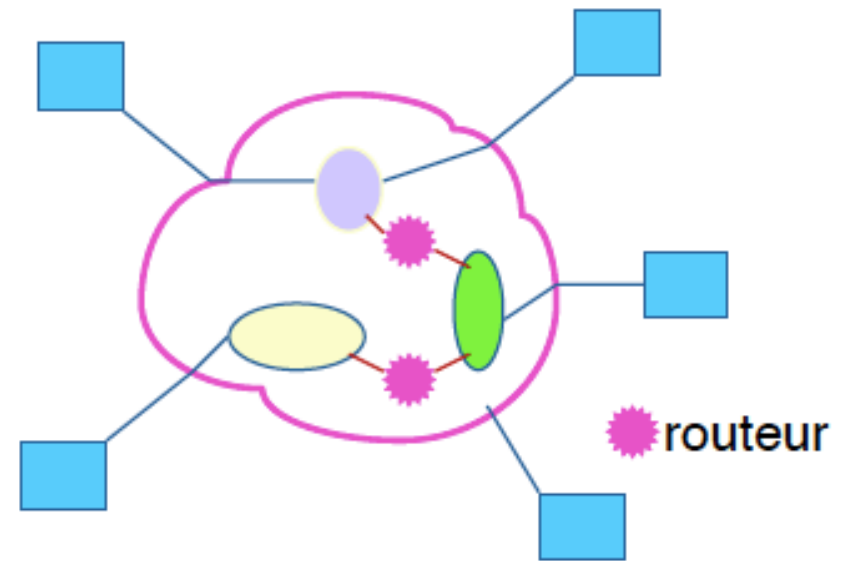
Qu'est ce qu'Internet ? 3 définitions

1. Une famille de protocoles de communication, appelée :
 - TCP / IP : Transmission Control Protocol / Internetworking Protocol
2. Un réseau mondial constitué de milliers de réseaux hétérogènes, et interconnecté au moyen des protocoles TCP/IP :
 - Réseaux locaux d'agences gouvernementales, institutions d'éducation, hôpitaux, des commerciaux, ...
 - Réseaux fédérateur de Campus,
 - Réseaux Régionaux, Nationaux, Intercontinentaux (Américains, Européen, EUNET, Ebone, Asiatiques, ...)
3. Une communauté de personnes utilisant différents services
 - Courrier électronique, Web, Transfert de fichiers FTP, ...

Structure Physique de l'INTERNET



Vue utilisateur



Vue réelle du réseau



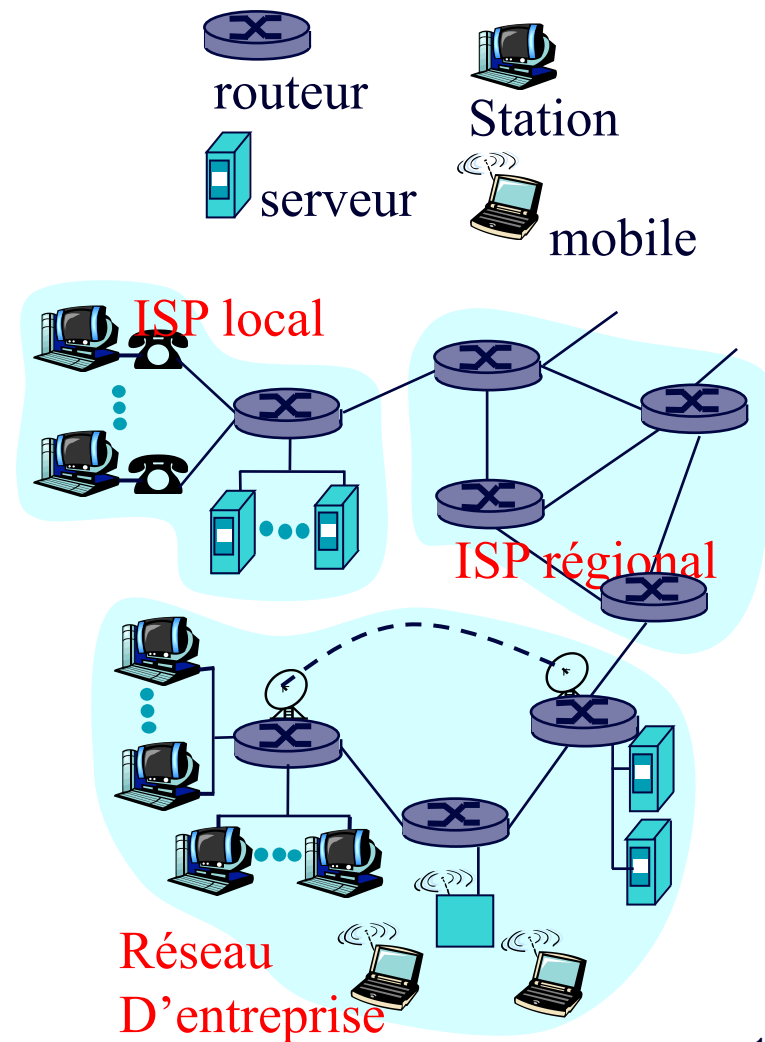
Qu'est ce qu'un Intranet ou Extranet ?

- Intranet : un réseau d'entreprise dans lequel les mêmes technologies et protocoles que l'Internet sont mis en oeuvres
 - Routeurs, protocoles TCP/IP, protocoles applicatifs : email, web, ...
- Extranet : un Intranet qui offre des accès distants aux usagers/employés/partenaires de l'entreprise
 - Problème de sécurité

Qu'est ce qu'Internet ?

Les composants

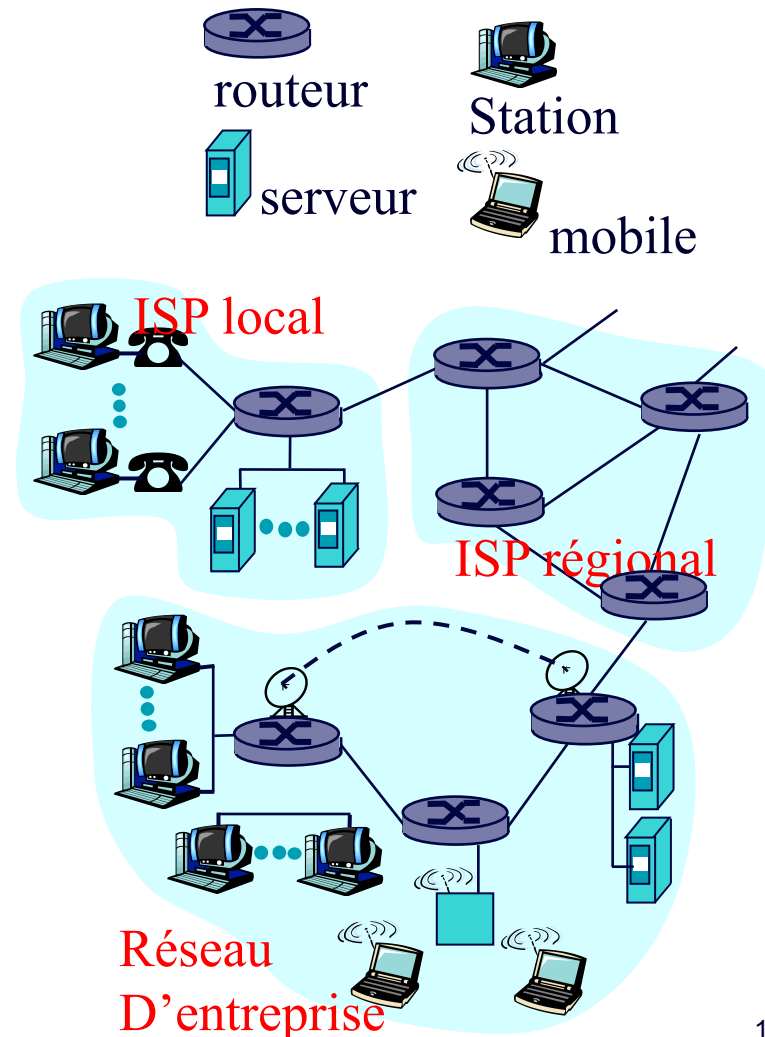
- Des millions de machines interconnectées...
 - Hôtes {
 - PCs, stations de travail, serveurs
 - PDAs, téléphones, grille-pain (!)
- ...exécutant des applications réseaux
- Protocoles : contrôle de l'émission et de la réception des infos
 - TCP, IP, HTTP, FTP...
- Liens de communication : fibre optique, cuivre, radio, satellite...
- Routeurs : transfèrent des paquets de données dans le réseau



Qu'est ce qu'Internet ?

Les composants

- **Commutation de paquets**
 - Partage des ressources
- **Internet = réseau de réseaux**
 - Contraintes : IP + conventions de nommage et d'adressage
 - Topologie : hiérarchique (ISPs...)

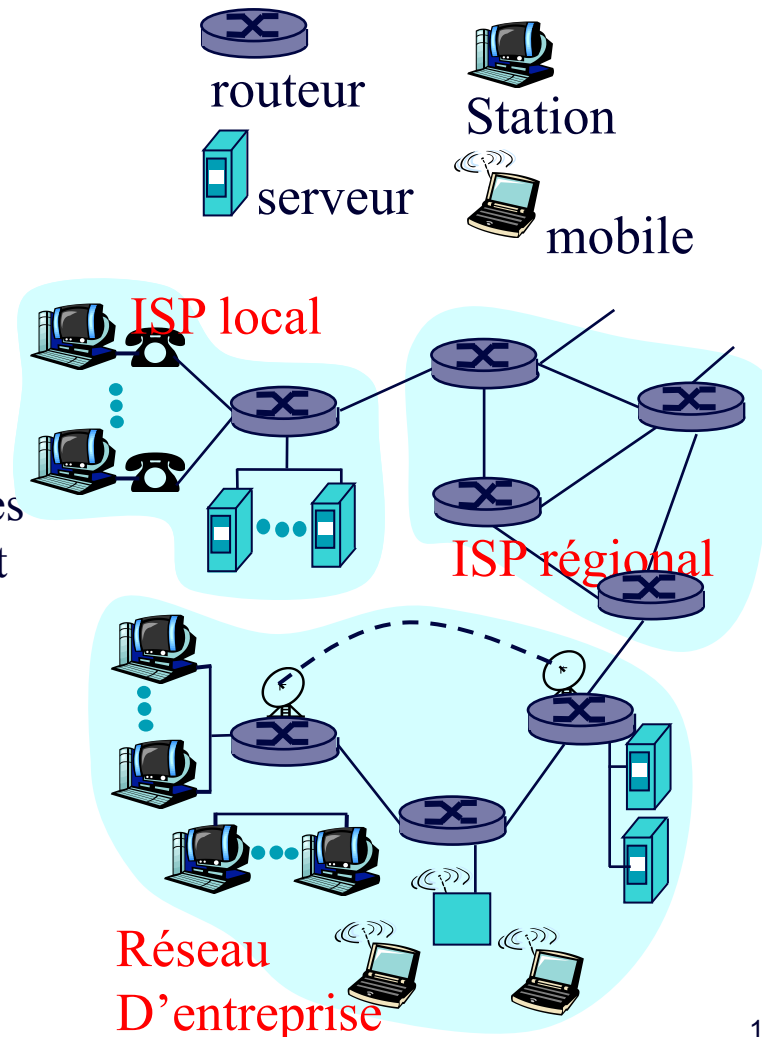


Qu'est ce qu'Internet ?

Les composants

□ Standards Internet

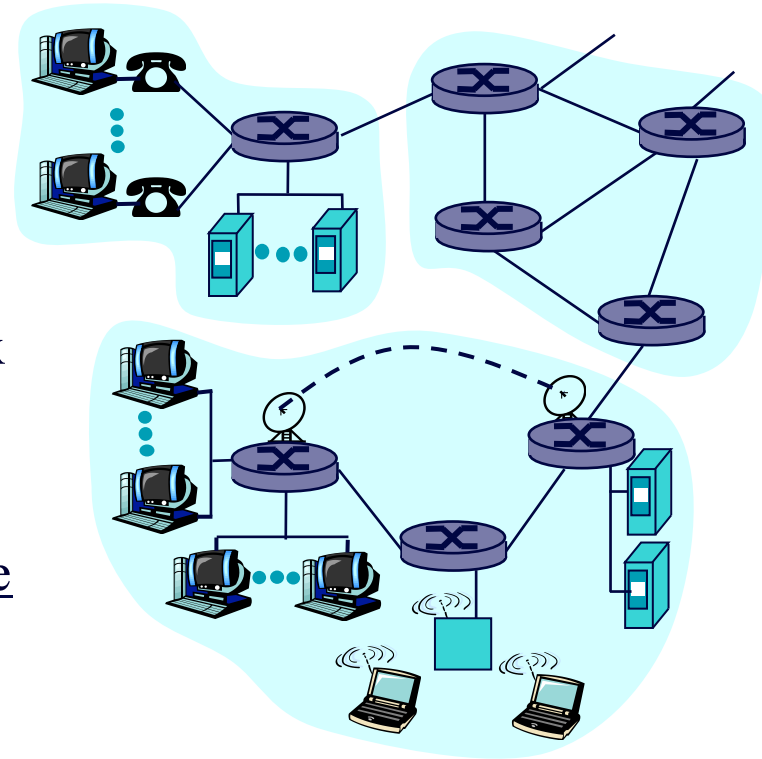
- Développés par l'IETF : Internet Engineering Task Force
- Documents = RFC : Request For Comments
 - Au départ pour résoudre les problèmes d'architecture du précurseur d'Internet
 - Aujourd'hui : considérés comme des standards
 - Documents techniques et détaillés définissant les protocoles tels que HTTP, TCP, IP...
 - + de 2000 RFCs



Qu'est ce qu'Internet ?

Les services

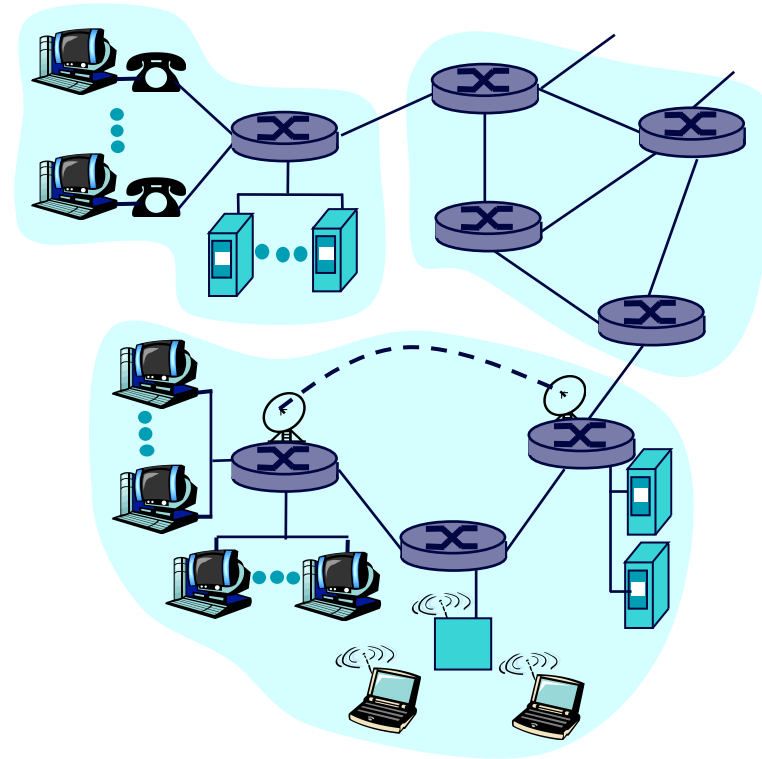
- **L'infrastructure de communication décentralisée** : rend possibles les applications distribuées :
 - Login distant, transfert de fichiers, streaming audio et vidéo, visioconférences, WWW, e-mail, jeux en réseau, e-commerce, bases de données, vote, ...
 - Pourquoi le Web fonctionne-t-il sur ce réseau ?
 - Seul réseau à commutation de paquets permettant d'interconnecter autant de machines
 - Nombre de machines connectés ?



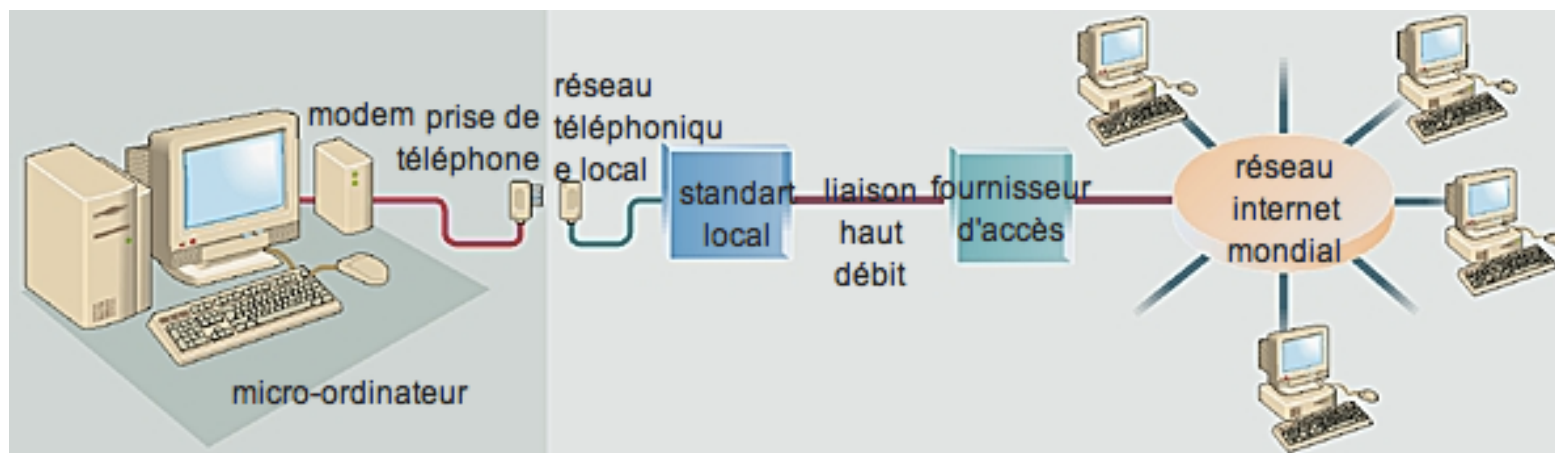
Qu'est ce qu'Internet ?

Les services

- **Services de communication offerts :**
 - Sans connexion
 - Orientés connexion
 - Chaque application utilise l'un de ces services
- **Pas de garantie en terme de délais**
 - ... même en payant !
- **Internet = infrastructure** sur laquelle de nouvelles applications sont constamment inventées et déployées
- **Cyberspace** [Gibson]:
 - “a consensual hallucination experienced daily by billions of operators, in every nation,”
 - “une hallucination consensuelle vécue quotidiennement en toute légalité par des dizaines de millions d'opérateurs, ...”

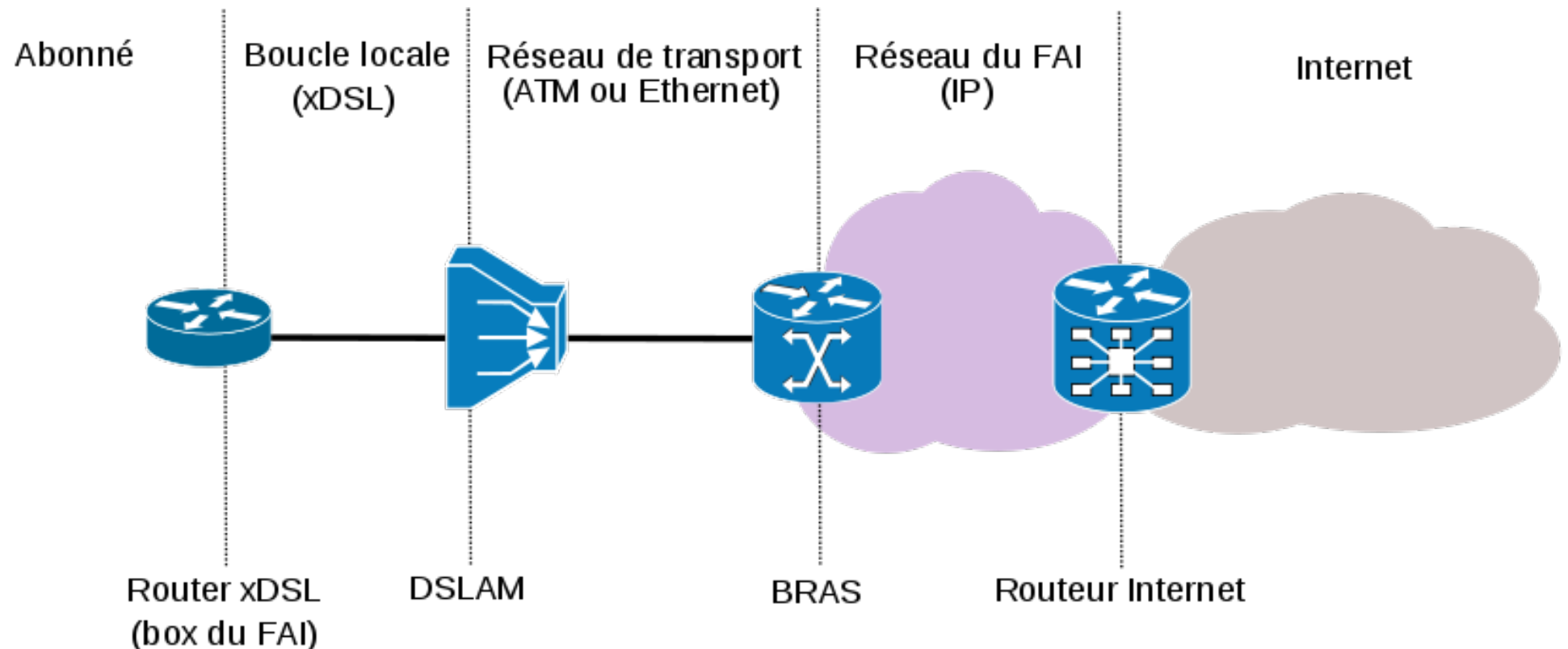


Fonctionnement de l'Internet



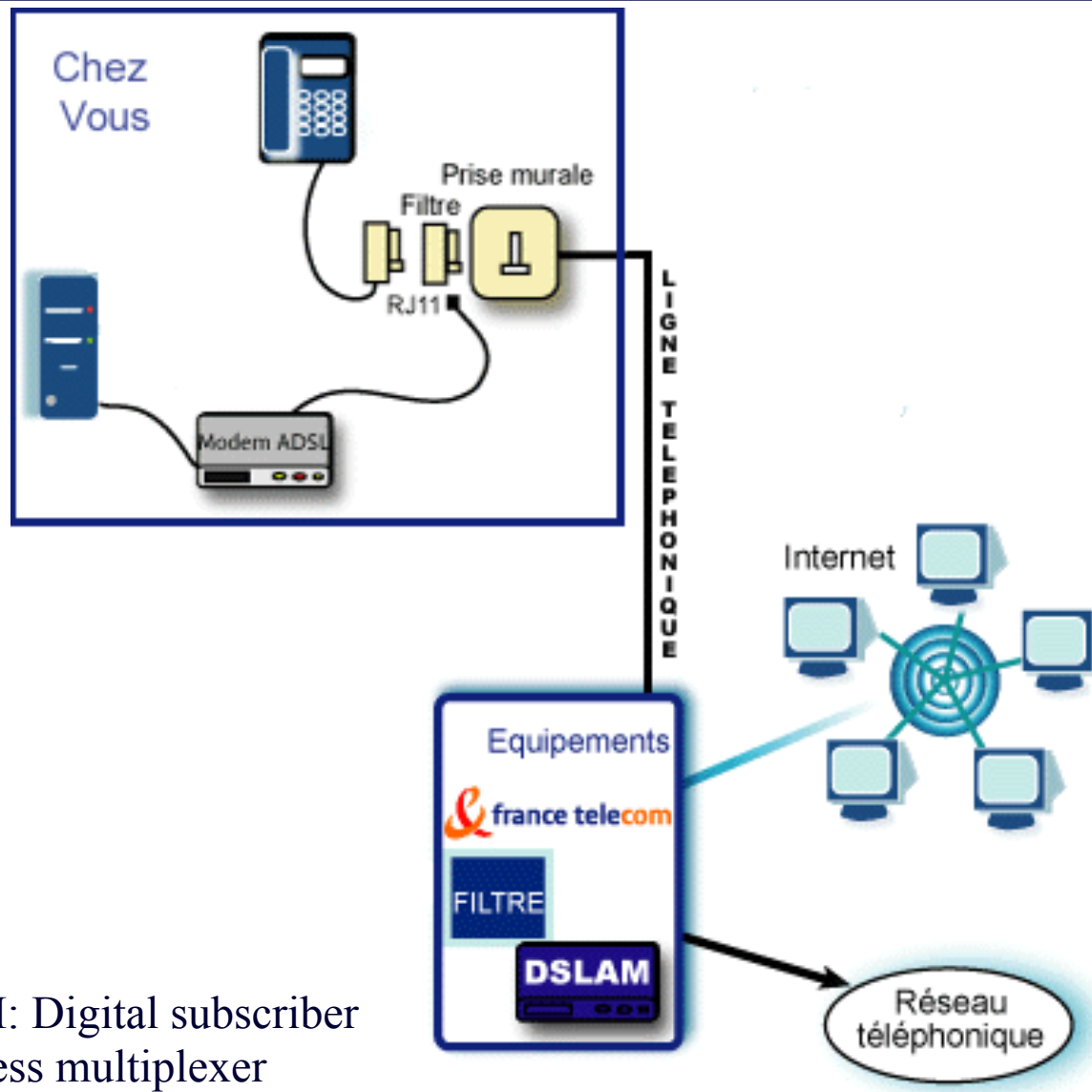
- Principe de fonctionnement. L'internaute connecte au réseau son terminal, micro-ordinateur ou Webphone, grâce à un modem. La communication est alors établie avec un fournisseur d'accès, plate-forme indispensable pour naviguer sur le Web et consulter son dossier électronique.

Accès à Internet aujourd'hui depuis chez vous



DSLAM: Digital subscriber line access multiplexer
DSL : Digital subscriber line

Accès à Internet aujourd'hui depuis chez vous



DSLAM: Digital subscriber
line access multiplexer



Voilà !

- Description d'Internet
 - Composants (hardware / software)
 - Services fournis aux applications distribuées

Liens utiles

- <http://www.ietf.org>
 - IETF
- <http://www.isoc.org>
 - Internet Society
- <http://www.w3.org>
 - World Wide Web Consortium
- <http://www.ieee.org>
 - IEEE (Institute of Electrical and Electronics Engineers)
- <http://www.acm.org>
 - ACM (Association for Computing Machinery)

Qu'est ce qu'un protocole ?

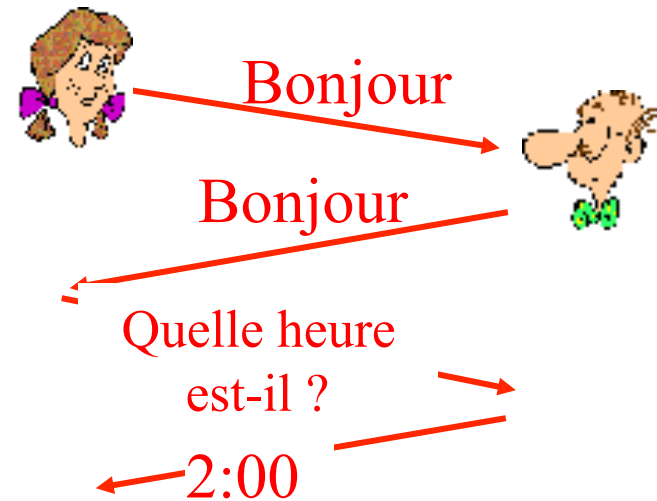
Les humains utilisent des protocoles sans arrêt...

Protocoles humains :

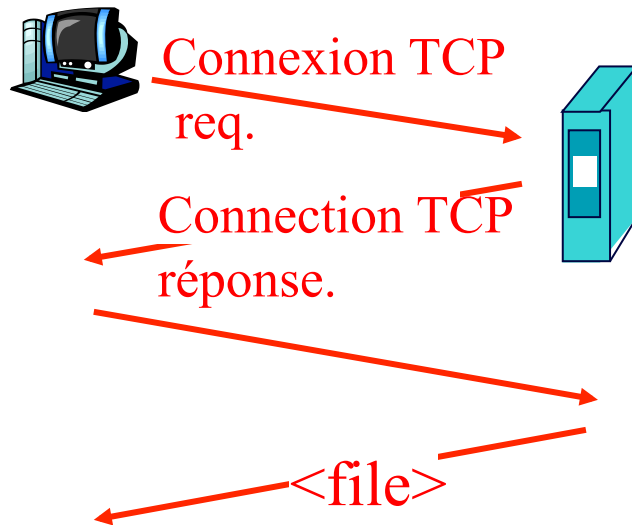
- “Quelle heure est-il ?”
- “J’ai une question”

... Messages spécifiques émis

... Actions spécifiques accomplies après réception de messages ou d'événements particuliers



Qu'est ce qu'un protocole ?



Protocoles réseau :

- ❑ Relient des machines
- ❑ Toutes les communications sur Internet sont gouvernées par des protocoles
- ❑ Les machines qui communiquent doivent utiliser le même protocole

Qu'est ce qu'un protocole ?

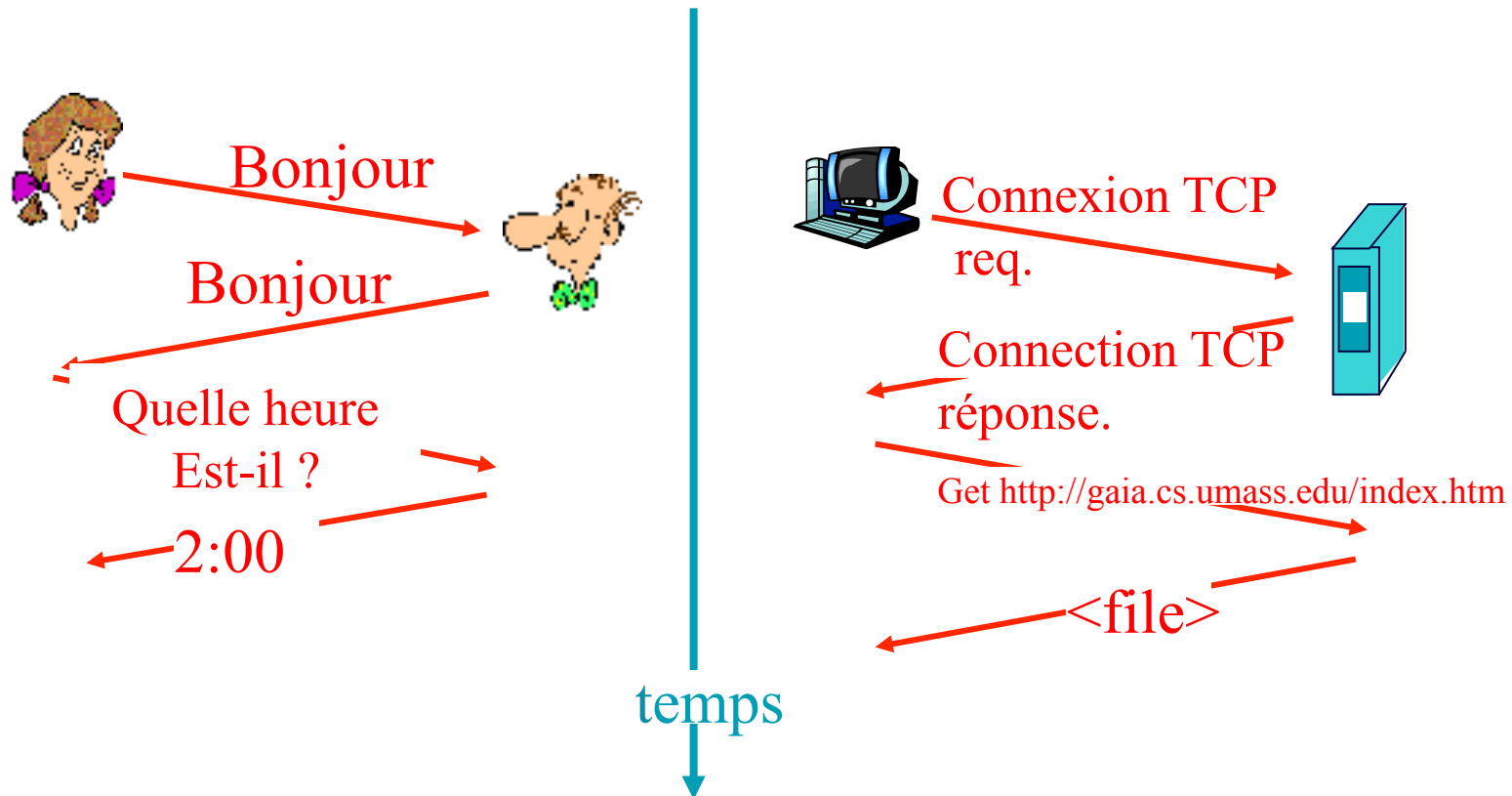
Protocoles de réseau :

- ❑ Dans les routeurs : déterminent le chemin d'un paquet de la source à la destination
- ❑ Au niveau physique : contrôlent le flot de bits sur le support entre 2 machines
- ❑ Protocoles de contrôle de congestion : contrôlent le débit d'émission des paquets transmis
- ❑ Protocole HTTP
- ❑ ...

Les protocoles définissent le format, l'ordre des messages émis et reçus entre les entités réseaux, ainsi que les réactions à ces messages et aux événements

Qu'est ce qu'un protocole?

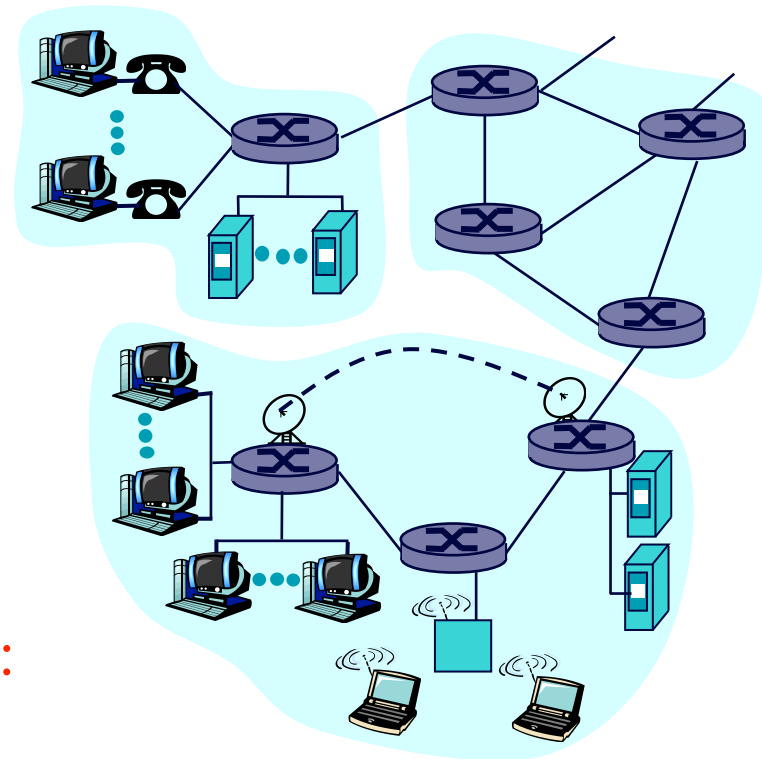
Un protocole humain et un protocole réseau:

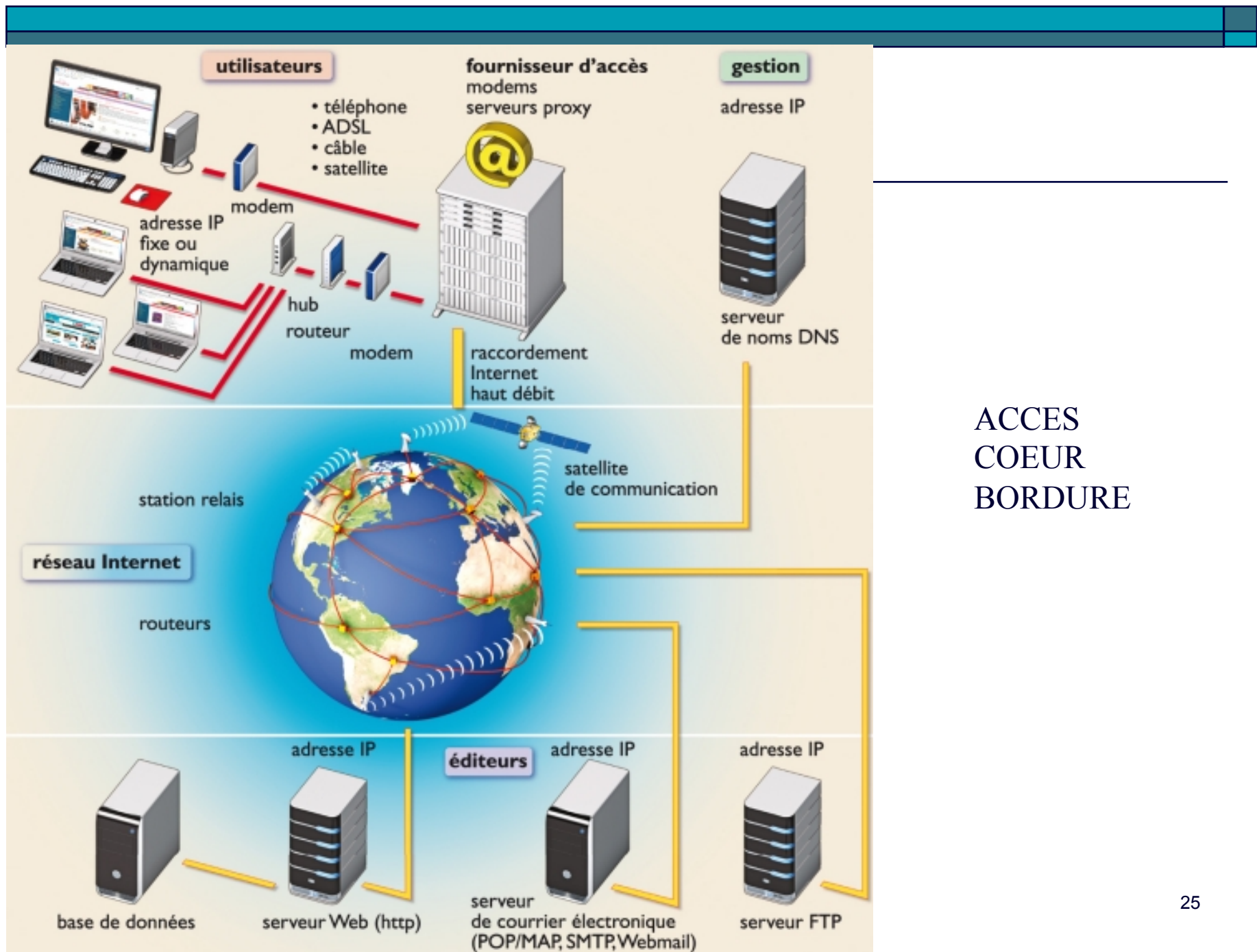


Format, Ordre et Réactions à ces messages et aux événements

Précisions sur l'architecture du réseau :

- Description de "haut niveau"
- Bordure du réseau:
 - Applications et hôtes
- Cœur du réseau:
 - Routeurs
 - Réseau de réseaux
- Réseaux d'accès, liens physiques :
 - Liens de communication
 - ISP (Internet Service Provider)
 - Réseau permettant aux terminaux de se connecter à Internet

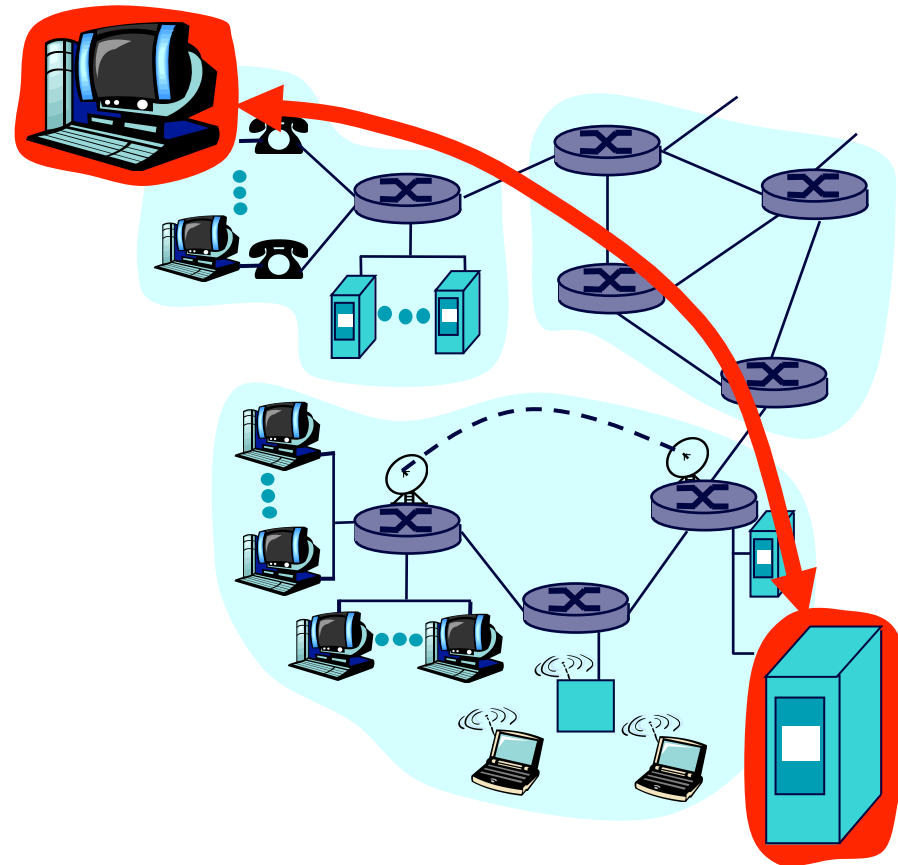




ACCES
COEUR
BORDURE

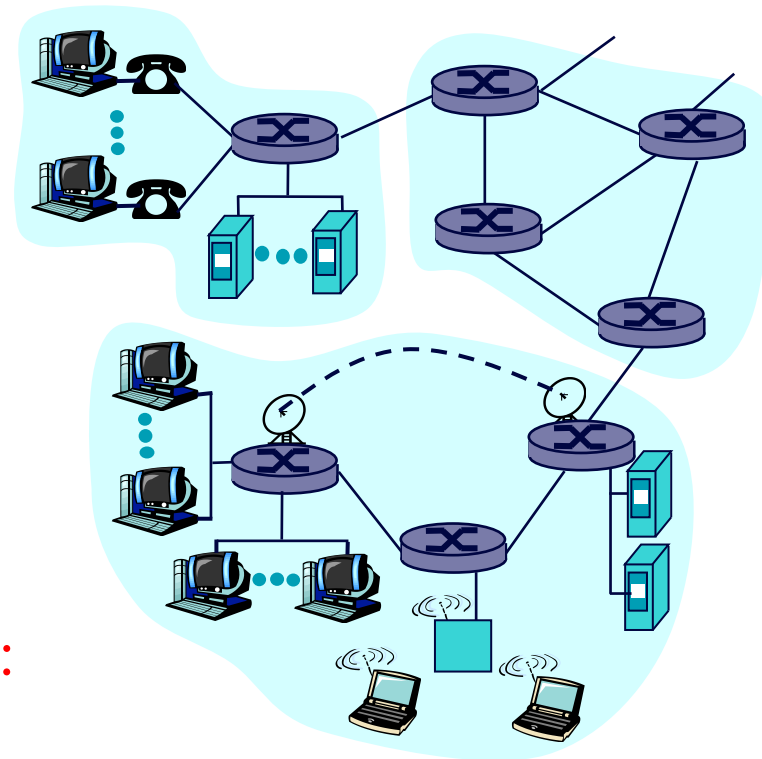
Bordure du réseau :

- **Terminaux (hôtes):**
 - "hébergent" et exécutent des applications
 - Ex : WWW, email, remote login, FTP...
 - au "bord du réseau"
 - PC, station, appareil photo, PDA, Web TV...
- **Modèle peer-peer :**
 - Interaction symétrique entre les hôtes
 - Ex : visioconférence
- **Modèle client/serveur**
 - Le client demande (requiert), le serveur fournit un service
 - Ex : WWW client (browser)/ serveur
email client/serveur
 - P2P : l'hôte est à la fois client et serveur



Précisions sur l'architecture du réseau :

- Description de "haut niveau"
- Bordure du réseau:
 - Applications et hôtes
- Cœur du réseau:
 - Routeurs
 - Réseau de réseaux
- Réseaux d'accès, liens physiques :
 - Liens de communication
 - ISP (Internet Service Provider) ou FAI
 - Réseau permettant aux terminaux de se connecter à Internet



Cœur du réseau

- Ensemble de routeurs interconnectés
- **Question fondamentale :**
Comment les données sont-elles transmises sur le réseau ?

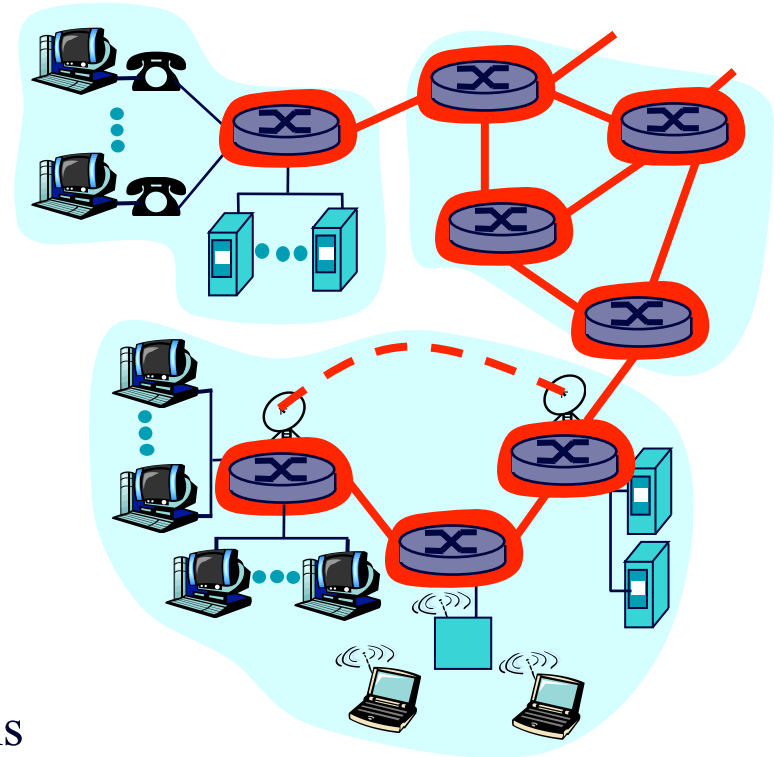
- **Commutation de circuits :**

- Réserve des ressources :
circuit dédié pour chaque appel
- Ex : réseau téléphonique

- **Commutation de paquets :**

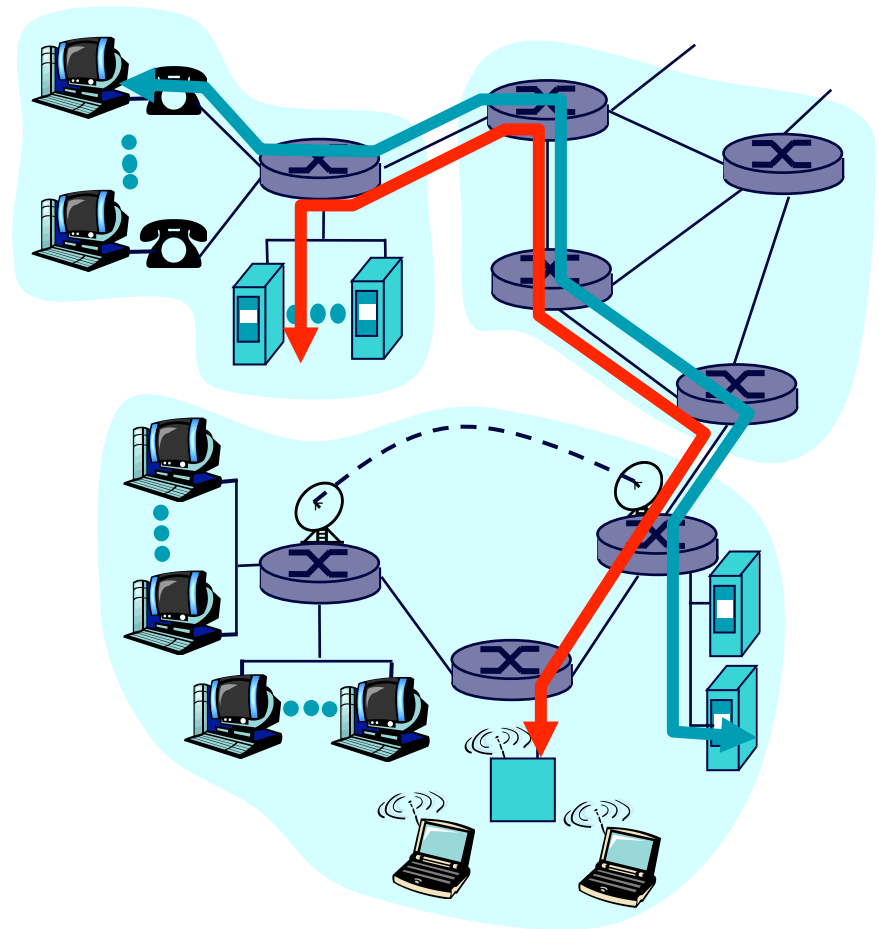
- Les données sont transmises
dans le réseau en paquets
- Pas de réservation des ressources
- Pas de garanties
 - Internet : *Best-effort*

- Certains réseaux de télécommunications
sont difficiles à classer : réseaux ATM



Cœur du réseau : Commutation de Circuits

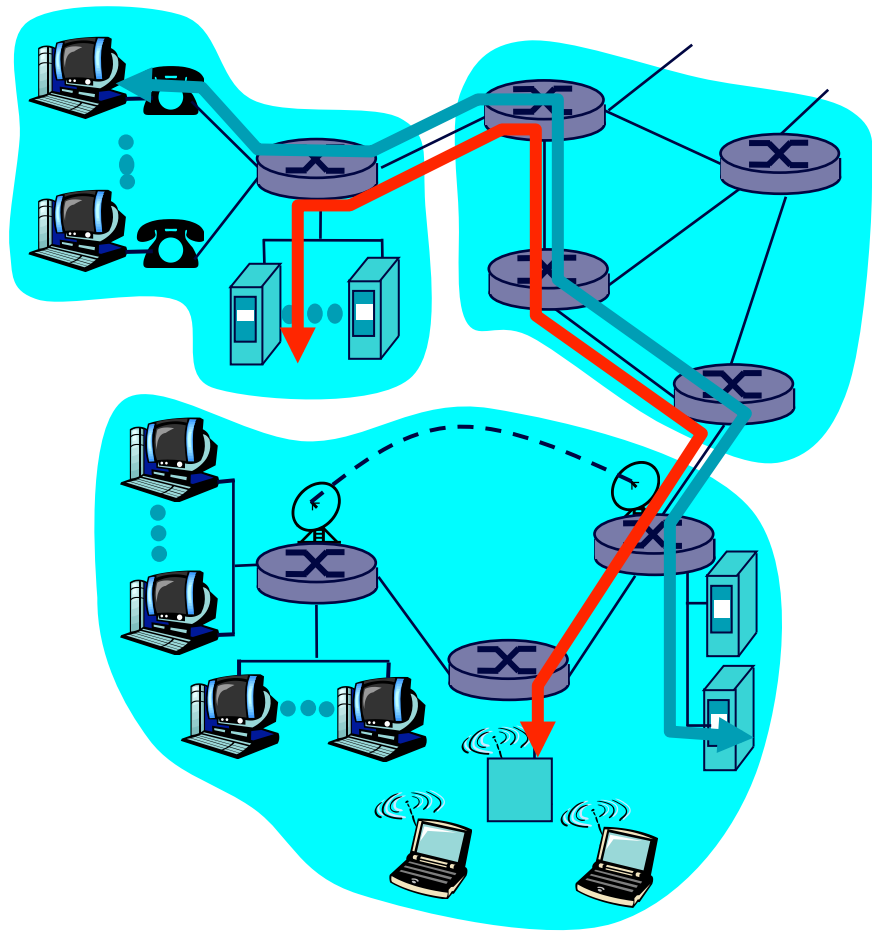
- **Réservation de ressources de bout-en-bout pour chaque «appel»**
 - Bande passante du lien, capacité du lien
 - Ressources dédiées : sans partage
 - Performances garanties (débit)
 - Nécessite l'établissement de la connexion
 - 1 connexion = 1 circuit
 - Les routeurs maintiennent un état de la connexion



Réseau coeur: commutation de Circuits

ressources réservées de
bout en bout par
“appel”

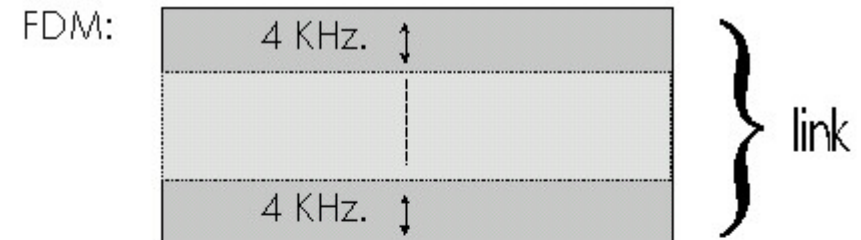
- ❑ bande passante de lien, capacité de commutation
- ❑ ressources: non partagées
- ❑ initialisation de l'appel demandé



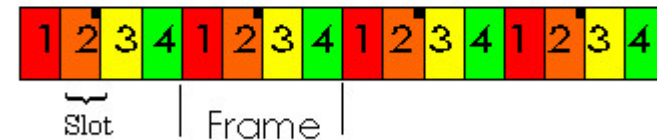
Cœur du réseau : Commutation de Circuits

Ressources réseau (bande passante) **partitionnées**

- Parties allouées aux appels
- Ressources *inutiles* si elles ne sont pas utilisées par l'appel (*pas de partage*)
- Division de la bande passante
 - Division fréquentielle
 - Division temporelle= multiplexage



TDM:



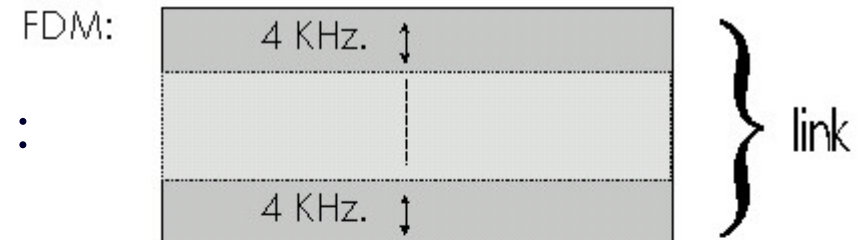
All slots labelled **2** are dedicated to a specific sender-receiver pair.

Cœur du réseau : Commutation de Circuits

□ Multiplexage

- *Division fréquentielle de la BP :*
FDMA

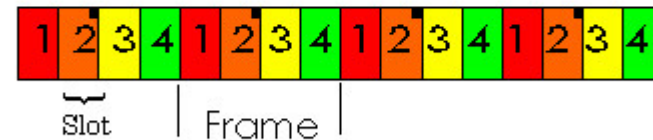
(Frequency-division Multiplexing)



- *Division temporelle de la BP :*
TDMA

(Time-Division Multiplexing)

TDM:



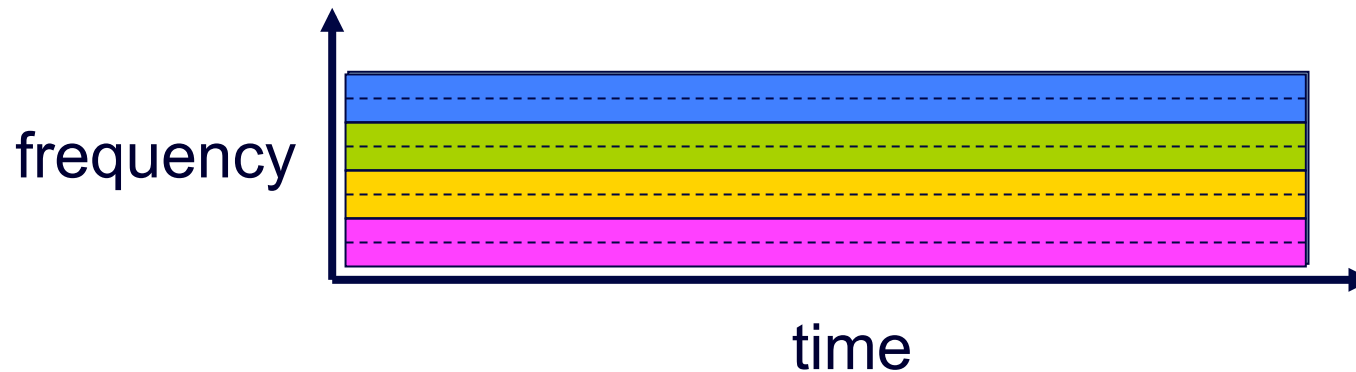
All slots labelled  are dedicated to a specific sender-receiver pair.

Commutation de Circuits: FDMA et TDMA

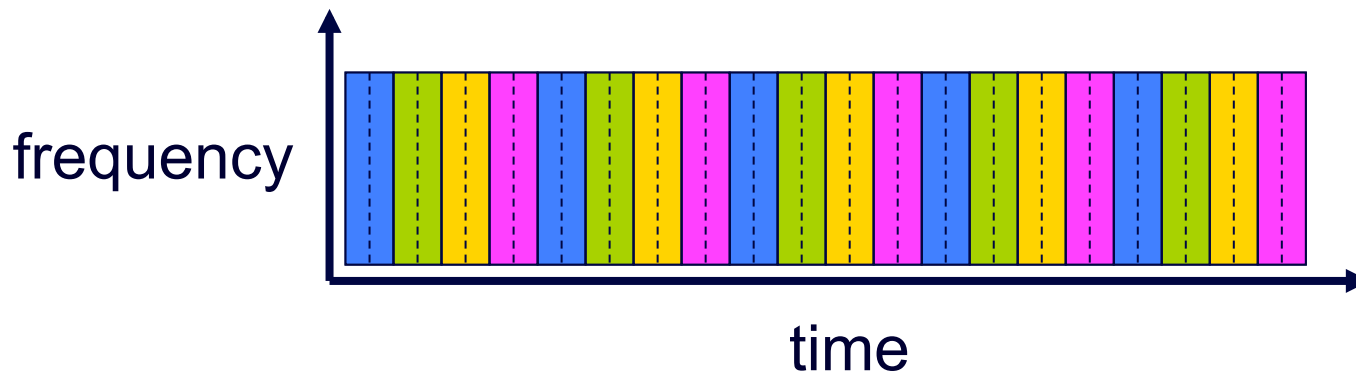
FDMA

Example:

4 users



TDMA





Cœur du réseau : commutation de paquets

- Les protocoles applicatifs échangent des messages

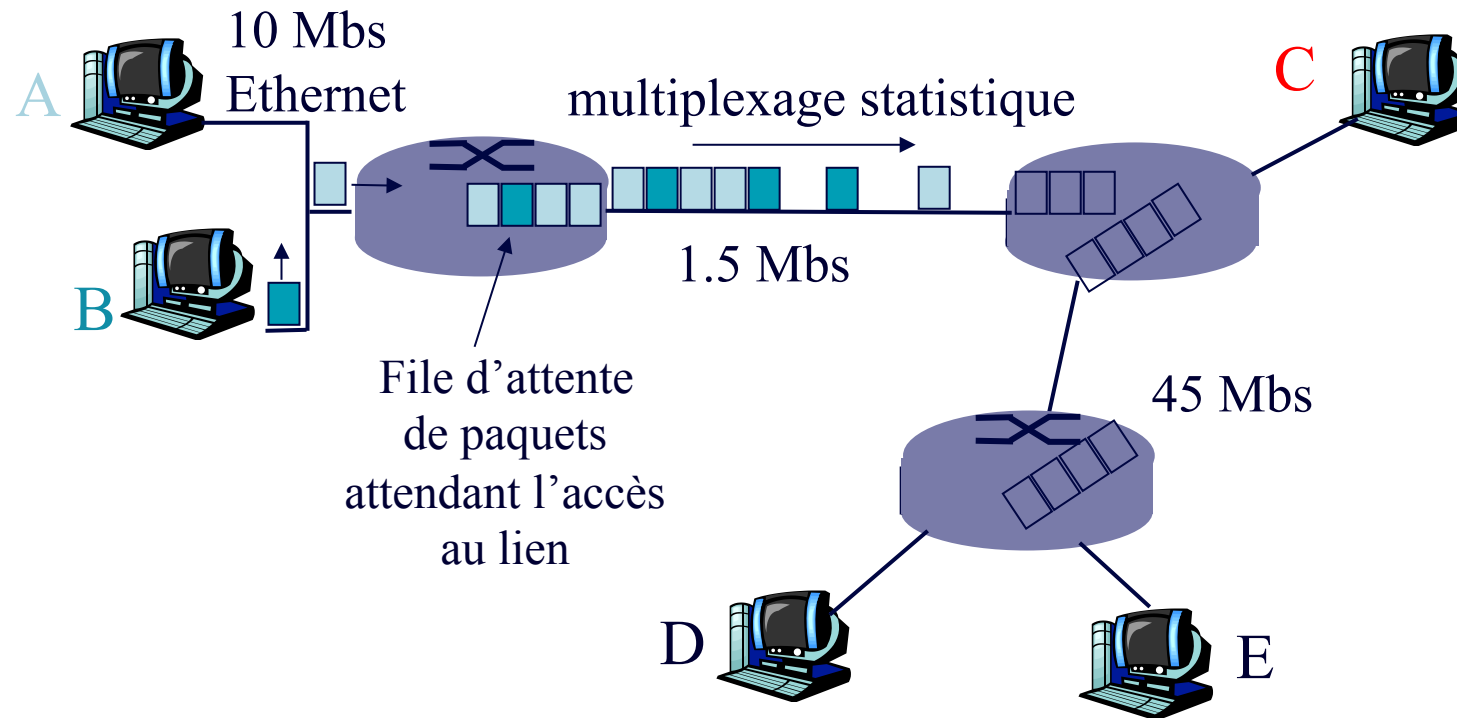
Les messages contiennent tout ce que le concepteur du protocole souhaite

- Fonctions de contrôle ("Hi!" = handshake)
- Données (fichier ASCII)

- Réseaux à commutation de paquets : messages longs divisés en paquets plus petits

- Les paquets traversent les liens de communication et les routeurs

Cœur du réseau : commutation de paquets



Les Séquences de paquets A & B n'ont pas les mêmes intervalles de temps alloués ➡
multiplexage statistique.

Réseau coeur: commutation par paquets

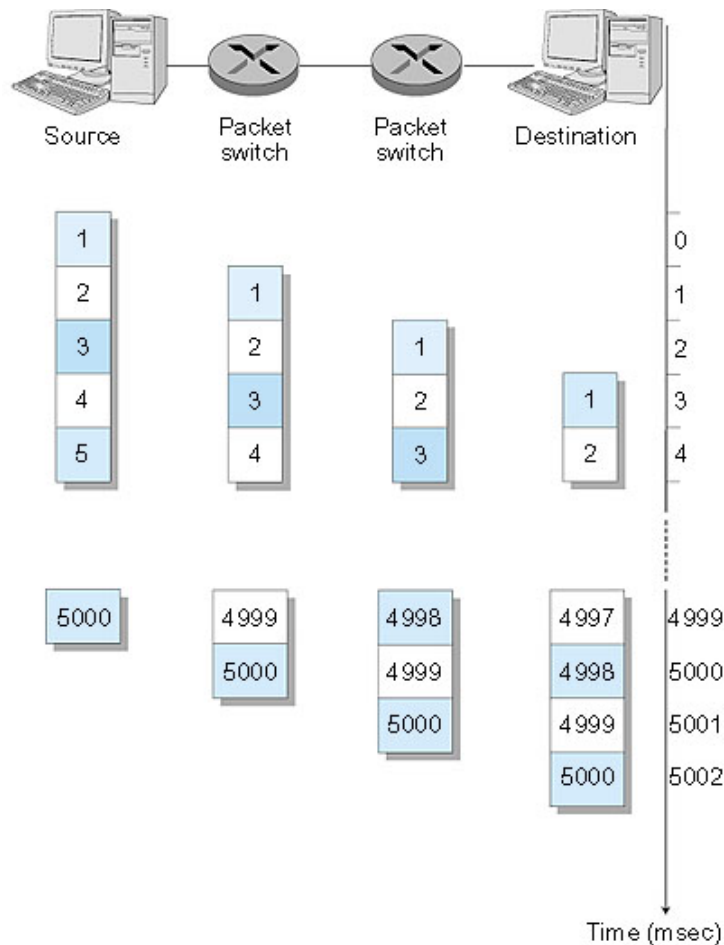
chaque flux de données est
divisé en paquets

- les paquets des utilisateurs A, B partagent les ressources de réseau
- chaque paquet utilise la bande passante totale de lien

Problèmes de ressources:

- la demande d'agrégation de ressources peut dépasser la capacité
- congestion: paquets s'amoncellent en file, attente pour l'utilisation de lien
- store and forward (enregistrement et retransmission)
 - Transmission sur un lien
 - Attente du service

Commutation par paquets: segmentation du Message



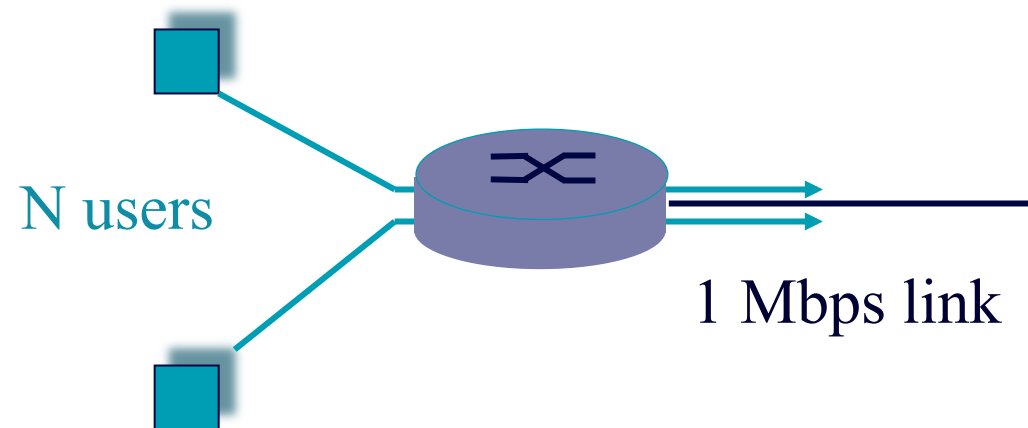
Découpage du message en 5000 paquets

- 1,500 bits par paquet
- 1 msec pour transmettre un paquet sur un lien
- *pipelining*: chaque lien travaille en parallèle
- Délai réduit de 15 sec à 5,002 sec

Commutation de Paquets /Circuits

La Commutations de paquets permet à plus d'utilisateurs de partager le réseau

- Lien 1 Mbit
- Chaque utilisateur:
 - 100Kbps quand il est actif
 - actif 10% du temps
- Commutation de circuits
 - 10 utilisateurs
- Commutation de paquets
 - Avec 35 utilisateurs, probabilité > 10 actifs inférieure à 0.004





Cœur du réseau : Commutation de Paquets /Circuits

Commutation de Paquets

- Intérêt pour les flots irréguliers (bursty)
 - Partage de ressources
 - Sans mise en place d'appel
- **Congestion excessive:** délai et pertes de paquets
 - protocoles nécessaires pour le transfert fiable de données, contrôle de congestion

Commutation de Paquet : routage

- Objectif: déplacer les paquets de la source à la destination
 - **Reseau datagram:**
 - L'adresse de destination détermine à chaque pas le routage
 - Les routes peuvent changer durant la session.
 - **Réseau à circuit virtuel :**
 - Chaque paquet contient un tag (ou label) définissant le chemin à suivre,
 - La route est fixée au début de la connexion
 - Chaque routeur doit garder une table d'état pour chaque appel

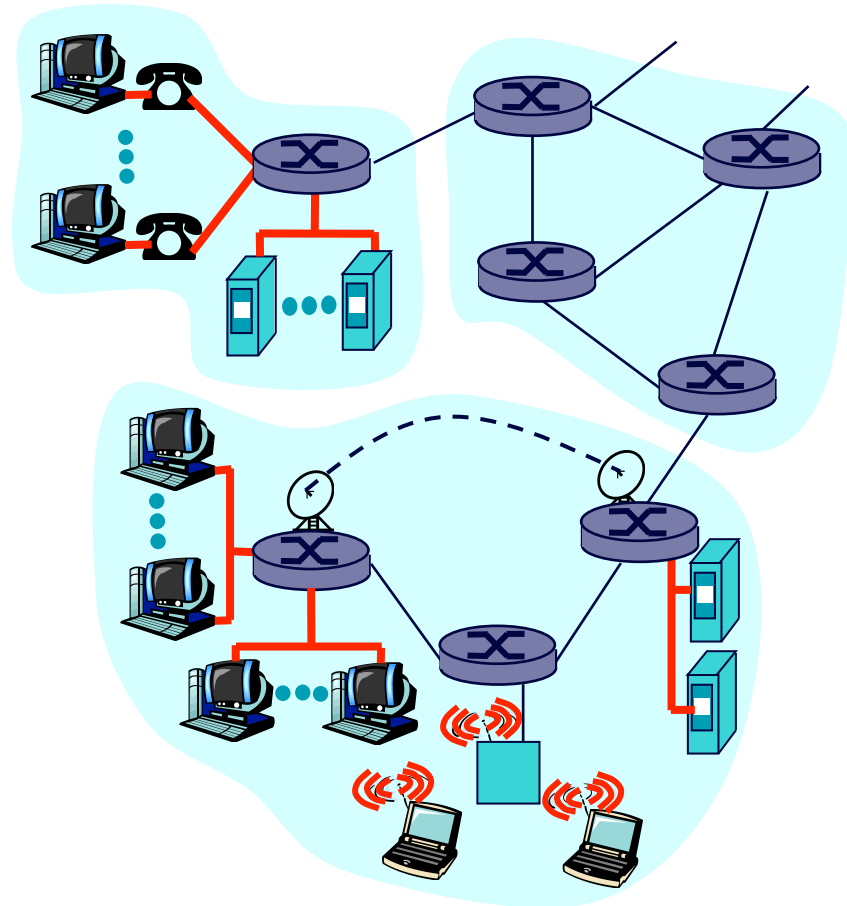
Réseaux d'accès et média physique

Q: Comment connecter les terminaux au routeur de bordure?

- ❑ Accès résidentiel
- ❑ Accès institutionnel
- ❑ Réseau d'accès sans fil

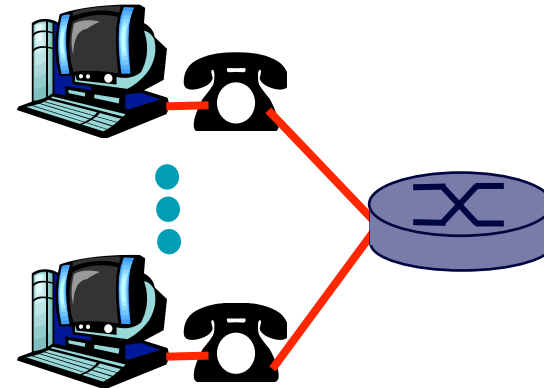
A prendre en compte:

- ❑ Bande passante (bits par seconde)?
- ❑ Partagée ou dédiée?



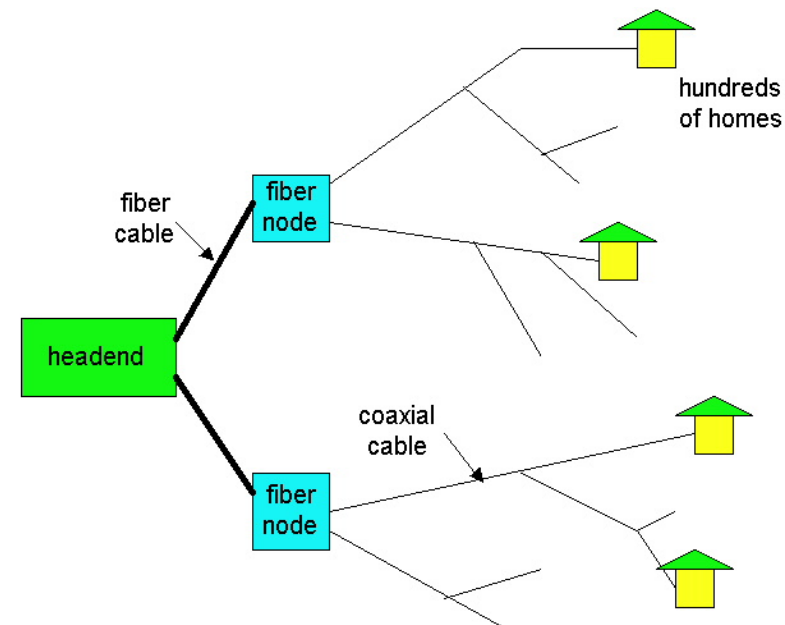
Accès résidentiel : accès point à point

- Accès par ligne téléphonique via un modem
 - Jusqu'à 56Kbps
- ISDN:
 - Accès numérique : jusqu'à 128Kbps
- ADSL: asymmetric digital subscriber line
 - Jusqu'à 1 Mbps du modem vers le DSLAM
 - Jusqu'à 8 Mbps du DSLAM vers le modem



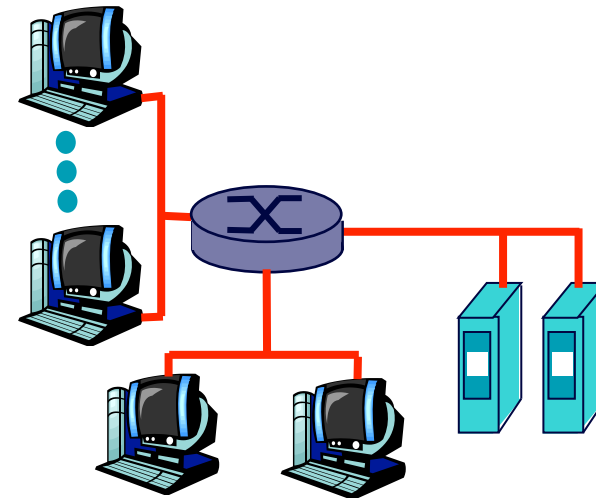
Accès résidentiels: le cable

- Le cable est constitué de HFC (Hybrid Fiber Coax)
 - Lien asymétrique: jusqu'à 10Mbps en voie descendante, 1 Mbps en voie montante
- Réseau de cables et de fibres optiques connectant les résidences aux ISPs
 - Le lien montant est partagé
 - Problèmes: congestion, dimensionnement



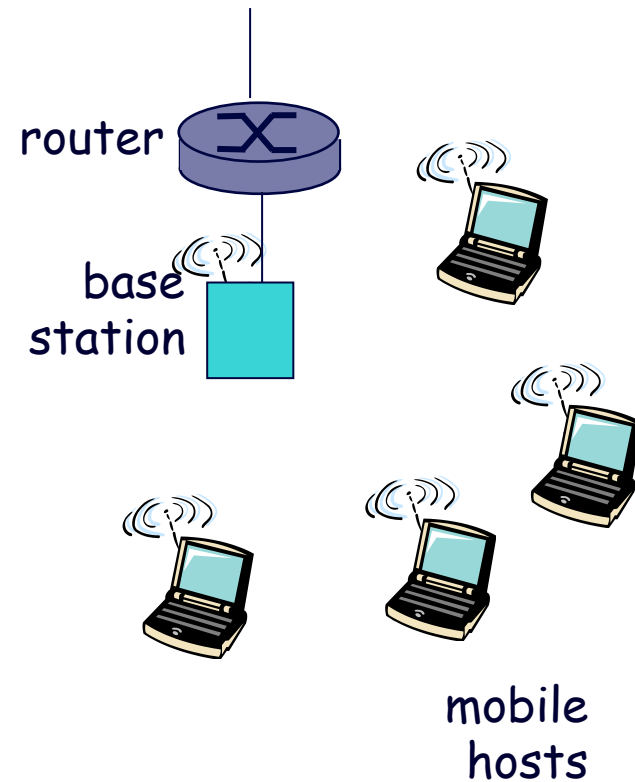
Accès institutionnel : réseaux locaux LAN

- Un réseau local (**LAN**) connecte les terminaux au routeur de cœur
- **Ethernet:**
 - Des liens partagés ou dédiés peuvent être utilisés
 - 10 Mbps, 100Mbps, Gigabit Ethernet



Réseaux d'accès sans fil

- Un accès partagé *sans fil* connecte les terminaux au cœur de réseau
- **LANs sans fils:**
 - Le câble est remplacé par le médium radio
 - e.g., Lucent Wavelan 10 Mbps
- **Boucle locale sans fil WLL (Wireless Local Loop)**
 - GPRS: extension du GSM à la transmission de données
 - UMTS: Universal Mobile Transmission System



Couche Réseau

Sondes Kallel

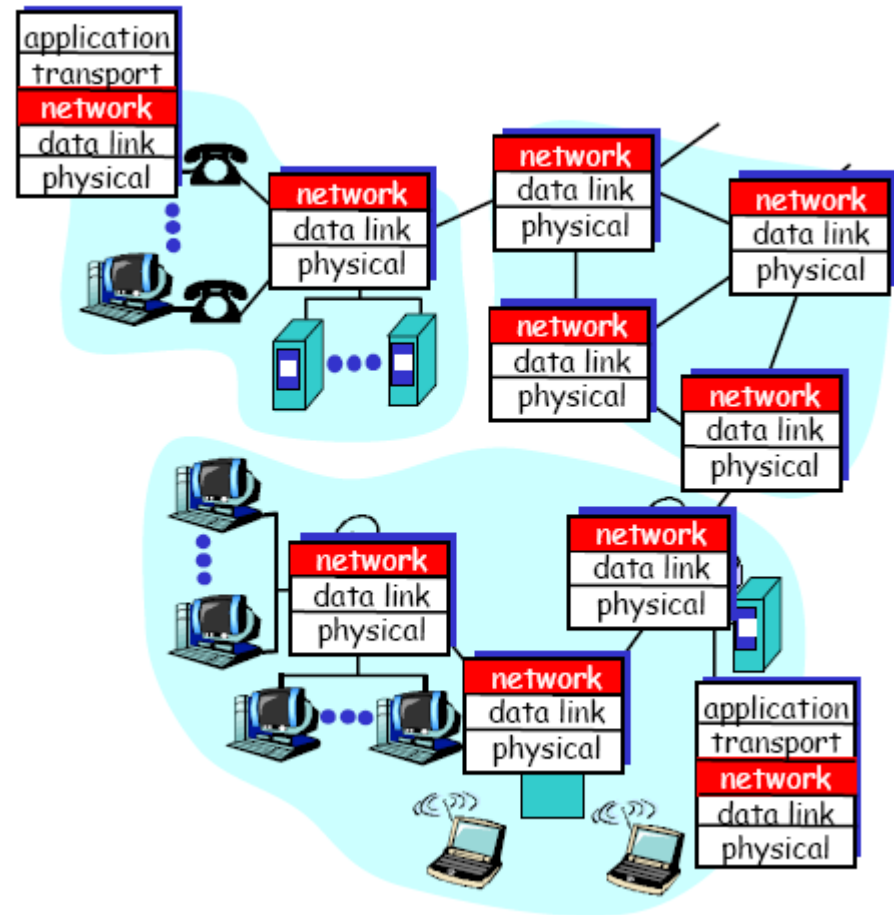


Plan

- ❑ Fonctionnalités de la couche réseau
- ❑ Modèle de service : Circuit virtuel/Datagramme
- ❑ Service IP
- ❑ Datagramme IP
- ❑ Adressage IP et CIDR
- ❑ Network Address Translation: NAT
- ❑ Protocole ICMP
- ❑ Quelques exemples: Ping et Traceroute

Fonctionnalités de la couche réseau

- ❑ Transporter des paquets de l'émetteur vers le récepteur
- ❑ Les protocoles de couche réseau s'exécutent dans chaque hôte et routeur.
- ❑ Trois fonctions principales :
 - Choix du chemin : route suivie par les paquets de la source à la dest. Algorithmes de routage
 - Commutation : transporter les paquets du port d'entrée vers le bon port de sortie.
 - Mise en place de l'appel : Dans les réseaux à commutation de circuits, la mise en place du circuit est effectuée par la couche réseau.



Modèle de service de la couche réseau

- Q : Quel est le modèle de service pour les canaux transportant des paquets de la source à la destination ?
 - Bande passante garantie ?
 - Préservation du délai inter paquet (pas de gigue) ?
 - Transmission sans pertes ?
 - Réception dans l'ordre ?
 - Annoncer une indication de congestion à l'émetteur ?

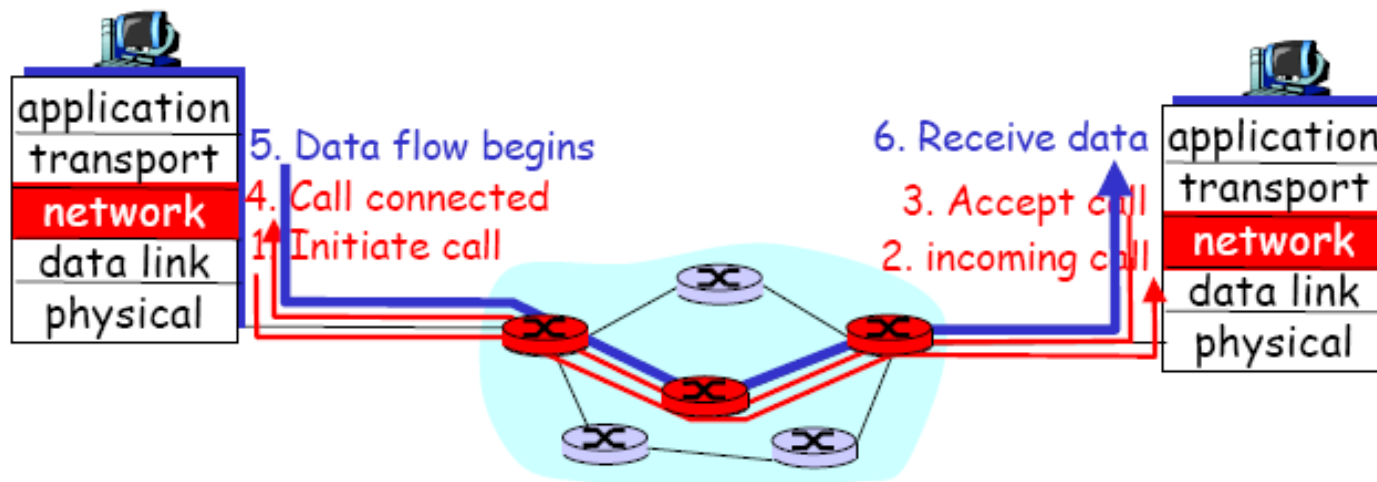
Circuit virtuel
ou
datagramme ?

Circuits virtuels

- Le « chemin » de la source à la destination se comporte comme un circuit téléphonique
- Avant d'émettre des données, le circuit doit être mis en place
 - Chaque paquet contient un identificateur de VC (et non pas l'adresse de la destination)
 - Chaque routeur maintient un « état » pour chaque connexion qui traverse le routeur
 - Les connexions dans la couche transport ne mettent en jeu que les systèmes terminaux
 - Des ressources du lien (bande passante) ou du routeur (mémoire) peuvent être allouées au VC
 - Pour garantir des performances

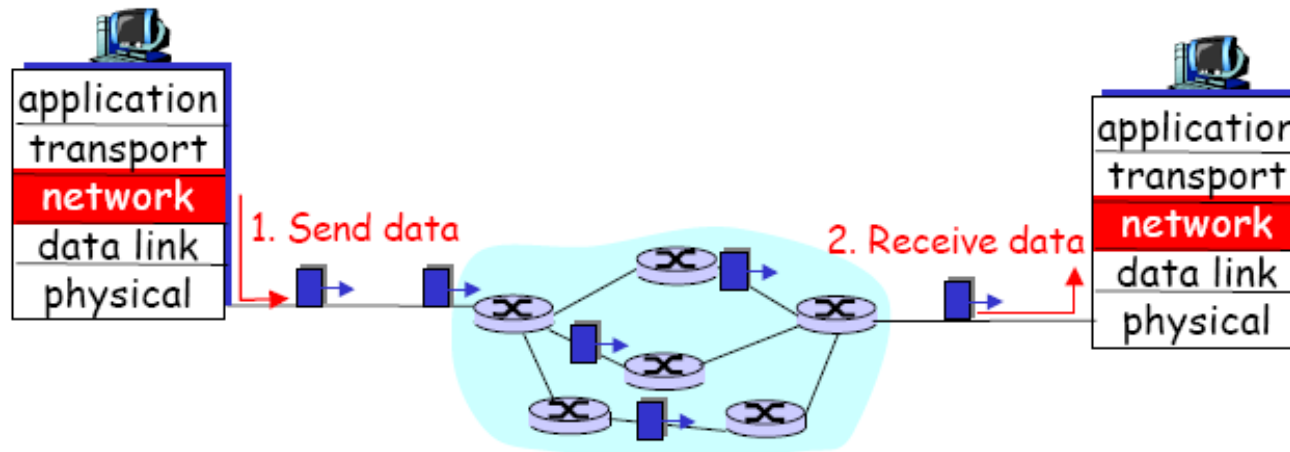
Circuits virtuels : protocoles de signalisation

- ❑ Utilisés pour mettre en place et gérer un VC
- ❑ Utilisés dans ATM, frame-relay et X.25
- ❑ Ne sont pas utilisés (du moins de façon visible) dans l'Internet actuel



Réseaux Datagramme : le modèle Internet

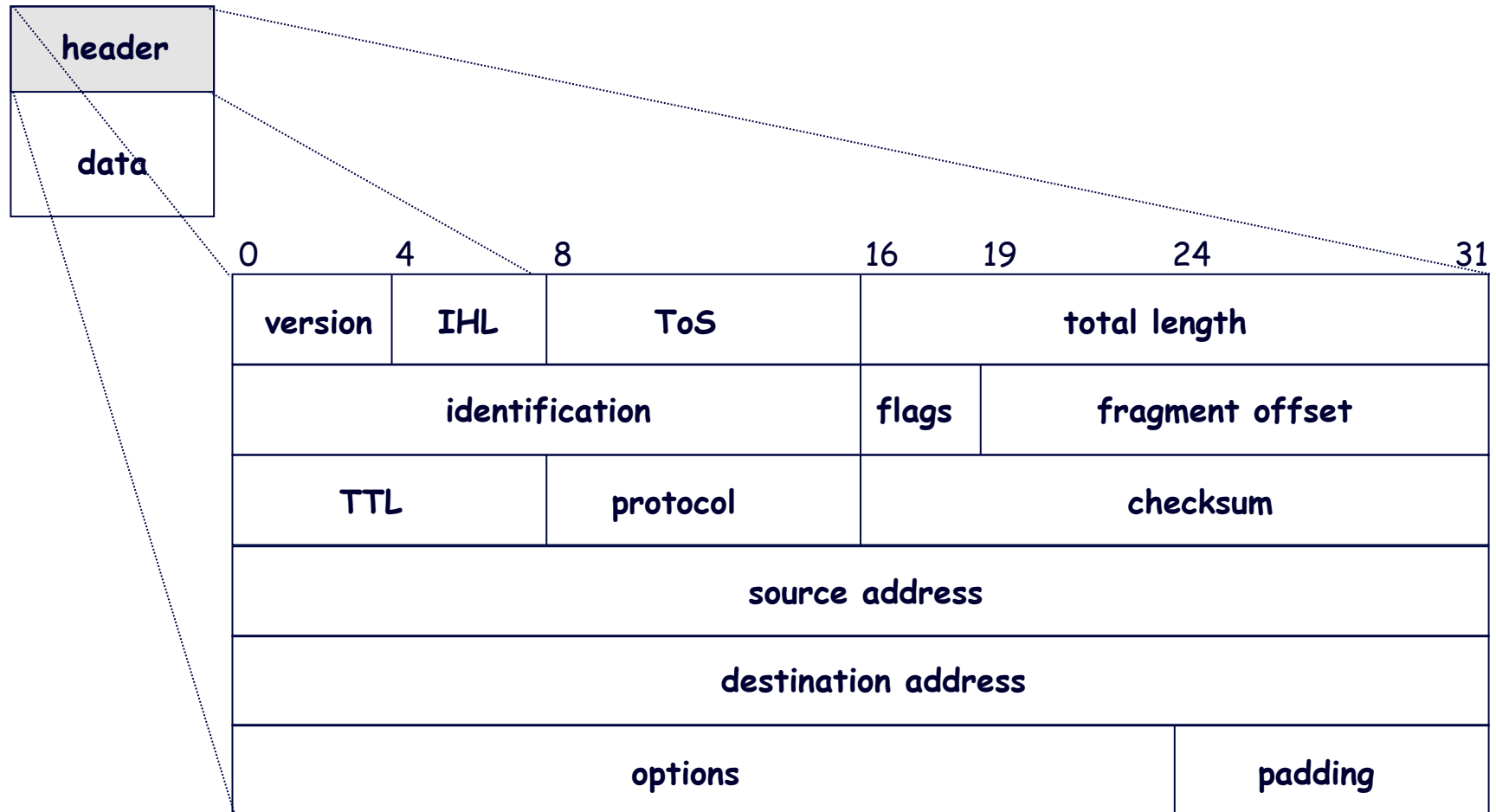
- ❑ Pas de mise en place de circuit
- ❑ routeurs : aucun état mémorisé au sujet des connexions
 - Pas de notion de connexion au niveau réseau
- ❑ Les paquets sont typiquement routés en fonction de l'adresse de destination
 - Des paquets avec la même source et destination peuvent suivre des trajets différents



Service IP

- Utilise un service minimum
 - envoi d'une unité de transfert d'un point à ses voisins
 - voisin : partage la même connexion physique
- Rend un service minimum
 - service en mode non connecté
 - absence d'états dans les routeurs
 - transmission de datagrammes
 - remise *best effort*
 - service non fiable
 - service de connectivité
- Avantages
 - ☺ efficace pour les échanges brefs
 - ☺ simplicité d'utilisation
 - ☺ robustesse

Le datagramme IP



Les champs de l'en-tête IP

- **version** : identification de la version courante du protocole (4 pour IPv4)
- **IHL** (*IP Header Length*) : longueur de l'en-tête IP (en mots de 32 bits)
- **TOS** (*Type Of Service*) : type de service à appliquer au paquet en fonction de certains paramètres comme le délai de transit, la sécurité
- **total length** : longueur totale du datagramme (en octets)
- **identification** : valeur fournie par la source aidant la destination au réassemblage des différents fragments du datagramme
- **flags** : utilisé par la fragmentation et composé de
 - DF (*Don't Fragment*)
 - MF (*More Fragment*)
 - réservé
- **offset** : déplacement par rapport au datagramme initial (en multiple de 8 octets)
- **TTL** (*Time To Live*) : limite supérieure du temps de vie d'un datagramme
- **protocol** : protocole utilisé pour le champ de données
 - 1 pour ICMP
 - 6 pour TCP
 - 17 pour UDP
- **checksum** : zone de contrôle d'erreur portant uniquement sur l'en-tête du datagramme
- **source address** : @ IP de la source du datagramme
- **destination address** : @ IP de la destination du datagramme
- **options** : fonctions de contrôle utiles dans certaines situations (estampillage temporel, sécurité, routage particulier, etc.)
- **padding** : pour aligner l'en-tête sur 32 bits

Exercice : Analyse de paquet IP

Décoder l'en-tête du paquet IPv4 suivant (en hexadécimal) et en extraire toutes les informations possibles.

45 00 00 50 20 61 00 00 80 01 C5 64 C7 F5 B4 0A C7 F5 B4 09
08 00 00 1C 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10
11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F 20 21 22 23 24
25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38

Correction :

45→4 = protocole IP version 4 ; 5 = longueur de l'en-tête du datagramme = $5 \times 4 = 20$ octets = longueur par défaut d'un en-tête sans option.

00→Type Of Service = 0 = pas de service particulier (en fait avec IPv4, il n'y a pas de service particulier. Ce champ est donc toujours nul !).

00 50→longueur totale = $0 \times 4096 + 0 \times 256 + 5 \times 16 + 0 \times 1 = 80$ octets donc la longueur du contenu du champ de données est de $80 - 20 = 60$ octets.

20 61→identificateur du datagramme (ne sera utile que s'il est fragmenté).

00 00→drapeaux et déplacement = tout à zéro = datagramme non fragmenté.

80→durée de vie = $80 = 8 \times 16 + 0 \times 1 = 128$ routeurs que le datagramme pourrait encore traverser.

01→protocole transporté dans le datagramme : 1 = code du protocole ICMP.

C5 64→Bloc de contrôle d'erreur de l'en-tête.

C7 F5 B4 0A→adresse IP émetteur = 199.245.180.10

C7 F5 B4 09→adresse IP destinataire = 199.245.180.9

Les deux machines sont dans le même réseau de classe C, le réseau 199.245.180.0

Que fait un routeur ?

Pour chaque datagramme IP qui traverse le routeur, IP :

- vérifie le checksum, si faux → destruction du datagramme
- détermine si ce sont des données *utilisateur* ou de *contrôle* destinées au routeur
- décrémente la durée de vie, si nulle → destruction du datagramme
- **décide du routage**
- **fragmente** le datagramme si nécessaire (MTU)
- **reconstruit l'en-tête IP** avec les champs mis à jour
- transmet le(s) datagramme(s) au protocole d'accès de l'interface réseau de sortie avec **l'adresse de sous-réseau correspondante**

A réception dans l'hôte destinataire, IP :

- vérifie le checksum
- s'il y a eu fragmentation, mémorise puis **réassemble**
- **délivre au niveau supérieur** les données

Adressage IP

- adressage
 - pour l'identification d'un équipement réseau
 - pour le routage
- plan d'adressage homogène
 - format : 4 octets ➔ 4,3 milliards d'adresses ???
 - notation décimale pointée : x1.x2.x3.x4
- adresse globalement unique et hiérarchique
- format : <réseau> <machine>
 - localisateur ou préfixe réseau : identificateur de réseau
 - identificateur : identificateur de machine





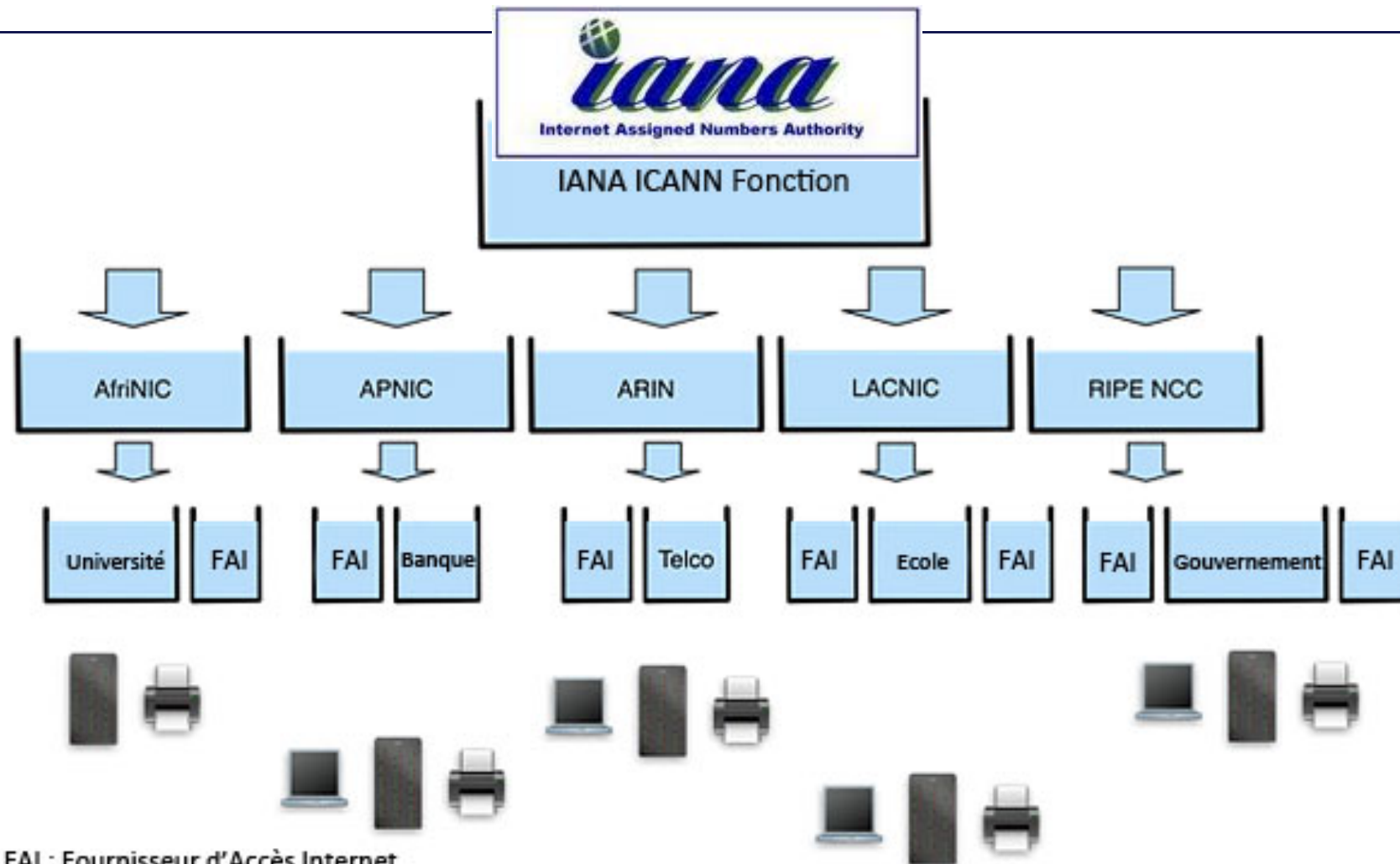
Attribution des adresses IP

Q : Comment un ISP récupère-t-il un bloc d'adresses IP ?

R : **ICANN** : Internet Corporation for Assigned Names and Numbers

- alloue les adresses
- Gère le DNS
- Assigne les noms de domaines

Attribution des adresses



FAI : Fournisseur d'Accès Internet

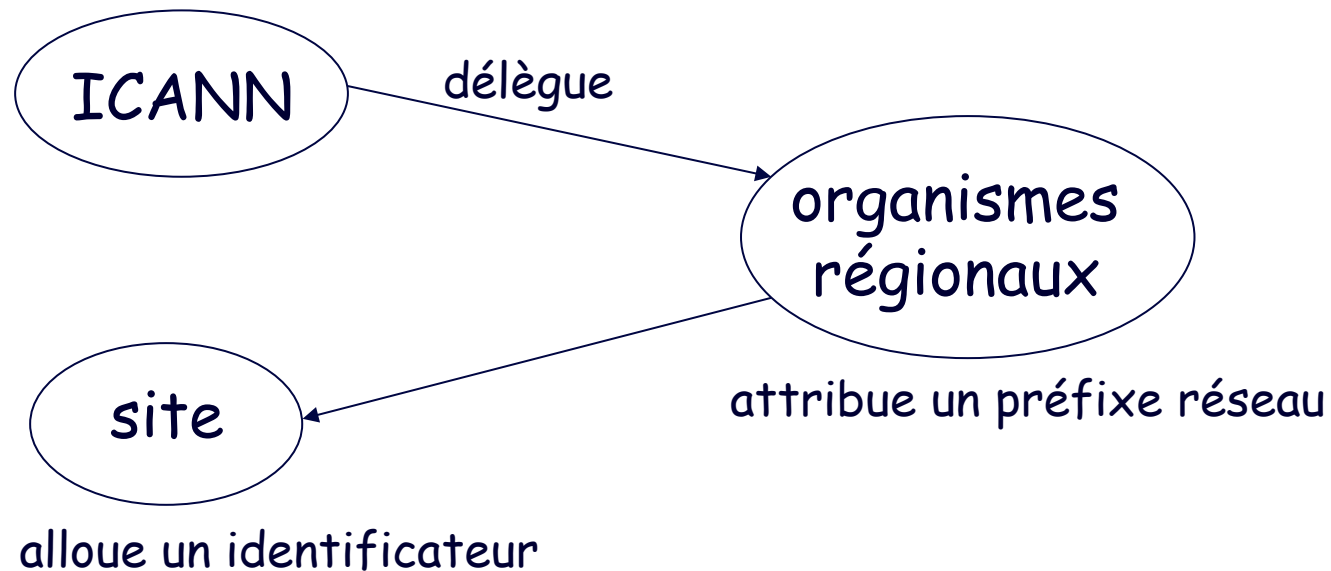
ICANN : Internet Corporation for Assigned Names and Numbers : c'est l'autorité suprême de régulation de l'Internet.

IANA : L'Internet Assigned Numbers Authority est une organisation dont le rôle est la gestion de l'espace d'adressage, c'est une composante de l'ICANN

Attribution des adresses: Registres Internet Régionaux (dits RIRs)



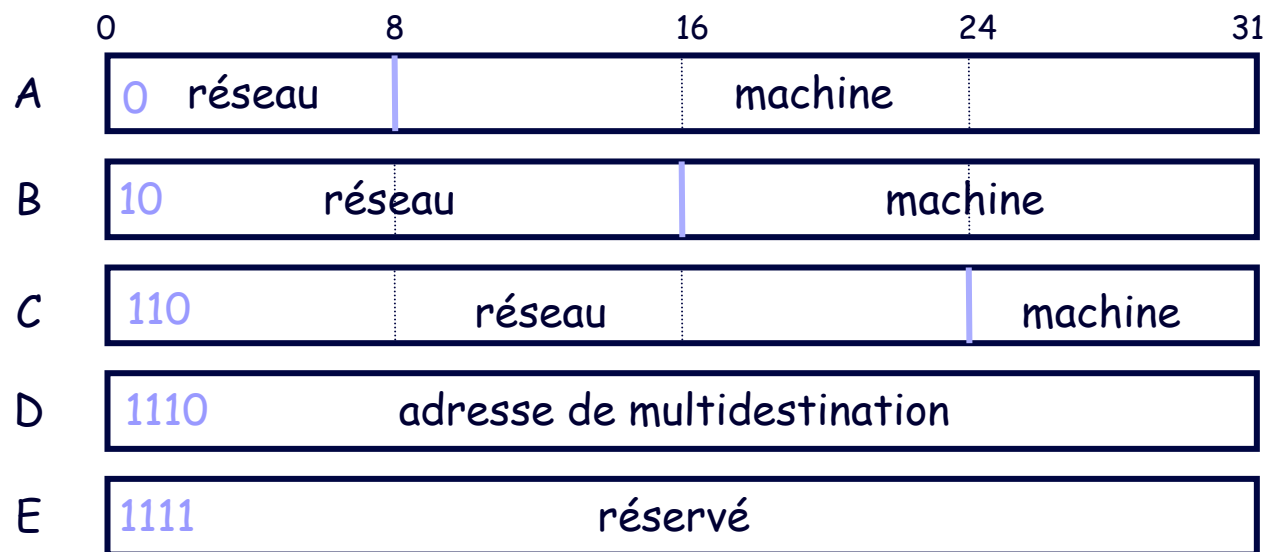
Attribution des adresses



- Les adresses IP sont distribuées selon un système hiérarchique :
 - l'ICANN alloue les blocs d'IP aux 5 Registres Internet Régionaux (dits RIRs) autour du monde.
 - Les RIRs les redistribuent en plus petits blocs aux Fournisseurs d'Accès Internet (ISP) et autres opérateurs du réseau.
 - Ceux-ci les assignent enfin aux connections des individuels à Internet.

Classes d'adresses

- le découpage <réseau> / <machine> n'est pas fixe
- ⇒ 5 classes d'adresses



Multi-cast

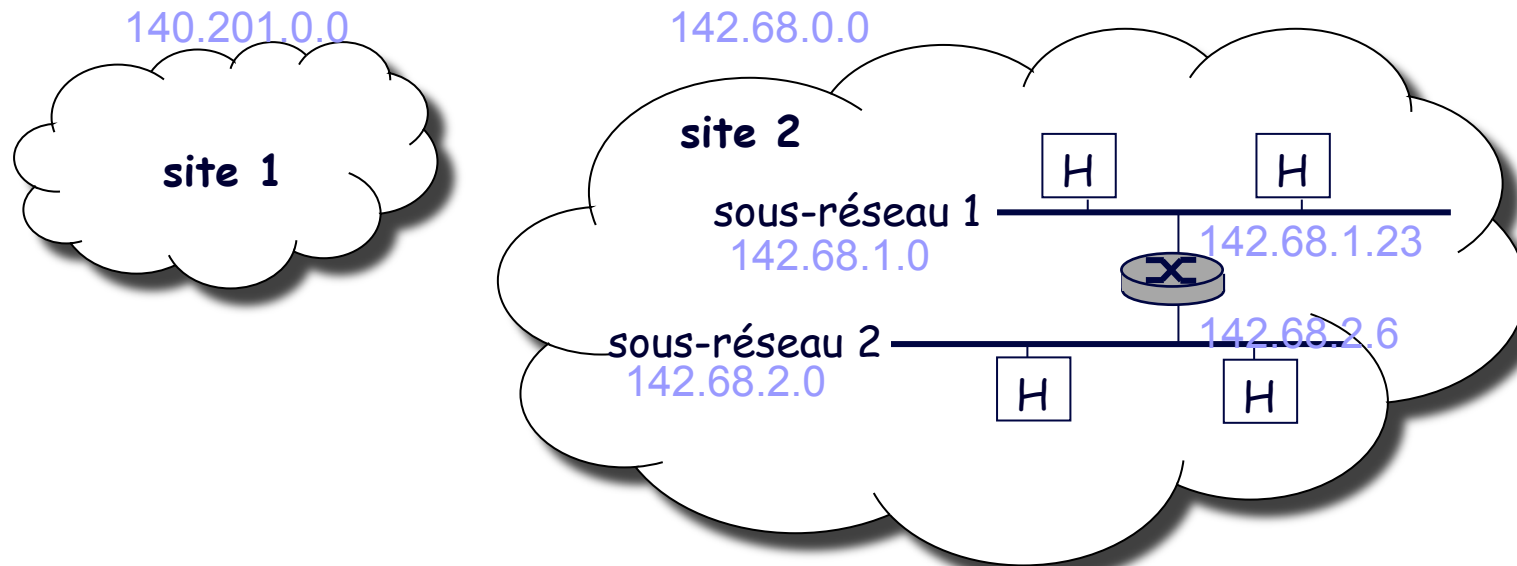
Classes d'adresses

- classe A : 2^7 réseaux (128)
 - réservé: 0.0.0.0 et 127.0.0.0
 - disponible: 1.0.0.0 à 126.0.0.0
 - 126 réseaux classe A et 16 777 214 machines/réseau
- classe B : 2^{14} réseaux (16 384)
 - réservé: 128.0.0.0 et 191.255.0.0
 - disponible 128.1.0.0 à 191.254.0.0
 - 16 382 réseaux classe B et 65 534 machines/réseau
- classe C : 2^{21} réseaux (2 097 152)
 - réservé 192.0.0.0 et 223.255.255.0
 - disponible 192.0.1.0 à 223.255.254.0
 - 2 097 150 réseaux classe C et 254 machines/réseau

Subnetting

□ Problème

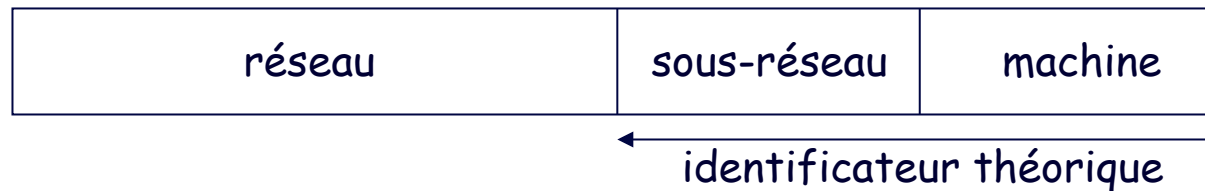
- distinction <réseau> / <hôte> insuffisante en pratique



- Une organisation dispose d'une seule adresse de réseau IP mais est composée de plusieurs sites/départements
 - -> diviser un réseau IP en plusieurs sous-réseaux
 - -> prendre quelques bits de la partie <HOST_ID> de l'adresse IP pour distinguer les sous-réseaux
 - -> transparent vis à vis de l'extérieur

Sous-adressage

- Principe
 - ajout d'un niveau hiérarchique dans l'adressage
 - adresse de sous-réseau
 - subdivision de la partie <hôte>



- le sous-réseau
 - est un réseau physique (i.e. un réseau IP connexe) du réseau de site
 - a une visibilité purement interne (transparent vis à vis de l'extérieur).

Le masque de sous-réseau

- Le masque indique la frontière entre la partie <sous-réseau> et la partie <machine>
- Le masque est propre au site et il est de 32 bits
- Bits du masque de sous-réseau (*subnet mask*)
 - positionnés à 1 → partie réseau
 - positionnés à 0 → partie machine
- Exemple
 - 11111111 11111111 11111111 00000000
 - ↳ 3 octets pour le champ réseau, 1 octet pour le champ machine
- Notations
 - décimale pointée
 - exemple : 255.255.255.0
 - adresse réseau/masque
 - exemple : 193.49.60.0/27 (27 = nombre de bits contigus du masque)

Masque de sous-réseau

□ Utilisation :

classe	réseau	machine
interne au site	masque réseau	
	&&	
	réseau	ss-réseau machine

□ Exemple :

- le réseau 142.68.0.0 (classe B!) a comme masque 255.255.255.0
- soit l'hôte d'@IP 142.68.2.6

$$\begin{array}{rcl}
 & 10001110.01000100.00000010.00000110 & 142.68.2.6 \\
 \&\& & 11111111.11111111.11111111.000000 & 255.255.255.0 \\
 \hline
 = & 10001110.01000100.00000010.00000000 & 142.68.2.0
 \end{array}$$

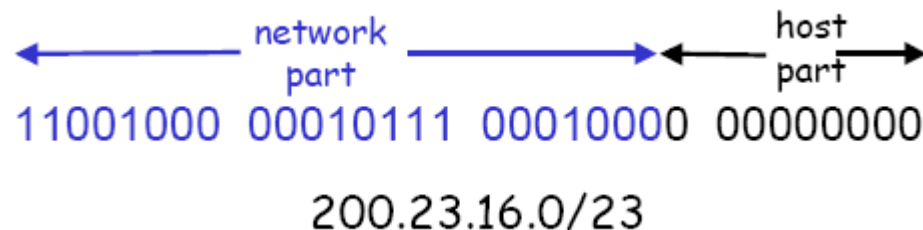
- ↗ l'hôte est sur le sous-réseau numéro 2, et a comme identificateur 6
- Le netmask permet de savoir si la machine source et destination sont sur le même sous-réseau.

Le masque de sous-réseau

- Le choix du découpage <réseau> / <hôte> dépend des perspectives d'évolution du site
 - exemple classe B :
 - 8 bits pour la partie sous réseau ➔ 256 sous réseaux de 254 machines
 - 3 bits pour la partie sous réseau ➔ 8 sous-réseaux de 8190 machines
 - exemple classe C :
 - 4 bits pour la partie sous-réseau ➔ 16 sous-réseaux de 14 machines

Adresse IP : CIDR

- Adressage par classe :
 - utilisation inefficace de l'espace d'adressage
 - Ex : une adresse de classe B a assez de place pour 65K hôtes, même si il n'y a que 2K hôtes dans ce réseau
 - Il n'y a plus de notion de classes et de sous-réseaux
- CIDR : Classless InterDomain Routing
 - La taille de la partie réseau est arbitraire
 - Format de l'adresse : a.b.c.d/x, où x est le # de bits dans la partie réseau de l'adresse
 - Ex: 128.96.0.0/16 : regroupe les numéros de 128.96.0.0 à 128.96.255.255
=> équivalent d'une classe B en notation classique



Les adresses privées et le NAT

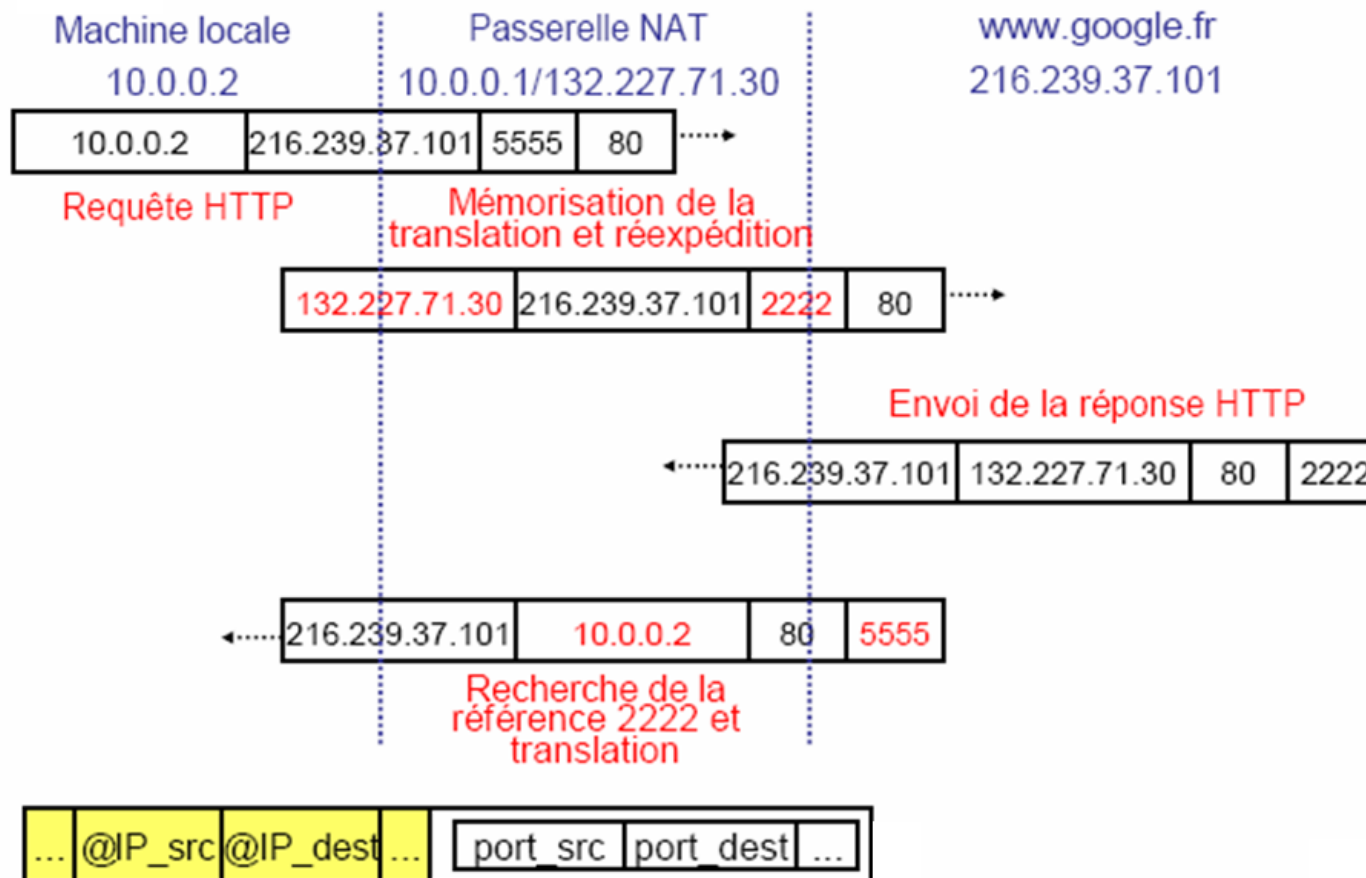
- Adresses privées (RFC 1918)
 - des adresses qui ne seront jamais attribuées (adresses illégales) sur Internet et qui ne sont pas routables sur l'Internet
 - classe A : de 10.0.0.0 à 10.255.255.255
 - classe B : de 172.16.0.0 à 172.31.255.255
 - classe C : de 192.168.0.0 à 192.168.255.255
- Si une entreprise qui utilise des adresses privées souhaite tout de même disposer d'une connexion à l'Internet, il faut
 - demander une adresse publique
 - faire des conversions adresse privée <--> adresse publique
 - Les adresses privées ne sont utilisables que dans son réseau local et sont non routables

Les adresses privées et le NAT

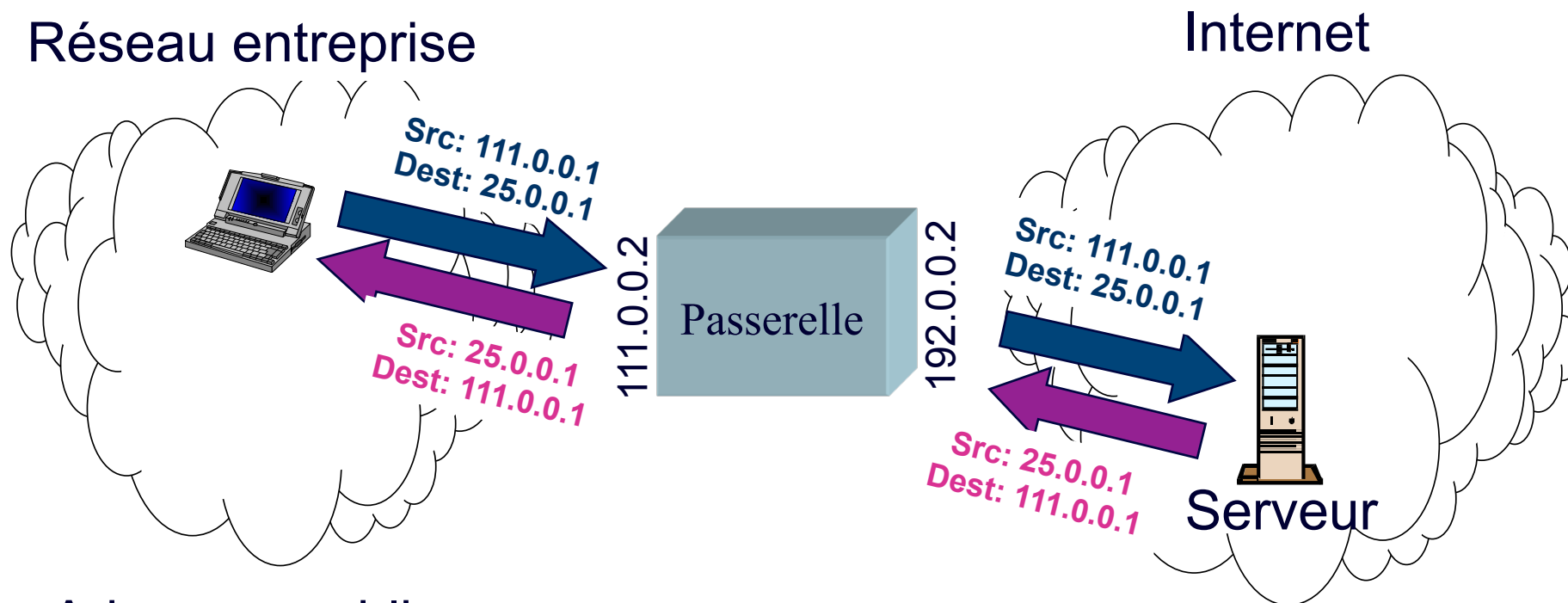
- NAT (RFC 3022) - Network Address Translator
 - mise en correspondance d'une adresse privée et d'une adresse publique
 - traduction statique ou dynamique (lors de la connexion)
 - une solution au manque d'adresses IP publiques : quelques adresses IP publiques pour beaucoup d'adresses IP privées mais le NAT est coûteux en perf.
- Fonctionnement du NAT
 - une table stockée dans le NAT fait la correspondance entre (@IP_src privée, port_src) et une @IP_publicue
 - quand le paquet part : @IP_src devient @IP_publicue, port_src devient la référence de l'entrée dans la table
 - quand la réponse revient : port_dest du paquet permet de retrouver dans la table @IP et port src

NAT

Exemple de requête sortante



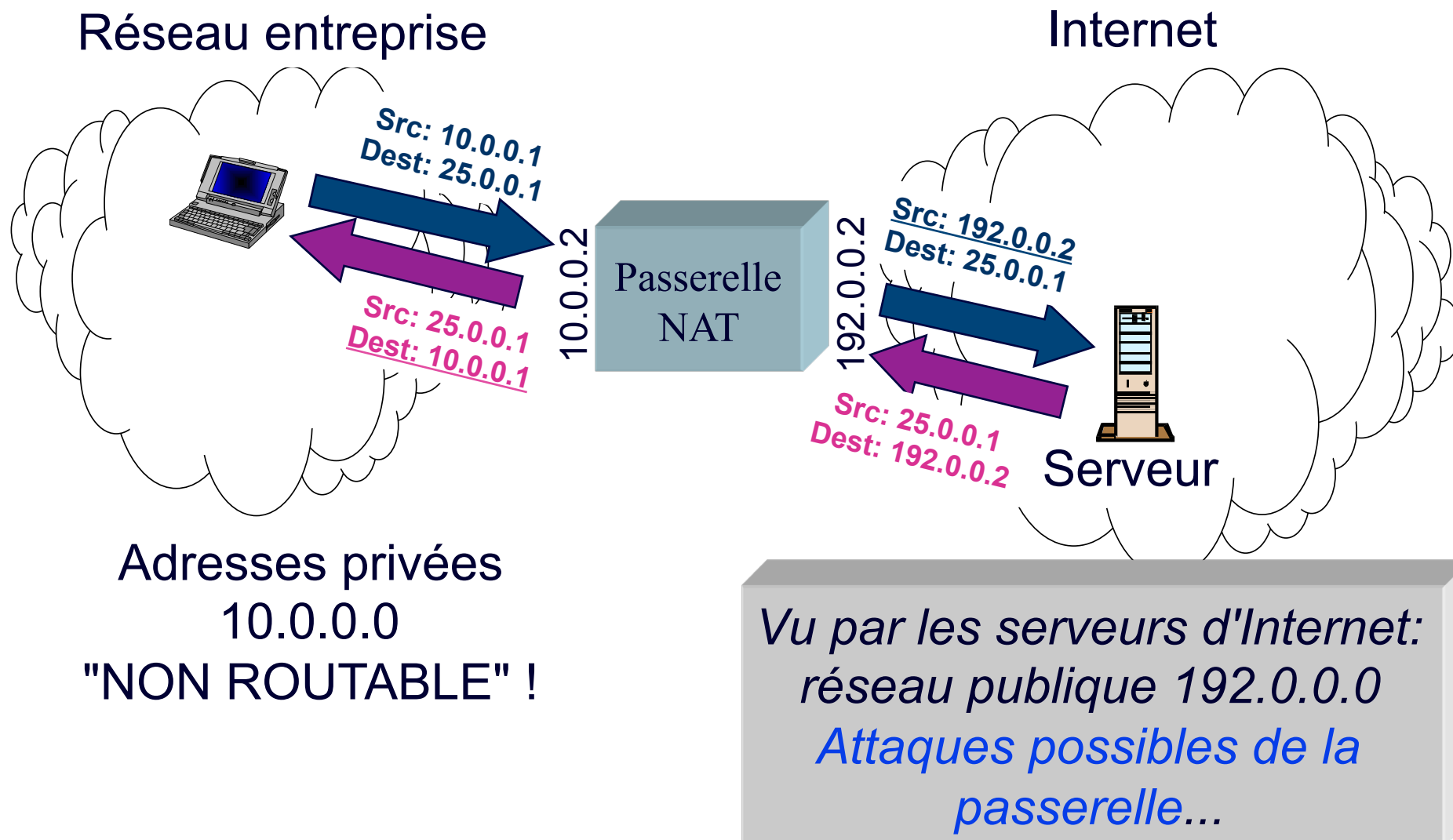
Passerelle sans NAT



Adresses publiques
111.0.0.0

*Vu par les serveurs d'Internet:
réseau publique 111
Le monde entier peut attaquer tous les
postes de l'entreprise*

Passerelle avec NAT





Protocole ICMP

- ❑ Internet Control Message Protocol, RFC 792
- ❑ Objectif
 - Rapport d'erreurs de la couche Réseau
- ❑ Exemple
 - Au cours d'une session HTTP, un message d'erreur « Réseau de destination inaccessible » est affiché
 - Quand un routeur ne peut pas trouver le chemin spécifié par l'application, il génère un message d'erreur à la source
 - Le terminal reçoit le message ICMP et renvoie le code d'erreur à la couche TCP qui à son tour le renvoie à l'application



Protocole ICMP

- Basé sur IP, Protocol ID = 1
- Chaque message ICMP est doté d'un champ de code et de catégorie qui signifie le contenu du message
 - Exemples
 - Type = 0, code = 0 : message d'écho
 - Type = 8, code = 0 : demande d'écho
 - Type = 11, code = 0 : expiration de la durée de vie

Ping

- Ping
 - Le programme *ping* envoie à une destination un message ICMP avec type = 8, code = 0 (demande d'écho)
 - La machine destination répond par un message d'écho ICMP (type = 0, code = 0)
 - Le programme affiche le délai du parcours à l'utilisateur

```
C:\Users\Univ P & M Curie>ping www.lip6.fr

Envoi d'une requête 'ping' sur w.lip6.fr [132.227.73.20] avec 32 octets de données :
Réponse de 132.227.73.20 : octets=32 temps=22 ms TTL=53
Réponse de 132.227.73.20 : octets=32 temps=22 ms TTL=53
Réponse de 132.227.73.20 : octets=32 temps=23 ms TTL=53
Réponse de 132.227.73.20 : octets=32 temps=21 ms TTL=53

Statistiques Ping pour 132.227.73.20:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 21ms, Maximum = 23ms, Moyenne = 22ms
```

ping

```
C:\Users\E218>ping google.fr

Envoi d'une requête 'ping' sur google.fr [74.125.230.82] avec 32 octets de données :
Réponse de 74.125.230.82 : octets=32 temps=31 ms TTL=55
Réponse de 74.125.230.82 : octets=32 temps=31 ms TTL=55
Réponse de 74.125.230.82 : octets=32 temps=31 ms TTL=55
Réponse de 74.125.230.82 : octets=32 temps=30 ms TTL=55

Statistiques Ping pour 74.125.230.82:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 30ms, Maximum = 31ms, Moyenne = 30ms
```

Traceroute (1)

□ Traceroute

- Le programme *traceroute* envoie des paquets IP destinés à une destination avec les valeurs TTL incrémentées (1, 2, 3, ...)
- Le N^{ième} routeur va recevoir le N^{ième} paquet dont sa durée de vie expire à ce routeur
- Les routeurs qui écartent le paquet IP envoient un message ICMP (type=11, code = 0) à la source lui permettant de déterminer les noms et adresses IP de tous les routeurs jalonnant le parcours du paquet ainsi que les délais correspondants

traceroute

```
C:\Users\E218>tracert google.fr

Détermination de l'itinéraire vers google.fr [74.125.230.82]
avec un maximum de 30 sauts :

  1      1 ms      1 ms      1 ms  192.168.0.254
  2     22 ms     21 ms     22 ms  78.232.102.254
  3     50 ms     20 ms     22 ms  213.228.8.254
  4     22 ms     22 ms     24 ms  th2-crs16-1-be1011.intf.routers.proxad.net [212.
27.50.211]
  5      *        *        22 ms  ix-15-547.tcore1.PUU-Paris.as6453.net [195.219.2
41.173]
  6     34 ms     31 ms     31 ms  if-4-2.tcore1.FR0-Frankfurt.as6453.net [80.231.1
53.9]
  7     31 ms     30 ms     30 ms  Port-channel2.har1.FR1-Frankfurt.as6453.net [195
.219.50.38]
  8     32 ms     32 ms     31 ms  de-cix20.net.google.com [80.81.193.108]
  9     33 ms     31 ms     43 ms  209.85.255.178
 10     31 ms     34 ms     31 ms  72.14.233.104
 11     32 ms     31 ms     32 ms  64.233.175.115
 12     32 ms     34 ms     30 ms  74.125.230.82

Itinéraire déterminé.
```

Traceroute (2)

```
C:\Users\Univ P & M Curie>tracert www.lip6.fr
```

```
Détermination de l'itinéraire vers w.lip6.fr [132.227.73.20]  
avec un maximum de 30 sauts :
```

hop	rtt1	rtt2	rtt3	interface
1	1 ms	1 ms	1 ms	192.168.0.254
2	24 ms	21 ms	21 ms	diderot-3-81-57-106-254.fbx.proxad.net [81.57.106.254]
3	24 ms	*	*	th2-6k-2-a5.routers.proxad.net [213.228.7.254]
4	23 ms	22 ms	21 ms	bzn-crs16-1-be1004.intf.routers.proxad.net [212.27.50.173]
5	21 ms	22 ms	21 ms	aub-6k-1-po20.intf.routers.proxad.net [212.27.51.82]
6	22 ms	21 ms	22 ms	renater.routers.proxad.net [212.27.38.206]
7	21 ms	22 ms	22 ms	te1-1-jussieu-rtr-021.noc.renater.fr [193.51.189.229]
8	22 ms	22 ms	22 ms	rap-ipv4-v1165-te3-2-jussieu-rtr-021.noc.renater.fr [193.51.181.101]
9	21 ms	22 ms	22 ms	site-6-01-jussieu.rap.prd.fr [195.221.127.182]
10	23 ms	22 ms	23 ms	r-kennedy.reseau.jussieu.fr [134.157.254.29]
11	23 ms	22 ms	22 ms	lip6-routeur.lip6.fr [132.227.106.31]
12	23 ms	23 ms	22 ms	w.lip6.fr [132.227.73.20]

```
Itinéraire déterminé.
```

Afficher la table de routage

□ Windows

■ C> route PRINT

IPv4 Table de routage

```
=====
Itinéraires actifs :
Destination réseau      Masque réseau  Adr. passerelle  Adr. interface  Métrique
0.0.0.0                 0.0.0.0        192.168.0.254    192.168.0.4      25
127.0.0.0               255.0.0.0      On-link          127.0.0.1        306
127.0.0.1               255.255.255.255 On-link          127.0.0.1        306
127.255.255.255         255.255.255.255 On-link          127.0.0.1        306
192.168.0.0             255.255.255.0  On-link          192.168.0.4      281
192.168.0.4             255.255.255.255 On-link          192.168.0.4      281
192.168.0.255           255.255.255.255 On-link          192.168.0.4      281
224.0.0.0               240.0.0.0      On-link          127.0.0.1        306
224.0.0.0               240.0.0.0      On-link          192.168.0.4      281
255.255.255.255         255.255.255.255 On-link          127.0.0.1        306
255.255.255.255         255.255.255.255 On-link          192.168.0.4      281
=====
```

■ C> ipconfig /all

□ Voir la passerelle par défaut

```
C:\Users\E218>tracert fr.wikipedia.org
```

```
Détermination de l'itinéraire vers text.esams.wikimedia.org [91.198.174.232]  
avec un maximum de 30 sauts :
```

1	3 ms	1 ms	1 ms	192.168.0.254
2	22 ms	21 ms	21 ms	78.232.102.254
3	22 ms	21 ms	21 ms	213.228.8.254
4	21 ms	25 ms	22 ms	th2-crs16-1-be1011.intf.routers.proxad.net [212.27.50.211]
5	28 ms	27 ms	27 ms	strasbourg-crs16-1-be2000.intf.routers.proxad.net [212.27.50.101]
6	31 ms	31 ms	30 ms	francfort-6k-1-po100.intf.routers.proxad.net [212.27.56.301]
7	38 ms	37 ms	38 ms	amsterdam-6k-1-po100.intf.routers.proxad.net [212.27.56.381]
8	38 ms	42 ms	37 ms	te-1-4.br1-knams.wikimedia.org [195.69.145.176]
9	38 ms	41 ms	37 ms	te-8-2.csw1-esams.wikimedia.org [91.198.174.254]
10	38 ms	38 ms	38 ms	text.esams.wikimedia.org [91.198.174.232]

```
Itinéraire déterminé.
```

```
C:\Users\E218>tracert google.fr
```

```
Détermination de l'itinéraire vers google.fr [209.85.147.103]  
avec un maximum de 30 sauts :
```

1	1 ms	1 ms	1 ms	192.168.0.254
2	21 ms	21 ms	20 ms	78.232.102.254
3	*	*	21 ms	213.228.8.254
4	21 ms	21 ms	21 ms	th2-crs16-1-be1011.intf.routers.proxad.net [212.27.50.211]
5	*	21 ms	21 ms	ix-15-547.tcore1.PUU-Paris.as6453.net [195.219.241.173]
6	30 ms	61 ms	37 ms	if-4-2.tcore1.FR0-Frankfurt.as6453.net [80.231.153.91]
7	31 ms	31 ms	30 ms	Port-channel2.har1.FR1-Frankfurt.as6453.net [195.219.50.381]
8	31 ms	32 ms	33 ms	de-cix20.net.google.com [80.81.193.108]
9	32 ms	31 ms	42 ms	209.85.255.178
10	43 ms	38 ms	41 ms	209.85.250.140
11	37 ms	35 ms	112 ms	209.85.240.221
12	38 ms	36 ms	49 ms	216.239.46.117
13	36 ms	36 ms	36 ms	bru01m01-in-f103.1e100.net [209.85.147.103]

```
Itinéraire déterminé.
```



ARP (1)

- ❑ Address Resolution Protocol
- ❑ Un terminal veut envoyer un paquet IP à un autre terminal sur le même réseau Ethernet
- ❑ L'émetteur doit connaître l'adresse MAC du récepteur pour préparer la trame Ethernet
- ❑ Le protocole ARP permet à l'émetteur de trouver l'adresse MAC du récepteur à partir de son adresse IP (i.e. adresse IP du récepteur)

ARP (2)



ARP (3)

□ Table ARP

```
C:\Users\Univ P & M Curie>arp -a
```

```
Interface : 192.168.0.2 --- 0x9
```

Adresse Internet	Adresse physique	Type
192.168.0.254	00-07-cb-3e-d2-91	dynamique
192.168.0.255	ff-ff-ff-ff-ff-ff	statique
224.0.0.22	01-00-5e-00-00-16	statique
224.0.0.252	01-00-5e-00-00-fc	statique
239.255.255.250	01-00-5e-7f-ff-fa	statique

Rappel

A lire

Modèle OSI : Architecture en couches

Rappel

○ Modèle de référence OSI

· Open Systems Interconnection

- modèle fondé sur un principe énoncé par Jules César :
diviser pour mieux régner
- le principe de base est la description des réseaux sous forme d'un ensemble de couches superposées les unes aux autres
- l'étude du tout est réduit à celle de ses parties, l'ensemble devient plus facile à manipuler

Pourquoi une architecture en couches

Rappel

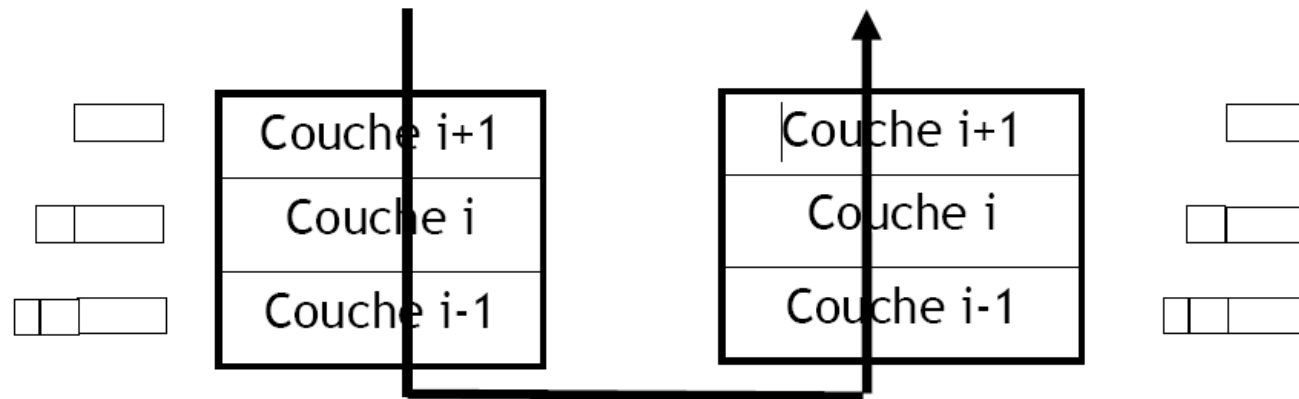
- Lorsqu'on doit concevoir un système complexe
 - Autant de fonctions différentes => découpage en couche où chaque couche est en charge de différentes fonctions
- La modularité facilite la maintenance et la mise à jour du système
 - La modification d'une couche reste transparente au reste du système
 - Tâches identifiées pour les réseaux :
 - Support physique (envoyer des 0 et des 1)
 - Contrôle et correction d'erreurs
 - Adressage
 - Routage (différent de l'adressage ?)
 - Mise en paquet
 - Sécurité
 - Contrôle de flux
 - ...
- 2 aspects : vertical et horizontal

Généralités:

Aspect vertical: Principe des couches

Rappel

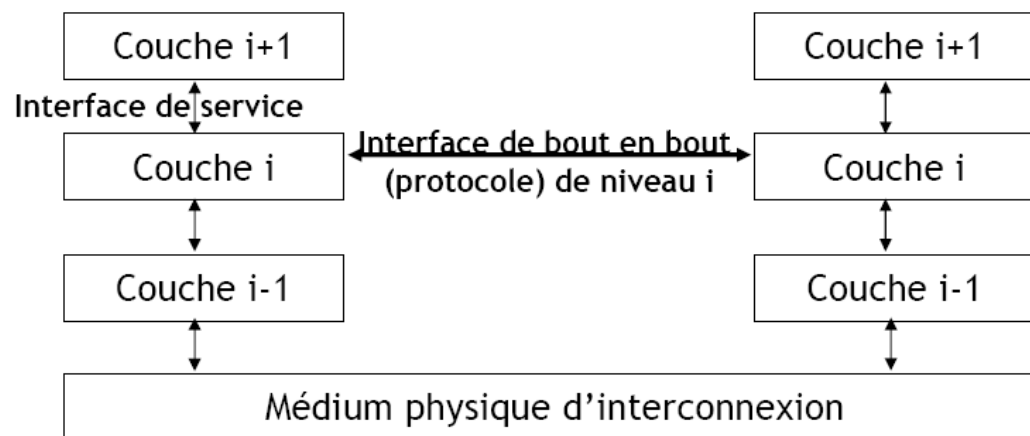
- Une couche i fournit un service à une couche $i+1$ en s'appuyant par le service fourni par la couche $i-1$.
 - La couche $i+1$ voit la couche i uniquement par le service offert.
 - La couche $i+1$ n'a aucune vue sur la couche $i-1$
- Abstraction pour masquer la complexité à la couche supérieure (1 couche = 1 boîte noire)
- Découpage des messages et encapsulation



Aspect horizontal: Protocoles

Rappel

- Interface de service : définit les opérations sur le protocole
- Interface de bout en bout : définit les messages échangés avec l'entité distante
 - *2 couches de niveau i de 2 systèmes différents dialoguent avec le même protocole*
 - *Protocole = Ensemble de règles et de conventions pour la conversation*



Communications entre couches

Rappel

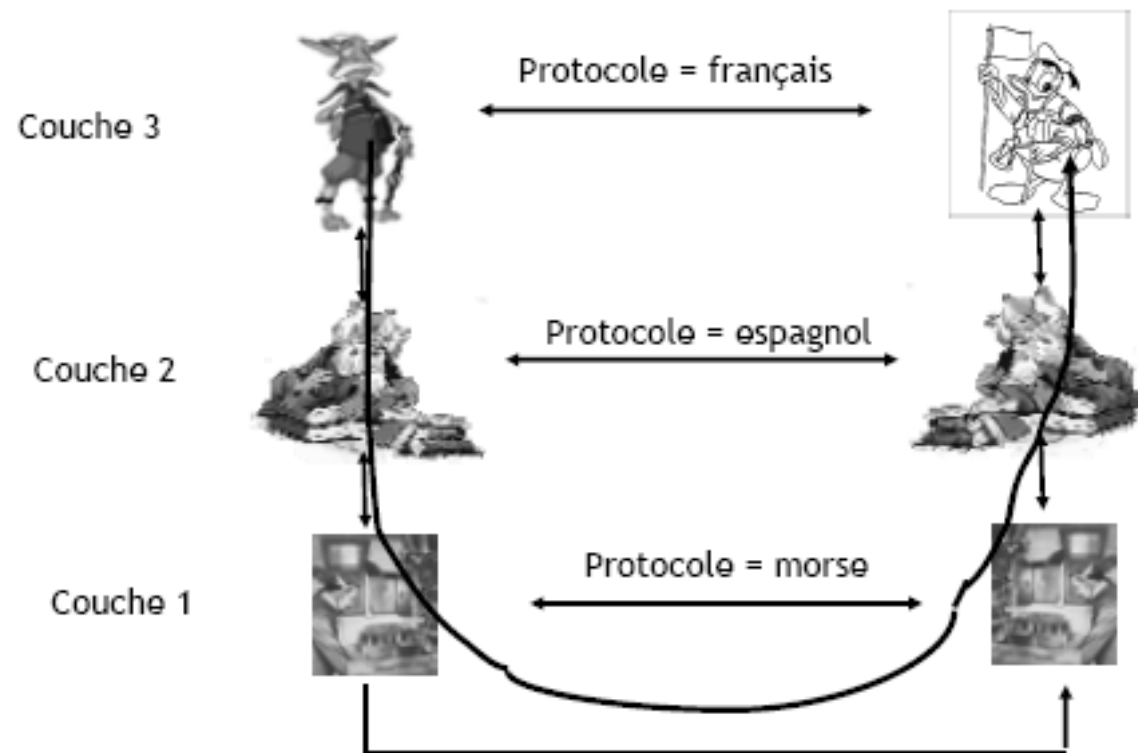
- La couche i du système A dialogue uniquement avec la couche i du système B en utilisant un protocole de niveau i .
- Deux couches de niveau i ne peuvent dialoguer qu' en traversant les couches $j < i$.
- Pour mieux comprendre, un exemple :
 - Soient 2 explorateurs français, l'un en Espagne, l'autre en Bolivie
 - Ils ne peuvent parler directement car ils ne savent pas utiliser le télégraphe
=> *médium de transmission*
 - Ils ont besoin d'un technicien pour envoyer et recevoir les infos. => *couche de niveau 1*
 - Ils ne parlent pas espagnols, ils ont besoin d'un interprète. => *couche de niveau 2*

Généralités

Communications entre couches

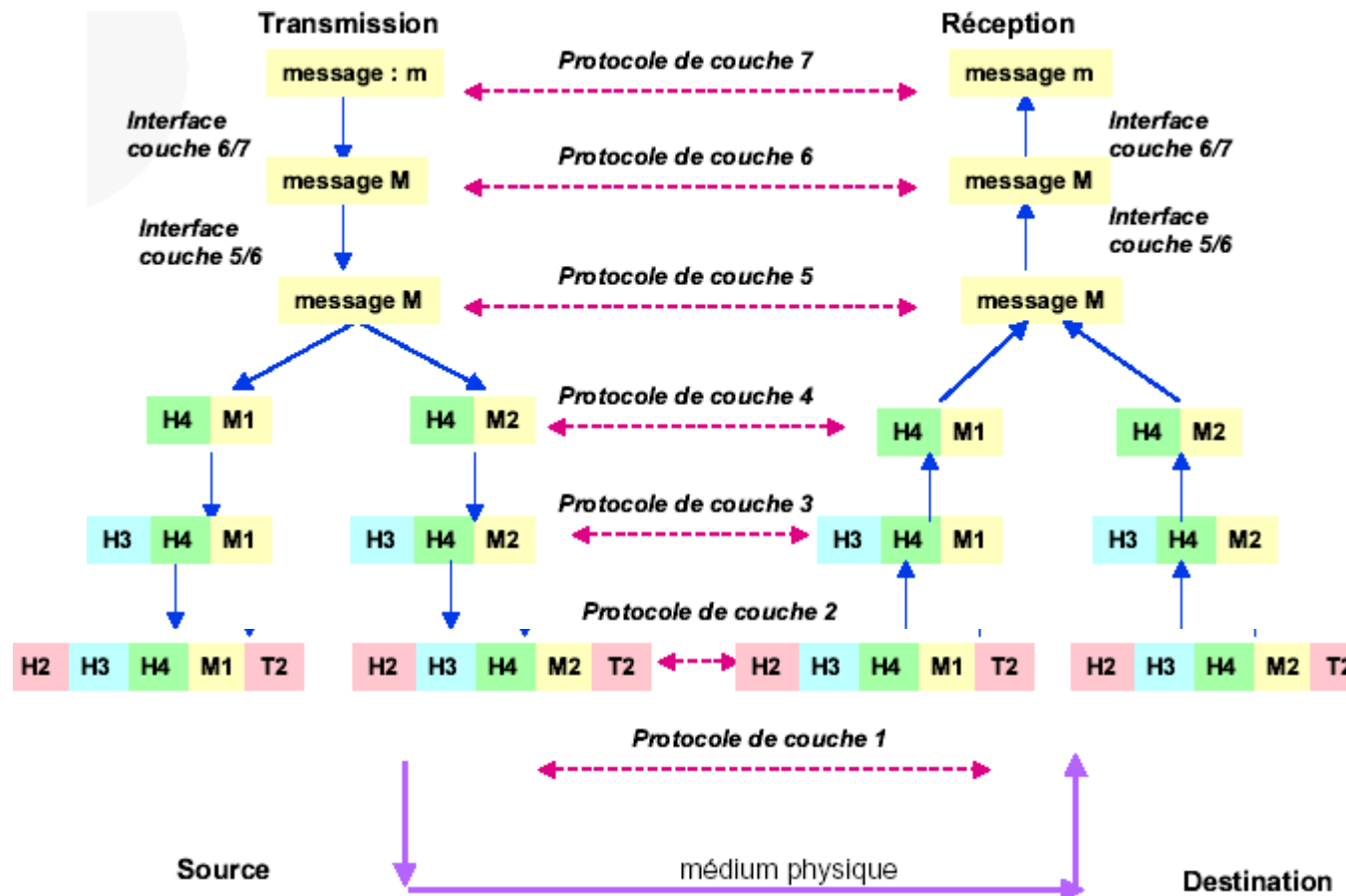
Rappel

- ❑ Les explorateurs (niveau 3) communiquent en traversant les couches.



Généralités

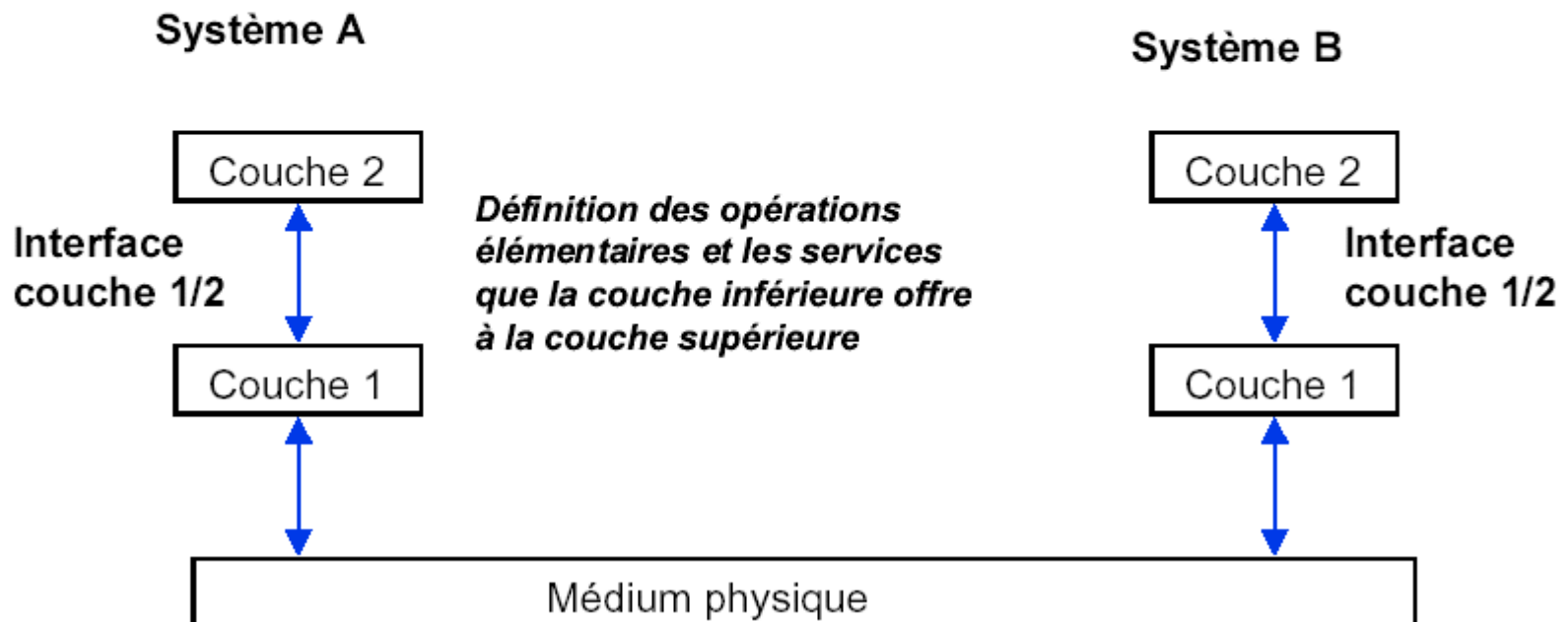
Rappel



Généralités

Rappel

- Organisation en séries de couches ou niveaux.
 - leur nombre, leur nom, leur fonction varie selon les réseaux
 - l'objet de chaque couche est d'offrir certains services aux couches plus hautes
 - ces dernières ne connaissant pas la mise en oeuvre de ces services.



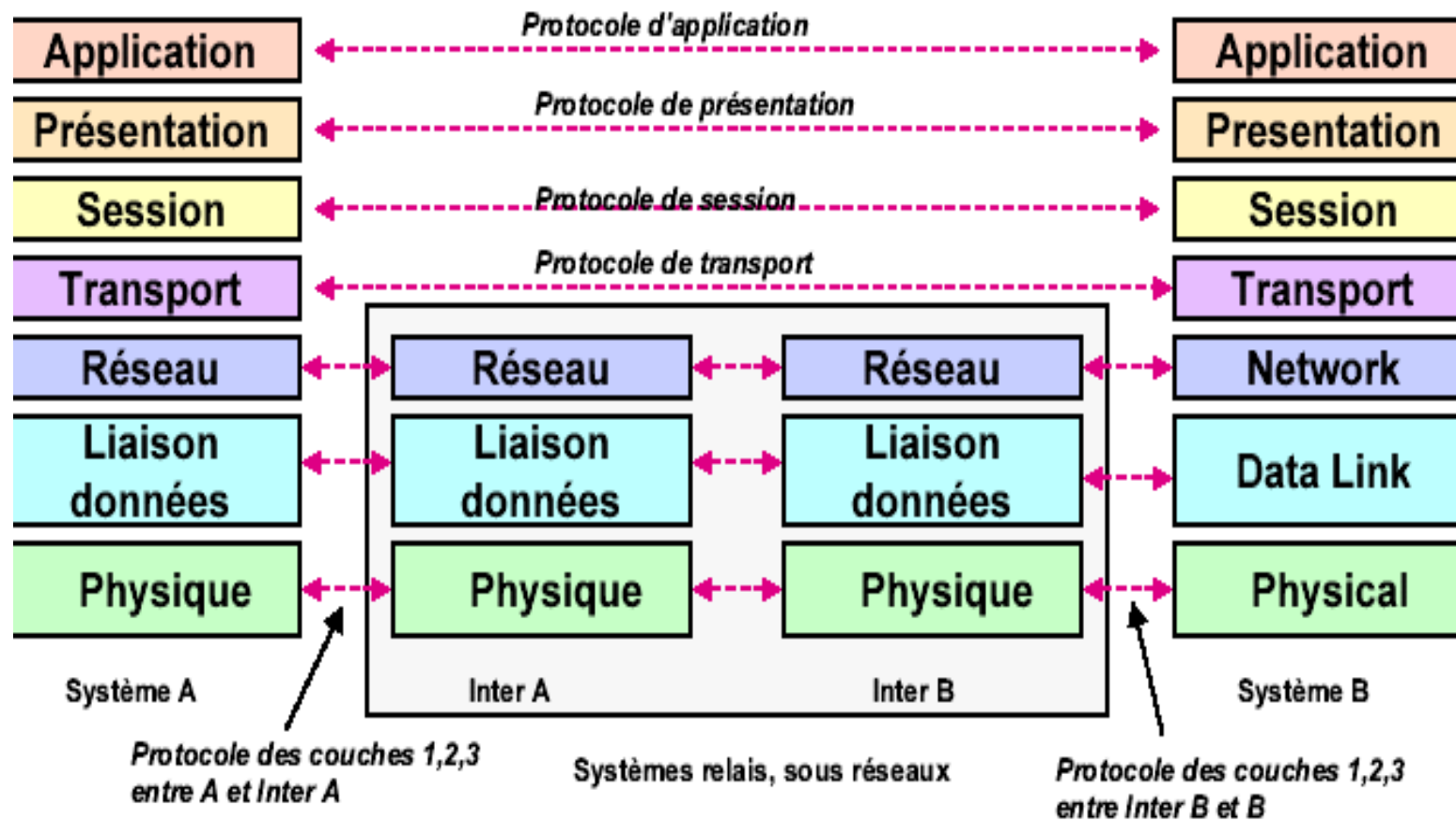
Modèles de référence

Rappel

- Le modèle OSI
 - Norme
 - Très précis
 - Vaste
- Le modèle Internet ou TCP/IP
 - Standard de fait
 - Plus ciblé
 - Plus pratique
 - Imposé par sa simplicité
- Tous 2 des modèles de couches

OSI : Modèle de Référence

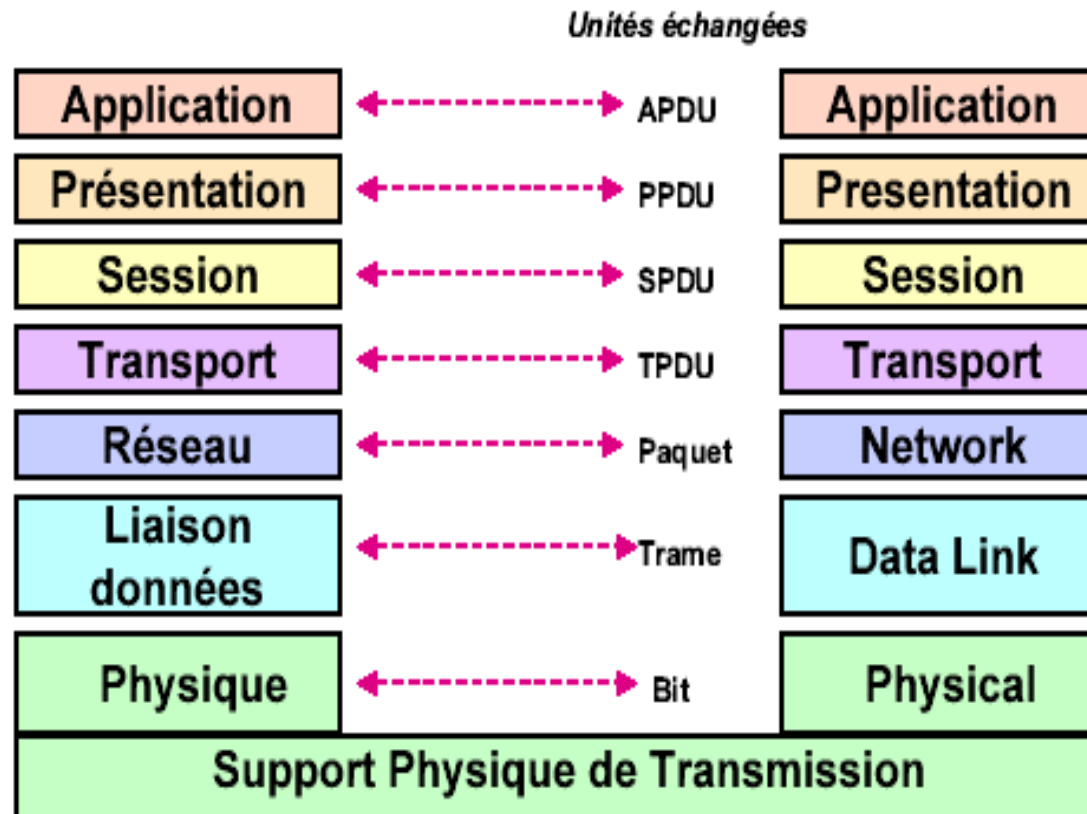
Rappel



OSI : Modèle de Référence

Rappel

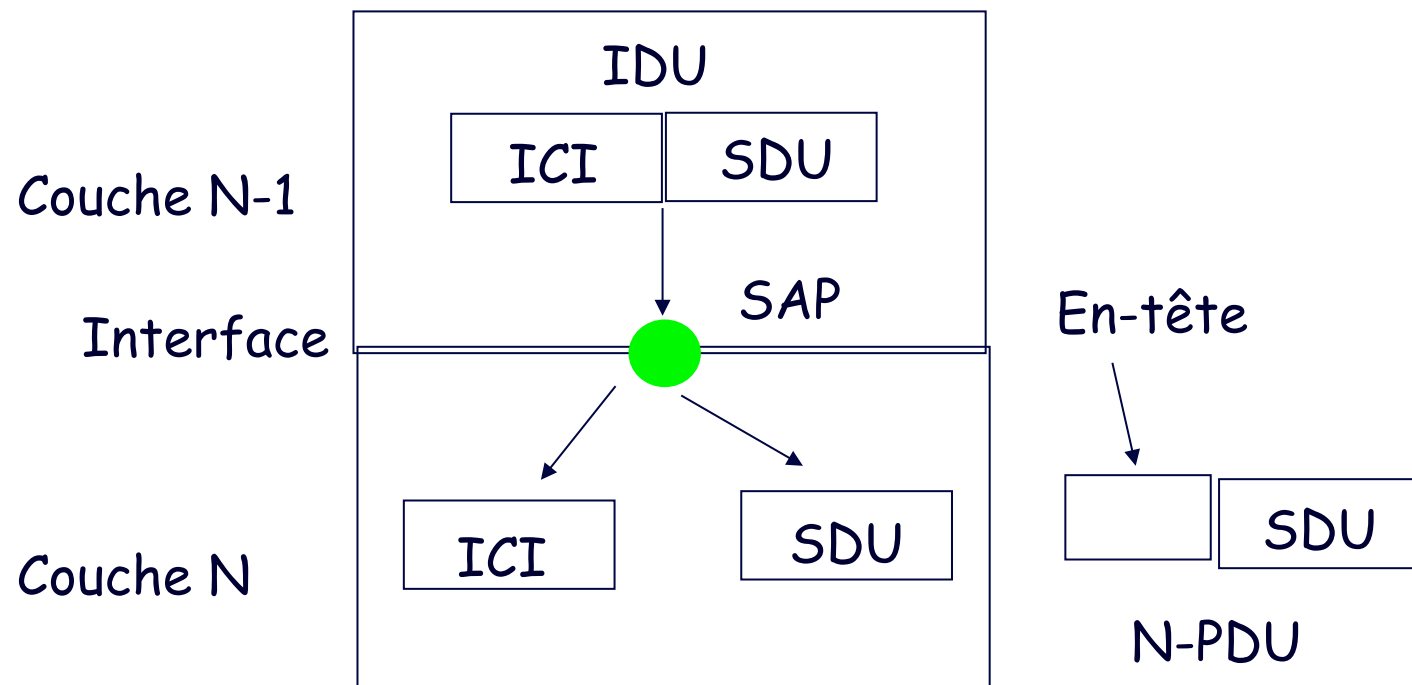
- 1) ISO 7498-1: le modèle de référence OSI de base
- 2) ISO 7498-2 : l'architecture de sécurité
- 3) ISO 7498-3 : la dénomination et l'adressage
- 4) ISO 7498-4 : le cadre général pour la gestion OSI
- 1/Ad-1) : la transmission en mode sans connexion
- 1/Ad-2) : la transmission en multipoint



PDU : Protocol Data Unit

OSI: SAP-SDU-PDU

Rappel



IDU: Interface Data Unit
ICI: Interface Control Information
SDU: Service Data Unit
SAP: Service Access Point
N-PDU: N-Protocol Data Unit

Le Modèle OSI

Rappel

N°	Nom	Fonctions de la couche
3	Réseau	Elle réalise l'acheminement et le routage (choix d'un chemin) des informations au travers du réseau.
2	Liaison	Elle permet le transfert fiable de données entre systèmes adjacents (directement connectés). Elle détecte et corrige des erreurs de transmission. Elle contrôle et régule le flux d'information sur la liaison.
1	Physique	Elle décrit les interfaces mécaniques et électriques et les protocoles d'échange des bits. Par exemple elle définit les modalités de transmission (half ou full duplex), le type de liaison (parallèle ou série), le codage des informations, le fonctionnement des interfaces électriques, etc.

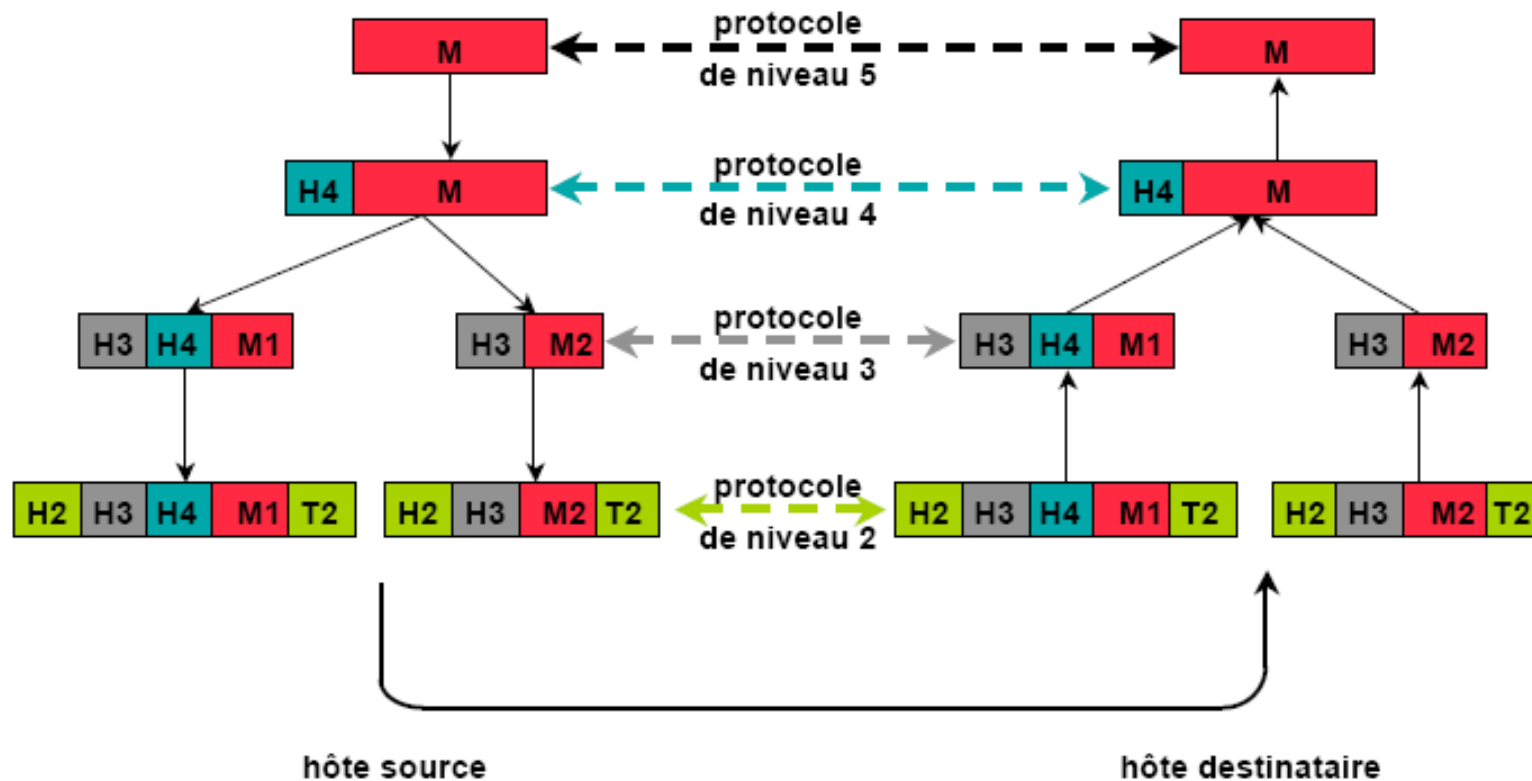
Le Modèle OSI

Rappel

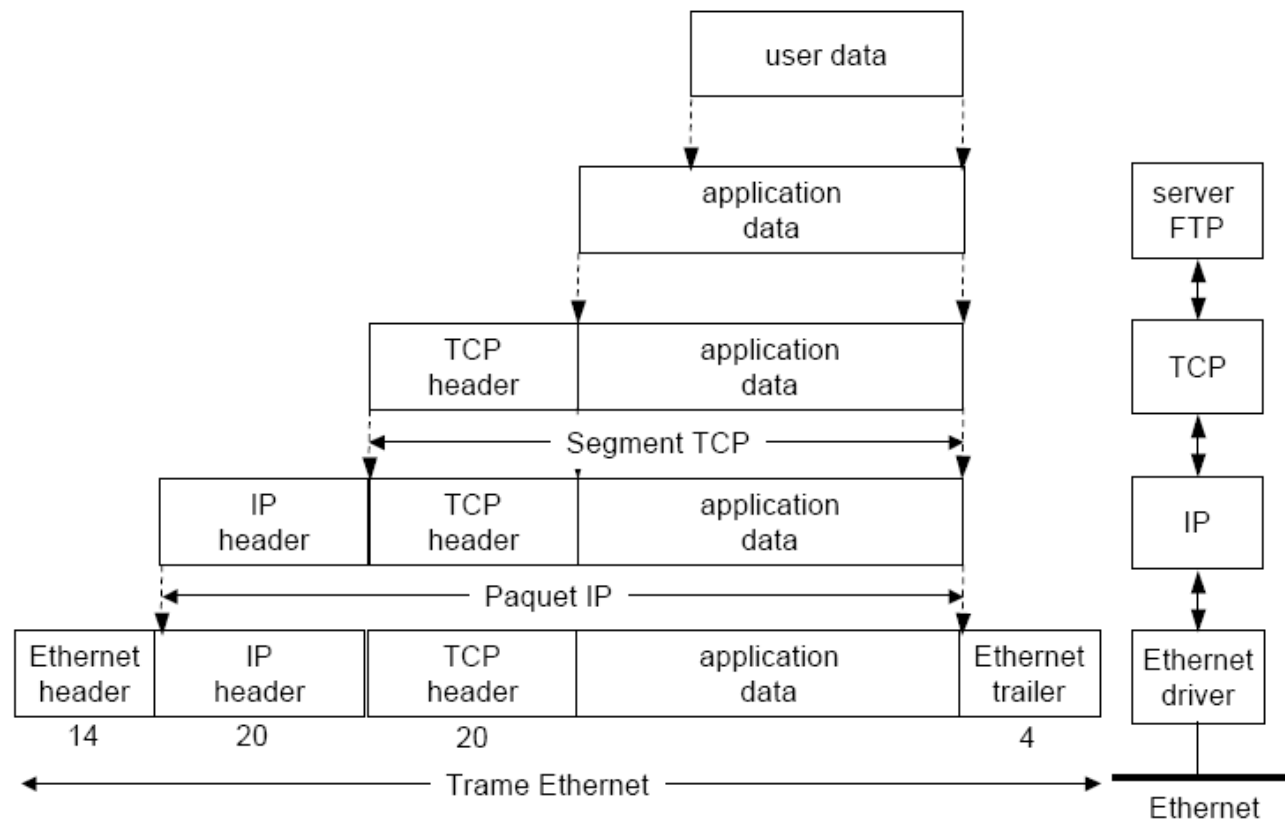
N°	Nom	Fonctions de la couche
7	Application	Elle définit les mécanismes communs aux applications et la signification des informations échangées.
6	Présentation	Elle se préoccupe de la syntaxe, compression, cryptage.
5	Session	Elle fournit les outils de synchronisation et de gestion du dialogue entre les entités communicantes.
4	Transport	Elle fournit les moyens de transport d'information d'un bout à l'autre d'un réseau entre deux utilisateurs situés dans des systèmes différents, indépendamment des caractéristiques du réseau réellement utilisé et de la présentation des données.

Encapsulation / Décapsulation

Rappel



Encapsulation TCP/IP : exemple *Rappel*



Fin du Rappel
