Contenu du cours

10h de Cours

Bases des réseaux, modèle OSI, TCP/IP

La liaison physique

Les réseaux Ethernet, ATM, SONET, ADSL

Architecture INET: adressage, multicast, congestion, IP, TCP, UDP, ARP, DNS, ...

Les protocoles pour le transport des images animées : RTP, RSVP, RTCP, RTSP, HTTP

Quelques applications et outils: streaming, VOD, MBONE

Objectifs des réseaux

partager des ressources : données ou équipements accessibles par tous

- fichiers, imprimantes, applications, ...

assurer une plus grande fiabilité : ne pas être dépendant d'un serveur ou d'une liaison :

- domaines sensibles militaires, bancaires, ...

réduction des coûts : meilleur rapport prix/performances pour le client/serveur

faciliter la communication, les loisirs

Caractéristiques physiques des réseaux

Deux types de réseaux :

- à *diffusion* : un message vers tous, seul le (ou les) destinataires s'en sert.
  - exemple : radio, télévision
- *point à point* : un message est transmis de proche en proche vers le destinataire : routage nécessaire dans ce cas.
  - exemple : la Poste

Types de commutation

Impossibilité d'avoir une liaison permanente entre chaque couple de station : commutateurs nécessaires

3 types de commutations :

- commutation de circuit
- commutation de messages
- commutation de paquets

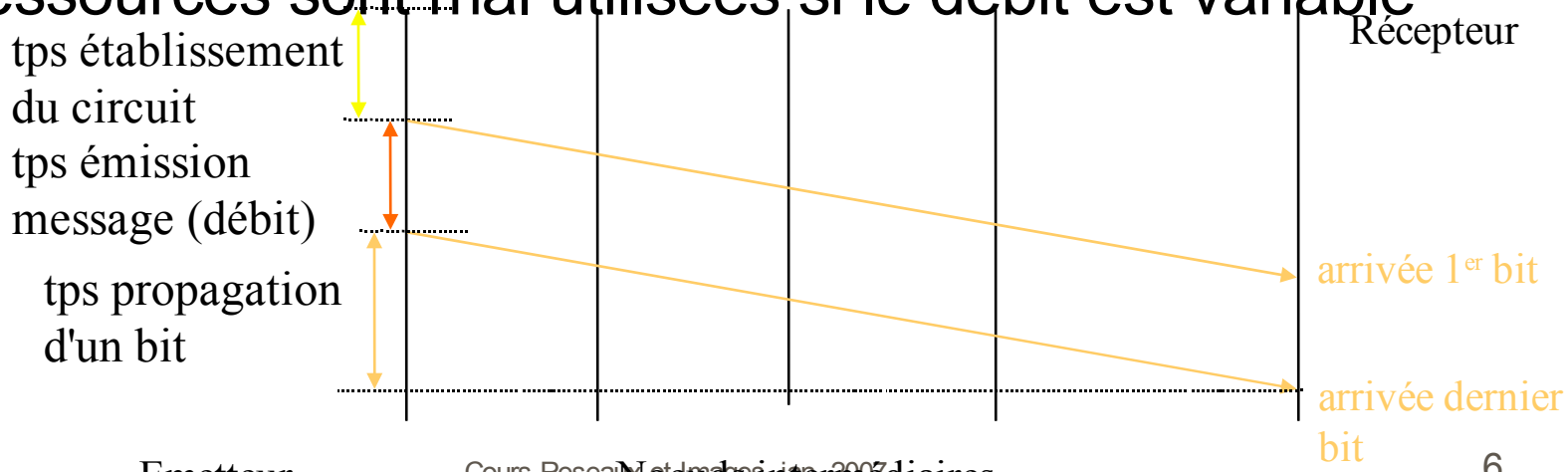
Commutation de circuit

une communication ☝ un circuit est établi (un ensemble de lignes est réservé)

exemple : RTC (Réseau Téléphonique Commuté), RNIS

Avantage : le temps de traversée est court

Inconvénients : l'établissement du circuit est long, les ressources sont mal utilisées si le débit est variable



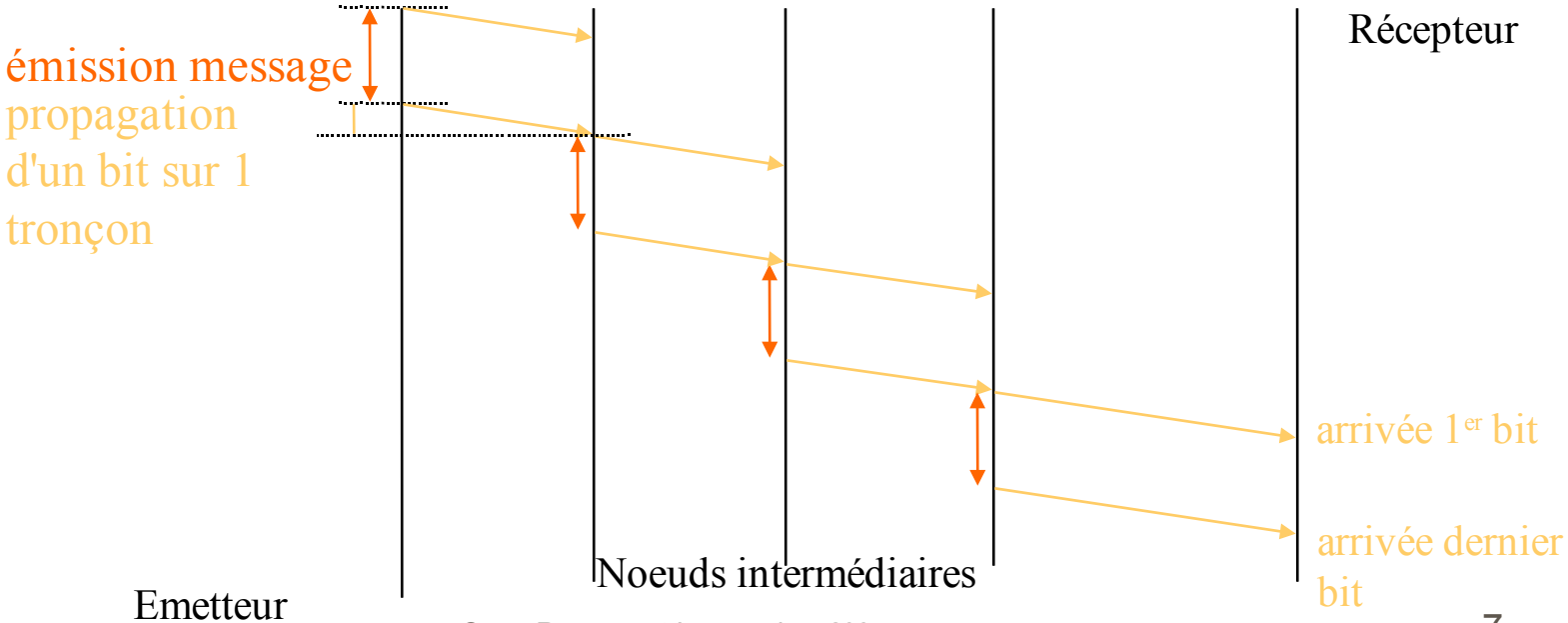
Commutation de messages

progression de proche en proche des messages, stockés sur les noeuds intermédiaires

exemple : le courrier pour la Poste

Avantage : pas de connexion

Inconvénients : delais de traversée longs, gestion/stockage des messages

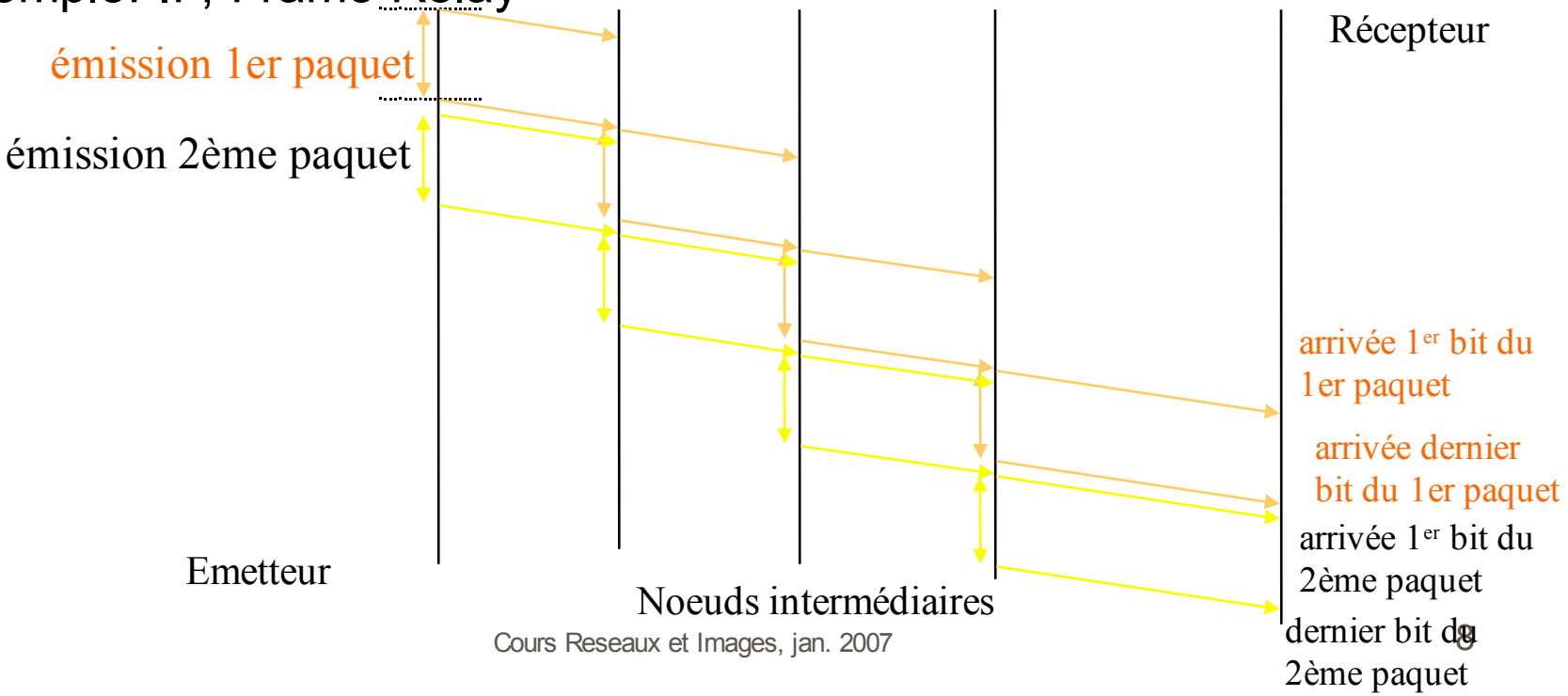


Commutation de paquets

organisation du message à transmettre en paquets de taille bornée; les paquets de plusieurs communications peuvent se succéder sur une même ligne

Avantages : temps de traversées courts, meilleure utilisation des lignes, gestion du commutateur simplifié

Exemple: IP, Frame Relay



Taille d'un réseau

d = distance entre deux machines

- d<1 m, machine multiprocesseurs (parallèle)
- d<1 km, réseau local (LAN, ou RLE) : entreprise, campus
- d<10 km, réseau métropolitain (ville)
- d<1000 km, réseau longue distance (WAN)

LAN : Local Area Network

taille restreinte ☝ simplification de la gestion réseau (délai de transmission borné)

topologie : surtout à diffusion

bus : une seule machine autorisée à émettre; pb de collision, d'arbitrage centralisé ou réparti

exemple : Ethernet à 10, 100, 1000 Mbit/s

anneau : chaque bit est autonome et se déplace indépendamment du paquet auquel il appartient

exemple : Token Ring (IBM) à 4 ou 16 Mbit/s

WAN : Wide Area Network

un ensemble d'ordinateurs hôtes sont reliés par un sous-réseau de communication

le sous-réseau est constitué de lignes de transmissions et de commutateurs (routeurs)

topologie : surtout en point à point (sauf satellites) : store and forward

étoile, anneau, arbre, maillage complet, maillage irrégulier, anneaux interconnectés...

Logiciel de réseau

Organisation en séries de couches (ou niveaux)

chaque couche fournit des services aux couches supérieures, sans détails d'implémentation

une interface est la partie logicielle présente entre deux couches successives

un protocole représente les règles et conventions de la communication entre deux couches de même niveau

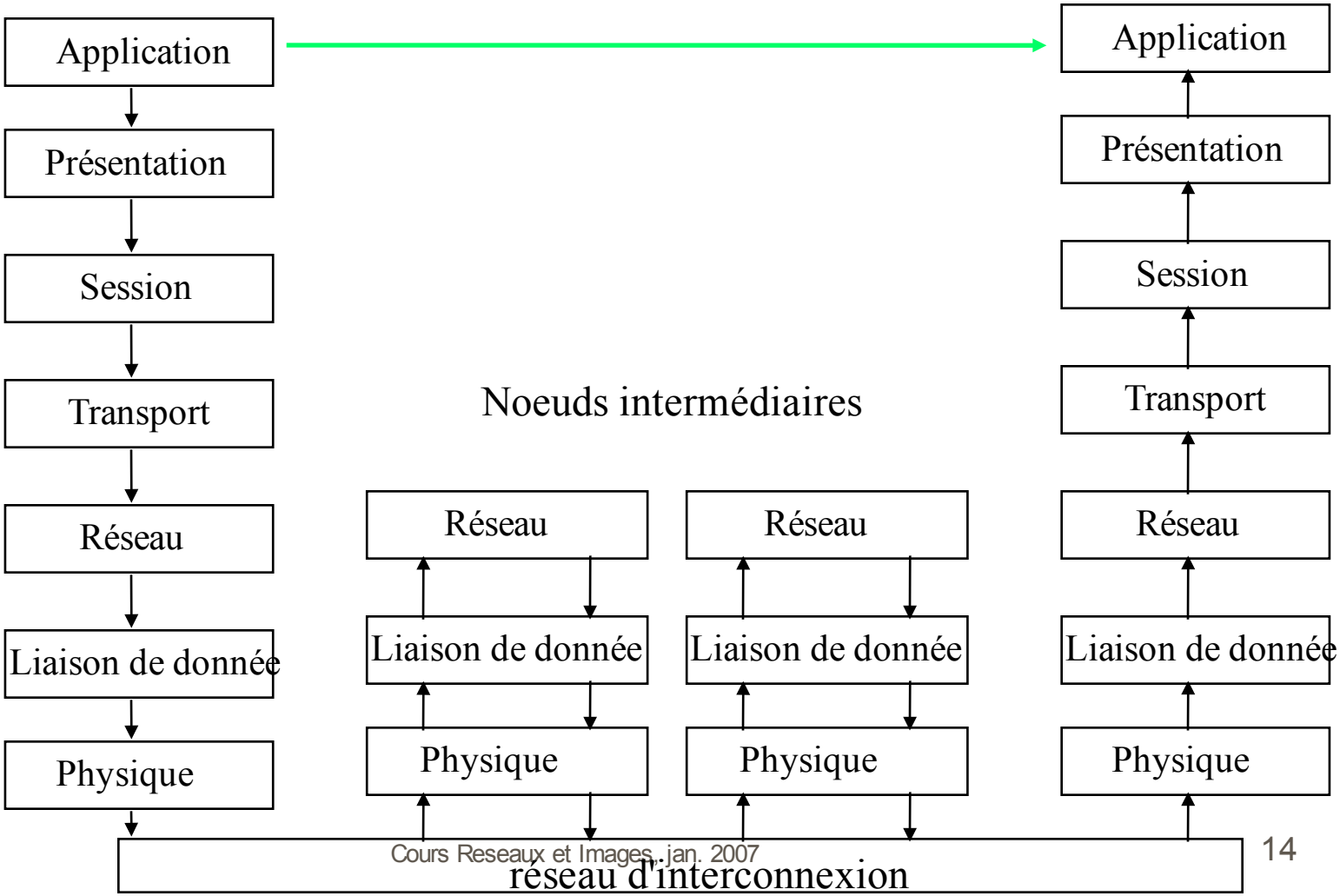
Deux modèles de références

- modèle OSI de l'ISO (International Standard Organisation)
  - normalisé
  - 7 couches
- modèle TCP/IP
  - norme de fait dans Internet
  - 4 couches

Modèle OSI : vue générale

transmission **physique** : traversée **verticale**

transmission **logique** : traversée **horizontale**



Modèle OSI : couche physique

Transmission brute de bits sur le canal physique

- quelle tension représente 0 ou 1 ?
- quelle durée de transmission pour 1 bit ?
- canal bidirectionnel ?
- quelle connectique utiliser ?

Modèle OSI
couche liaison de données

Transformer la transmission brute en une transmission exempte d'erreurs

- détection et correction des erreurs
- découpe des données en trames
- gestion des acquittements des trames
- gestion des duplications des trames
- gestion du flux (émetteur rapide, récepteur lent) sur une liaison point à point

Modèle OSI : couche réseau

Gestion du sous-réseau

- donne la manière dont les paquets sont acheminés de la source à la destination : routage
- contrôle de congestion pour éviter les engorgements sur le sous-réseau
- transit entre réseaux hétérogènes : adressage, compatibilité de protocoles

Modèle OSI : couche transport

Assurer une transmission efficace et transparente des évolutions technologiques

- elle peut décider de créer plusieurs connexions réseau pour une connexion transport : augmentation du débit
- au contraire, elle peut regrouper plusieurs connexions transport sur une connexion réseau : diminution du coût
- gestion de **bout en bout** d'une conversation entre une source et une destination.

Modèle OSI
couches supérieures

couche session : établir une session entre deux machines (mécanisme des RPC : Remote Procedure Call)

couche présentation : assurer une compatibilité sur la syntaxe et la sémantique des données (mécanisme XDR : eXternal Data Representation)

couche application : la plus haute

Modèle TCP/IP: 4 couches

la couche **hôte-réseau** :

rien de défini, si ce n'est que la connexion physique doit pouvoir envoyer des paquets IP

la couche **internet** :

elle doit permettre l'injection de paquets et leur acheminement indépendant les uns des autres;

format de paquets et protocole IP (Internet Protocol);

le réordonnancement des paquets est laissé aux couches supérieures.

TCP/IP

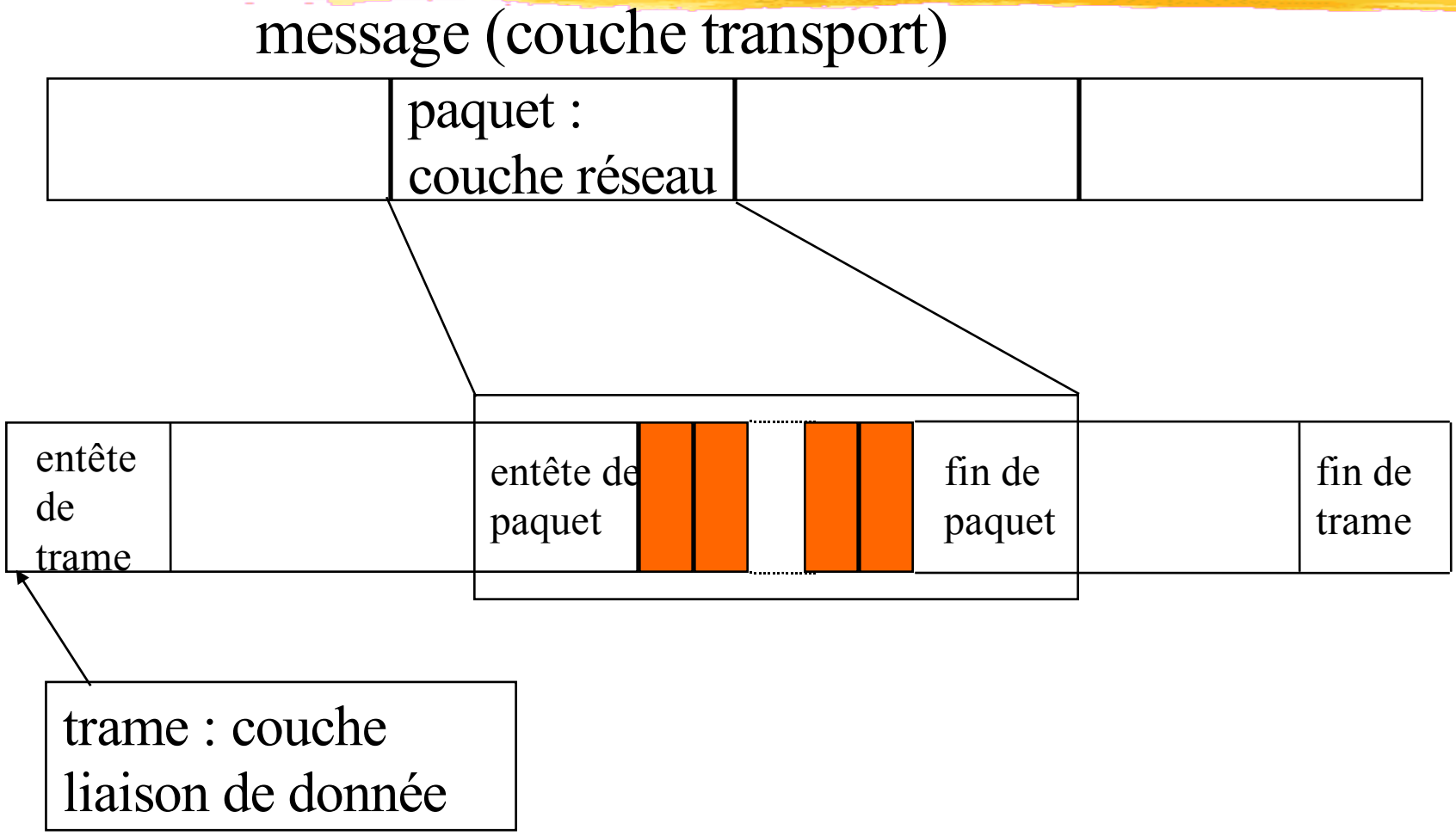
la couche **transport**

TCP : Transport Control Protocol : protocole fiable orienté connexion, contrôle de flux

UDP : User Datagram Protocol : non fiable, sans connexion : destiné aux applications qui souhaite faire le séquencement et contrôle de flux elle-même (par exemple transport de vidéo, ...)

la couche **application** : Telnet, FTP, DNS, NNTP, HTTP

Fragmentation



La couche physique : introduction

transmission basée sur le principe de la propagation des ondes :

- électriques (câbles métalliques)
- electromagnétiques (faisceaux hertziens, lumière)

l'onde émise est modifiée en fonction de l'information à émettre.

Notions de traitement du signal (Fourier, Nyquist, Shannon, affaiblissement, bande pasante, bruit), Support physique, Multiplexage

Décomposition en série de Fourier

Toute fonction périodique g(t) suffisamment régulière, de période T, peut être décomposée en série de Fourier :

$$g(t) = 1/2c + \sum_{n=1..} a_n \sin(2\ nft) + \sum_{n=1..} b_n \cos(2\ nft)$$

où : f = 1/T = fréquence fondamentale (en hertz)

a_n, b_n = amplitudes de la $n^{ième}$ harmonique

c = composante continue

Si T, c, a_n, b_n sont connus, g(t) peut être reconstruite

Inversement :

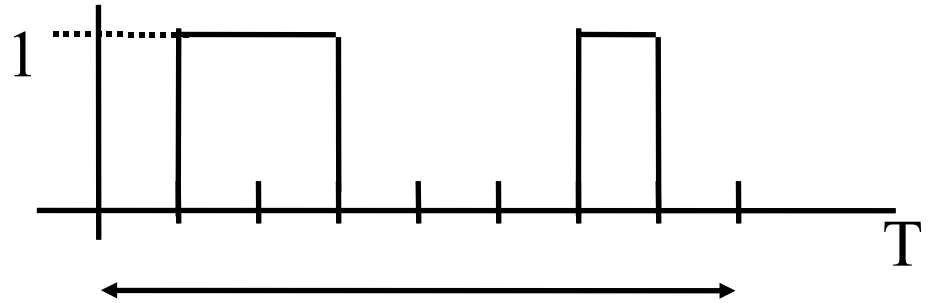
$$a_n \quad \frac{2}{T} \int_0^T g(t)\sin(2\ nft)dt$$

$$b_n \quad \frac{2}{T} \int_0^T g(t)\cos(2\ nft)dt$$

$$c \quad \frac{2}{T} \int_0^T g(t)dt$$

Exemple

considérons g(t) consistant en l'émission cyclique du caractère ASCII 'b': 01100010



$$a_n \quad \frac{1}{n}\cos\frac{n}{4} \quad \cos\frac{3\ n}{4} \quad \cos\frac{6\ n}{4} \quad \cos\frac{7\ n}{4}$$

$$b_n \quad \frac{1}{n}\sin\frac{3\ n}{4} \quad \sin\frac{n}{4} \quad \sin\frac{7\ n}{4} \quad \sin\frac{6\ n}{4}$$

$$c \quad \frac{3}{4}$$

Signal reconstitué

Plus le nombre d'harmoniques augmente, et plus on peut facilement retrouver le signal d'origine

Limitations dues à la ligne

T = temps de transmission de 8 bits

Si débit = *d* bit/s, on a T = 8/d et f=d/8 Hz

La ligne physique de transmission ne laisse passer que les fréquences inférieures à un seuil : (3000 Hz pour le RTC)

- limitation du nombre d'harmoniques: 3000/(d/8)

d (bit/s)	T (ms)	f (Hz)	Nbres harmoniques
300	26.67	37.5	80
600	13.33	75	40
1200	6.67	150	20
...			
9600	0.83	1200	2
19200	0.42	2400	1
38400	0.21	4800	0

Affaiblissement du signal

Un canal transforme le signal émis par :

- affaiblissement
- déphasage

La transformation dépend de la fréquence

S'applique sur chaque harmonique :

$a \sin(2 \quad ft)$ devient $a' \sin(2 \quad ft- \quad)$

avec : $a' < a$ = affaiblissement

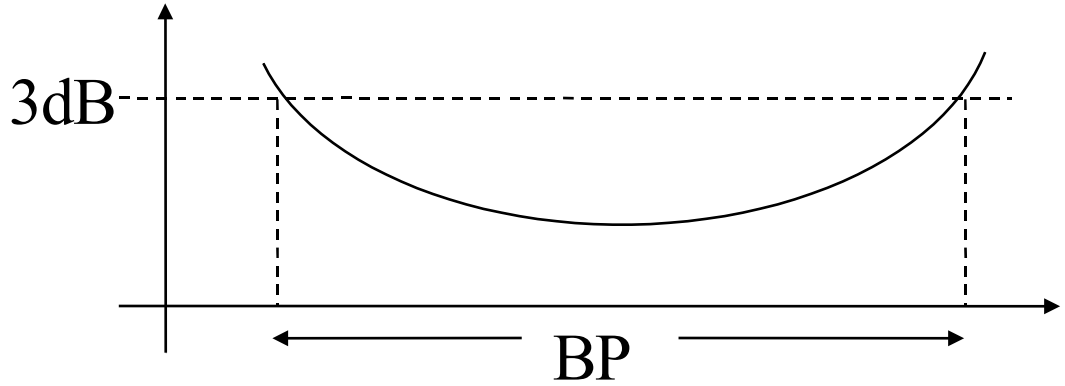
= retard de phase

$Aff = 10 \log(P_E/P_S)$ décibels (dB)

Bande passante

Définition :

la bande passante à n décibels est l'intervalle de fréquence où l'affaiblissement est inférieur à n décibels



On considère généralement la BP à 3 dB

Ex : le RTC a une BP = [300,3400] à 3dB, ce qui correspond à l'essentiel des fréquences vocales

1 support de transmission ☝ 1 BP particulière

Débit maximum d'un canal

Un signal sur un canal de BP *H* ne contient que les harmoniques de fréquences comprises entre 0 et H.

Théorème de Nyquist : un tel signal peut être interpolé exactement en l'échantillonnant à une fréquence 2H

D'où : $D_{max} = 2H \log_2 V$ bit/s

où V = valence du signal (nbre de valeurs possibles en entrée)

ex RTC : H = 3kHz donc D_{max} = 6000 bit/s si V = 2 (signal binaire)

Débit maximum : le bruit

La formule précédente ne limite pas le débit : si on augmente indéfiniment V, on augmente le débit

Présence de bruit !

Th. de Shannon : $D_{max} = H \log_2(1+S/N)$ bit/s

où S et N sont les puissances du signal et du bruit (rapport généralement exprimé en décibels par la formule $10\log_{10}(S/N)$)

ex RTC : rapport = 30dB, D_{max} = 30000 bit/s

Deux types de transmission

En fonction du débit souhaité, il faut maintenir assez d'harmoniques dans la BP

transmission en bande de base :

le signal est envoyé tel quel, ce qui nécessite beaucoup d'harmoniques et donc une grande BP. transformation suite de bits en signal (électrique, lumineux,...): codage NRZ, Manchester,...

transmission par modulation (modem)

on utilise la transposition de fréquence, le nombre d'harmoniques à transmettre peut être limité.

Transmission par modulation

transposition de fréquence en modulant une onde porteuse (dont la fréquence est choisie en fonction de la BP disponible)

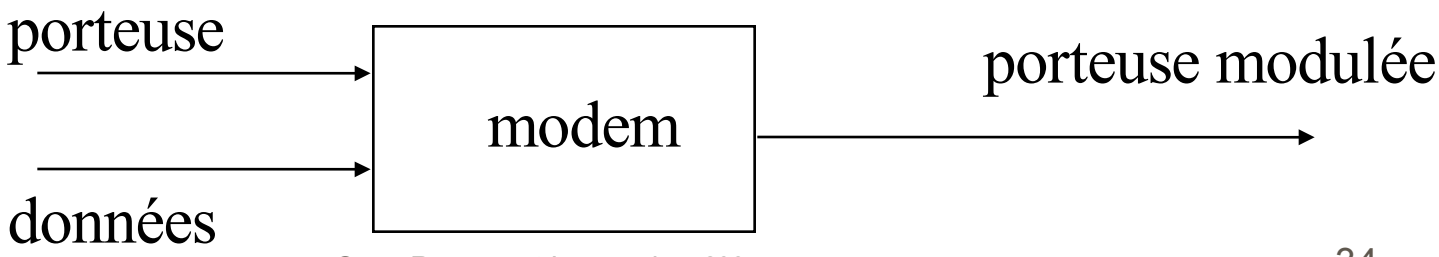
soit a(t) = a sin(t+) la porteuse

a = amplitude

f = /2 = fréquence

= phase

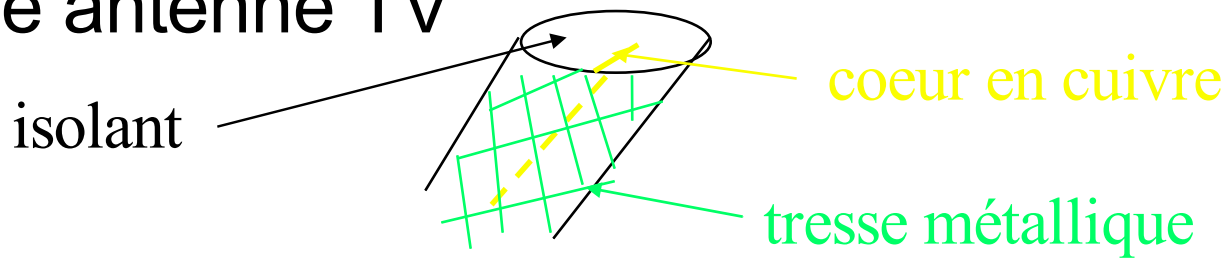
l'information à transmettre est codée en modifiant un ou plusieurs paramètres de la porteuse



Les médias de transmission

câble électrique à paire torsadée : le plus ancien. 2 fils enroulés de façon hélicoïdale (comme l'ADN), pour limiter l'interférence. Régénération du signal au delà de quelques km. BP 4000 Hz. ex : RTC

câble coaxial "bande de base" : meilleure isolation. ex : câble antenne TV



BP dépend des conducteurs, des isolants, de la longueur. 1 à 2 Gbit/s sur des distances de l'ordre du km

Câble coaxial Large Bande

Ethernet, TV par câble

meilleure qualité, moins d'affaiblissement

- Grande BP
- divisé en plusieurs canaux, par ex de 6 MHz
- chaque canal transmet indifféremment de la vidéo ou du son (numérisés) ou des données.
- dans les 2 sens (Full Duplex) :
  - soit deux câbles
  - soit une gamme de fréquences pour chaque sens

La fibre optique

BP énorme : entre 25000 et 30000 GHz

Th de Nyquist et Shannon désuets

débit théorique = 50000 Gbit/s

débit actuel : 100 Gbit/s en labo

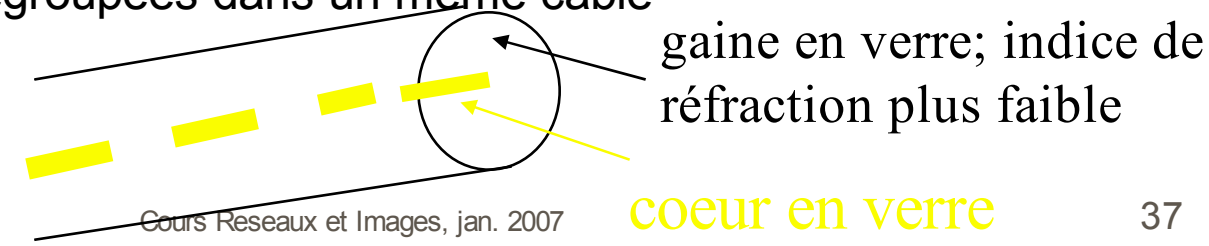
difficulté dues au matériel de conversion électricité-lumière

l'indice de réfraction donne la vitesse de propagation : indice = 1.45, ce qui donne comme Vitesse : 1/1.45 * c = 70% c

(vitesse de 5µs par km, équivalente au fil de cuivre)

Avantages :

- moins de répéteurs de signaux
- pas d'interférences électromagnétiques, pas de corrosion
- plusieurs fibres regroupées dans un même câble



Communications par satellites

ré-émission depuis un satellite : diffusion

transpondeurs : amplification des signaux, changement de fréquence (contre les télescopages)

Satellites géostationnaires

- 12 à 20 transpondeurs par satellite, BP de 36 à 50 MHz
- un transpondeur avec débit de 50 Mbit/s : 2 possibilités
  - soit un seul canal
  - soit 80 canaux téléphoniques à 64 Kbit/s (Multiplexage)
- vitesse du signal = vitesse des ondes dans le vide = c
- Mais distance grande : tps propagation = 270 ms
  (à comparer à 5µs par km pour le filaire)

Multiplexeurs et Concentrateurs

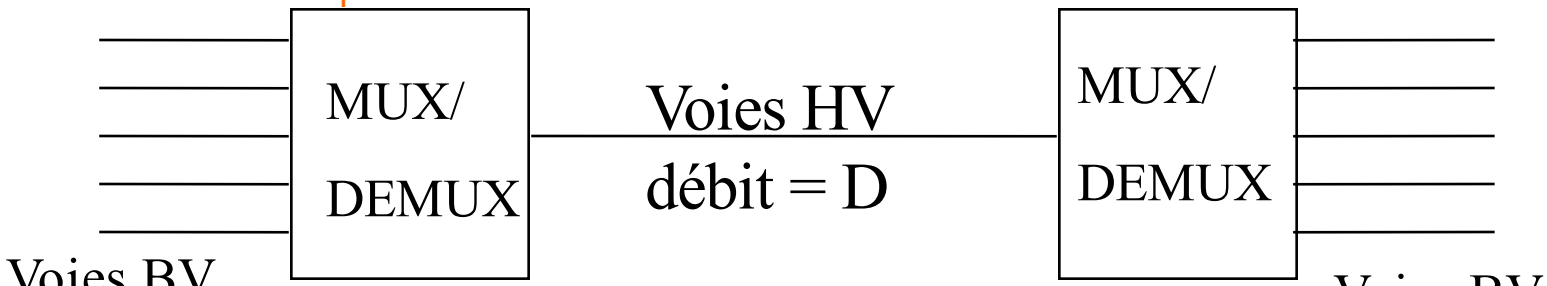
une voie Haute Vitesse (HV) écoule le trafic de plusieurs voies Basses Vitesses (BV)

utilité économique : le coût d'une ligne croît moins vite que son débit

multiplexeur : acheminement sans traitement des données des voies BV

concentrateur : multiplexeur statistique + des protocoles de niveau supérieur

efficacité : $e = d_i / D$



Multiplexages statiques

La voie HV est partagée de manière statique entre les voies BV

Efficacité < 1

Partage possible

- suivant les fréquences
- suivant le temps

Multiplexage fréquentiel

modulation de fréquence avec une porteuse par voie BV; la BP de la voie HV est découpée, chaque voie BV en utilise une partie.

multiplexeur : transpose le signal d'une voie BV dans la bande de fréquence qui lui est allouée : les bandes doivent être assez éloignées les unes des autres pour éviter les chevauchements

demultiplexeur : filtres passe-bande pour séparer et décoder les différentes voies

Multiplexage en longueur d'onde

même principe pour les ondes lumineuses

les ondes lumineuses se mélangent

utilisation d'un prisme au destinataire pour séparer les faisceaux lumineux.

Avantages :

dispositif passif : très fiable

BP énorme (25000 GHz) : grande possibilité de multiplexage

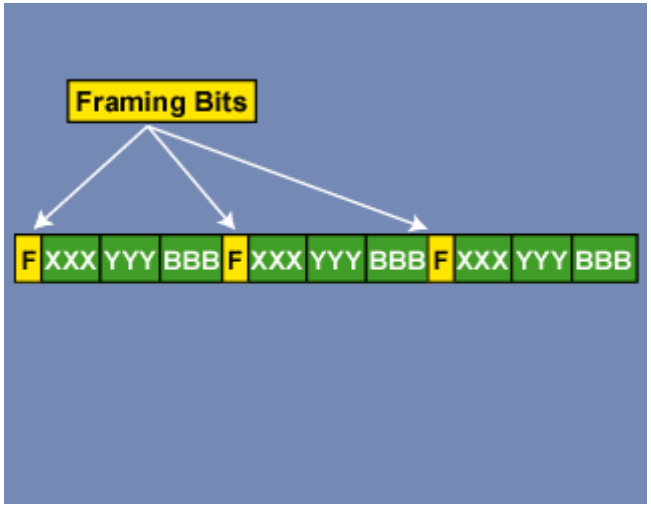
Multiplexage temporel

le temps est découpé de façon fixe en tranches de temps allouées cycliquement aux voies BV (qu'elles aient des données à transmettre ou non)

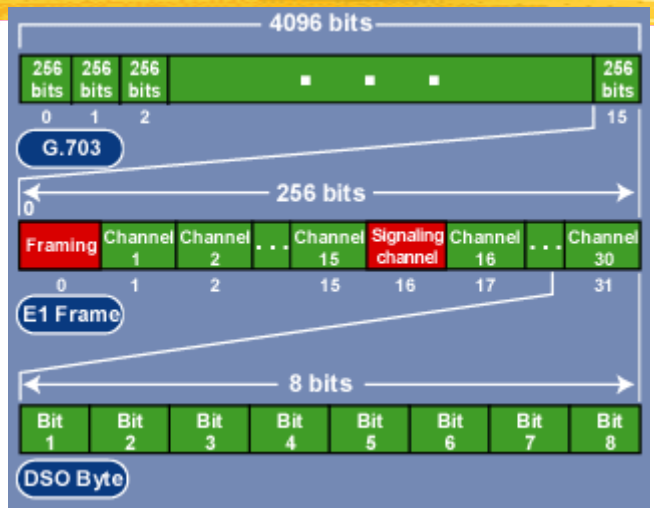
Framing

Agglomération de morceaux de données issus de flux différents suivant un multiplexage temporel

Frame/superframe-extended superframe



Frame Relay (E1-G703)



8 bits = 1 DS0 channel.

30 DS0 channels + 1 framing channel + 1 signaling channel =1 frame E-1 (CEPT-1 : Conférence Européenne des Administrations des Postes et des Télécommunications-1).

16 E-1 frames = 1 frame G.703 (ITU).

Frame Relay

Principe principal: pas de stockage des trames sur les nœuds intermédiaires

-> pas de gestion des erreurs

mais commutation très rapide

Multiplexage temporel statistique

idée : allouer dynamiquement les IT aux voies qui en ont besoin

un séparateur permet de distinguer les voies BV: il apparaît souvent

code à longueur variable (code de Huffman: les caractères qui apparaissent souvent sont codés sur moins de bits).

efficacité > 1 car le débit moyen est souvent inférieur au débit maximum, et on peut prendre D tel que $d_{i\ moyen} < D < d_{i\ max}$

nécessité d'avoir des tampons mémoires pour accepter les surcharges temporaires

La couche liaison de données

Rôle : établir, maintenir, libérer des connexions entre terminaux reliés directement par un support de transmission

Problèmes :

- débit binaire limité
- délai de propagation
- erreurs de transmission

Fonctions :

- contrôle de flux
- détection et contrôle d'erreur
- établissement et libération des connexions
- structuration des données (pour réaliser ces fonctions)

Services offerts par cette couche

sans connexion et sans accusé de réception

- si perte ou altération : couches supérieures
- adapté pour ligne fiable ou pour le temps réel

sans connexion avec accusé de réception

- l'émetteur sait qu'une trame est bien arrivée
- adapté aux liaisons peu fiables (sans fils)
- l'accusé de réception est une optimisation : si erreur, on retransmet une trame, pas un message.

avec connexion et accusé de réception

- établissement d'une connexion
- numérotation des trames
- garantit que les trames n'arrivent qu'une seule fois, et dans l'ordre d'émission
- un canal fiable est fourni à la couche réseau

Contrôle des erreurs

les taux d'erreurs varient :

fibre optique : très faible : 10^{-12}

fils électriques de mauvaise qualité : 10^{-5}

sans fils : 10^{-5}

deux sortes d'erreurs :

erreurs isolées, portant sur 1 bit

erreur en rafale, sur des groupes de bits

ex : si 1 bit est faux sur 1000,

avec des trames de 1000 bits, en moyenne toutes les trames sont fausses.

alors que si les erreurs sont en rafale de 100, un bloc sur 100 sera faux en moyenne.

Stratégies possibles en cas d'erreur

détection simple (ex: bit de parité): alarme

correction :

- automatique par le récepteur (code correcteur): ex: Hamming, Codage polynomiaux (CRC)
- par retransmission
  - avec arrêt et attente : protocole du bit alterné
  - transmission continue : protocole GoBackN
  - transmission continue et retransmission sélective : protocole HDLC

bits de contrôle : diminution du débit utile

nécessité de trouver un compromis

Norme IEEE 802 des LAN et WAN

Les différentes IEEE 802 sont compatibles au niveau liaison de données, mais elles diffèrent :

- au niveau de la couche physique
- au niveau de la sous couche MAC de la couche liaison de données qui contrôle l'accès

Norme 802.3 : réseau Ethernet

Norme 802.5 : anneau à jeton (token ring)

Norme 802.11 : WiFi

Norme 802.3 et réseau Ethernet

réseaux LAN type CSMA/CD-1 persistant

CS : Carrier Sense : écoute du câble avant de transmettre; si il n'y a rien, elle émet, sinon attente.

MA : Multiple Access : toutes les stations peuvent accéder au canal en même temps.

1-persistant : la probabilité d'émettre quand le canal est libre est de 1

CD : Collision Detection : les stations détectent la collision, observent un temps d'attente aléatoire et retransmettent

La trame 802.3 (en octets)

7 octets de préambule (synchro 01010101)

1 délimiteur début : 10101011

6 : adresse destination : adresse Ethernet, statique, positionné par le constructeur : id du constructeur : 3 octets+ numéro de la carte chez le constructeur : 3 octets

6 : adresse source

2 : longueur champ de donnée

[0..1024] : données

[0..46] : remplissage

4 : CRC (contrôle d'erreur)

Nature du remplissage

but : éviter que lors d'une transmission d'une trame trop courte, une collision survienne entre le moment où le dernier bit quitte la source et celui où le premier bit arrive à destination.

moyen : la transmission d'une trame ne peut pas prendre moins de 2 , où est le temps de propagation max jusqu'au bout du câble.

exemple : avec un câble de 2500m, le temps de propagation est de 51,2 µs, ce qui correspond à la transmission de 64 octets (si d=10Mbit/s) remplissage

Si d augmente, la longueur de la trame doit aussi augmenter, ou la longueur du câble diminuer...

Temps d'attente

lors d'une collision, la trame est ré-émise plus tard

après i collisions, un nombre aléatoire T entre 0 et 2^i - 1 est tiré

la station attend T * 51,2 µs avant de retransmettre

au maximum, attente de 1023*51,2 µs

Architecture INET

INET : vue générale

se base sur une infrastructure de niveau 2 (Liaison de Données) existante; par exemple Ethernet…

architecture en couche pour :

- niveau Réseau (IP, OSPF, ARP, ICMP)
- niveau Transport (TCP/UDP/RTP)
- niveau Session/Présentation/Application (SMTP, TELNET, HTTP, FTP, SNMP, RPC, DNS)

description des protocoles dans des RFC : Request For Comment

Inet: plan

- la couche Réseau
  - le problème du routage
  - l'adressage
  - le contrôle de congestion
  - IP, ARP
- la couche Transport
  - communication de bout en bout
  - TCP, UDP
- les couches hautes :
  - Application : DNS

La couche réseau

le niveau Liaison de Données fourni un transfert fiable entre deux noeuds directement reliés par une ligne

un réseau = un ensemble de lignes, de noeuds intermédiaires

Les problèmes :

- adressage : comment nommer les machines ?
- routage : trouver un chemin au destinataire ?
- fragmentation : réseaux traversés différents ?
- contrôle de congestion ?
- partage de liaison ?

Deux approches de niveau réseau

approche datagramme (sans connexion)

- paquets indépendants
- pas de connexion
- chaque paquet doit contenir l'@ destination pour pouvoir être traité indépendamment
- exemple : IP

approche circuit virtuel (connexion)

- chemin établit à la connexion
- les paquets contiennent seulement le numéro de circuit utilisé
- chaque noeud stocke les deux voies logiques (entrée-sortie) pour chaque circuit
- exemple : X25, ATM

Le routage

comment choisir un chemin le meilleur possible ? Sur quels critères ?

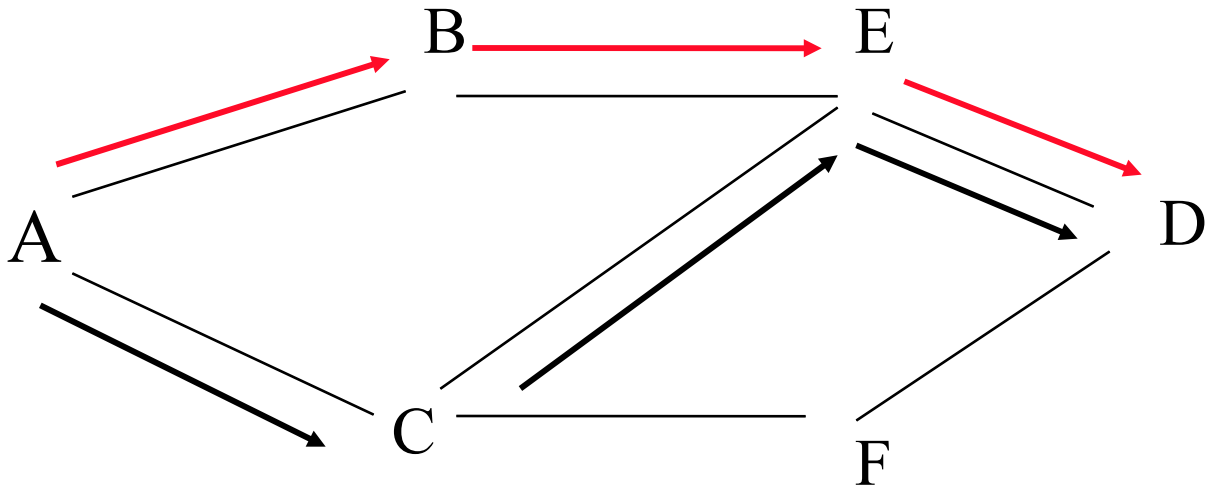


table de routage : sur A, pour envoyer un message à D, je l'envoie d'abord à C

Routage : critères de choix

minimiser le délai de transmission

maximiser le débit

prévenir la congestion

assurer l'équité entre utilisateur

gérer les défaillances du réseau

s'adapter aux modifications de configurations du réseau

Algorithmes statiques ou dynamiques, locaux ou globaux, centralisés ou répartis

Les techniques centralisées: noeud spécialisé

routage statique :

optimisation en fonction de caractéristiques statiques, distribution des tables de routage

pas de gestion défaillances ni de congestions

routage adaptatif :

recalcul des tables en fonction d'informations qui arrivent au noeud spécialisé : longueurs des files d'attente, pannes, ...

mises à jour synchrones (intervalle fixes) ou déclenchées par événement (seuil de congestion, panne,...)

augmentation du trafic si MAJ fréquentes

Les techniques distribuées

routage par inondation : chaque noeud réémet le paquet reçu vers toutes ses lignes.

- le destinataire recevra toujours le message par le plus court chemin
- les noeuds n'ont pas à connaître l'@ des autres
- robustesse aux pannes
- nombre de paquets très important, voire infini (boucle) : possibilité d'éliminer les paquets trop vieux ou repassant au même endroit

Les techniques distribuées

- routage adaptatif local
  - choix de la ligne de sortie en fonction de critères locaux : files d'attente, ...
- routage adaptatif global
  - adaptation de la table de routage en fonction de critères locaux et venant des autres noeuds
  - deux exemples :
    - RIP : Routing Internet Protocol
    - OSPF : Open Shortest Path First

OSPF : Open Shortest Path First

algorithme à état des liaisons

une Base de Données représentant la carte du réseau est distribuée sur chaque noeud

mise à jour par inondation

une entrée de la BD :

De à liaison distancen°MAJ

A B C d n

MAJ prise en compte si son n° est > n

calcul du meilleur chemin par l'algorithme des plus court chemin de Dijkstra

Routage hiérarchique

Internet = très grand réseau : impossibilité d'avoir une entrée pour chaque station dans chaque table de routage.

Division du réseau en sous-réseau

Une entrée pour un sous réseau dans la table de routage : routeur vers ce réseau

Donc :

- adressage hiérarchique
- topologie physique cohérente avec le découpage en sous-réseaux

Protocole IP

Protocole sans connexion !

réseaux hétérogènes : nécessité de choisir une représentation standard des octets : c'est la représentation réseau.

entête :

- numéro de version du protocole (IPv4, IPv6)
- longueur de l'entête (de 20 à 40 octets)
- longueur du datagramme (jusqu'à 65635)
- durée de vie du datagramme
- protocole : UDP/TCP, autres
- contrôle d'erreur de l'entête
- adresses sources et destinations

Adressage IPv4

adresse codée sur 4 octets :

- numéro de réseau (codé sur 1, 2 ou 3 octets)
- numéro de machine sur le réseau

3 classes de réseaux : A,B et C

- classe A : 0 <<7bits réseau>>.x.y.z : 2^7 réseaux de 2^{24} machines
- classe B : 10 <<réseau>>.<<réseau>>.x.y : 2^{14} réseaux de 2^{16} machines
- classe C : 110 <<réseau>>.<<réseau>>.<<réseau>>.x : 2^{21} réseaux de 2^8 machines
- classe D : adresses multidestinataires (multicast)

géré par le NIC au niveau mondial

Adresses particulières

Lorsque le numéro de machine n'est constitué que de 1, alors c'est l'adresse de broadcast : un message envoyé à cette adresse touche toutes les machines d'un réseau

Lorsque le numéro de machine n'est constitué que de 0, alors c'est l'adresse de réseau

Le protocole ARP (Address Resolution Protocol)

faire la correspondance entre une adresse physique (Ethernet) et une adresse logique (IP)

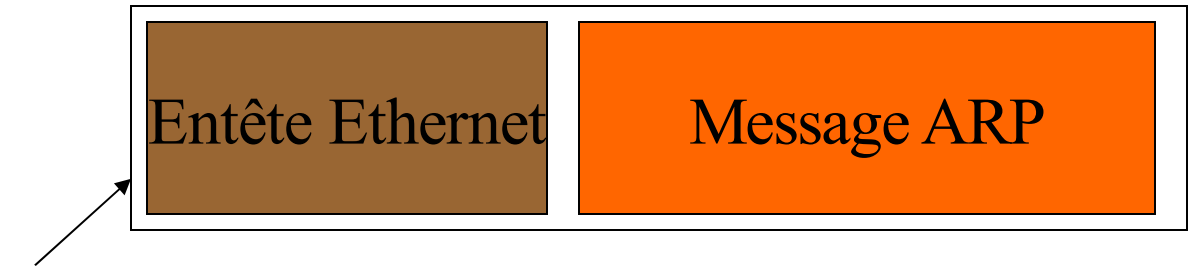
il masque les détails d'implémentation du réseau physique sous-jacent

donne une adresse physique compte-tenu d'une adresse logique lors d'une émission de trame (+gestion d'un cache)

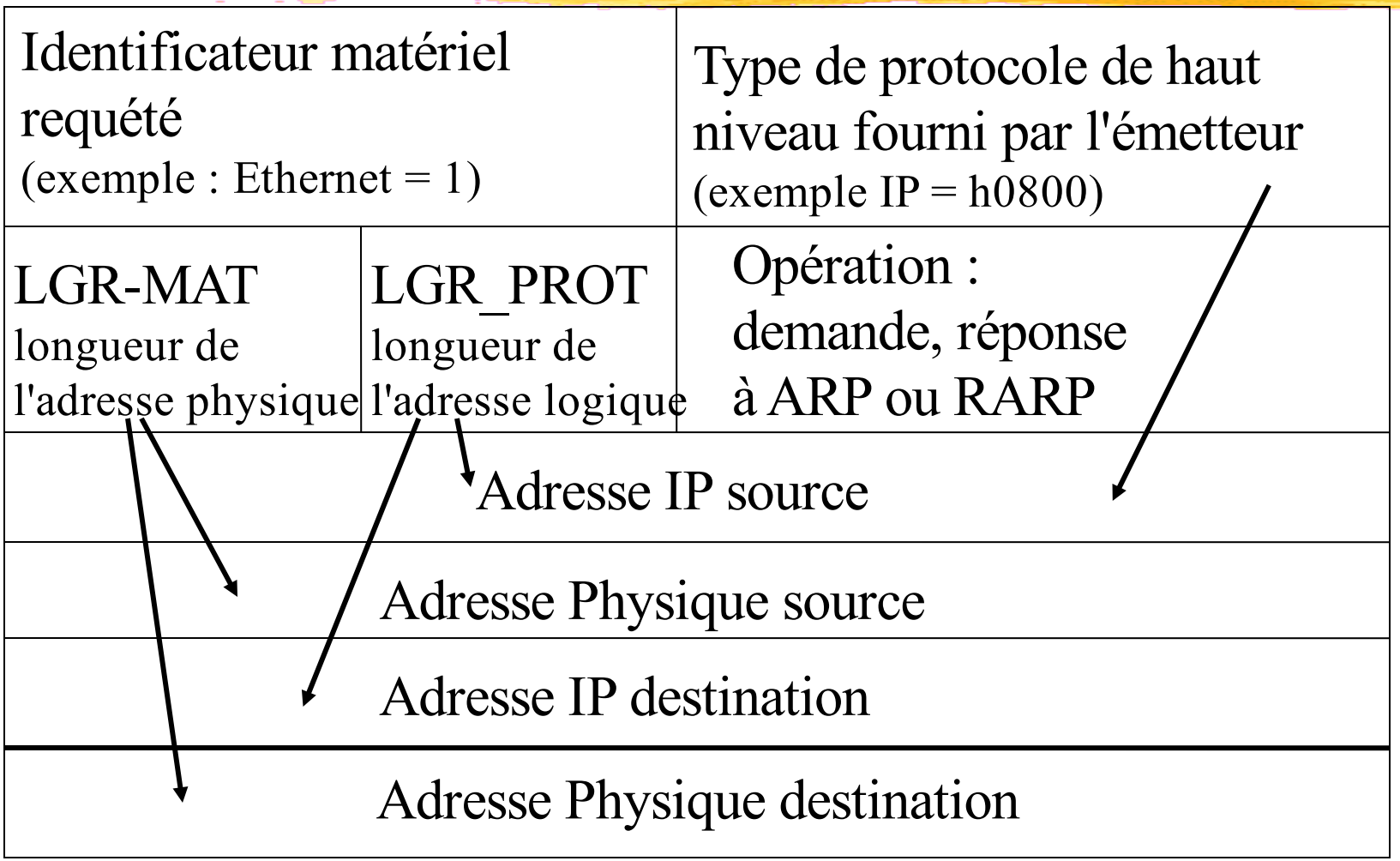
réponse aux requêtes des autres machines sur les interfaces physiques locales

La trame ARP

Encapsulée directement dans la trame Ethernet



Structure du message ARP



ARP : utilité et fonctionnement

quand une machine veut envoyer un message IP à une autre, elle doit construire une trame, par exemple Ethernet

elle fait appel à ARP pour récupérer l'adresse Ethernet de la machine destination :

- soit ARP possède la correspondance dans son cache : pas de requête, réponse immédiate
- sinon, ARP construit une trame Ethernet (adresse source = lui, adresse destination = broadcast) pour demander l'adresse Ethernet recherchée; celui qui connaît la correspondance répond

Notions de sous-réseaux

un réseau peut être, de façon interne, divisé en plusieurs sous-réseaux

par exemple : pour une adresse de classe B, 16 bits représentent l'identifiant d'une machine :

- possibilité de découper en deux champs, un de 6 bits représentant le numéro de sous réseau, et un de 10 bits identifiant une machine dans un sous-réseau : on ajoute un niveau de hiérarchie à IP
- cette organisation est interne à l'entreprise ou à l'université : invisible de l'extérieur
- réduction de la taille des tables de routage

Netmask : exemple

10 <<réseau>>.<<réseau>>. 8bits . 8bits .

8bits . 8bits : numéro de la machine dans le réseau de classe B

10 <<réseau>>.<<réseau>>. 6 bits . 10 bits .

6 bits : numéro du sous réseau

10 bits : numéro de la machine dans le sous-réseau

netmask : 16+6 = 22 bits à 1, et 10 bits à 0, soit :

255.255.253.0

Netmask, fonctionnement

un routeur recevant un paquet IP fait un ET logique entre l'adresse destination et le netmask, ce qui lui donne le numéro du sous réseau où se trouve le destinataire

le découpage en sous-réseau est interne à une entité : de l'extérieur, seules les adresses IP sont visibles, pas les masques de sous-réseau

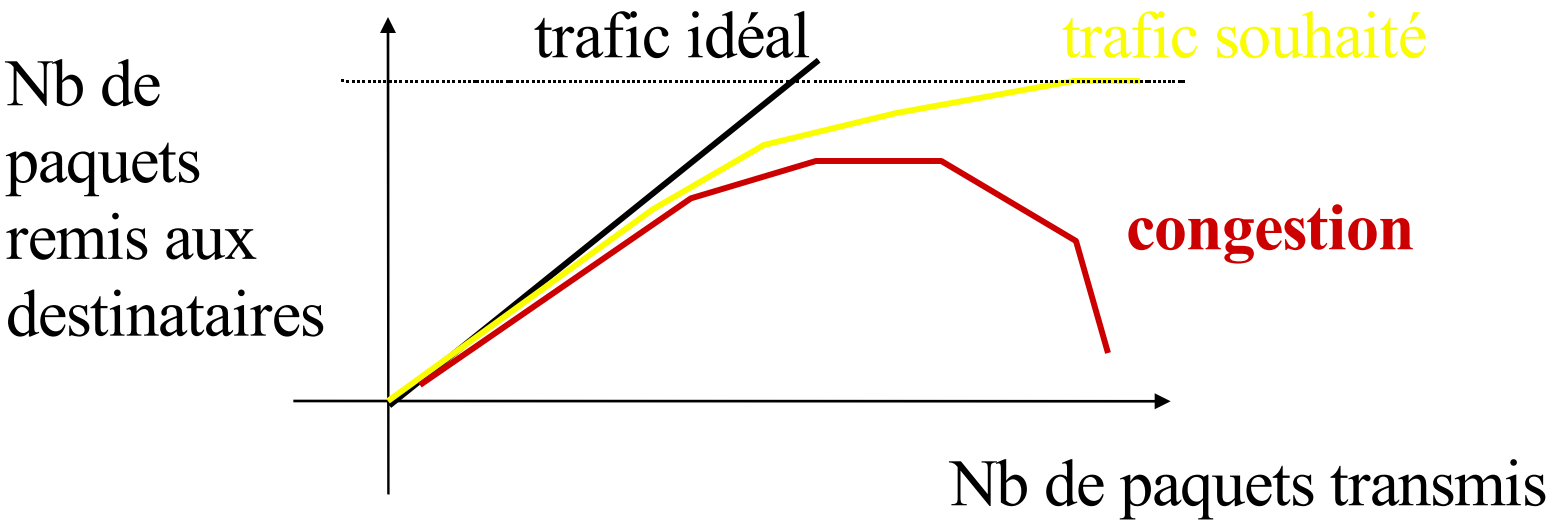
Fragmentation

un datagramme IP est émis avec un taille maximum fonction de la taille du réseau d'entrée. Si le datagramme emprunte des réseaux différents, nécessité de fragmenter

Contrôle de congestion

si le nombre de paquets injectés dans le réseau dépasse les capacités de traitements

destruction par les routeurs des paquets qui ne peuvent plus être traités



Raisons des congestions

arrivée sur 3 ou 4 lignes d'un routeur, sortie vers une seule ligne : problèmes dus à la taille de la file d'attente

faibles performances des processeurs internes aux routeurs

- gestion file d'attente
- MAJ des tables de routage
- commande de la retransmission des paquets

Différences entre contrôle de flux et contrôle de congestion

flux = trafic point à point entre un émetteur et un récepteur particulier

congestion = problème global prenant en compte :

- la source et la destination
- les routeurs et leurs paramètres
- le protocole de retransmission

Principes généraux du contrôle de congestion

Deux démarches possibles :

- prévention
- guérison

Prévention de la congestion

résolution des problèmes à la conception

moyens de contrôle : quand accepter

- d'augmenter le trafic
- de recevoir des nouveaux paquets
- de détruire des paquets
- lesquels ?

Voies d'action sur la congestion

- couche liaison de données :
  - politique de retransmission (délais)
  - politique de masquage sélectif des anomalies
  - politique de l'accusé de réception (piggybacking ?)
  - politique du contrôle de flux (taille des fenêtres d'anticipation)
- couche réseau :
  - circuits virtuels ou datagramme ?
  - politique de mises en attente et distribution des paquets
  - politique de destruction des paquets
  - politique de routage
  - gestion de la durée de vie des paquets

Guérison de la congestion

- basée sur le retour d'information
  - surveillance du réseau
  - envoyer l'information là où une action améliorant la situation peut être prise
- informations pertinentes
  - % de paquets détruits par manque de place
  - longueur de la file d'attente
  - nombre de paquets hors délai à retransmettre

Techniques contre congestion

DECbit: Congestion Notification bit, dans l'entête du paquet, mis à 1 quand une congestion détectée, dans l'ACK : en fonction du nombre d'ACK avec le DEBbit à 1, la source diminue (multiplicativement) ou augmente (linéairement) son débit

RED (Random Early Detection): rejet de paquets aléatoirement, en fonction de la file d'attente sur les routeurs

RED I/O, ECN,

La couche Transport

Première couche à fonctionner

de bout en bout,

de la source à la destination;

2 choix possibles au niveau de cette couche :

- utilisation de plusieurs connexions réseaux pour une seule connexion transport : augmentation du débit
- utilisation de plusieurs connexions transport pour une connexion réseau : diminution du coût par partage de la ligne

TCP et UDP

Dans Inet, deux protocoles particuliers pour la couche transport :

- UDP : User Datagram Protocol
- TCP : Transport Control Protocol

User Datagram Protocol

pas de connexion avant d'émettre des données;

pas de vérification de l'arrivée des messages : pas d'ordre, pas d'avertissement lors d'une mauvaise remise, pas de reprise sur erreur

adapté aux données non vitales

utilisé par exemple pour les transmissions multimédia temps réel

Transport Control Protocol

connexion entre émetteur et récepteur

contrôle des messages : ordre, erreurs détectées et corrigées

utilisation de crédit pour le contrôle de flux (taille d'une fenêtre de transmission)

reprise pour les segments non acquittés

pour les liaisons non fiables

plus de travail pour chaque message

Notions d'adresse Transport

Liaison de la couche Transport : liaison de bout en bout !

comment faire si plusieurs applications d'une machine émettrice veulent communiquer avec des applications d'une même machine réceptrice ?

Solution : pouvoir discerner toutes ces communications !

Adresse Transport

Une adresse Internet de la couche Transport = 1 adresse IP (niveau de la couche réseau) + 1 protocole Transport

+ 1 numéro de port

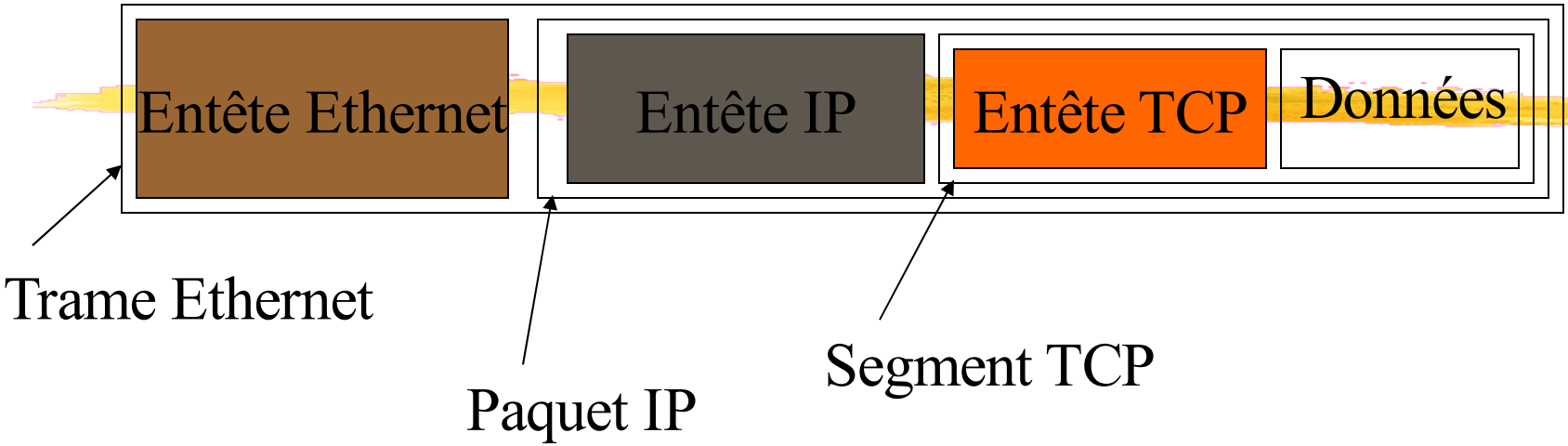
1 numéro de port par application et par protocole utilisé (TCP ou UDP)

exemple :

- protocole HTTP : numéro de port 80
- protocole SMTP : numéro de port 25
- protocole Utilisateurs : numéro > 1024

programmation réseau avec les sockets

Structure de segment TCP



Entête TCP

- numéros de ports sources et destinations
- numéro de paquet et numéro d'acquittement attendu
- fonction du segment (connexion, ack, déconn.,…)
- crédits
- somme de contrôle
- pointeur vers les données urgentes

La couche Application

Courrier : SMTP, POP, IMAP

News : NNTP

Web : HTTP

Transfert de fichiers : FTP

DNS

Tous les protocoles sont décrits dans des RFC (Request For Comment !)

Le DNS : Domain Name Service

Réalise l'association du nom logique d'une machine (www.insa-lyon.fr) et son adresse IP (134.214.78.51)

Aide donc à la création des paquets IP…

nom d'une machine sur Internet (Full Qualified Host Name) = nom de la machine en local (www) + nom du domaine (insa-lyon.fr)

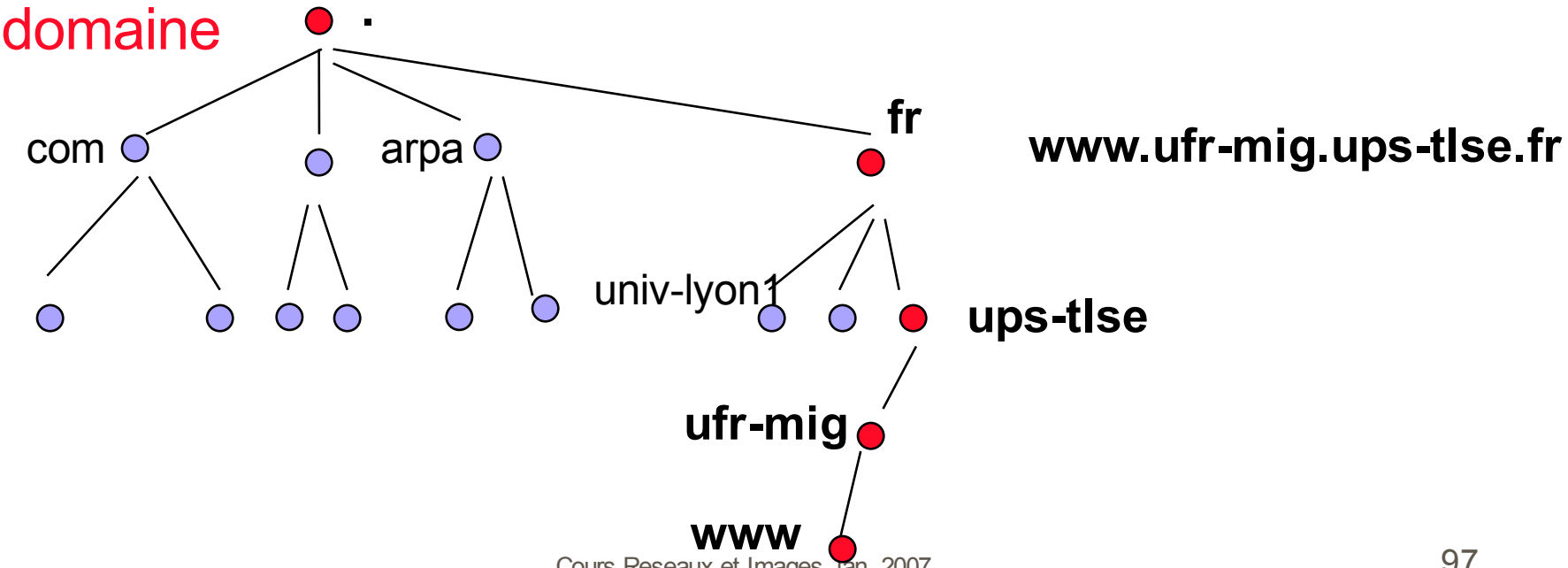
RFC 1035

DNS : principe général

des serveurs DNS coopèrent pour résoudre un nom de machine en adresse IP

une base de données distribuée au niveau mondial

indexation des données par un nom : ces noms constituent un chemin dans un arbre inversé appelé l'espace Nom de domaine



Principe de délégation

Le système DNS est entièrement distribué au niveau planétaire

A tout domaine est associé une responsabilité administrative

Une organisation responsable d'un domaine peut

- découper le domaine en sous-domaines
- déléguer les sous-domaines à d'autres organisations :
  - qui deviennent responsables du (des) sous-domaine(s) qui leurs sont délégué(s)
  - qui peuvent déléguer des sous-domaines des sous-domaines qu'elles gèrent

Le domaine parent contient alors seulement un pointeur vers le sous-domaine délégué

Les serveurs de noms (nameserver)

Les serveurs de nom enregistrent les données propres à une partie de l'espace nom de domaine dans une zone.

Le serveur de nom à autorité administrative sur cette zone.

Serveur de nom primaire : maintient la base de données de la zone dont il a l'autorité administrative

Serveur de nom secondaire : obtient les données de la zone via un autre serveur de nom qui a également l'autorité administrative (interrogation régulière)

Il y a un serveur primaire et généralement plusieurs secondaires: la redondance permet la tolérance aux pannes

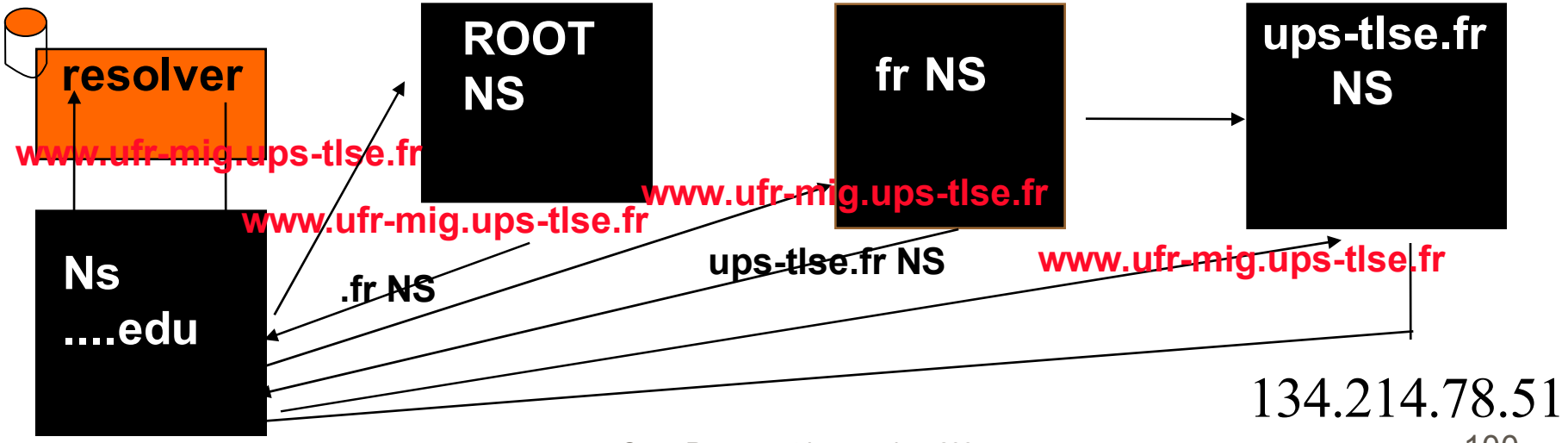
Un serveur de nom peut être primaire pour une (des) zone(s) et secondaire pour d'autre(s).

Les serveurs racines

Les serveurs racine connaissent les serveurs de nom ayant autorité sur tous les domaines racine (c-a-d au moins .com, .edu, .fr, etc.)

Indispensable au fonctionnement : il y en a plusieurs...

Exemple de résolution : www.insa-lyon.fr à partir d'un domaine extérieur....edu



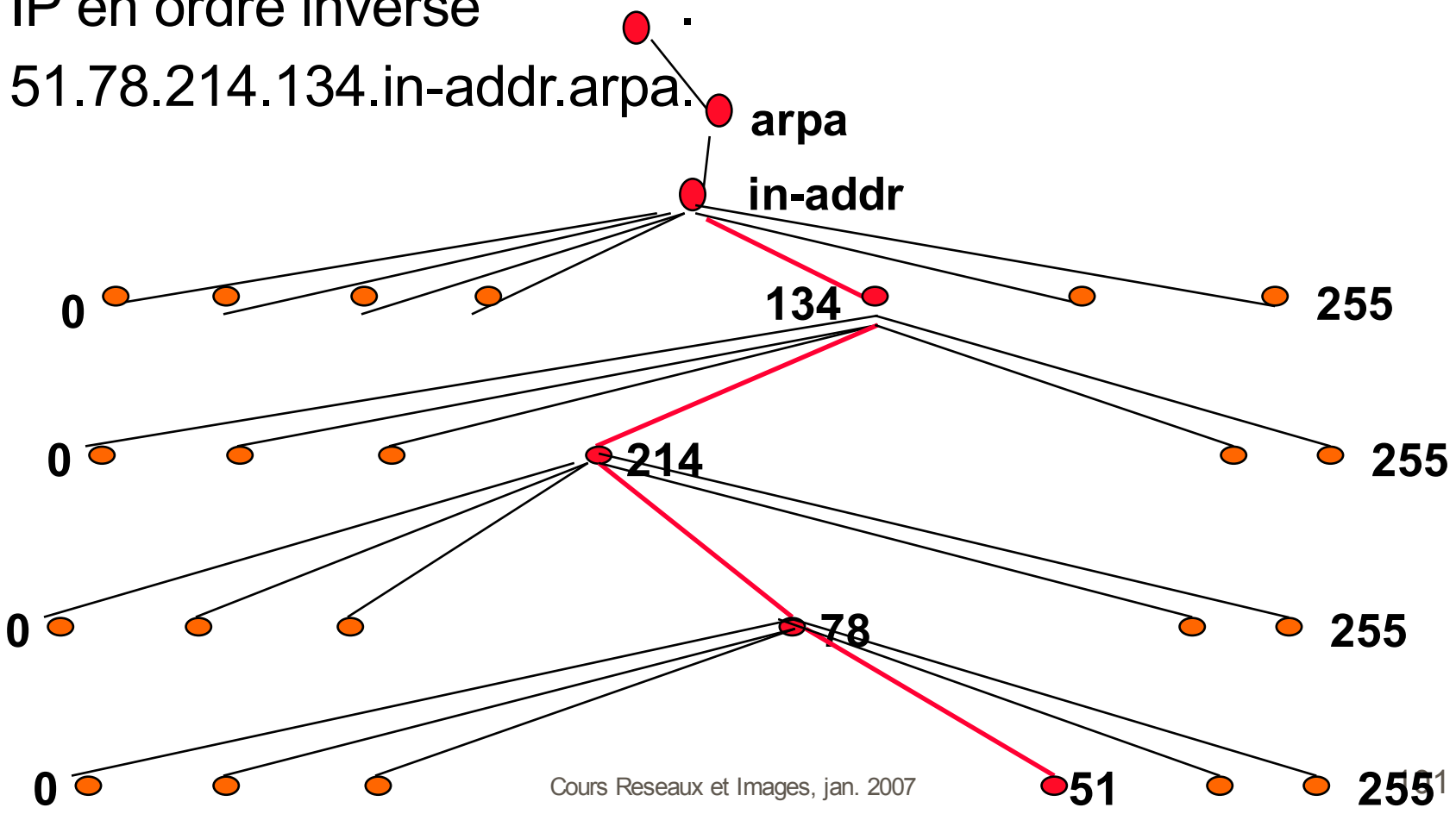
DNS : résolution inverse

Obtenir le nom de domaine à partir de l'adresse IP

le domaine in-addr.arpa

les noms des nœuds correspondent aux octets de l'adresse IP en ordre inverse

51.78.214.134.in-addr.arpa.

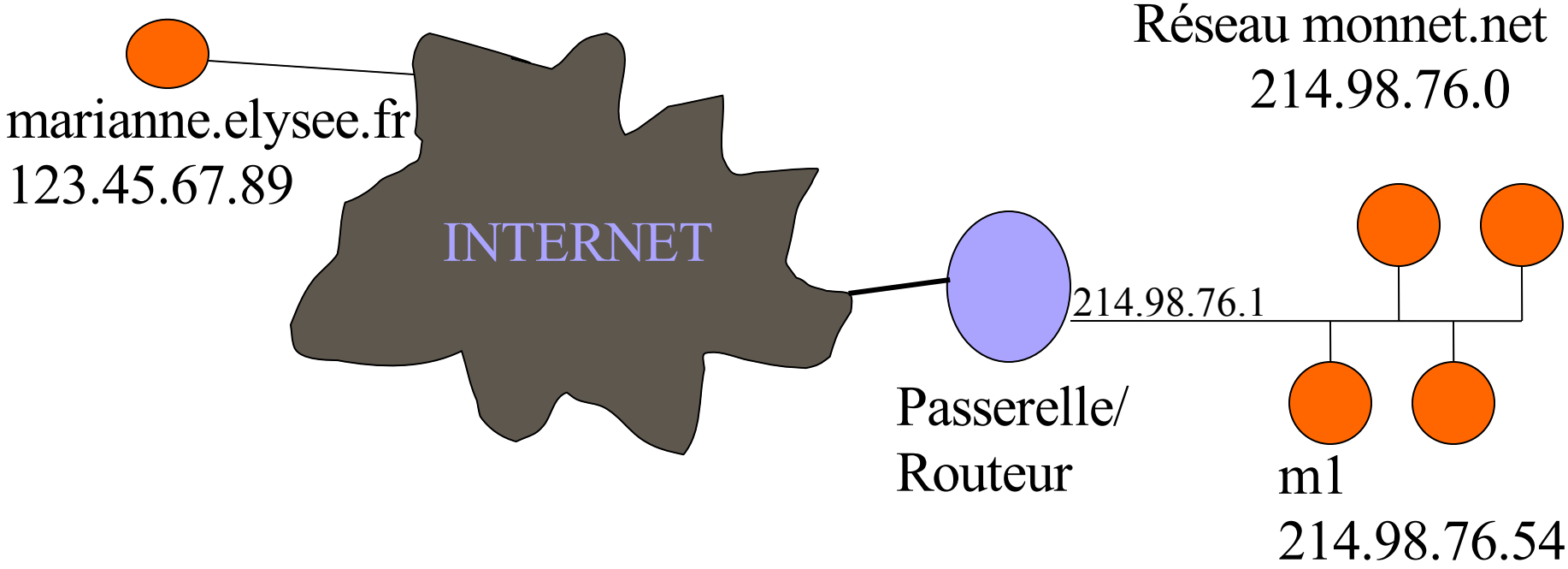


Au final, exemple...

Quels sont les protocoles et mécanismes mis en œuvre lorsqu'on fait par exemple : telnet marianne.elysee.fr

à partir de la machine m1 sur le réseau monnet.net ??

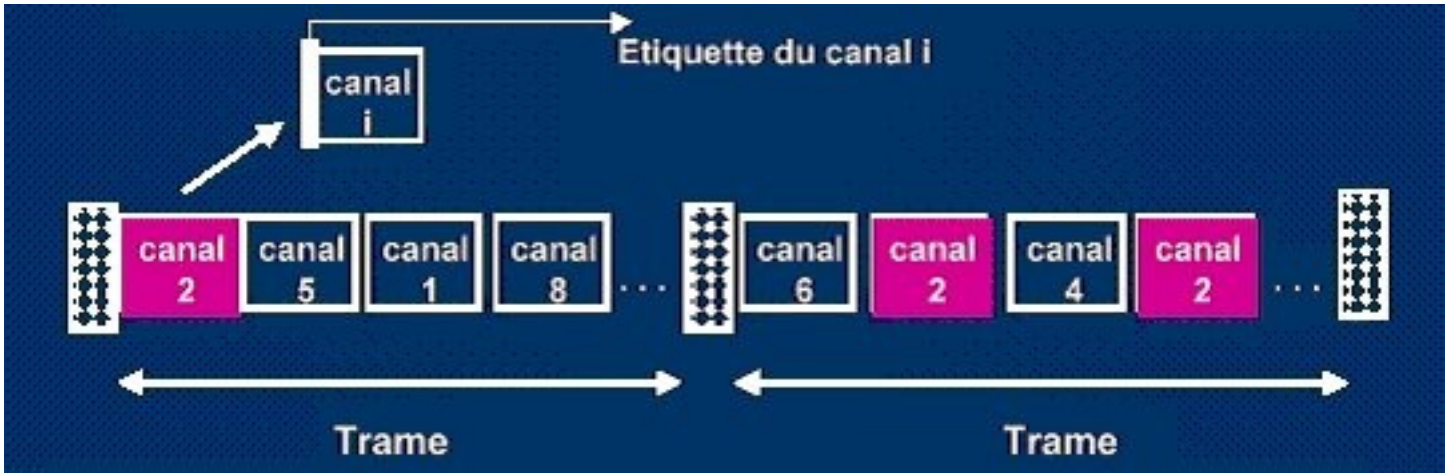
(Plus précisément, quels sont les paquets, trames qui sont construits ?)



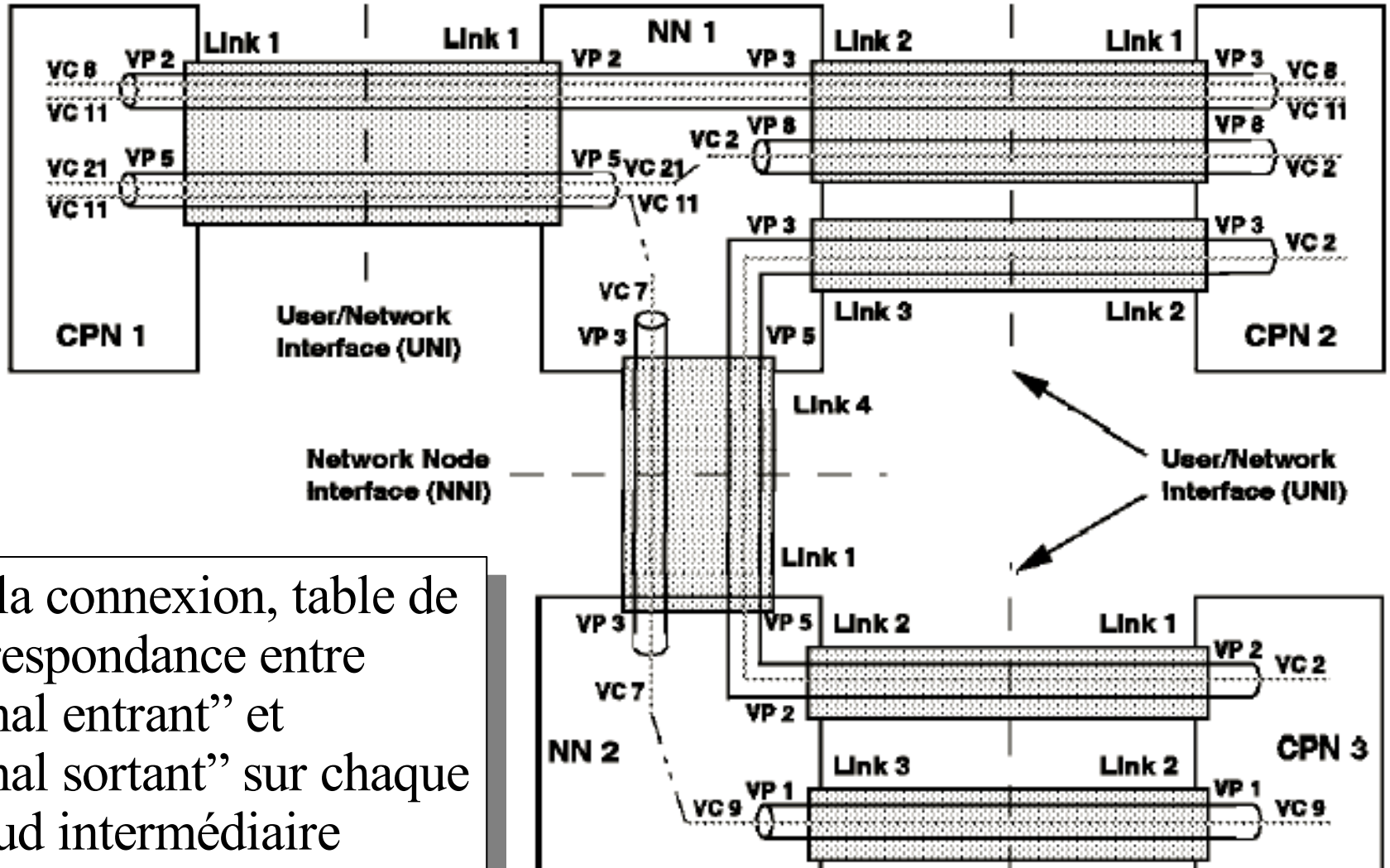
Le réseau ATM

ATM = Asynchronous Transfer Mode

Multiplexage temporel dynamique



Connexion: circuit virtuel / chemin virtuel



- A la connexion, table de correspondance entre “canal entrant” et “canal sortant” sur chaque noeud intermédiaire

ATM: taille des cellules

Commutation de cellules de taille fixe: 53 octets:

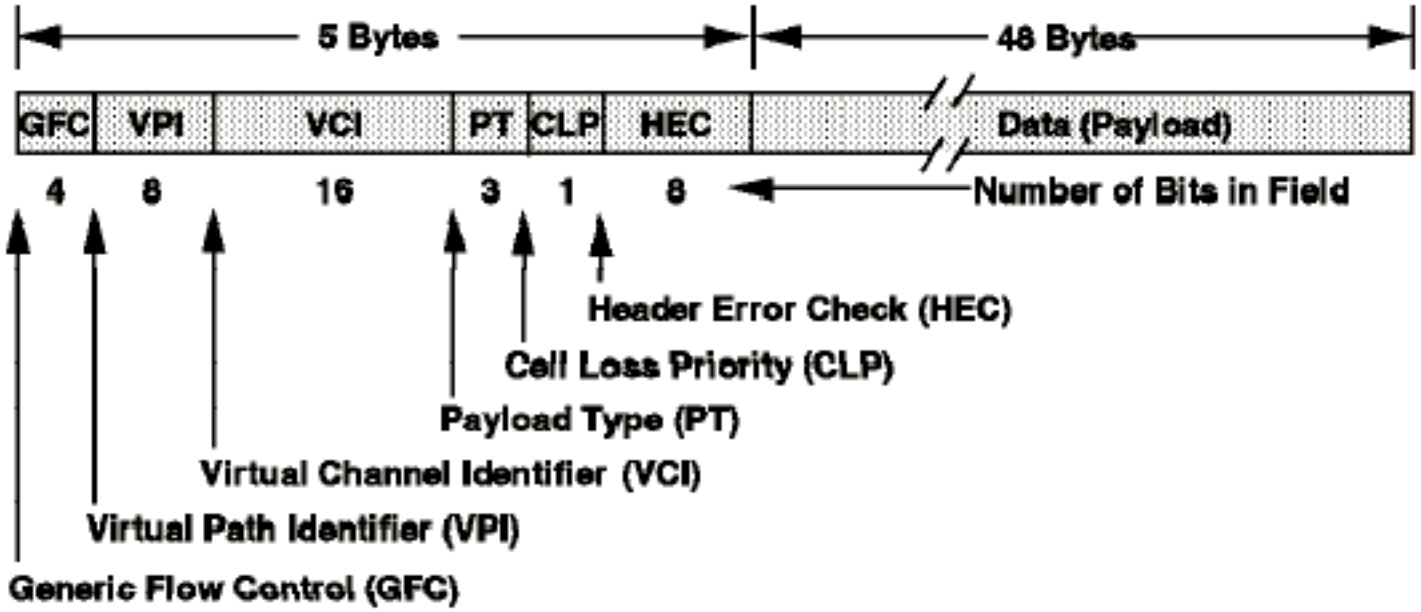
- entête = 5 octets
- données utiles: 48 octets

En cas de congestion, l'abandon d'une cellule entraîne la perte de peu d'info.

Longueur de taille fixe: facilité d'implémenter dans le hardware directement les fonctions

Pas de stockage d'une "grosse" trame sur les nœuds intermédiaires, renvoi immédiat vers le nœud suivant. Pas de gestion des erreurs. (sauf entête)

Cellule ATM


5 Bytes
48 Bytes
GFC
VPI
VCI
PT
CLP
HEC
Data (Payload)
4
8
16
3
1
8
Number of Bits in Field
Header Error Check (HEC)
Cell Loss Priority (CLP)
Payload Type (PT)
Virtual Channel Identifier (VCI)
Virtual Path Identifier (VPI)
Generic Flow Control (GFC)

ATM indépendance du média

ATM Forum Physical Layer UNI Interfaces		
Frame Format	**Bit rate**	**Transmission Media**
DS1	1.544 Mb/s	Twisted Pair
DS3	44.736 Mb/s	Coax Pair
STS-3c, STM-1	155.520 Mb/s	SMF
E1	2.048 Mb/s	Twisted or Coax Pair
E3	34.368 Mb/s	Coax Pair
J2	6.312 Mb/s	Coax Pair
N x T1	N x 1.544 Mb/s	Twisted Pair
N x E1	N x 2.048 Mb/s	Twisted Pair

ATM Adaptation Layer (AAL)

Rôle général: découpe des frames en cellules, ajoute des infos pour pouvoir reconstruire les frames, vérifie les erreurs au niveau des frames (si erreur, frame détruite).

Implémente 5 classes de services différents (avec/sans connexion, débit constant/variable)

Couche de bout en bout

AAL : qualité de service

- Constant Bit Rate (CBR) : voix, vidéo
- Variable Bit Rate (VBR) : données, vidéo compressée
  - Real-time Variable Bit Rate (rt-VBR) : synchronisation
  - Non-real-time Variable Bit Rate (nrt-VBR)
- Available Bit Rate (ABR)
- Unspecified Bit Rate (UBR)

Exemple : AAL-1

Class A (Circuit Emulation, Constant Byte Rate): AAL-1

Ce service emule une ligne louée

Pour les applications à débit constant (voix, vidéo)

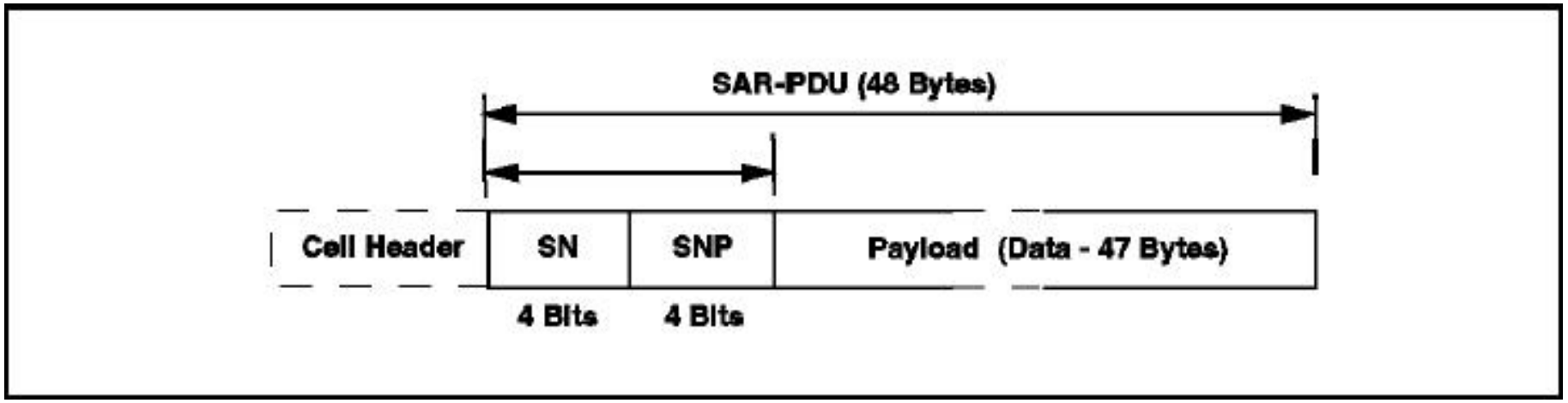
Caractéristiques des applications concernées:

- Débit constant voulu entre la source et la destination
- Relation dans le temps entre les deux partenaires.
- Une connexion existe entre les utilisateurs

Rôle de l'AAL-1:

- Segmentation et réassemblage des frames / cellules
- Mise en mémoire tampon pour gérer les variations de délai dans la transmission (car synchronisation voulue entre émetteur et récepteur)
- Détection et gestion de la perte, de la duplication, des erreurs d'aiguillage des celulles (erreurs dans l'entête)
- Synchronisation de l'horloge avec l'émetteur (très gros problème!)
- Detection des erreurs dans la partie données de la cellule

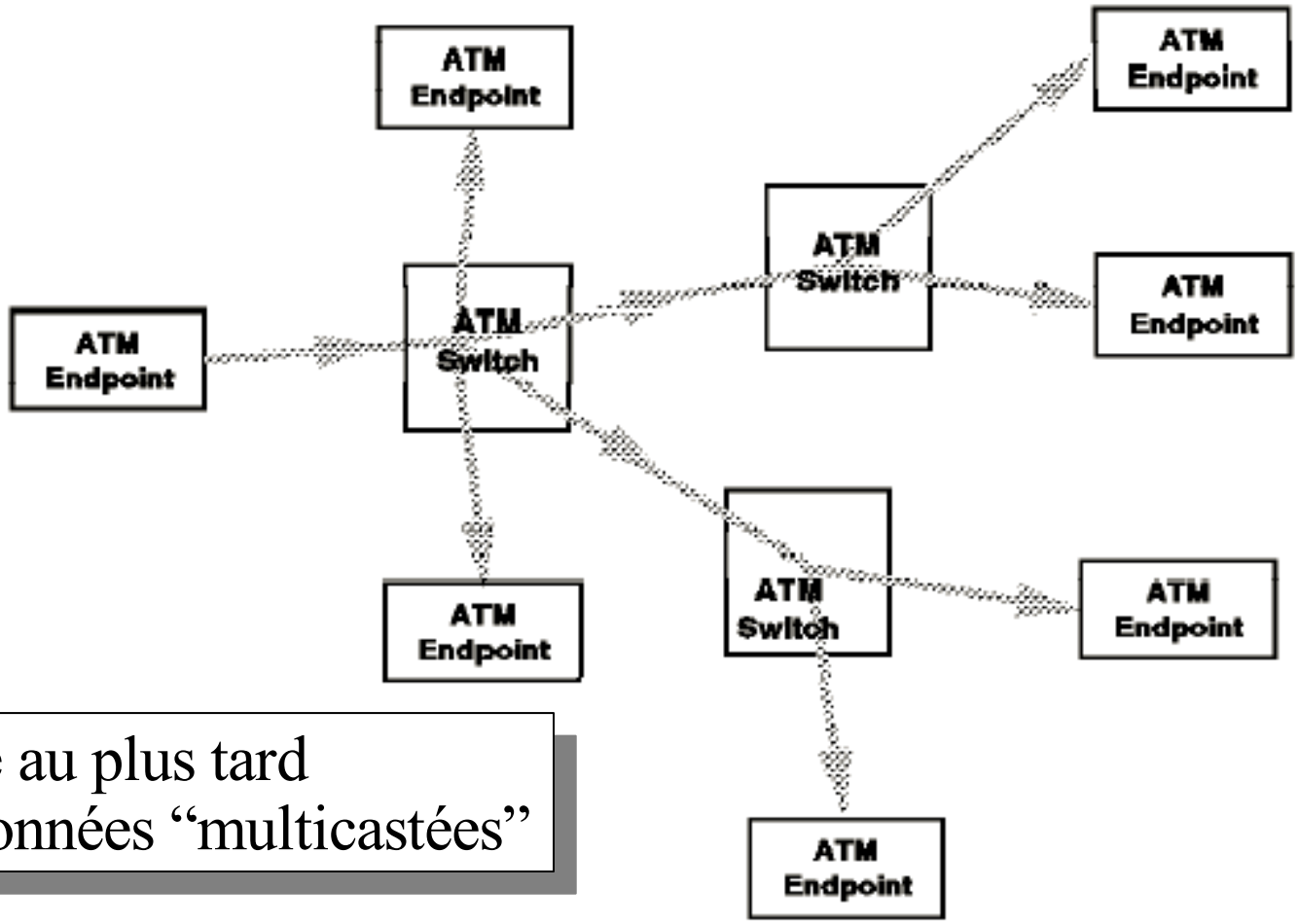
Cellule AAL-1



SN: Sequence Number

SNP: Sequence Number Protection (CRC sur SN). Si erreur, cellule abandonnée

Multicast natif sur ATM



Copie au plus tard
des données “multicastées”

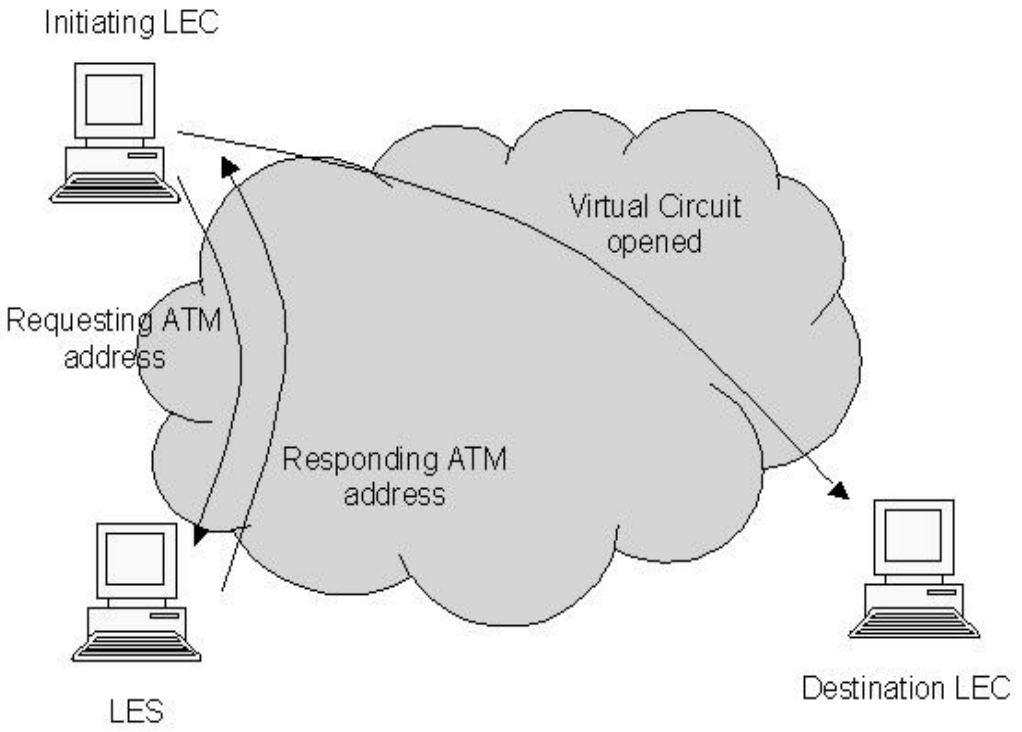
ATM et LAN (ex: Ethernet)

LANE (LAN Emulation)

Correspondance @MAC et @ATM dans le LES.

Possible plusieurs VLAN (LECS: LE Config Server

BUS (Broadcast and Unknow Server): multica mais double transport de données (vers serveur, puis destinataires)

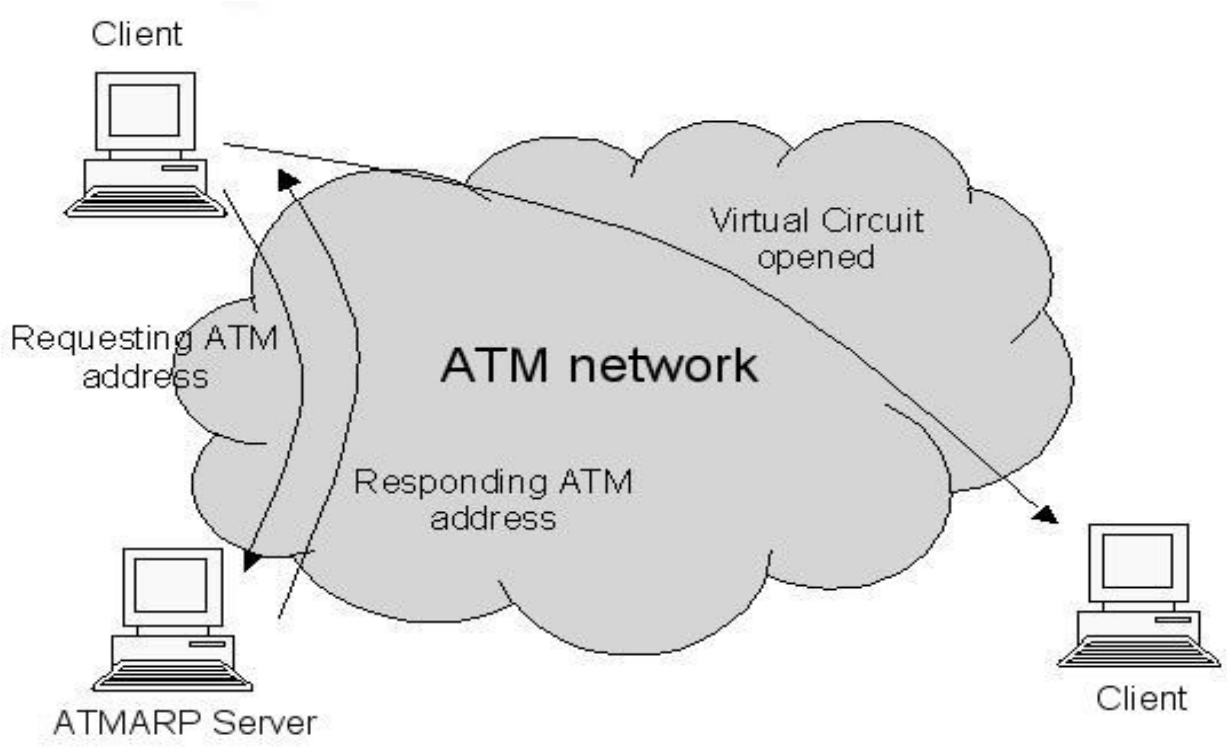


Pas de modif. des applications

mais double correspondance IP/MAC et MAC/ATM

ATM et IP: CIOA (Classical IP over ATM)

Même idée que LANE mais ici correspondance @ IP <-> @ ATM



RSVP

RFC 2205

Protocole de signalisation pour la réservation de ressources sur le chemin entre une source de flux et un récepteur: donc sur tous les élements traversés (routeurs, passerelles, ...)

Gestion de la QoS pour un flux donné.

Les noeuds intermédiaires réservent des ressources (BP, délai) et s'engagent sur: délais respectés, régulation du trafic (contre les rafales), tamporisation

RSVP: détails

Protocole de niveau Transport: fonctionne au dessus de IP, de bout en bout, donc nécessite un protocole de routage

Réservation dans les arbres multicast (unicast aussi, cas particulier)

Réservation initiée par le récepteur

Réservation annulée au bout d'un moment, si pas de message de raffraichissement (par le récepteur)

Implémente INTServ : Integrated Services

RSVP: format du message

Il existe sept types de message RSVP:

Path : envoyé par la source pour indiquer la liste des routeurs suivi par les données.

Resv : message de réservation vers les emetteurs.

PathErr : message d'erreur concernant le chemin.

ResvErr : message d'erreur de demande de réservation.

PathTear : indique aux routeurs d'annuler les états concernant la route.

ResvTear : indique aux routeurs d'annuler les états de réservation (fin de session).

ResvConf (optionnel) : message de confirmation

Entête : (64 bits). Entre autres:

Vers (4 bits) : version du protocole RSVP (c'est à dire: 1).

Type du message (8 bits) : voir ci-dessus , valeur de 0 à 7.

CheckSum (16 bits): contrôle d'erreur.

Send_TTL (8 bits) : valeur du TTL (time to live) IP à comparer avec le TTL du paquet IP pour savoir s'il y a des routeurs non-RSVP.

Longueur du message(16 bits) : longueur du message en octets (entête et objets).

RSVP: mécanisme de réservation

Message PATH envoyé régulièrement par l'émetteur: contient (@ émetteur, caractéristique du trafic: débit, taille max paquet, taille seau percé, ...)

Chaque routeur traversé ajoute ses caractéristiques

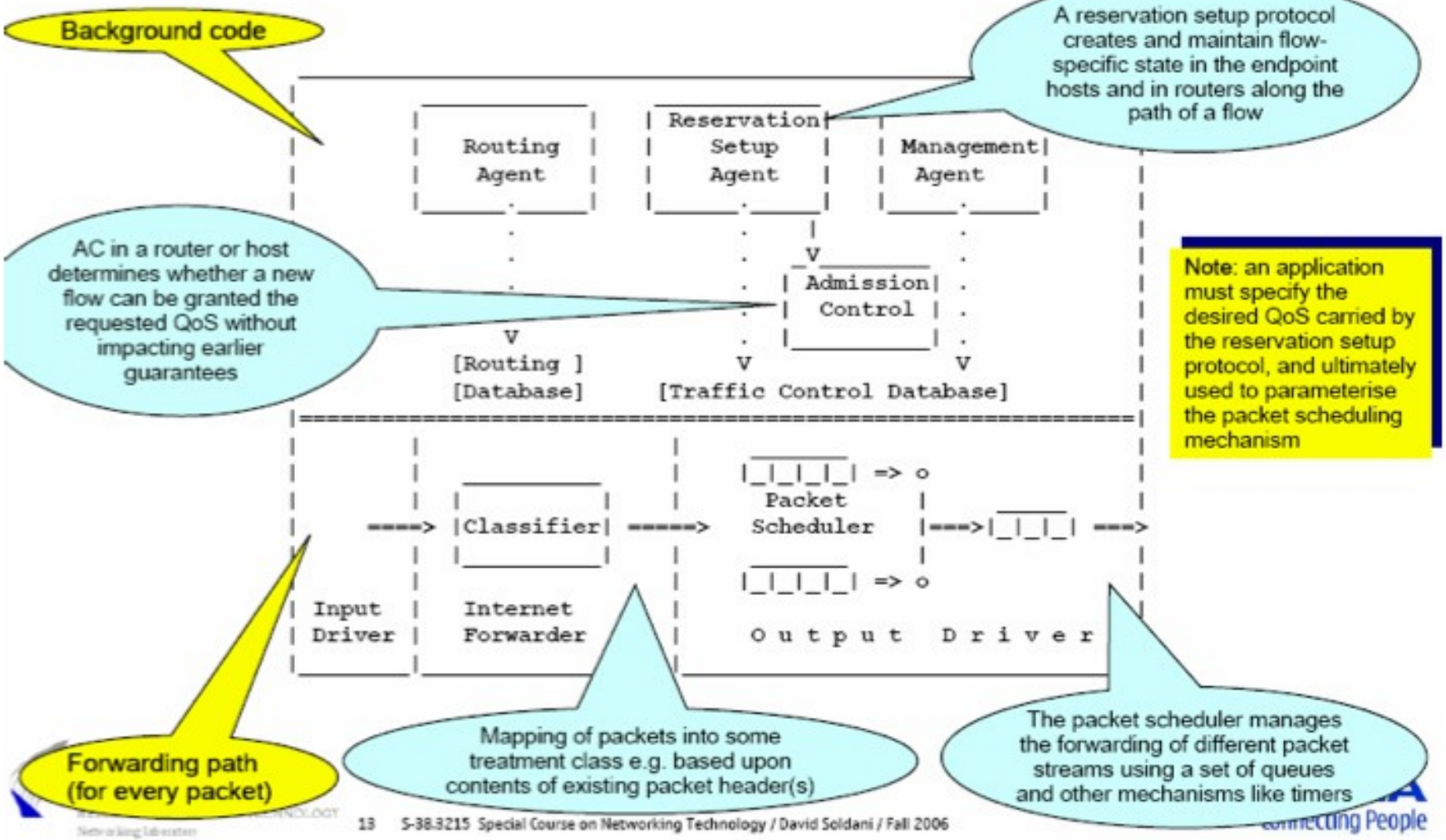
Pas de réservation à cette étape

Pas de gestion des paramètres de QoS par RSVP: ce sont des modules sur les routeurs qui le fait

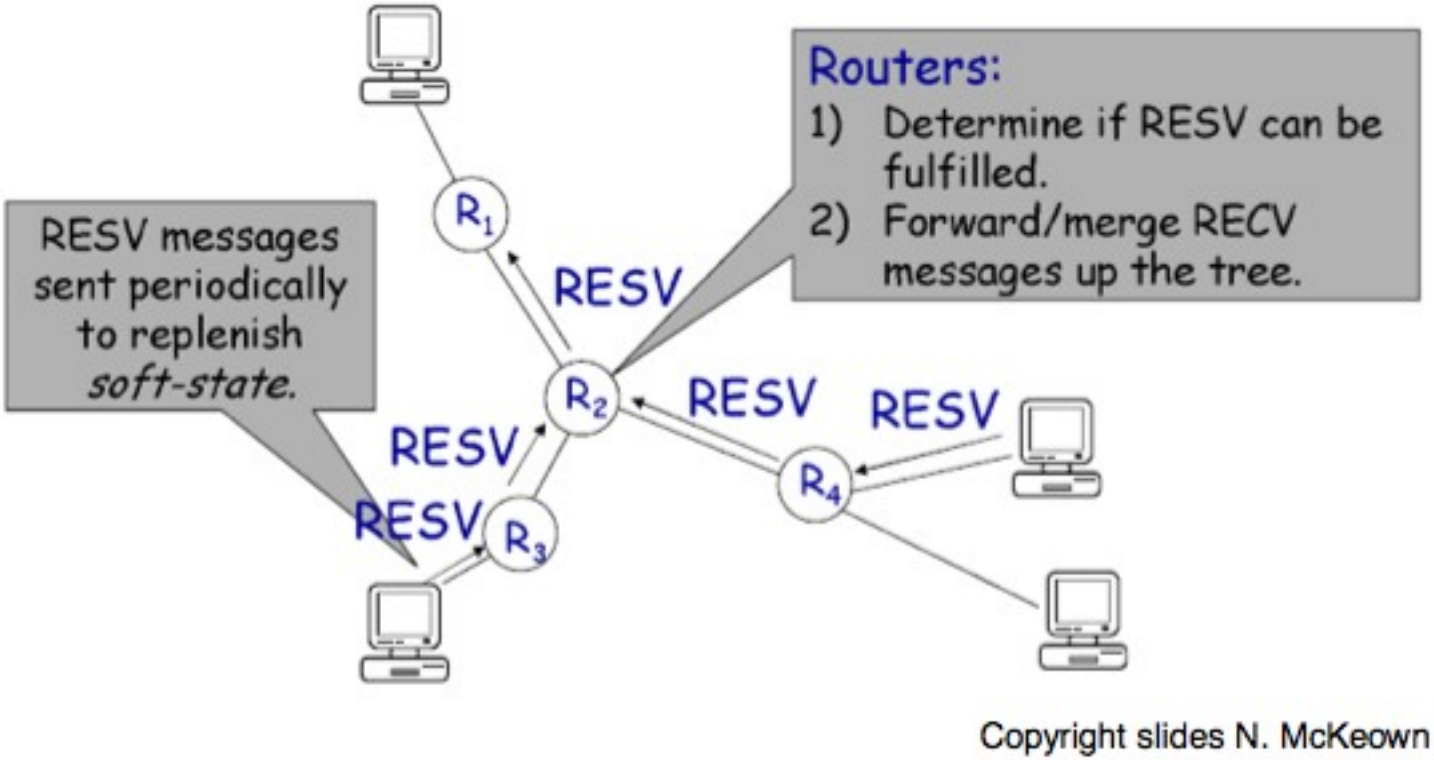
RSVP: demande de réservation

- A la réception d'un message PATH, le récepteur émet un message RESV contenant ses caractéristiques de QoS et celles de la source, plus les routeurs
- Chaque noeud recevant un msg RESV:
  - Vérifie les droits de faire de la réservation
  - Vérifie que les ressources sont disponibles (sans dégrader les réservations déjà faites)
  - Si pb, message d'erreur
  - Si ok, envoi du message vers deux modules:
    - Module de classification du message+routage
    - Module d'ordonnancement dans différentes files en fonction de la classe de service

IntServ Architecture for Routers [RFC1633]



RSVP: messages RESV



Copyright slides N. McKeown

Fusion de msg RESV dans l'arbre multicast

(Attention: ce n'est pas la somme des QoS demandées, exemple: 10 clients audio de 2 Mbit/s=2 Mbit/s en multicast)

RSVP: problèmes

Si certains routeurs ne font pas de réservation de ressources: le protocole marche, mais quid de la QoS ?

Basé sur une symétrie du trafic réseau: rien de garanti dans IP

Limite du nombre de classes de trafic, de différenciation des applications --> DiffServ

- Classe de service dans l'entête IP (champ DS)
- Mis en place par des routeurs périphériques (Edge routeur) à l'admission dans le réseau

Multicast

Un émetteur envoie à un ensemble de récepteurs

Broadcast : à tout le monde sur le réseau

Multicast : à un nombre quelconque de destinataires

Protocoles pour éviter de dupliquer les envois, ou tout du moins pour dupliquer les données au plus tard

Adresses Multicast IPv4

Des adresses de classes D
224.0.0.0 –239.255.255.255

En binaire :
4 bits : 1110 + 28 bits correspondant au groupe

Plages d'adresses réservées ou plages libres, allouées de façon permanente ou dynamiquement

Adresses Multicast, exemples

224.0.0.0/8 pour diffusion sur le lien-local

- 224.0.0.0.1 tous les noeuds multicast sur le lien-local
- 224.0.0.0.2 tous les routeurs IGMP sur le lien-local
- 224.0.0.0.4 tous les routeurs DVMRP sur le lien-local
- 224.0.0.0.13 tous les routeurs PIM sur le lien-local

224.2.0.0 -224.2.255.255 (224.2/16) : SDP/SAP Block

- Plage d'adresses allouées dynamiquement

239.0.0.0/8 : Limited scope (RFC 2365)

- Site-local : 239.253.0.0/16
- Organization-local : 239.192.0.0/14
- Global : 224.0.1.0 –238.255.255.255

Portée limitée grace au TTL aussi

Multicast et adressage

Une adresse multicast ne peut être que destinataire

Une adresse Multicast = adresse d'un groupe de machines abonnées à une session multicast

Les sources (émetteurs) sont connues par leur adresse unicast

Etre membre d'un groupe est indépendant d'envoyer à ce groupe : une source n'est pas obligatoirement membre du groupe multicast auquel elle envoie des données

Les routeurs utilisent des protocoles de routage multicast pour acheminer les datagrammes des groupes multicast

Multicast dans un LAN

Par défaut, la sous-couche MAC (ex:Ethernet) n'écoute que sur son adresse, et sur celle de broadcast Ethernet.

Il faut donc programmer explicitement l'écoute sur des adresses multicast

Donc conversion nécessaire entre adresse multicast et adresse MAC: basé sur l'adresse MAC et sur l'adresse de multicast

Exemple:

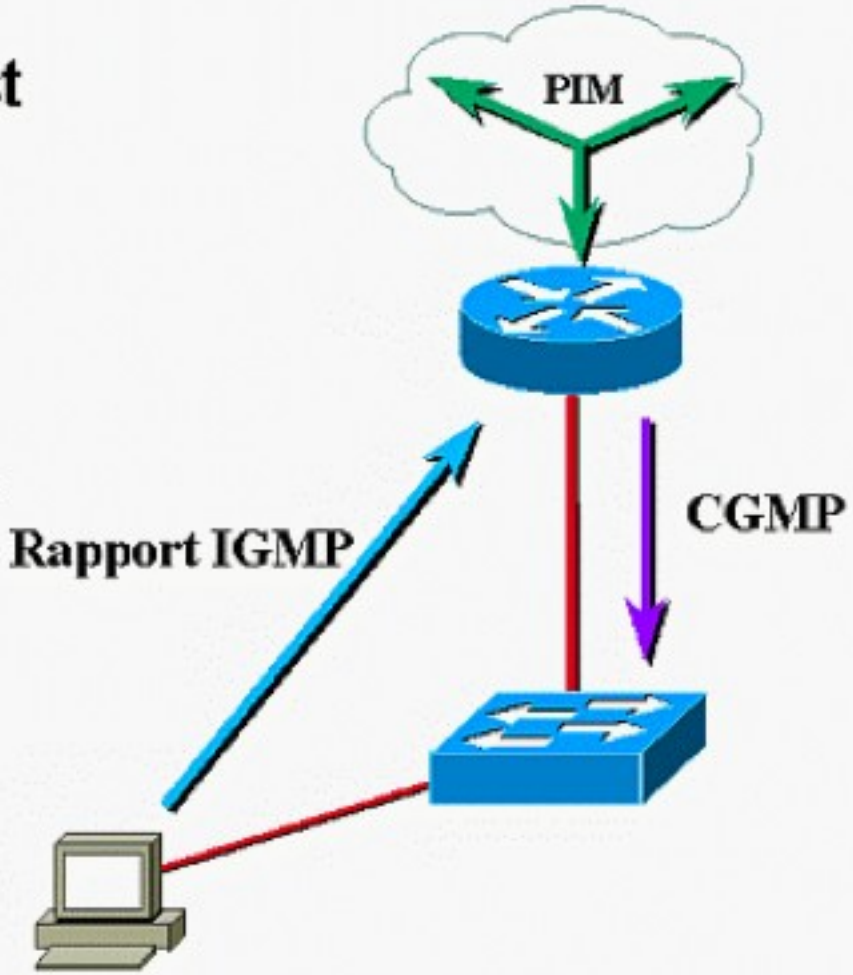
224.0.0.1 (tous les hôtes multicast du LAN) : 01-00-5e-00-00-01

IGMP: Gestion des groupes multicast dans un LAN

- Protocole d'interaction entre les routeurs multicast du LAN et les hôtes multicast du LAN
- Gère les abonnements et désabonnements
- Utilise l'adresse 224.0.0.1 (tous les hôtes multicast) pour les requetes d'abonnement, et l'adresse 224.0.0.2 (tous les routeurs) pour les rapports et les désabonnements
- Possibilité de coupler avec un protocole de niveau L2 pour commander les commutateurs (et éviter la diffusion vers des hôtes non intéressés): IGMP Snooping

Exemple avec Cisco GMP

- **Performance de commutation du multicast maintenue au niveau 2**
- **CGMP programme dynamiquement les tables de commutation avec les informations sur les adresses multicast**
- **Ne requiert pas de changement sur les ordinateurs**



Cours DIM du 22/10/02 : IP multicast - guy.bisiaux@univ-valenciennes.fr Comité Réseau des Universités

Protocole de routage multicast

Construction d'un arbre multicast

- L’arbre minimal de diffusion est dynamique
- L’émetteur (la source) est la racine de l’arbre de diffusion
- Toutes les branches sont utiles (id. ont au moins un abonné qui sont les feuilles de l'arbre)
- Mécanismes nécessaires d'ajout (suppression) d’une feuille/branche dans l'arbre.

Deux familles:

- Mode dense: beaucoup d'abonnés, principe de l'inondation et de l'élagage. Ex: DVMRP, MOSPF, PIM-DM
- Mode clairsemé: greffe et élagage. Ex: PIM-SM, CBT

DVMRP

Distance Vector Routing Multicast Protocol

RFC 1075

On inonde tout l'arbre multicast, ceux qui ne sont pas intéressés le disent

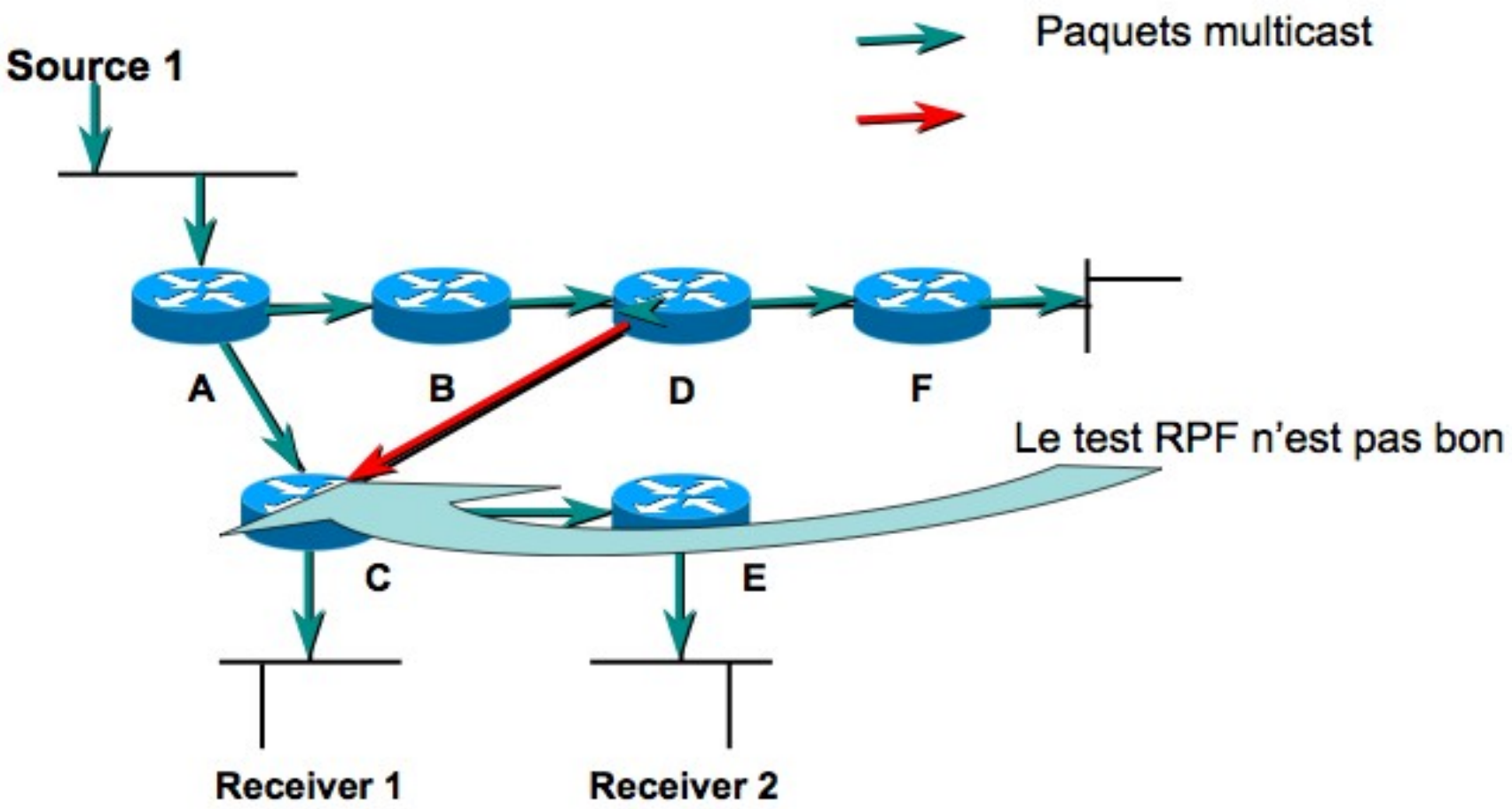
Pour éviter les boucles, algorithme RPF

Routage multicast

Le routage multicast s'intéresse à la question de savoir **d'où vient un paquet** plutôt que *où va un paquet*

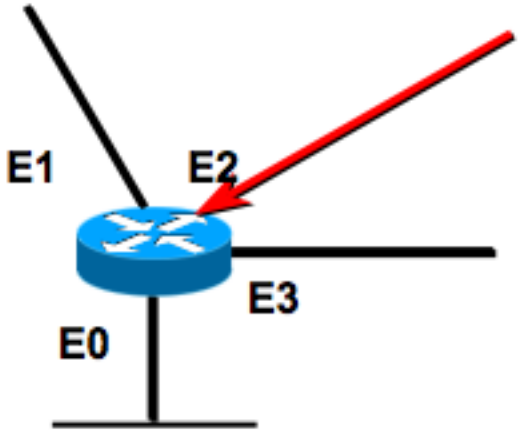
Mécanisme du Reverse Path Forwarding (RPF) : un routeur R recevant un paquet multicast depuis une source S transmet ce paquet seulement si il arrive d'une interface que R utiliserait pour envoyer vers la source S (consultation de la table de routage)

Un exemple de test RPF



Un exemple de test RPF

Un paquet multicast arrive de la source 130.190.2.1 sur l'interface E2



Le paquet arrive sur une mauvaise interface
On rejette le paquet

Table de routage Unicast	
Réseau	Interface
195.221.44.0/24	E0
130.190.0.0/16	E1
82.233.104.0/24	E2

Un exemple de test RPF

Un paquet multicast arrive de la source 130.190.2.1 sur l'interface E1

Le paquet arrive sur la bonne interface
Le test est bon
On réexpédie le paquet sur les interfaces indiquées dans une liste de «sortie» OLIST

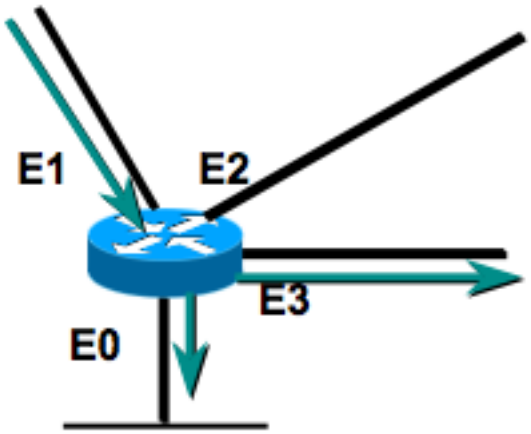


Table de routage Unicast	
Réseau	Interface
195.221.44.0/24	E0
130.190.0.0/16	E1
82.233.104.0/24	E2

DVMRP : table de routage?

Une route = destination, métrique

Destination = vers les sources (voir RPF)

Métrique = nombre de routeurs DVMRP traversés jusqu'à la source

Echange par IGMPv3 des routes multicast entre routeurs DVMRP: utilisation de l'adresse multicast 224.0.0.4 (pour la découverte et la mise à jour). Messages possibles: route, route?, élagage, greffe

Tous les routeurs ont la même vue de l'arbre de diffusion

DVMRP - PIM

DVMRP a son propre protocole de routage

PIM : Protocol Independent Multicast. Il repose sur le protocole de routage sous-jacent

PIM repose sur deux concepts:

- Arbres partagés pour les zones à faible trafic
- Arbres basés sur la source pour les zones à fort trafic

PIM – SM : Sparse Mode

1. Une route = 1 source S, 1 destinataire D, 1 point de rendez vous (RP) pour un groupe G
2. D envoie un “Join (*,G)” vers le RP
3. S envoie des données. Son routeur s'enregistre auprès d'un RP (“Register” (S, G)), et le RP diffuse cette donnée sur son arbre de diffusion
4. Le RP est la racine de l'arbre de diffusion partagé: celui-ci correspond à l'arbre de diffusion par défaut
5. Quand le routeur de D reçoit la donnée de S, il envoie un “Join(S,G)” à S. A la réception d'une nouvelle donnée par un canal différent de RP, un routeur en déduit avoir trouvé un plus court chemin vers S, et envoie un “Prune(S,G)” vers RP (qui le supprime alors des destinataires des paquets venant de S)

Problèmes de PIM-SM

Adressage : comment allouer les adresses multicast de manière globale ? Pas de mécanisme d'allocation dynamique fonctionnel. --> allocation statique (ex: GLOP)

Pas de contrôle d'accès sur les sources : brouillage des communications, volontaire (deny de service) ou pas (oubli)

Travail inutile si sources et destinations connues à l'avance (RP inutile)

PIM : SSM, Source Specific Multicast

- Utilise des arbres centrés sur la source
- Hypothèse: modèle One-To-Many
- Les récepteurs sont responsables de la découverte des sources (page web, annuaire, ...)
- Donc pas de RP
- Les flux venant de diverses sources dans le même groupe sont distincts

Le réseau MBONE: Multicast Backbone

Réseau virtuel de noeuds multicast sur Internet
- reliés par des "tunnels »
- au dessus de la topologie unicast
- Pour palier au fait que tous les routeurs ne sont pas multicast

Ensemble d'outils :
- pour annoncer la diffusion de programmes multimédia (sdr)
- pour assister les utilisateurs à rejoindre les groupes (sdr)
- et à suivre ou diffuser les programmes (vat, vic, wb, nt,…)

Protocole de routage : DVMRP, MOSPF

Topologie :
- maillage des réseaux régionaux par des machines "mroutées" à travers des tunnels
- étoiles au niveau du réseau du site
- hiérarchie

Multicast Transport Protocol

Transport Protocol:

- UDP : pas de garantie, mais le plus souvent utilisé
- TCP : problèmes dus, entres autres, à la connexion, au nombre de ACK

Protocoles dédiés pour prendre en compte: delais, pertes, ordres, retransmission, contrôle de flux et de congestion, gestion des groupes, ...

- RTP, SRM (Scalable Reliable Multicast), URGC (Uniform Reliable Group Communication Protocol), MFTP, STORM, ...

RTP

Protocole de niveau “session-applicatif”, fonctionnant au dessus de UDP/TCP (le + souvent UDP), ou AAL5/ATM

Définit le format des informations additionelles requises par l'application (estampillage, numéro de séquence)

Associé à RTCP pour l'échange de rapports

1 session RTP : 1 type de donnée

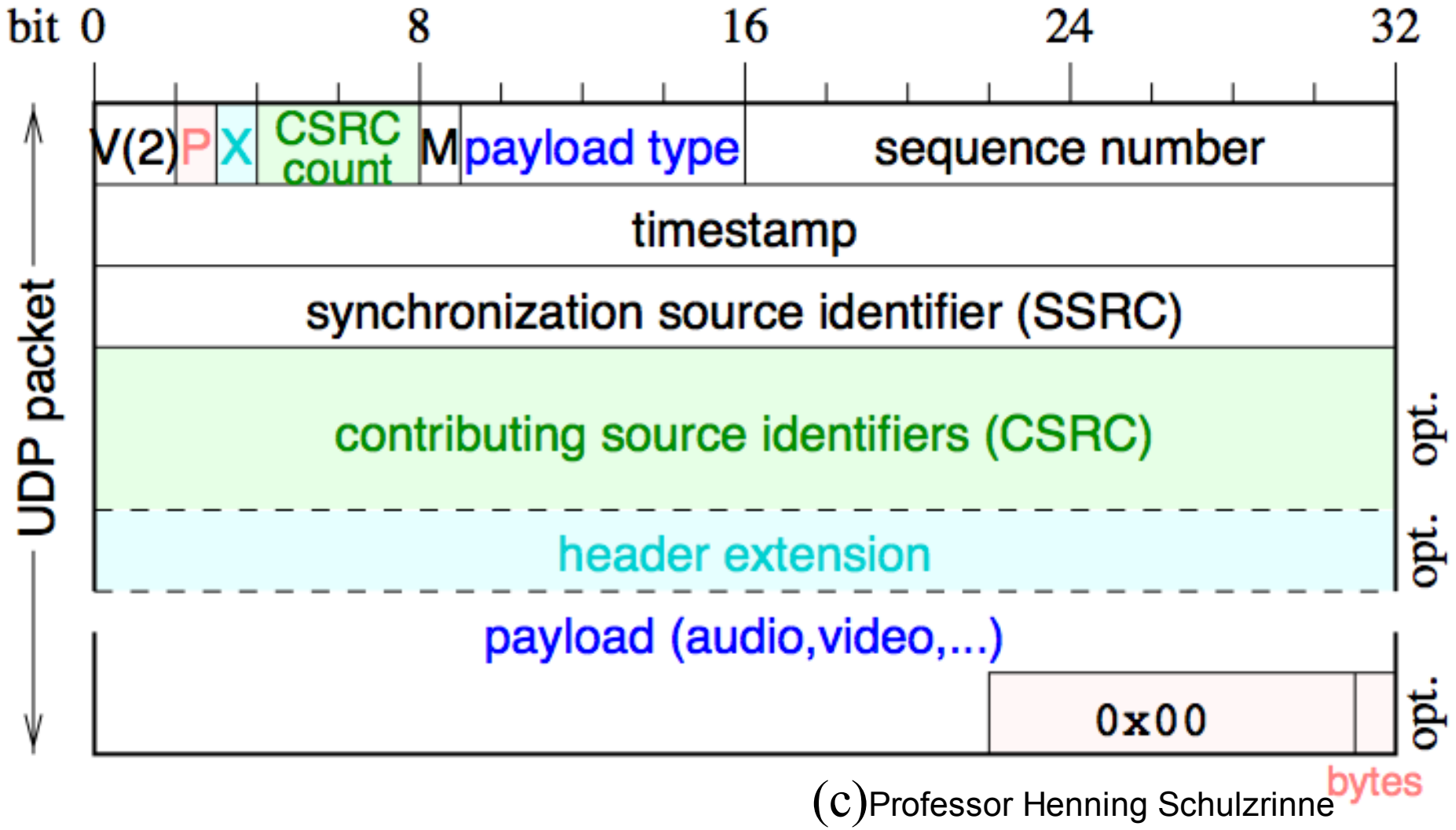
Rôle de RTP

identifier le type de l'information transportée,

ajouter des marqueurs temporels (synchronisation intra et inter média) et des numéros de séquence à l'information transportée

contrôler l'arrivée à destination des paquets.

RTP packet header



RTP: format de l'entête

Entre autres:

- CC : nombre de CSRC qui suivent
- PT : Payload Type. Indique le type de la donnée qui suit (ex: MPEG2, PCM, ...)
- Sequence: numérotation des paquets (à partir random)
- Timestamp : reflète l'instant où le premier bit du paquet a été échantilloné. Sert à la synchronisation et au calcul de la gigue à la destination
- SSRC: identifie la source de synchronisation (numéro aléatoire)
- CSRC: identifie les sources contribuant au paquet

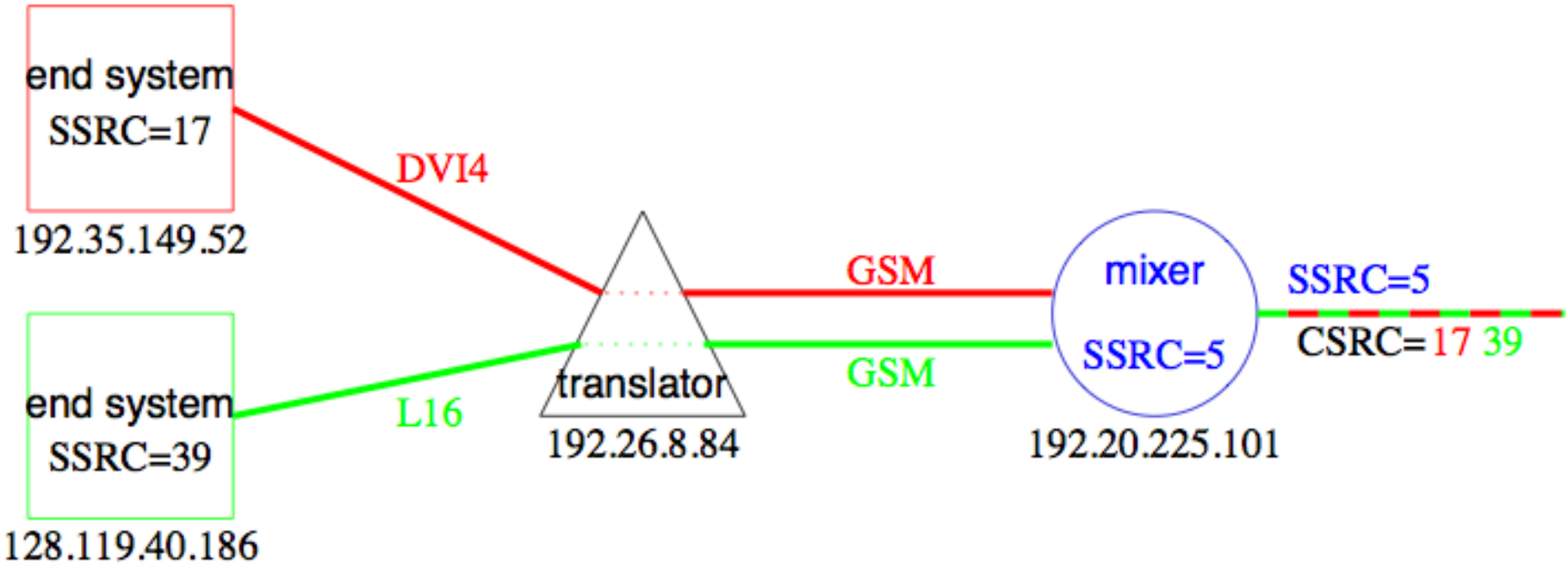
RTP: Rôle du mixer et translator

Mixer:

- permet de combiner plusieurs flux RTP dans une même session (différents CSRC)
- Peut changer l'encodage (le format des paquets)
- Apparaît comme une nouvelle source

Translator:

- Peut changer l'encodage (le format des paquets)
- Translation de protocoles (IP<->ATM)
- Apparaît comme une nouvelle source



RTCP: Real Time Control Protocol

Associé à RTP pour la signalisation du transport des données par RTP

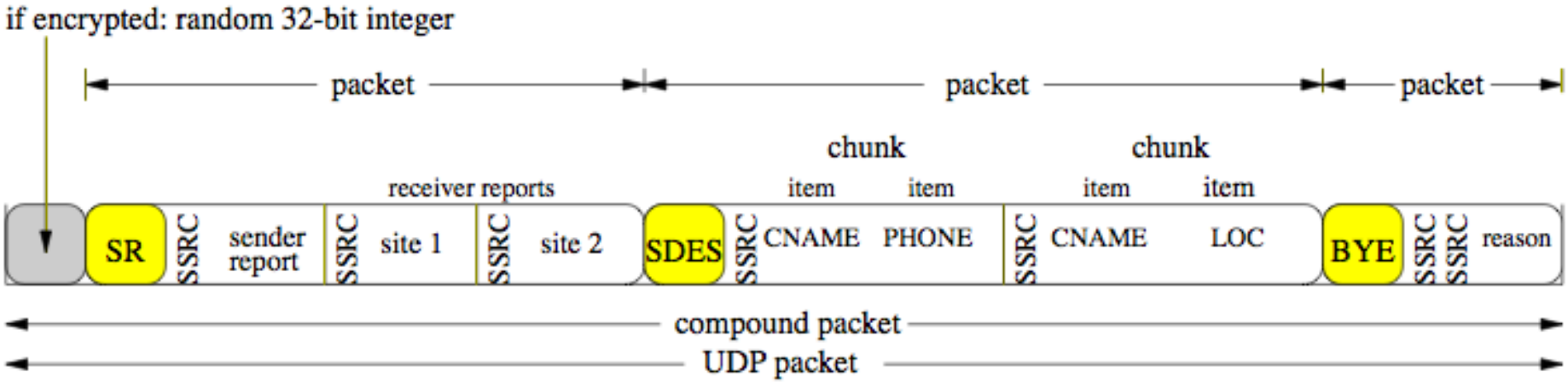
Permet de savoir comment la transmission s'effectue: délais, gigue, taux de perte (Receiver Report)

Permet de resynchroniser les flux et de synchroniser divers flux différents (Sender Report)

Permet d'identifier les partenaires des communications (Source Description)

Permet de fermer une session explicitement (BYE)

RTCP packet structure



(c)Professor Henning Schulzrinne

RTCP: Sender Report (SR)

SSRC: identifiant de la source de la donnée

NTP: temps auquel le SR a été envoyé

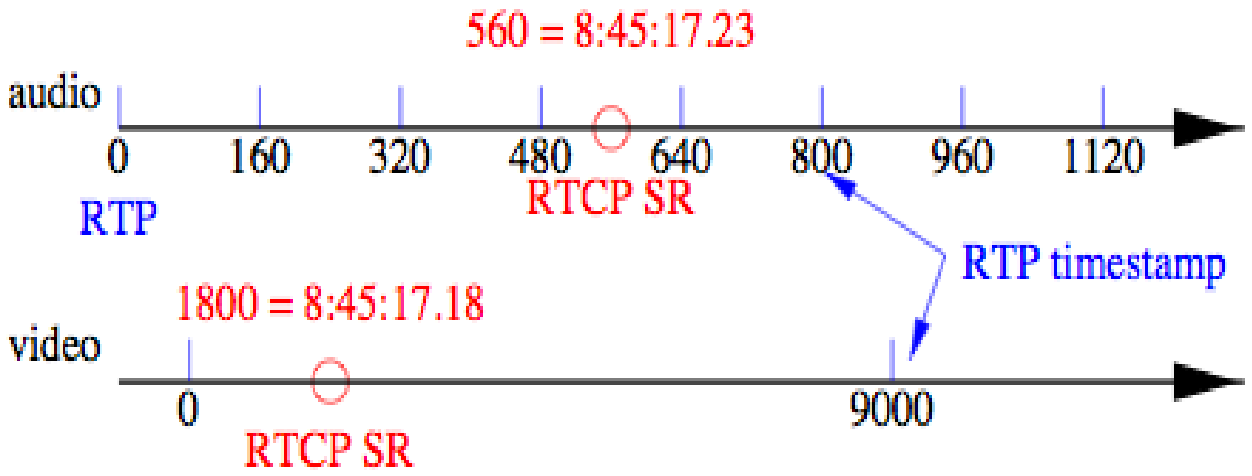
RTP: temps “RTP” correspondant à NTP

Nombre de paquets et nombre d'octets émis

Puis des Receiver Report

RTCP: synchronisation inter-média

Pour correler les différents timestamp RTP, utilisation des paquets SR



RTCP: Receiver Report

SSRC: identifiant de la source que l'on monitore

Ratio de perte

Nombre de paquets perdus en tout

Dernier numéro de séquence reçu

Gigue inter-arrivée

Temps du dernier SR reçu

Délai depuis le dernier SR reçu

RTCP: Estimation de la gigue

S_i = RTP timestamp du paquet i

R_i = Instant de réception du paquet i

D_i = Estimation de la gigue pour le paquet i

$$D_i = (R_i - R_{i-1}) - (S_i - S_{i-1})$$

$$J_i = 15/16\ J_{i-1} + 1/16\ |\ D_i\ |$$

Sert à gérer les buffers (taille notamment)

RTCP: Bande passante

Si chaque recepteur envoie à tous les autres, la consommation de BP est trop importante

Donc RTCP calcule l'intervalle de temps entre deux rapports en fonction du nombre de récepteurs

En général, trafic < 5% BP

RTSP: Real Time Streaming Protocol

Utilisé pour gérer les sessions RTP

Description des sources disponibles

Etablissement des sessions RTP

Contrôle de la lecture, comme sur un magnétoscope: start, resume, pause, end

RTP-RTCP-RTSP, ensemble...

/Users/jean-marcpierson/Documents/Enseignement Toulouse/Cours Reseau Multimedia IIN/rtsp-rtp.html

Applications: Video on Demand/Streaming

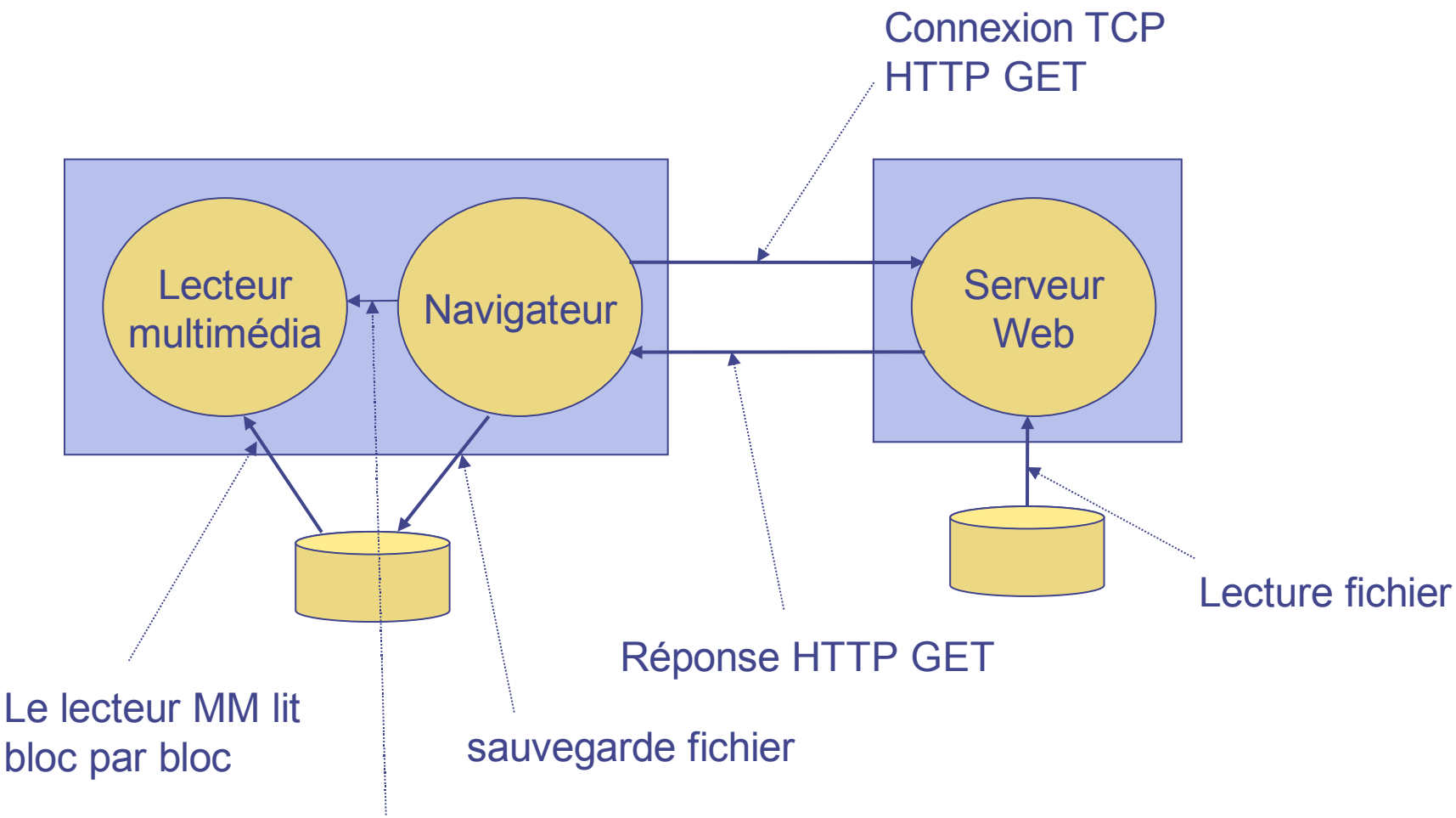
Architecture matérielle/logicielle

Streaming

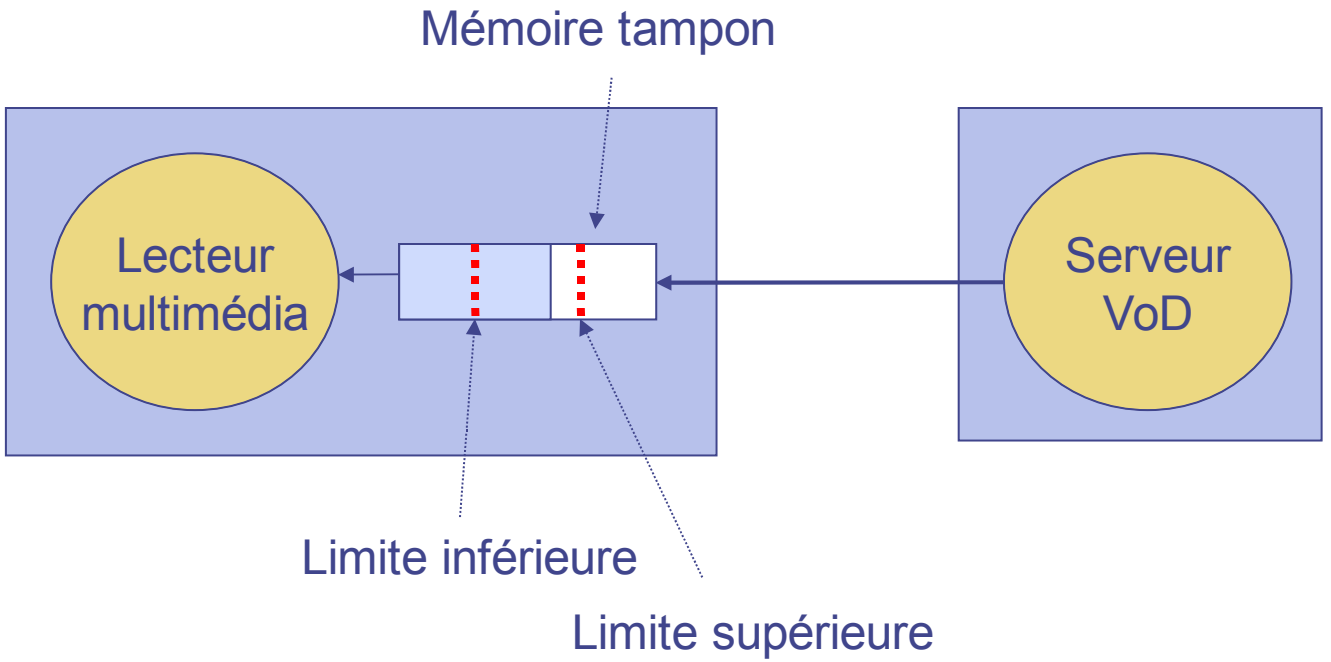
VOD

Slides suivants: © M. Scuturici, Insa Lyon

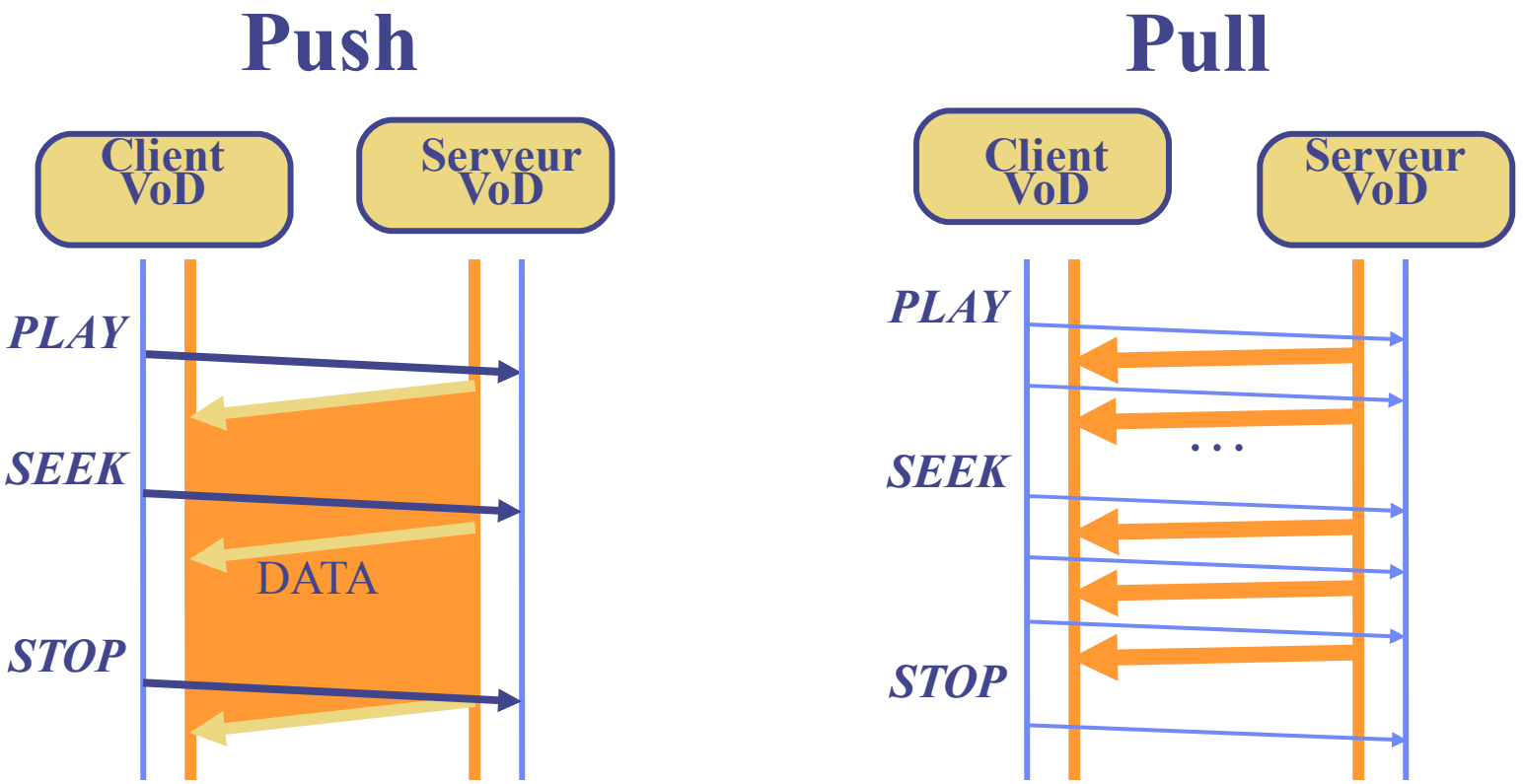
Vidéo à la demande (download and play)



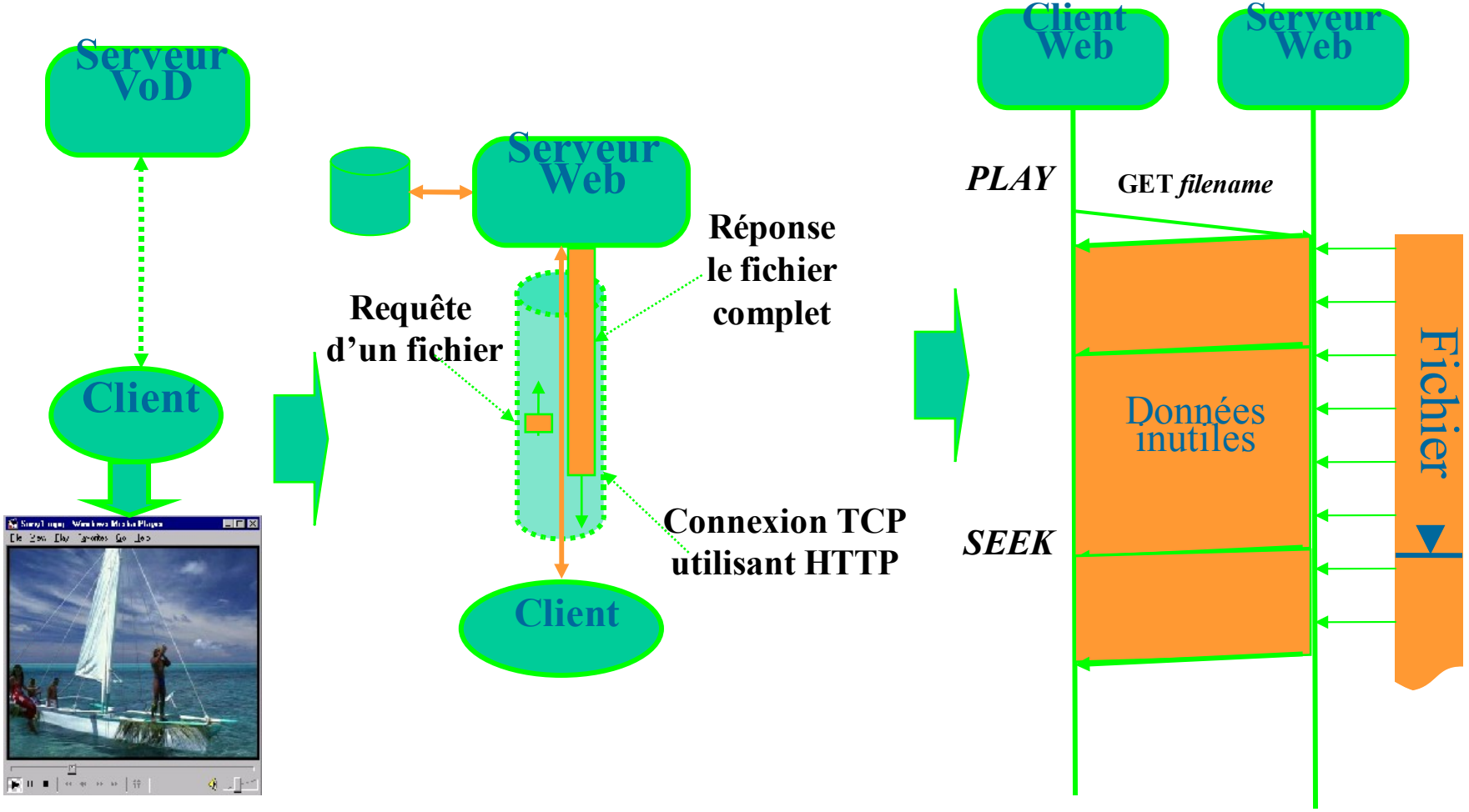
Streaming


Mémoire tampon
Lecteur multimédia
Serveur VoD
Limite inférieure
Limite supérieure

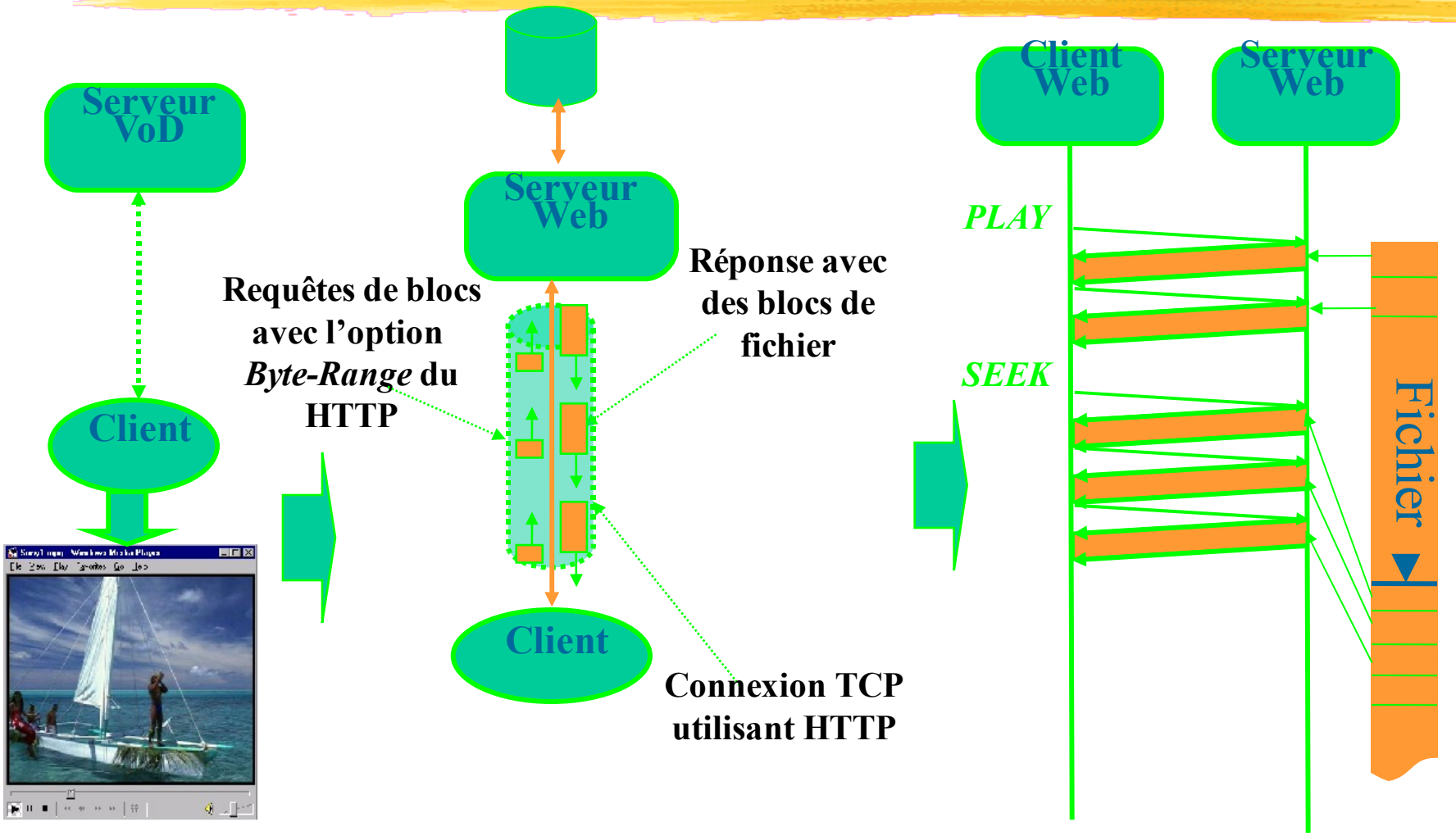
Streaming – stratégies de communication



VoD sur le Web
HTTP actuel : «transfert complet»



VoD sur le Web
HTTP modifié : «transfert par blocs»



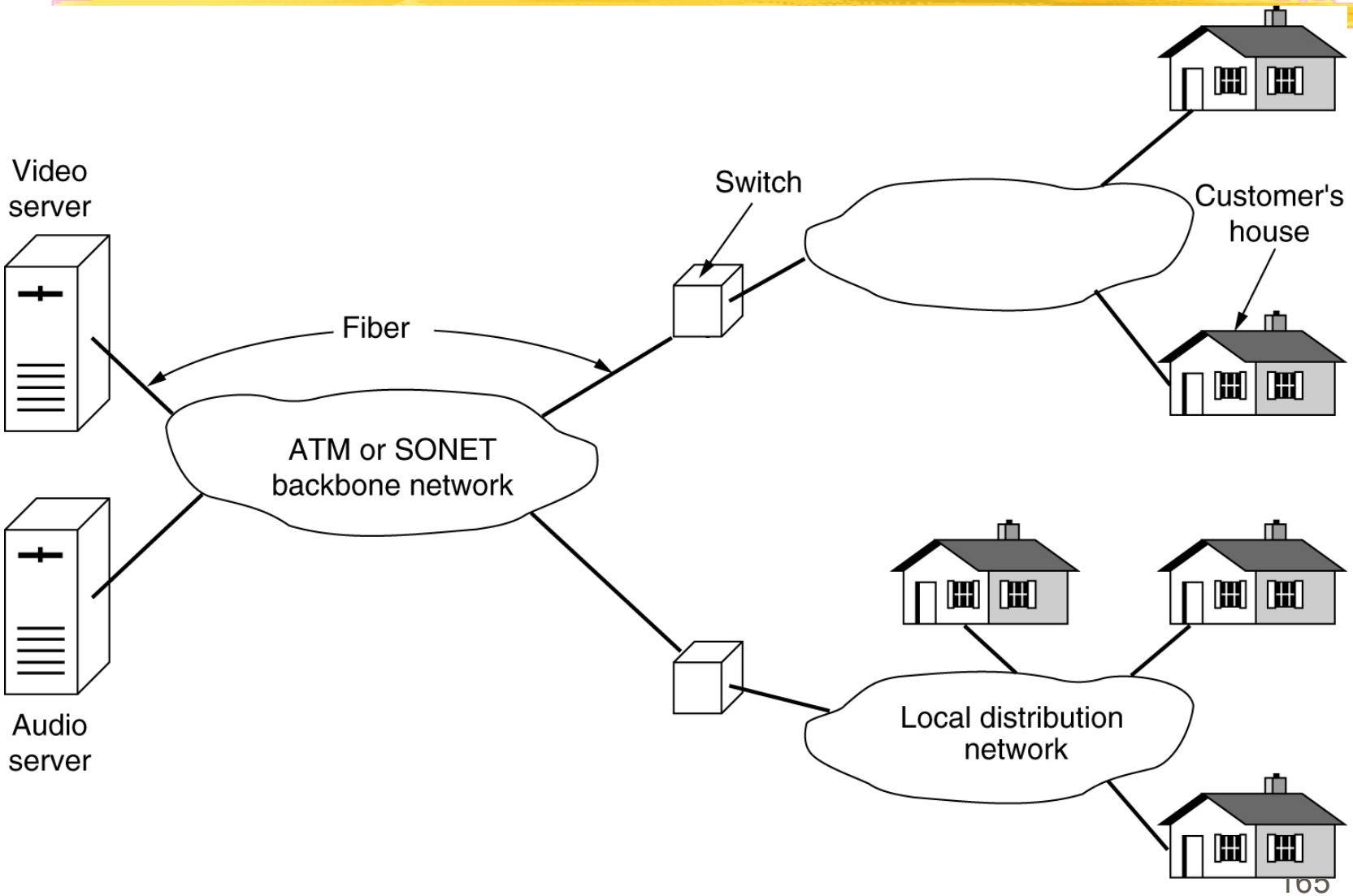
Utilisation de HTTP pour la visualisation des séquences vidéo

Lecteur multimédia

Filtre DirectX qui implémente la stratégie HTTP "transfert par blocs"

Serveur Web

Systèmes vidéo à la demande



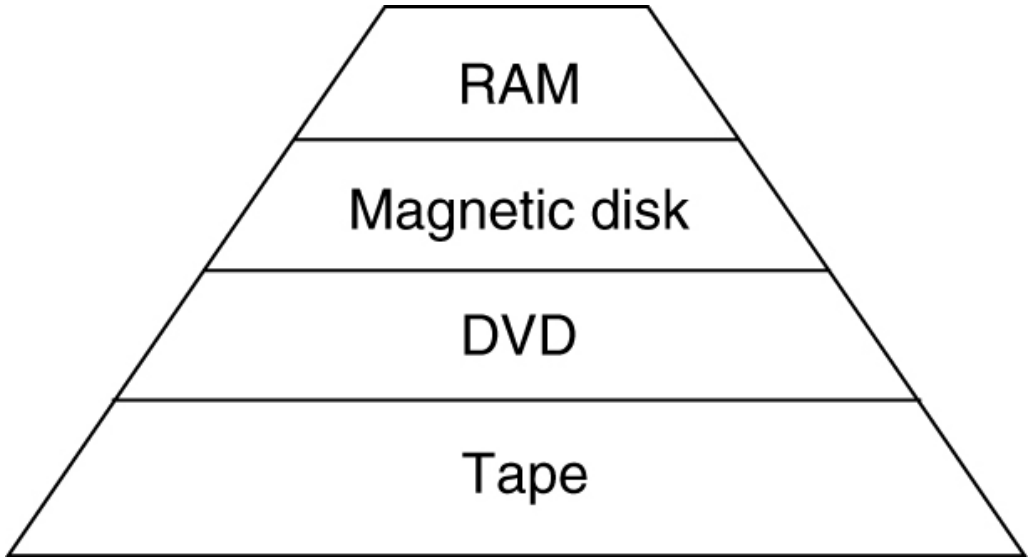
Serveurs vidéo

65000 films * 4 GB = 260 TB

Loi de Zipf

- N films disponibles
- le k-ème le plus populaire : la fraction de demandes = C/k
- C = 1/(1+1/2+1/3+…+1/N)

Serveur VoD - Stockage



Architecture d'un serveur VoD