

Les Réseaux

ENSAM

Karim Boudjemaa

Études et Projets – RENATER

Karim.boudjemaa@renater.fr

Cours n°1

Plan du cours 1

1. Introduction aux télécommunications

- ▶ Paysage des Télécoms
- ▶ Historique
- ▶ Grands principes de télécommunication

2. Les réseaux numériques

- ▶ « Définition »
- ▶ Classification
- ▶ Réseaux LAN,WAN

3. Mécanismes réseau

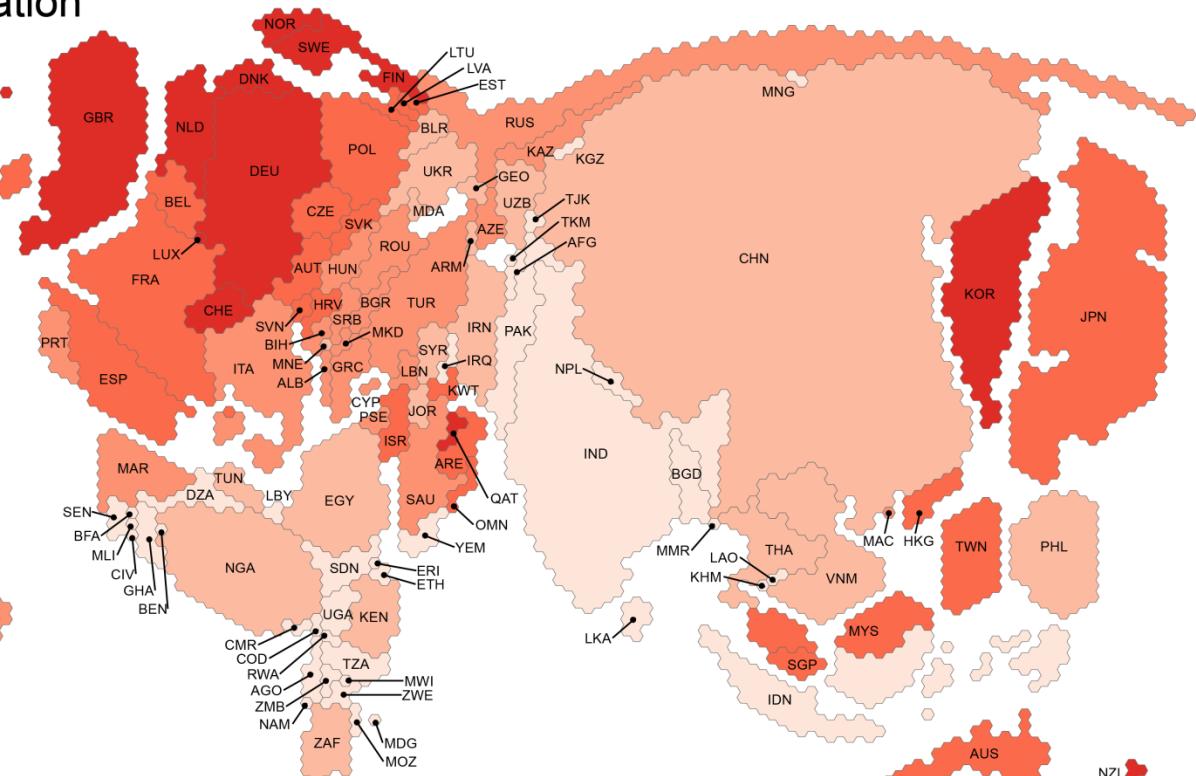
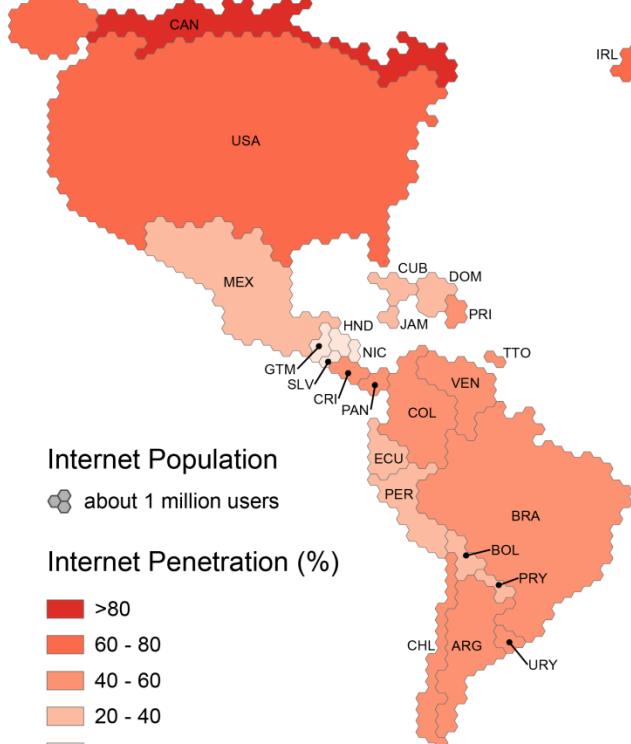
- ▶ Commutation de circuit
- ▶ Commutation de paquets
- ▶ Multiplexage
- ▶ Adressage

Introduction aux télécommunications

Paysage des Télécoms

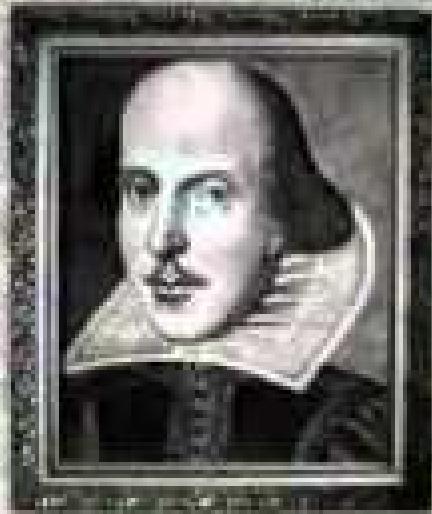
▶ http://en.wikipedia.org/wiki/Global_Internet_usage

Internet Population and Penetration



by Mark Graham (@geoplace) and Stefano De Sabbata (@maps4thought)
Internet Geographies at the Oxford Internet Institute
October 2013 • geography.oi.ox.ac.uk

data source: World Bank 2011
<http://data.worldbank.org>



About **5X** as many as during
Shakespeare's time



L'Arcep like

Le théorème du Pikachu

... ou quand l'explosion des usages mobiles récompense les investissements des opérateurs.

" Plus de 10 % de la population française est tombée cet été sous le charme de Pikachu et de ses amis monstres. 5 à 10 millions de Français ont marché des heures, l'oeil rivé sur le smartphone et son application de " réalité augmentée ", qui fait apparaître les petites bêtes dans son environnement immédiat. Tout cela consomme des quantités phénoménales de données et convertit plus d'abonnés à l'Internet mobile "

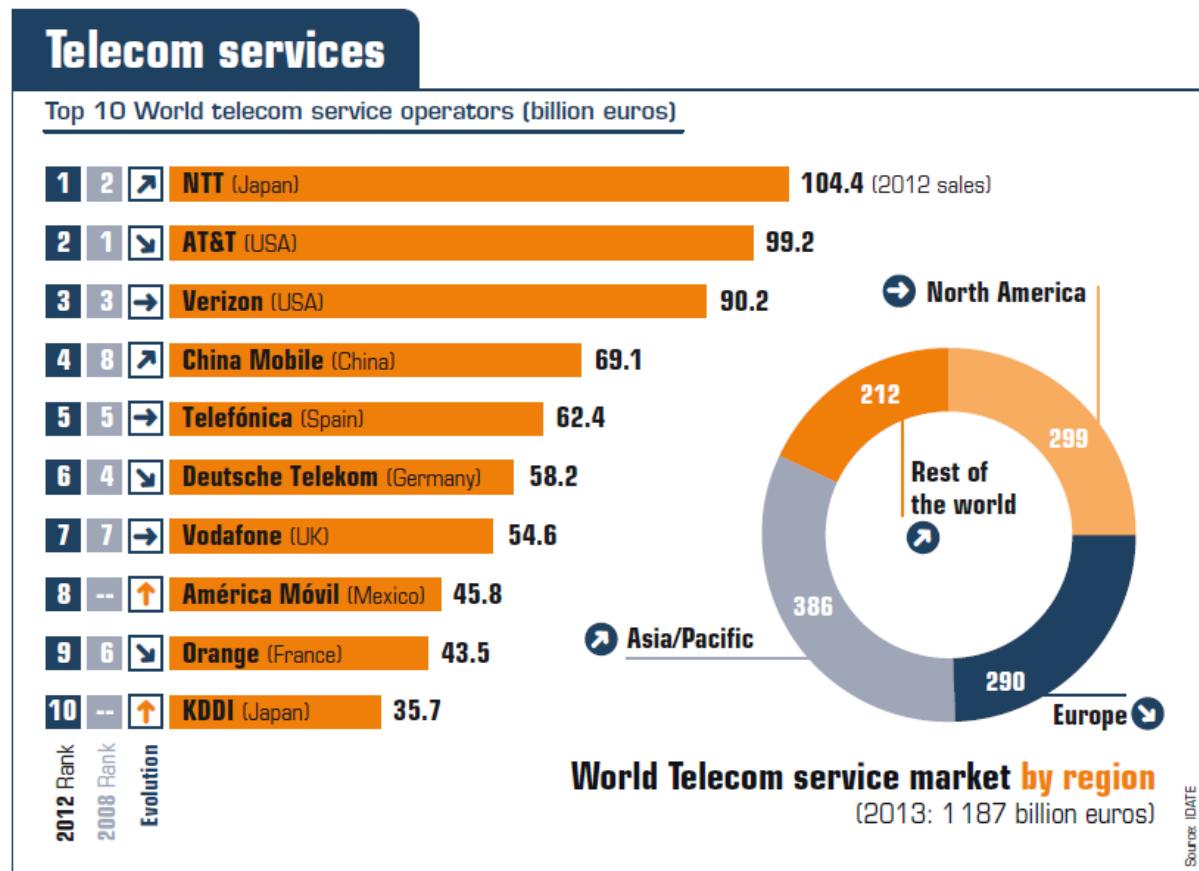
constate Philippe Escande, journaliste au Monde.

" On appellera cela le théorème du Pikachu " conclut le journaliste : une belle formule qui nous rappelle que les usages restent le moteur principal alimentant le cercle vertueux prôné par l'Arcep entre investissement, couverture/qualité de service et monétisation.

Introduction aux télécommunications

Paysage des Télécoms

► Les opérateurs :



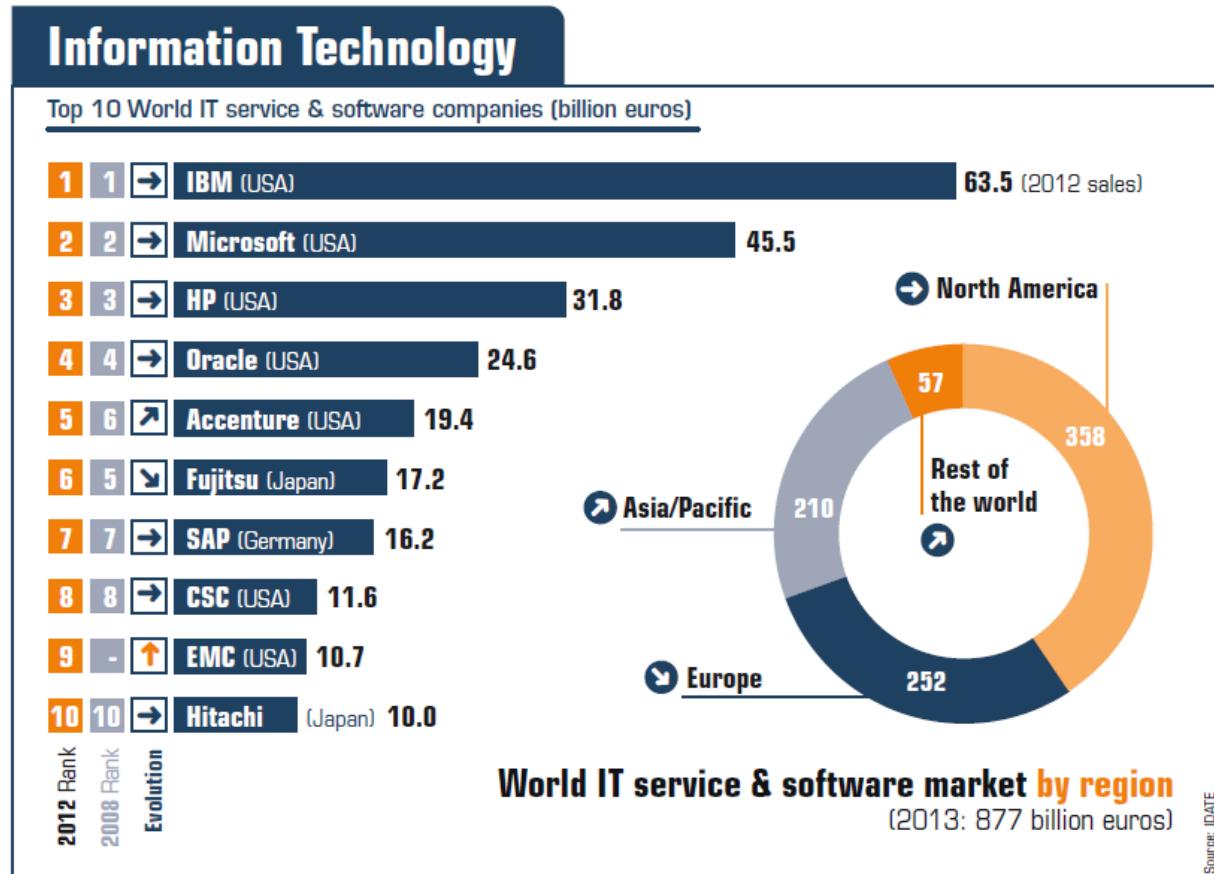
► En France :

- Numericable/SFR, Bouygues Telecom, opérateurs locaux (DSP)....

Introduction aux télécommunications

Paysage des Télécoms

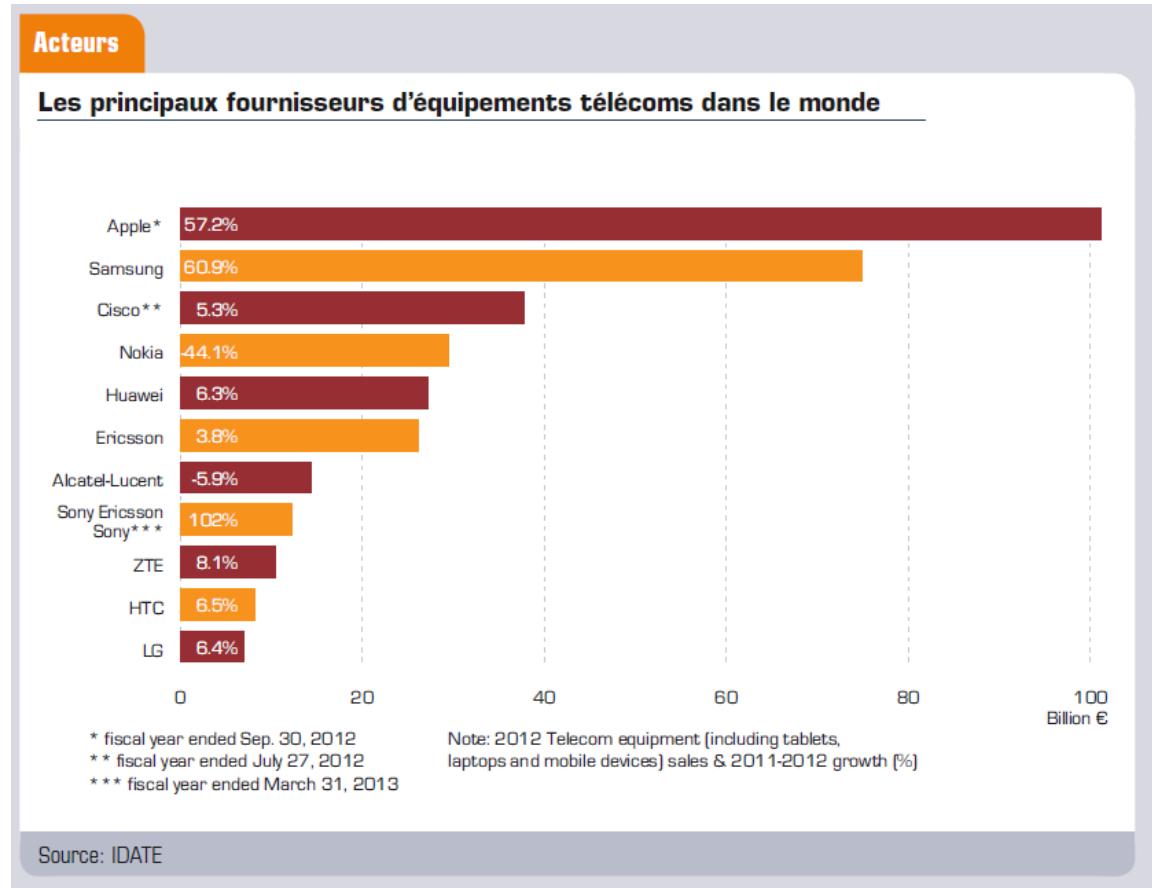
► Les fabricants de logiciels



Introduction aux télécommunications

Paysage des Télécoms

▶ Les équipementiers



Introduction aux télécommunications

Paysage des Télécoms

► Poids croissant des « G.A.F.A. »

Évolution des cours d'actions de grands groupes des secteurs des TIC

(Index) Week beginning...	Feb 25 2008	Feb 23 2009	Feb 22 2010	Feb 28 2011	Feb 27 2012	Feb 18 2013	Feb 24 2014
Apple (NASDAQ)	100	71	164	288	436	361	421
Deutsche Telekom (Xetra)	100	76	75	77	69	65	98
Orange (Paris)	100	80	77	70	51	34	41
Google (NASDAQ)	100	72	112	127	132	170	258
Facebook* (NASDAQ)						71	185
IBM (NYSE)	100	81	112	142	175	177	163
Microsoft (NASDAQ)	100	59	105	95	118	102	141
Alcatel-Lucent (NYSE)	100	22	52	96	41	24	73
NTT (NYSE)	100	105	106	130	117	104	114
Verizon (NYSE)	100	79	80	99	106	125	131
Vodafone (London)	100	77	87	110	105	100	152

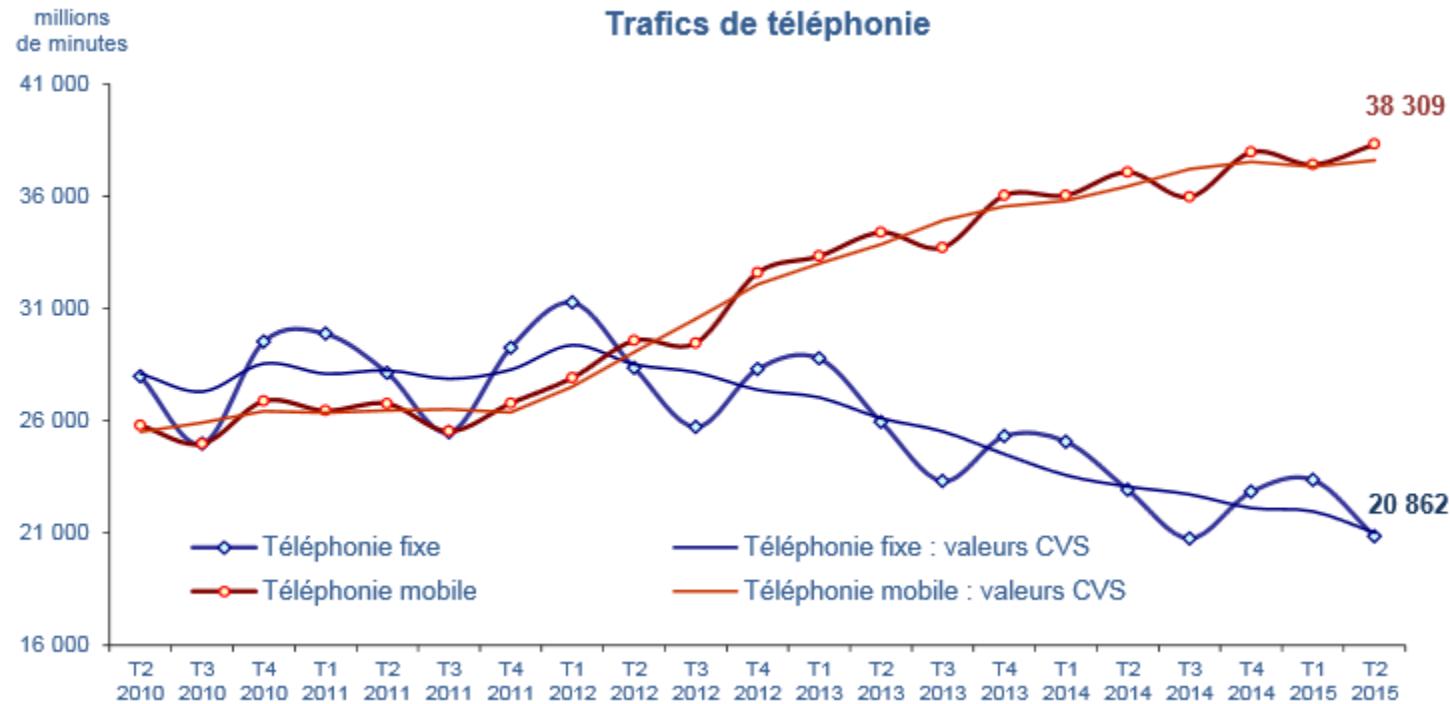
* 100 index = introduction quote price on May 18, 2012

Source: Yahoo! Finance

Introduction aux télécommunications

Paysage des Télécoms

▶ Evolution des consommations

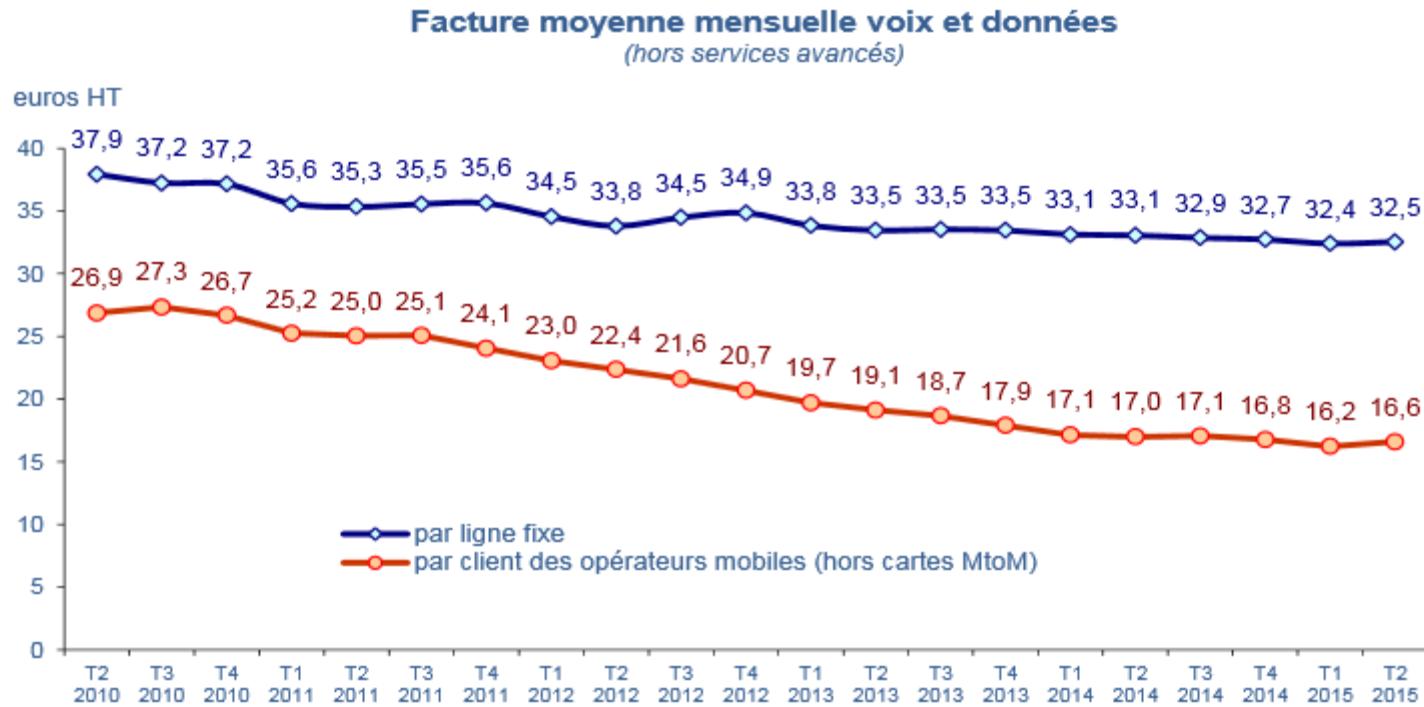


Source : ARCEP

Introduction aux télécommunications

Paysage des Télécoms

▶ Evolution des tarifs



Source : ARCEP

Introduction aux télécommunications

Paysage des Télécoms

► Comparatif des tarifs en Europe

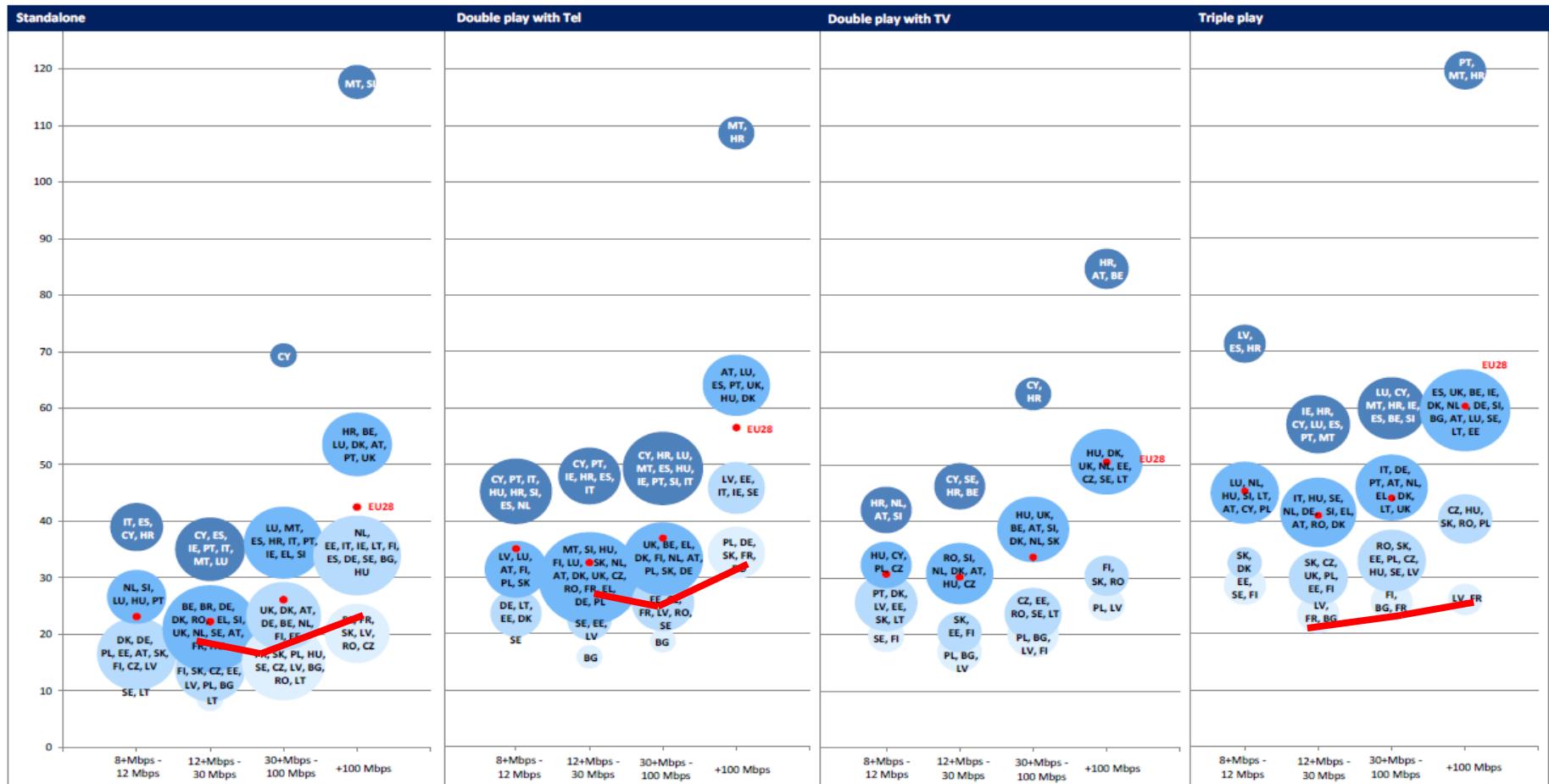


Figure 4: Clustering of countries based on prices for the least expensive offer available for Standalone, Double Play and Triple Play (expressed in EUR/PPP, VAT included)

Source : C.E.

Introduction aux télécommunications

Paysage des Télécoms (1/3)

▶ Les organismes

▶ ARCEP :

- précise les droits et obligations en matière de réseaux et services
- Fonctionnement du marché et concurrence,
- Conformité des terminaux



ITU-T : International Telecommunication Union

- Produit des « Recommandations » : normes internationales sur le fonctionnement des télécoms,
- Ex. : [G.652](#)



SERIES G: TRANSMISSION SYSTEMS AND MEDIA,
DIGITAL SYSTEMS AND NETWORKS
Transmission media and optical systems characteristics –
Optical fibre cables

Characteristics of a single-mode optical fibre
and cable

Introduction aux télécommunications

Paysage des Télécoms (2/3)

- ▶ **Les organismes**
 - ▶ **IETF : Internet Engineering Task Force**
 - regroupe des experts techniques dans des domaines variés, fournit les RFC.
 - But: Améliorer le fonctionnement d'Internet.
 - Ex. : [RFC1918](#)
 - ▶ **IEEE : Institute of Electrical and Electronics Engineer**
 - Organisée autour de plusieurs comités cherchant à résoudre des problématiques techniques et innover.
 - Ex., Le groupe 802 se charge des normes autour des réseaux LAN
 - ▶ **IANA: Internet Assigned Numbers Authority**
 - Assure la coordination globale des noms de domaine,
 - Assure la répartition des adresses IP,
 - Maintient le registre détaillant les protocoles utilisés sur Internet
 - -> RIPE NCC

Introduction aux télécommunications

Paysage des Télécoms (3/3)

▶ Les organismes

▶ IANA: Internet Assigned Numbers Authority

- Assure la coordination globale des noms de domaine,
- Assure la répartition des adresses IP,
- Maintient le registre détaillant les protocoles utilisés sur Internet
- -> RIPE NCC

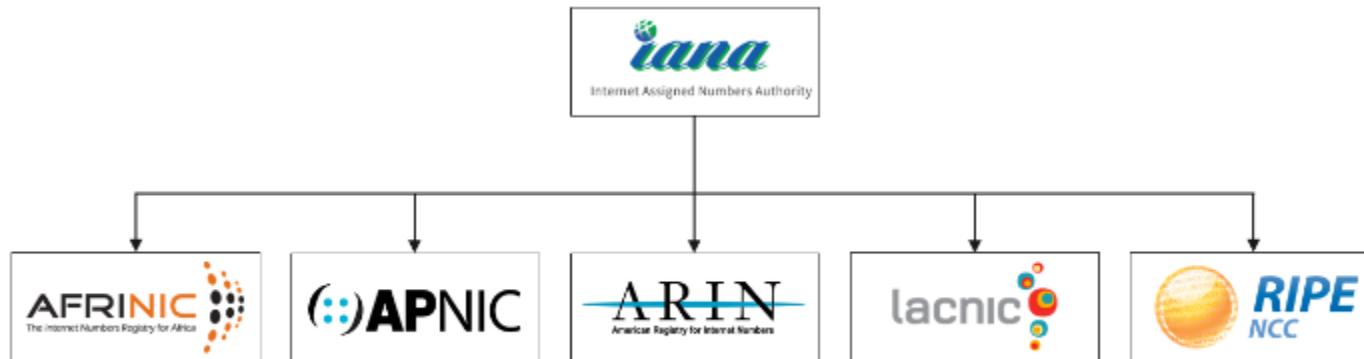


Figure 2 : Autorités régionales attribuant les adresses IP.

Introduction aux télécommunications

Historique

- ▶ Antique : Signaux de fumée, tambours, missives...



- ▶ 1464 : Crédit de la Poste Royale par Louis XI (France)

Introduction aux télécommunications

Historique

- ▶ 1793-1854 : Télégraphe optique de Claude Chappe

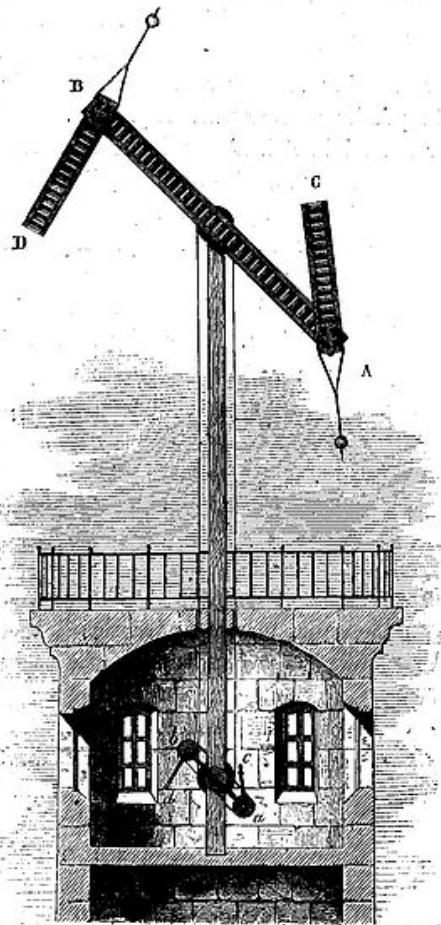
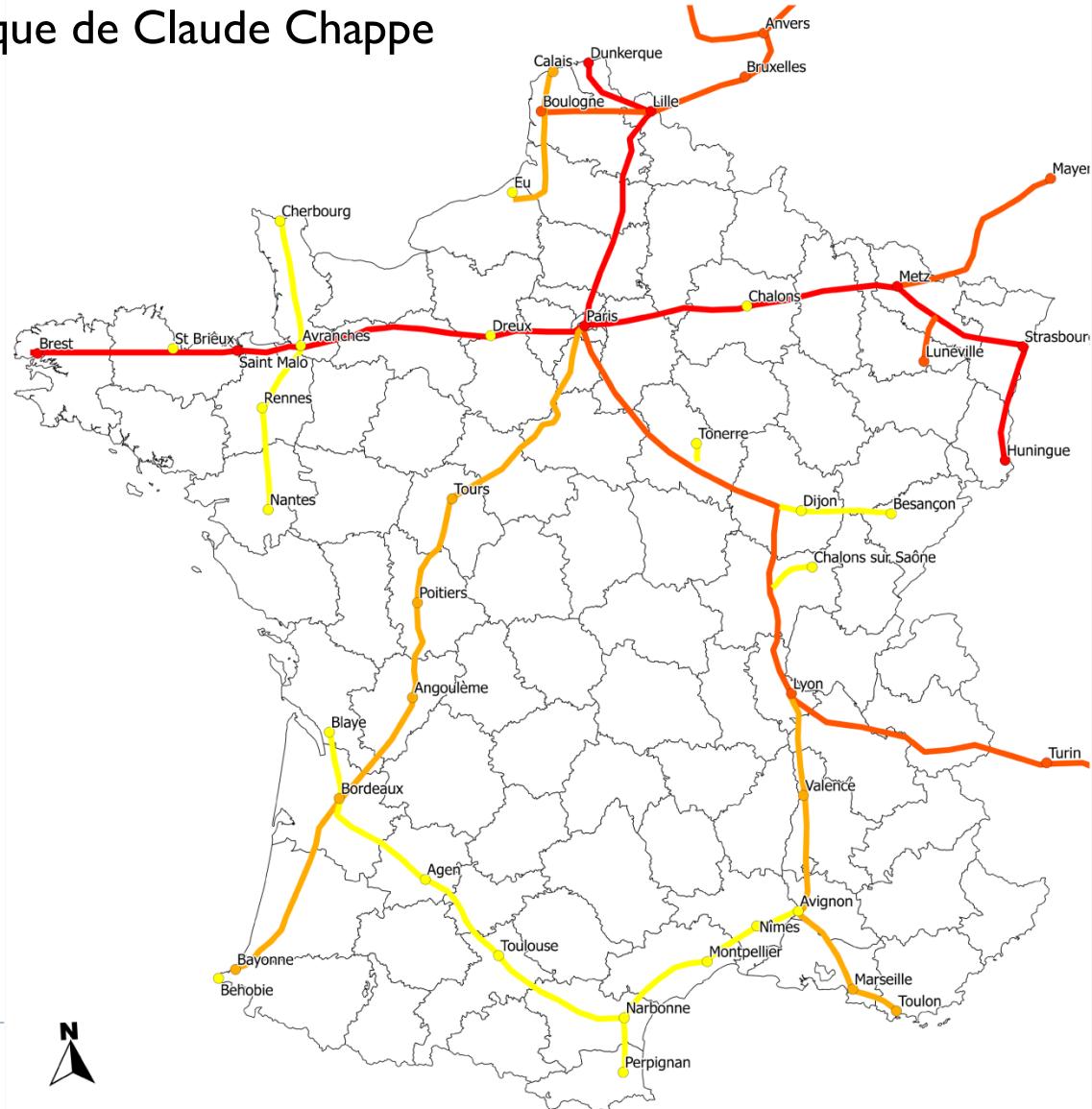


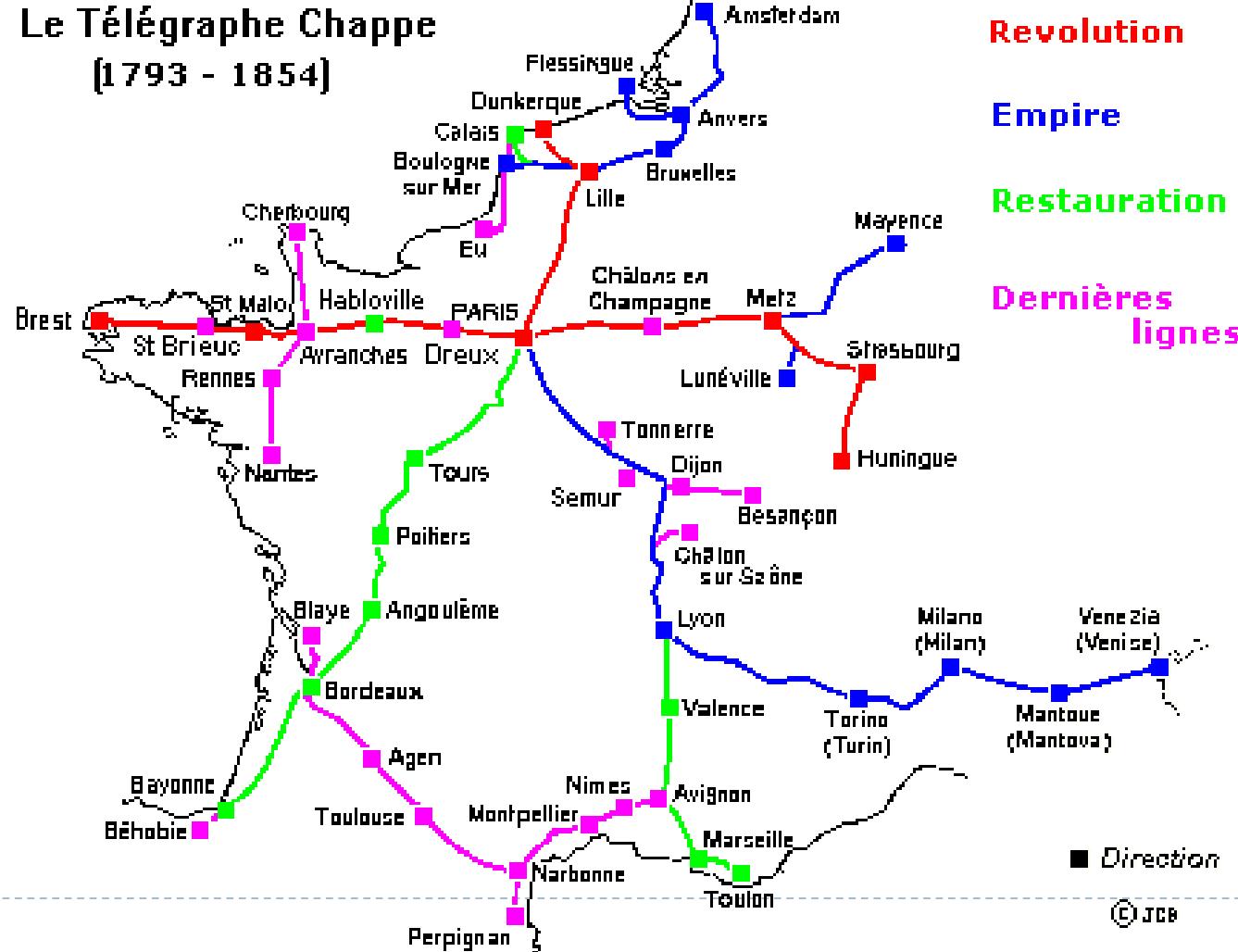
Fig. 19. — Télégraphe de Chappe.



Introduction aux télécommunications

Historique

- ▶ 1793-1854 : Télégraphe optique de Claude Chappe



Introduction aux télécommunications

Historique

- ▶ 1793-1854 : Télégraphe optique de Claude Chappe
- ▶ Codage – Transmission - Protocole – Réception – Décodage

Extrait du Vocabulaire	
(Livre tenu secret par le Directeur, permettant de décoder les dépêches)	
1	Absenter
	Actif
Age	HOGUE (cap de la)
Antipathie	HOLLANDAIS
Assesseur	HOLLANDE (prince royal)
Aumône	50 HOLSTEIN
Après avoir	HONFLEUR
Baisse	HONGRIE
Bénéficier	HONGROIS
10 Boudier	Horaire
Buisson	HORN (cap)
Caravane	Horloge - Marine
Avec celui	Hospice
Chargement	HOTTENTOTS (pays des)
Civiliser	HOTWIEL
Commodité	60 HOUNDEL (le)
Conduire	HUDSON (baie de)
Consternation	HUDSON (détroit d')
Conviction	Huée
Craindre	Huer
Débaucher	HUESCA
Défense	HULST
Démontrer	HUNDURAS (pont de)
Devenir	Hune
Dire	Hunier
Domination	70 HUMINGUE
Donner une haute idée de	HUMINGUE (pont de)
Echoué	HUNTINGTON
Electriser	HURON (lac)
30 Empoisonnement	Hussard
Enrôlé	Escadron de Hussards
Équivalent	Hydraulique
Etouffer	Hymne
Sur eux	Hypocrisie
Extorquer	Hypothèque
Félicitation	80 Idée
Fois	Identifier
Friche (en)	Identité
Général – commandant à Lyon	Idôlatre
40 GRAVELINES (port)	Idôlatrer
HESSORS	Idôlatrie
HIERES (îles d')	Idole
HILDELSHEIM	Ignorance
Historien	Ignorant
Hivernage	Ignoré
HOCHSTET	90 Ignorer
	ILANTE
	ILDEFONSE (Saint)

Grille des signaux de correspondance	
↑	1
↓	2
↔	3
↖	4
↗	5
↙	6
↘	7
↑↓	8
↑↔	9
↑↖	10
↑↗	11
↓↔	12
↓↖	13
↔↖	14
↖↖	15
↖↗	16
↖↓	17
↖↑	18
↗↖	19
↗↓	20
↗↑	21
↓↖	22
↓↗	23
↓↑	24
↖↑	25
↖↖	26
↖↖↖	27
↖↖↖↖	28
↖↖↖↖↖	29
↖↖↖↖↖↖	30
↖↖↖↖↖↖↖	31
↖↖↖↖↖↖↖↖	32
↖↖↖↖↖↖↖↖↖	33
↖↖↖↖↖↖↖↖↖↖	34
↖↖↖↖↖↖↖↖↖↖↖	35
↖↖↖↖↖↖↖↖↖↖↖↖	36
↖↖↖↖↖↖↖↖↖↖↖↖↖	37
↖↖↖↖↖↖↖↖↖↖↖↖↖↖	38
↖↖↖↖↖↖↖↖↖↖↖↖↖↖↖	39
↖↖↖↖↖↖↖↖↖↖↖↖↖↖↖	40
↖↖↖↖↖↖↖↖↖↖↖↖↖↖↖↖	41
↖↖↖↖↖↖↖↖↖↖↖↖↖↖↖↖↖	42
↖↖↖↖↖↖↖↖↖↖↖↖↖↖↖↖↖	43
↖↖↖↖↖↖↖↖↖↖↖↖↖↖↖↖↖	44
↖↖↖↖↖↖↖↖↖↖↖↖↖↖↖↖↖	45
↖↖↖↖↖↖↖↖↖↖↖↖↖↖↖↖↖	46
↖↖↖↖↖↖↖↖↖↖↖↖↖↖↖↖↖	47
↖↖↖↖↖↖↖↖↖↖↖↖↖↖↖↖	48
↖↖↖↖↖↖↖↖↖↖↖↖↖↖↖	49
↖↖↖↖↖↖↖↖↖↖↖↖↖	50
↖↖↖↖↖↖↖↖↖↖	51
↖↖↖↖↖↖↖	52
↖↖↖↖↖	53
↖↖↖↖	54
↖↖↖	55
↖↖	56
↖	57
↖↖↖↖↖↖↖↖↖↖↖↖↖↖↖	58
↖↖↖↖↖↖↖↖↖↖↖↖↖	59
↖↖↖↖↖↖↖↖↖	60
↖↖↖↖↖↖	61
↖↖↖↖↖	62
↖↖↖↖	63
↖↖↖	64
↖↖	65
↖	66
↖↖↖↖↖↖↖↖↖↖	67
↖↖↖↖↖	68
↖↖↖↖	69
↖↖↖	70
↖↖	71
↖	72
↖↖↖↖↖	73
↖↖↖	74
↖↖	75
↖	76
↖↖↖↖	77
↖↖	78
↖	79
↖↖↖	80
↖↖	81
↖	82
↖↖↖↖	83
↖↖	84
↖	85
↖↖↖	86
↖↖	87
↖	88
↖↖↖↖	89
↖↖	90
↖	91
↖↖↖	92

Introduction aux télécommunications

Historique - Telecoms

- ▶ 1832 : Invention du télégraphe électrique par Samuel Morse
- ▶ 1865 : Création de l'Union internationale du télégraphe (UIT)
- ▶ **1866 : Premier câble télégraphique transatlantique**
- ▶ 1876 : Téléphone de Graham Bell & Elisha Gray
- ▶ 1876 : Premiers enregistrements de Thomas Edison
- ▶ 1887 : Ondes radioélectriques de H. Hertz
- ▶ 1892 : Radiodiffusion par W. Crookes
- ▶ 1897 : Émission radio au Panthéon de Paris par Eugène Ducretet
- ▶ **1901 : Première liaison radio transatlantique**
- ▶ 1922 : Premières émissions régulières de radio de la tour Eiffel
- ▶ 1935 : Émissions régulières de télévision depuis la tour Eiffel
- ▶ **1962 : Première transmission transatlantique via satellite de la télévision
(site du radome à Pleumeur Bodou, côtes d'armor)**

Introduction aux télécommunications

Historique - Telecoms

- ▶ 1969 : ARPAnet - TCP/IP (US GOV)
- ▶ 1970 : Premier réseau en fibres optiques
- ▶ 1971 : CYCLADES (INRIA) – Premières connexion « paquet » entre l'Europe et les USA.
- ▶ 1979 : TRANSPAC (X25 PTT) – Minitel

Introduction aux télécommunications

Historique - Informatique

- ▶ 1947 : Invention du transistor par W. Shockley
- ▶ 60's : Ordinateurs de première génération (Armée, universités)
- ▶ 60's : Usages Mainframe – Terminal.
- ▶ 1971 : Premiers microprocesseurs
- ▶ 80's : Débuts de l'informatique personnelle

Introduction aux télécommunications

Historique - Telecoms

- ▶ 1998 : Réseaux DWDM. Fondation de 3GPP (organisme de spécifications pour réseaux mobiles : GSM, GPRS, EDGE, UMTS, ... LTE)
- ▶ 1999 : Liaisons ADSL (France)
- ▶ 2000's : Réseaux mobiles 1 – 2 – 2,5 – 3 – 3,5 G
- ▶ 2012 :
 - ▶ Arrêt de Transpac (X25)
 - ▶ $1,5 \cdot 10^9$ d'utilisateurs d'Internet, $500 \cdot 10^6$ de comptes Facebook
- ▶ 2015 :
 - ▶ $3 \cdot 10^9$ d'utilisateurs d'Internet, $1,5 \cdot 10^9$ de comptes Facebook
 - ▶ Réseaux 4G en voie de généralisation
 - ▶ Le trafic Internet Global va quadrupler par rapport à 2014.
- ▶ 2020 :
 - ▶ 5 à $7 \cdot 10^9$ d'utilisateurs d'Internet
 - ▶ Généralisation des usages de services en « Cloud »
 - ▶ IoT massivement présent ???

Introduction aux télécommunications

Principes généraux



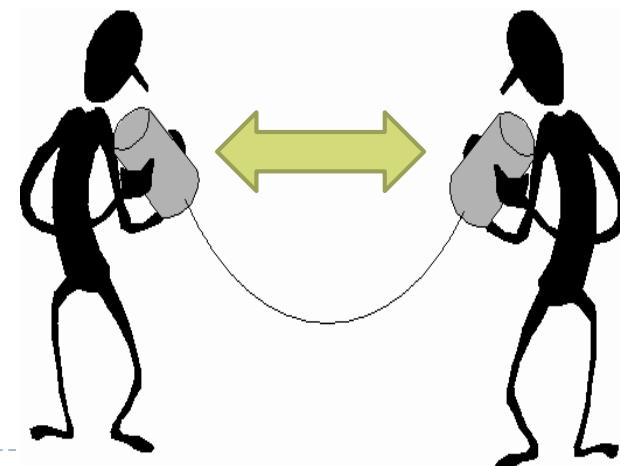
Source : MOOC FUN - Principes des réseaux

Introduction aux télécommunications

Principes généraux

- ▶ Communication Humaine
 - ▶ Message, information à transmettre
- ▶ Se comprendre
 - ▶ Langage → Codage de l'information
- ▶ S'entendre
 - ▶ Voix = émetteur,
 - ▶ Oreille = Récepteur
 - ▶ Air = médium
- ▶ Plusieurs type de communications
 - ▶ I à I = dialogue
 - ▶ I à plusieurs = discours
 - ▶ Plusieurs à plusieurs = cacophonie

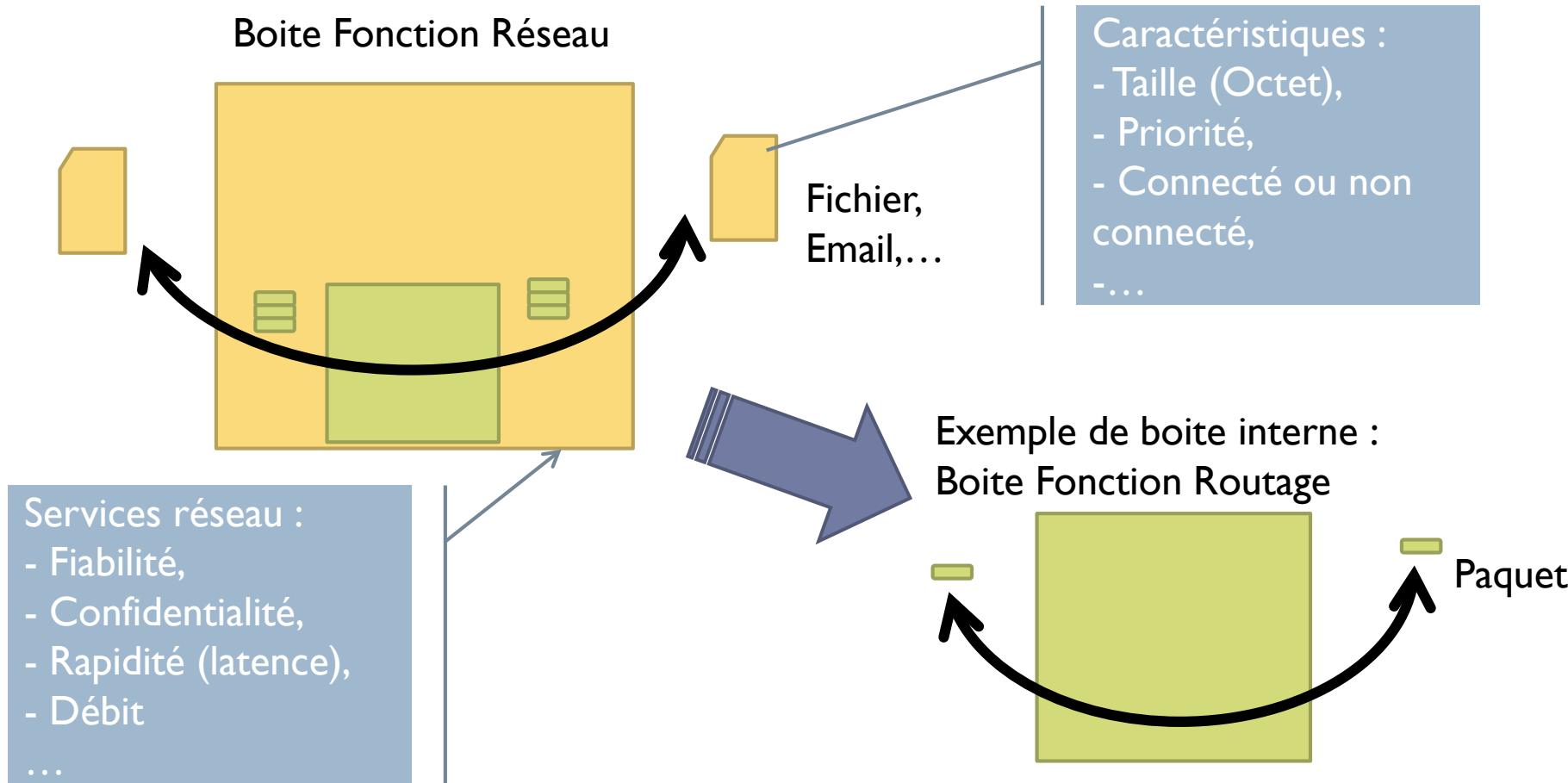
} → Transport de l'information



Introduction aux télécommunications

Principes généraux

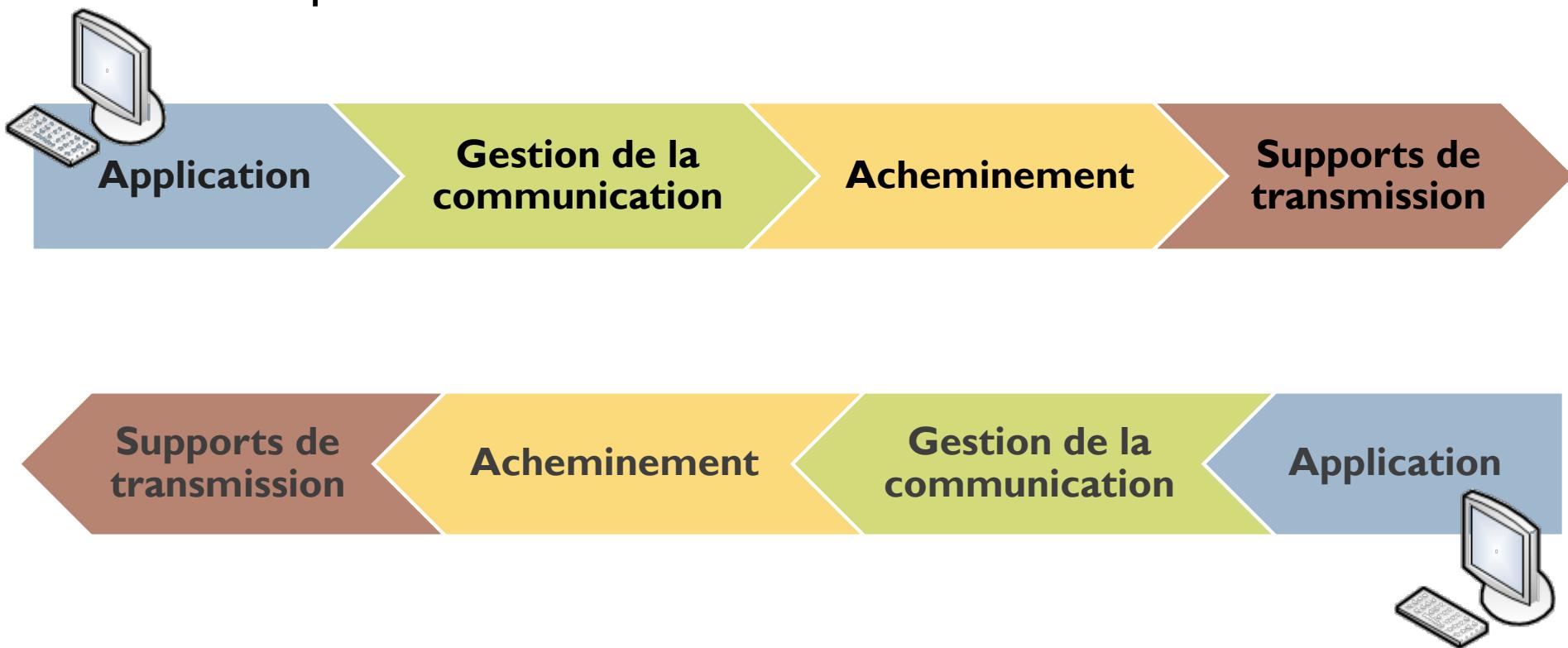
► Vue fonctionnelle : concept des boîtes récursives



Introduction aux télécommunications

Principes généraux

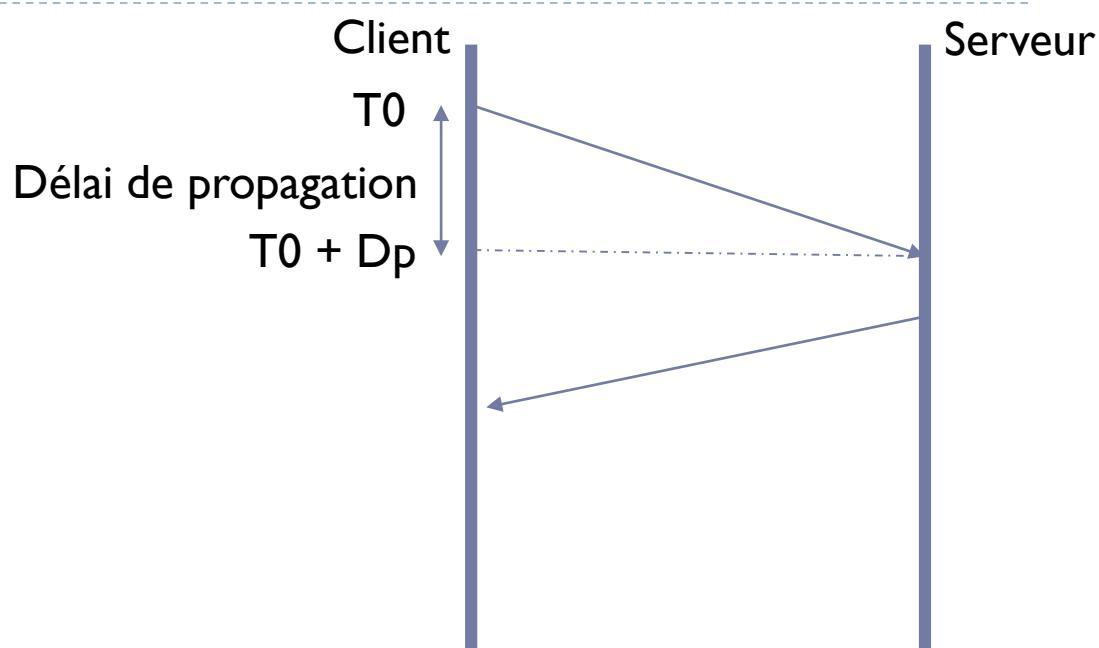
- ▶ Processus d'émission/réception d'un message dans un réseau numérique



Introduction aux télécommunications

Principes généraux

▶ Principe du chronogramme



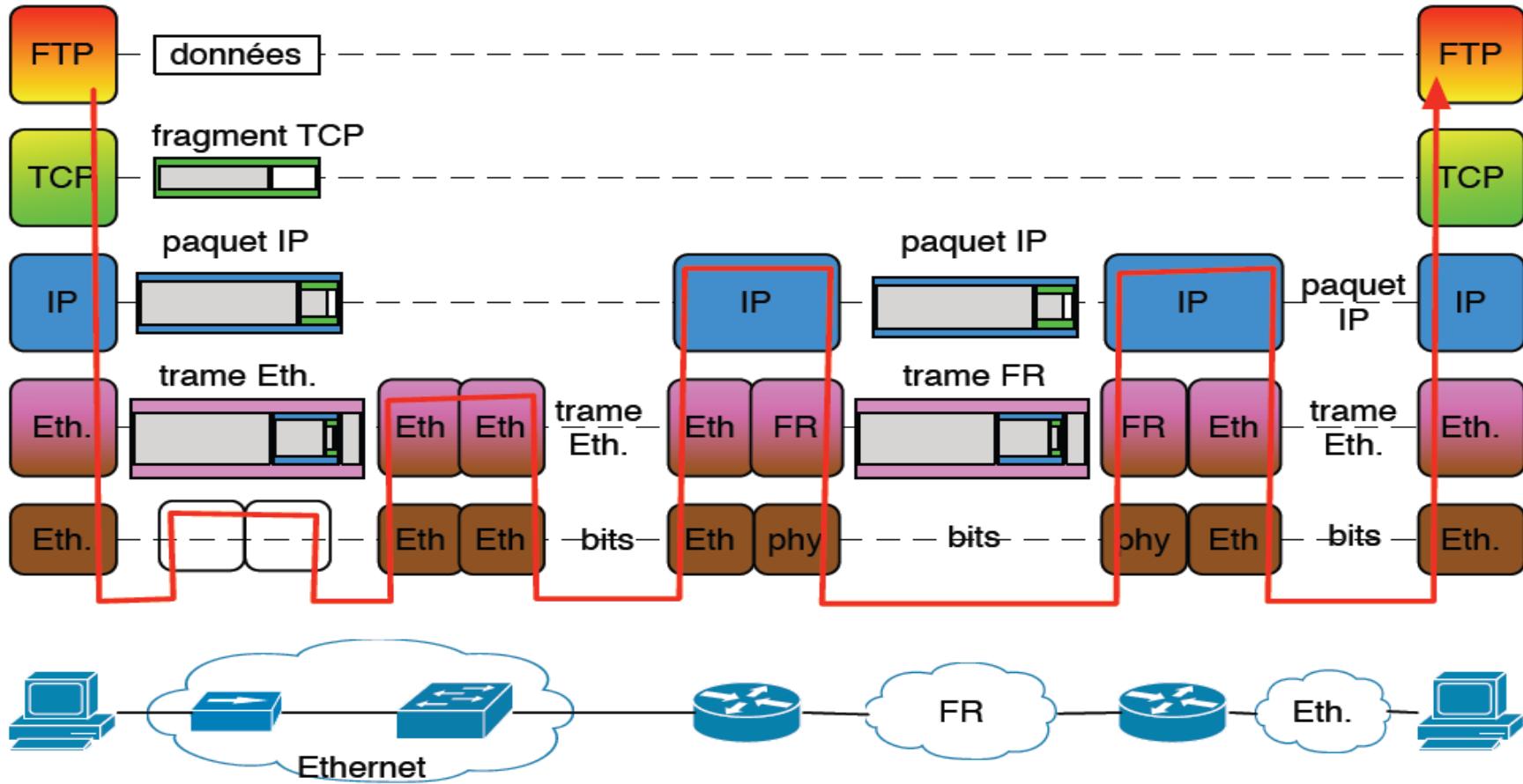
▶ Délai d'acheminement = délai de transmission + délai de propagation

- ▶ Délai de transmission (émission/réception) dépend de la taille du message à envoyer, du codage, de la modulation du Modem...
- ▶ Délai de propagation dépend du support : Fibre Optique, Satellite, Wifi....

Introduction aux télécommunications

Principes généraux

▶ Principe des couches protocolaires



Introduction aux télécommunications

Principes généraux

- ▶ Un Réseau, c'est un ensemble d'individus (ou de machines) capable d'échanger des informations et des services d'un point à un autre.
- ▶ Exemple :
 - ▶ Les réseaux téléphonique : transfert de la parole en **mode connecté**



- ▶ Les réseaux postaux : transfert de texte en **mode non connecté**



Les réseaux numériques

« Définition »

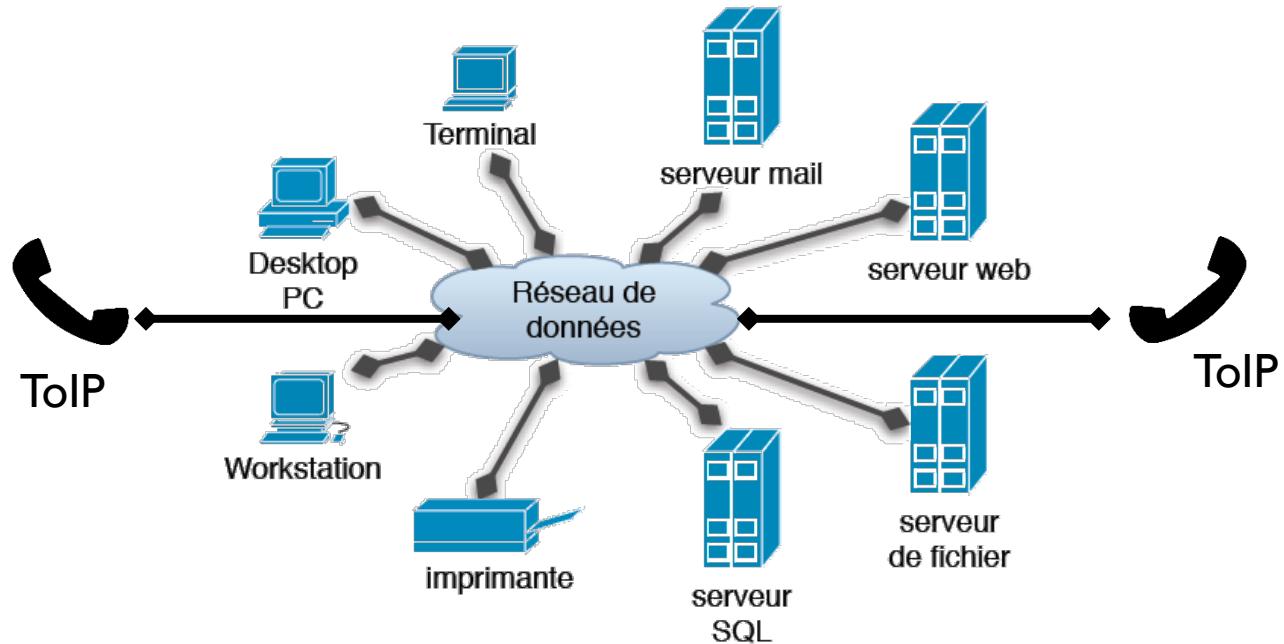
- ▶ Nous nous intéressons ici aux réseaux de données :
 - ▶ Les acteurs sont les machines (ordinateur, imprimante, fax, éléments réseaux ...).
 - ▶ Les informations échangées sont des signaux (numériques ou analogiques)
 - ▶ Les transmissions s'effectuent en mode connecté ou non.

- ▶ Un réseau de données nécessite :
 - ▶ Des supports/medium de transmission (fil de cuivre, fibre optique, air), permettant de transmettre les informations d'un acteur à l'autre.
 - ▶ Des machines aux extrémités de ces supports permettant la commutation/le routage,
 - ▶ Des protocoles de communications décrivant selon quelles règles et quelles stratégies les machines communiquent :
 - ▶ quel codage utiliser ?
 - ▶ que faire en cas de perte d'un paquet ?
 - ▶ à quelle vitesse communiquer ?
 - ▶ comment l'information arrive-t-elle (par bit ou par bloc) ?
 - ▶ comment atteindre un destinataire ?
 - ▶ quelles applications peuvent communiquer ?

Les réseaux numériques

« Définition »

- ▶ Echanger des informations variées
- ▶ Gérer le partage des ressources physiques
- ▶ Assurer la sécurité des informations



Les réseaux numériques

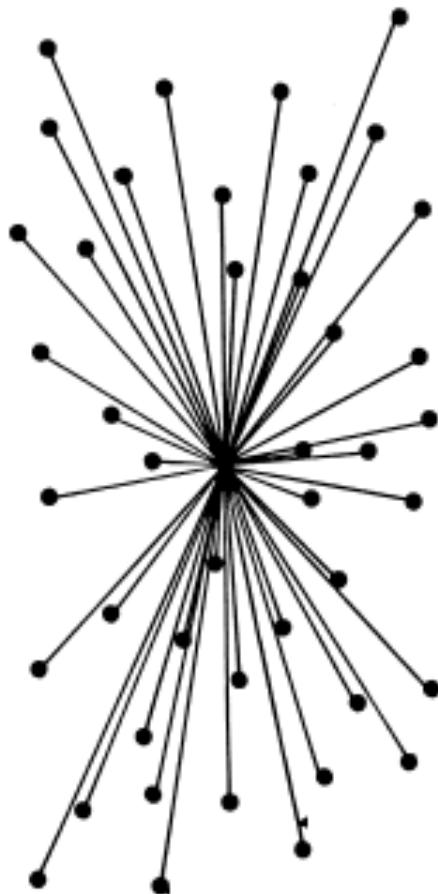
Classification

- ▶ Pas un réseau mais des réseaux !
- ▶ => fonction de la topologie
 - ▶ Réseaux informatiques
 - Locaux : LAN,
 - Étendus : MAN,WAN,
- ▶ => fonction des services attendus
 - Réseau téléphonique
 - Réseaux câblo-opérateurs (ex Numericable)
- ▶ => fonction des technologies
 - Réseaux mobiles
 - Réseau xDSL, FTTH, Ethernet,...
 - Réseau Radio/TV
- ▶ Et pourtant, de plus en plus, depuis la fin des années 90's
 - ▶ => convergence vers un seul réseau **IP**

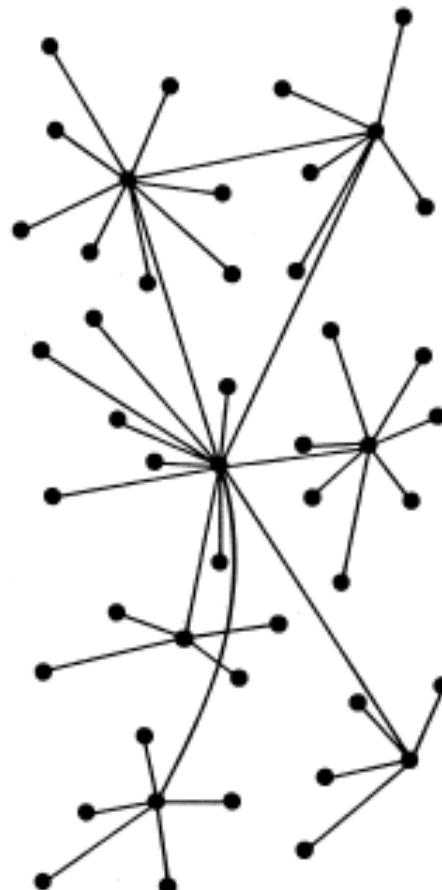
Le passage entre ces réseaux se fait en général par **des passerelles**

Les réseaux numériques

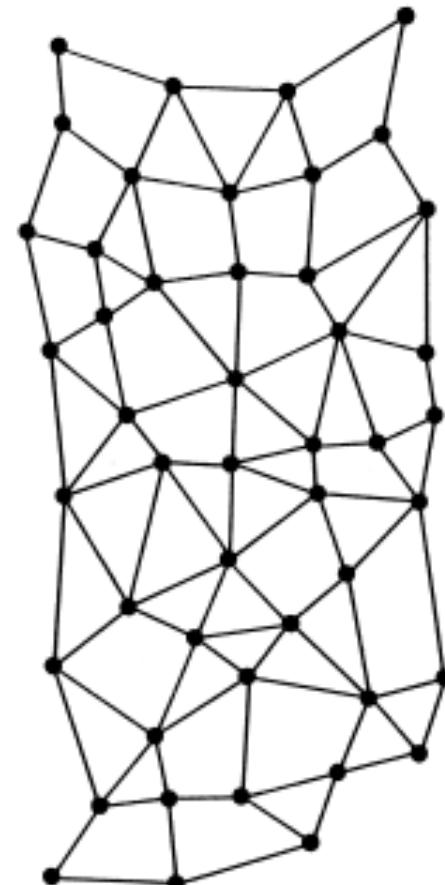
Classification – par type de topologies



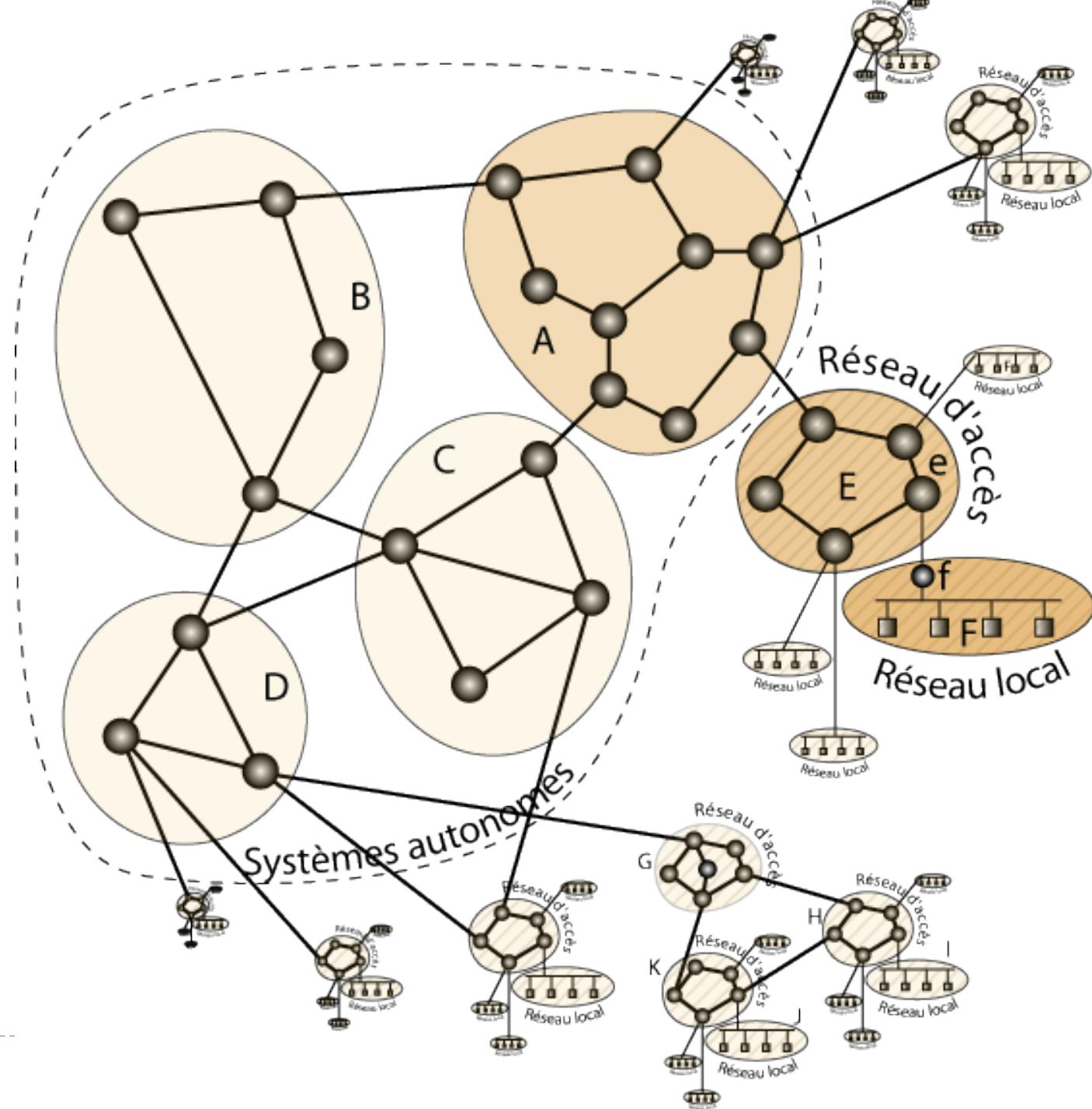
Centralisé



Décentralisé

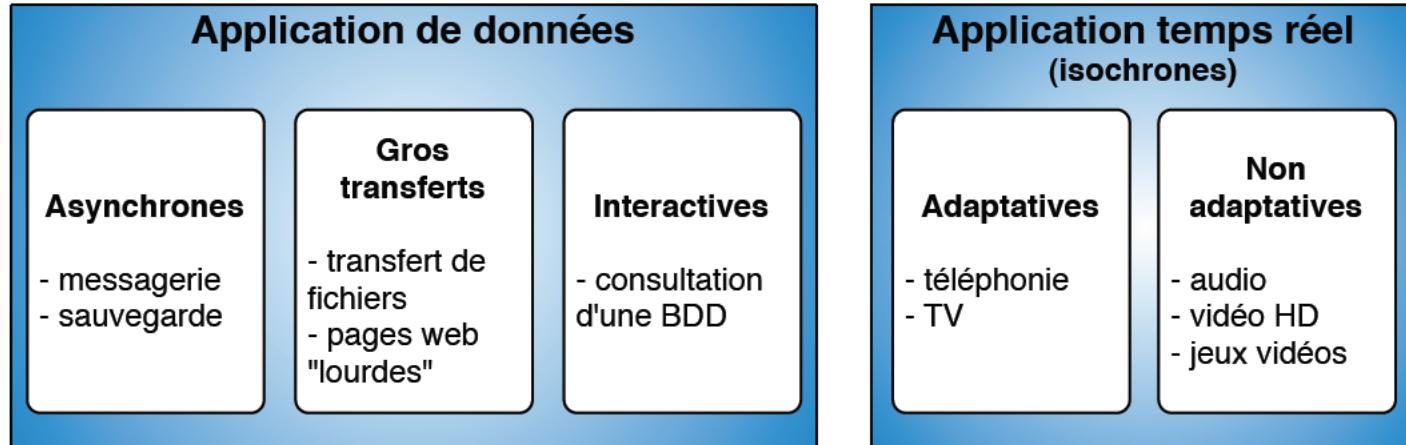


Distribué



Les réseaux numériques

Classification - Notions de qualité de service



niveau de qualité
de service requis

- ▶ Principaux paramètres de la **qualité de service** : délai, débit, disponibilité (avec/sans connexion, à la demande, etc), temps de réponse, fiabilité, etc.

Les réseaux numériques

Classification par technologies

▶ réseaux à diffusion

- ▶ Ex. Réseau de diffusion de la télévision



▶ réseaux point-a-point

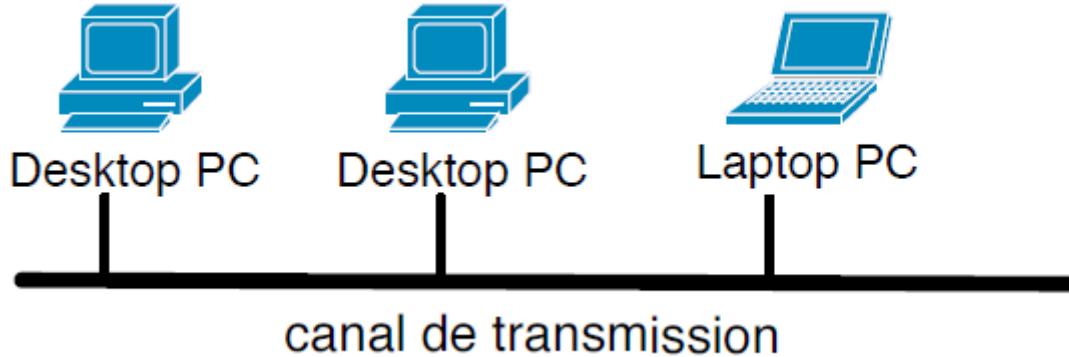
- ▶ Ex. Réseau de contrôle/commande

▶ Réseaux mobiles

- ▶ GSM
- ▶ GPRS
- ▶ 4G

Les réseaux numériques

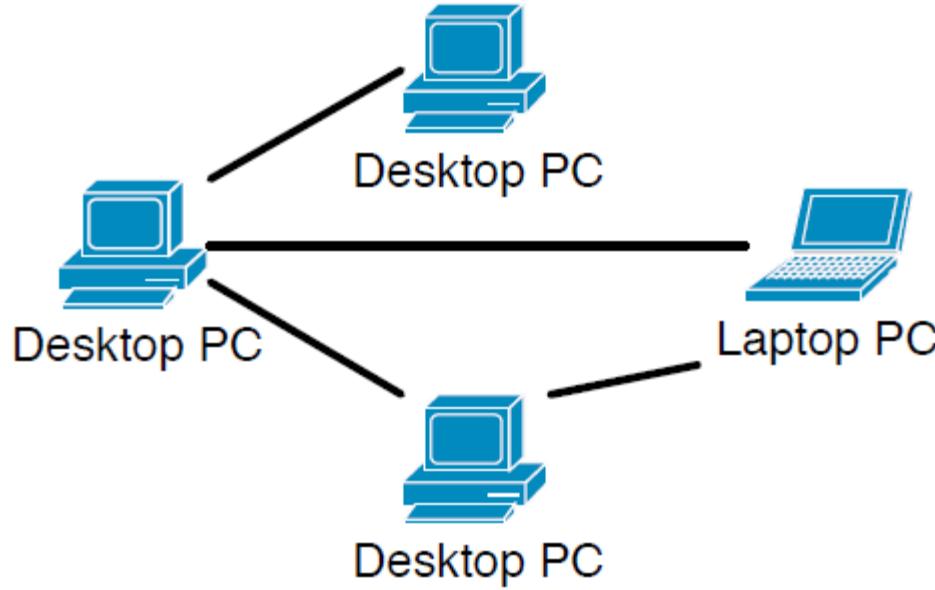
Réseaux à diffusion



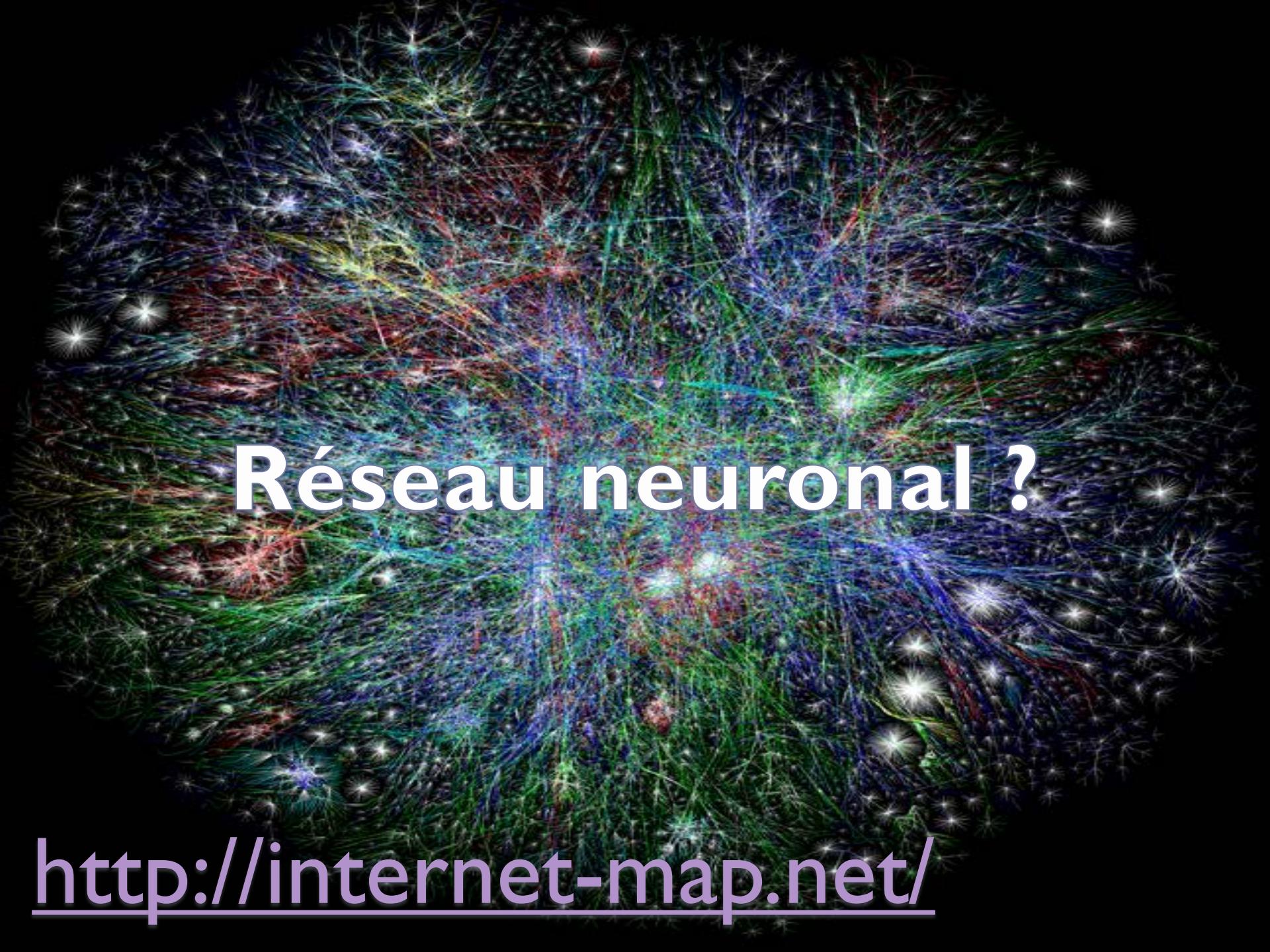
- ▶ Un seul canal de transmission partage par toutes les machines
- ▶ Un message envoyé est reçu par toutes les machines, mais seul le destinataire du message en tient compte
- ▶ Diffusion générale (broadcast) ou restreinte (multicast)
- ▶ Allocation du canal statique (multiplexage) ou dynamique (méthode d'attribution du canal centralisée ou décentralisée).
- ▶ Surtout utilisé dans les « vieux » LAN (normes Ethernet, IEEE 802.3)

Les réseaux numériques

Réseaux point-à-point



- ▶ Un canal de transmission entre deux machines
- ▶ Un message peut transiter via plusieurs machines pour atteindre le destinataire : besoin d'un système d'adressage et de routage



Réseau neuronal ?

<http://internet-map.net/>

Les réseaux numériques

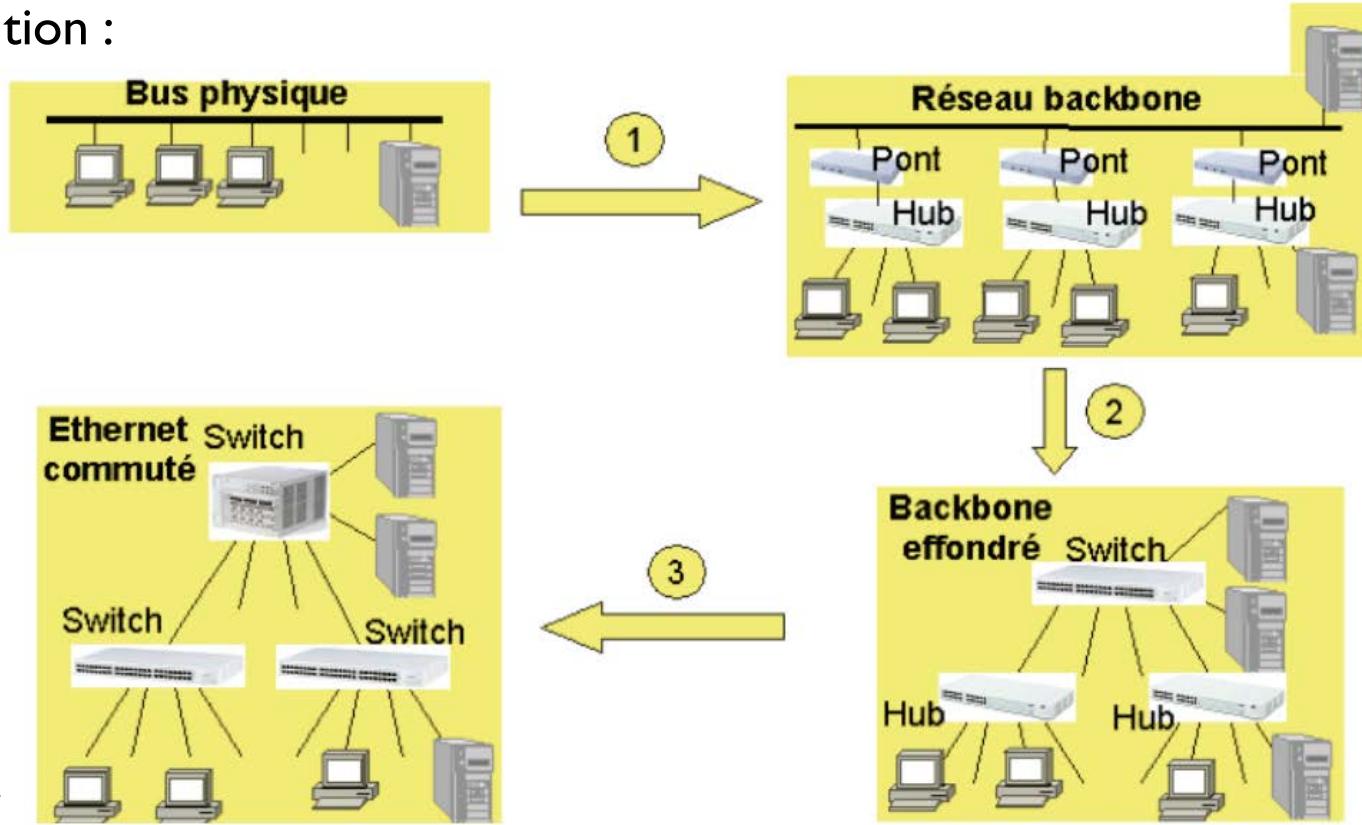
Réseaux LAN

- ▶ Taille restreinte, quelques kilomètres au maximum.
- ▶ Médias de transmission :
 - ▶ Cœur de réseau : optique.
 - ▶ Serveurs : optique, cuivre.
 - ▶ Desserte utilisateurs : cuivre, ondes.
- ▶ Nombre restreint d'ordinateurs.
- ▶ Débit variant de quelques Mbit/s jusqu'à plusieurs Gbit/s.
- ▶ Types de LAN
 - ▶ aujourd'hui : **Ethernet commuté** uniquement.
 - ▶ Hier : Ethernet non commuté, anneaux.

Les réseaux numériques

Réseaux LAN - Ethernet

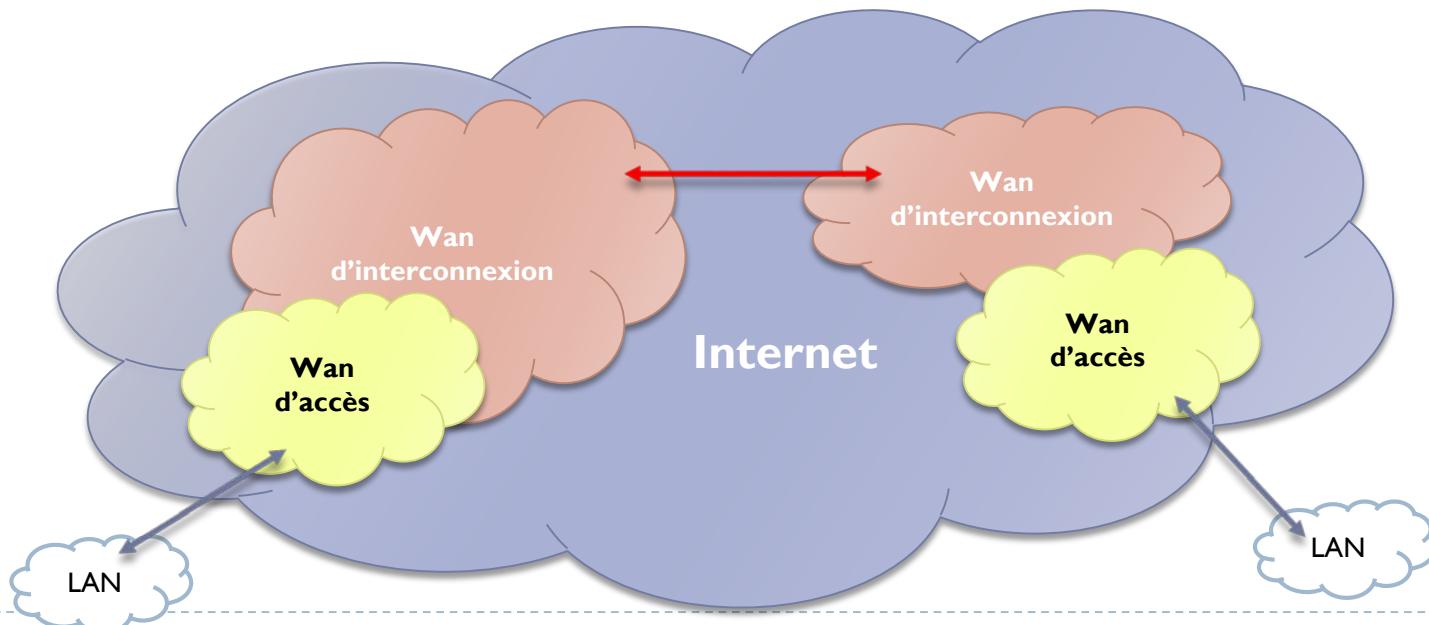
- ▶ Famille des normes IEEE 802.3
- ▶ Support en paires torsadées et fibres optiques
- ▶ Débit de 10 Mbit/s à 10 Gbit/s
- ▶ Evolution :



Les réseaux numériques

Réseaux WAN

- ▶ Une région, un pays ou le monde (Internet)
- ▶ Peut être composé de différents types de medias de transmission
- ▶ Constitué de différents réseaux interconnectés.
- ▶ Distinction entre les **WAN d'interconnexion (Cœur de réseau)** des **MAN/WAN d'accès (réseau client)**



Les réseaux numériques

Réseaux MAN/WAN

▶ Technologies de transmission

▶ MAN d'accès

- ▶ RTC, RNIS – 56/128 Kbit/s
- ▶ xDSL, Câble, FTTx – 1Mbit/s à 1Gbit/s

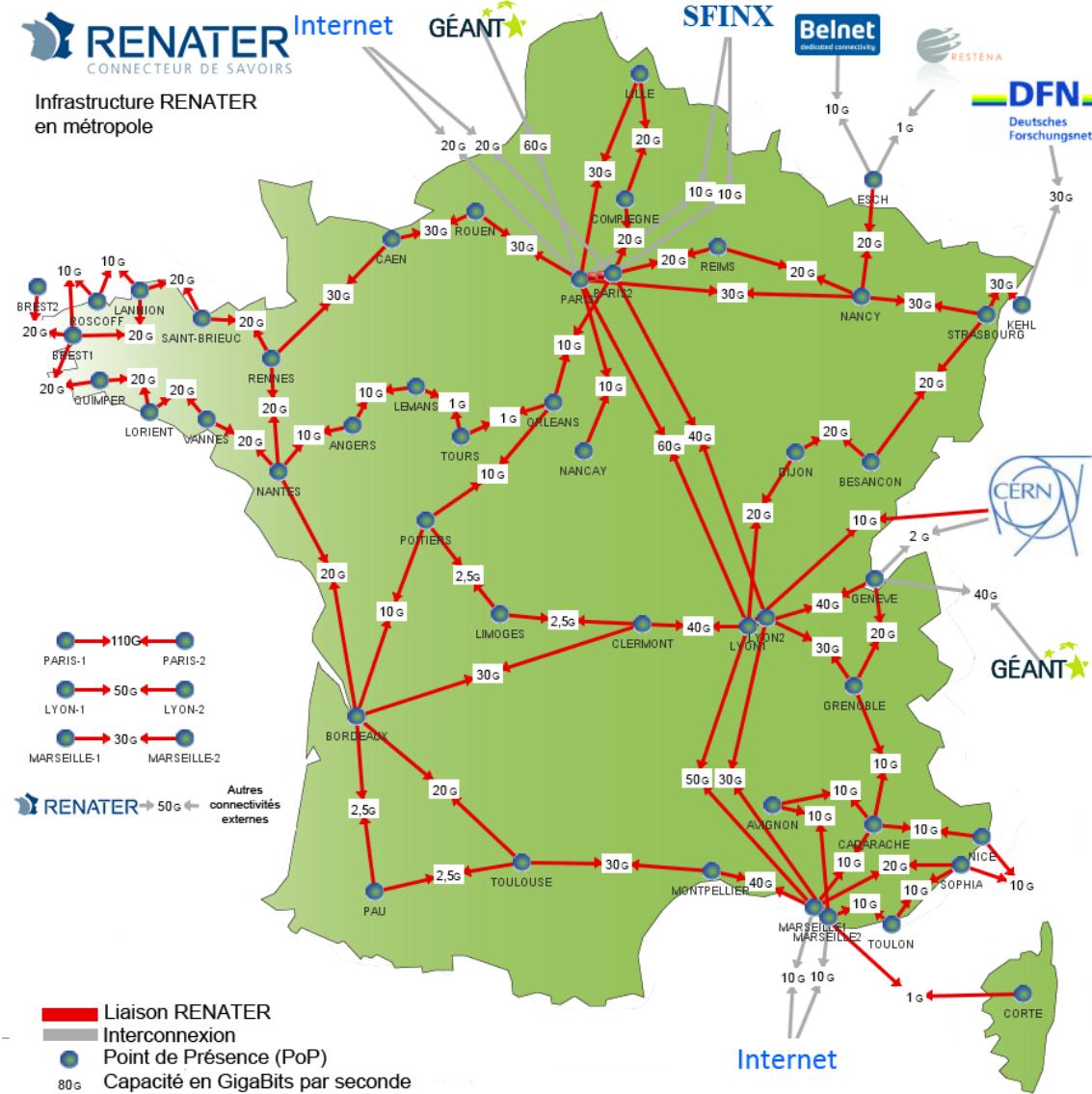
▶ WAN

- ▶ SDH, OTN <= 100Gbits
- ▶ DWDM > 100Gbits
- ▶ Carrier Grade Ethernet
- ▶ Réseau mobiles :
 - GPRS(2G) – 15Kbit/s
 - UMTS (3G) – 40Mbit/s
 - LTE (4G) – 100Mbit/s

Les réseaux numériques

Réseaux WAN d'interconnexion

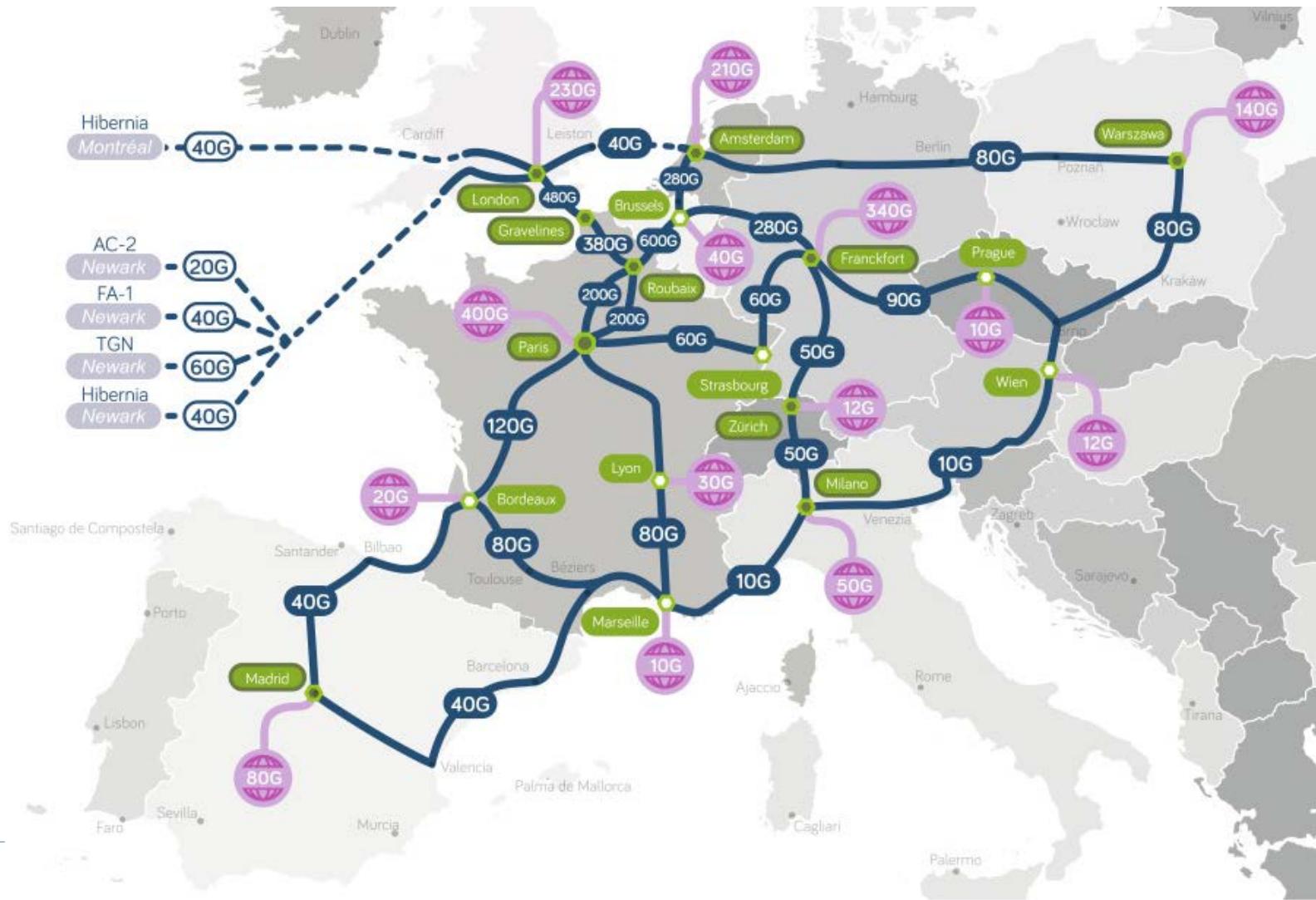
Exemple RENATER



Les réseaux numériques

Réseaux WAN d'interconnexion

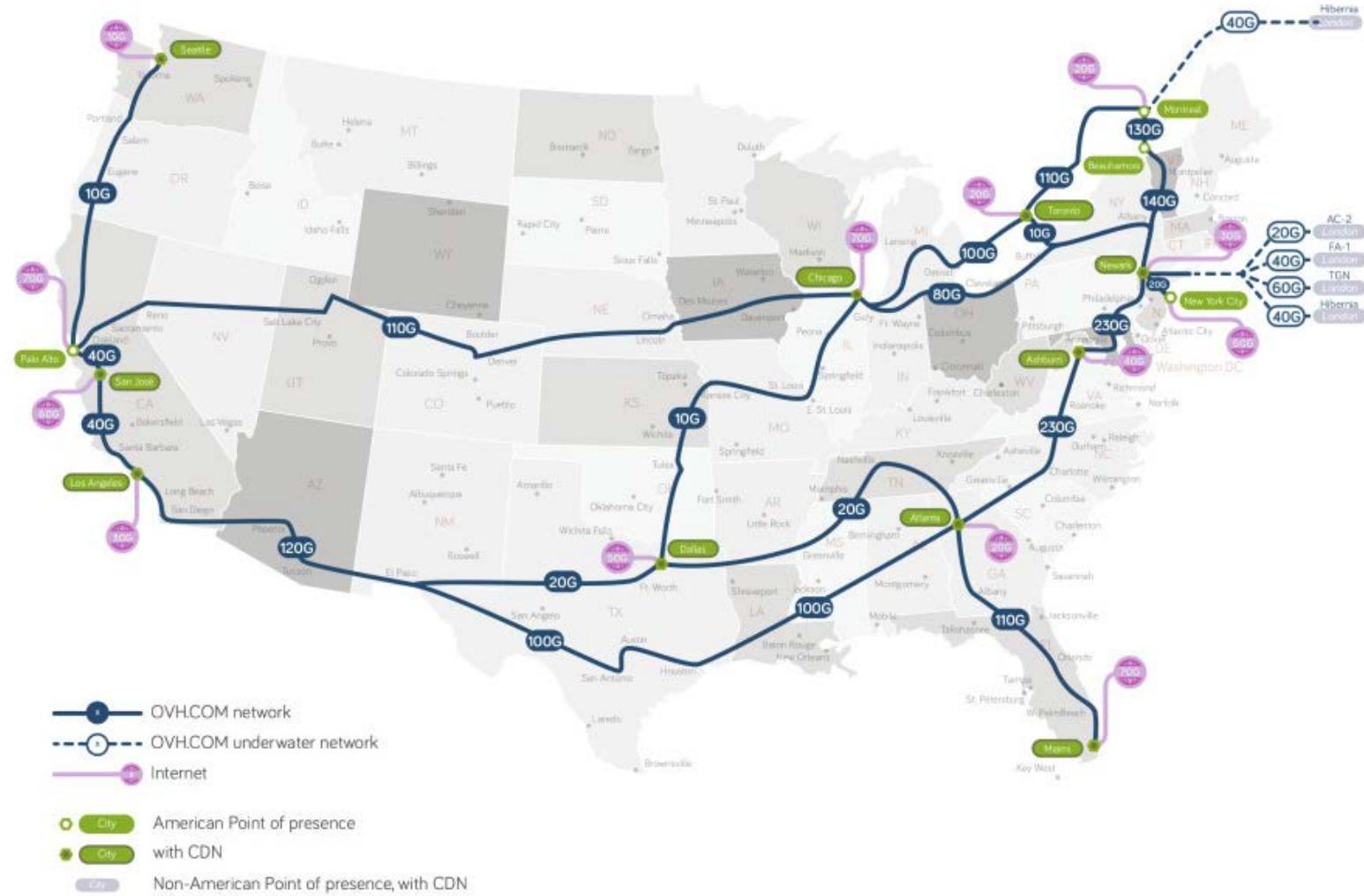
Exemple OVH <http://www.ovh.com/fr/apropos/reseau.xml>



Les réseaux numériques

Réseaux WAN d'interconnexion

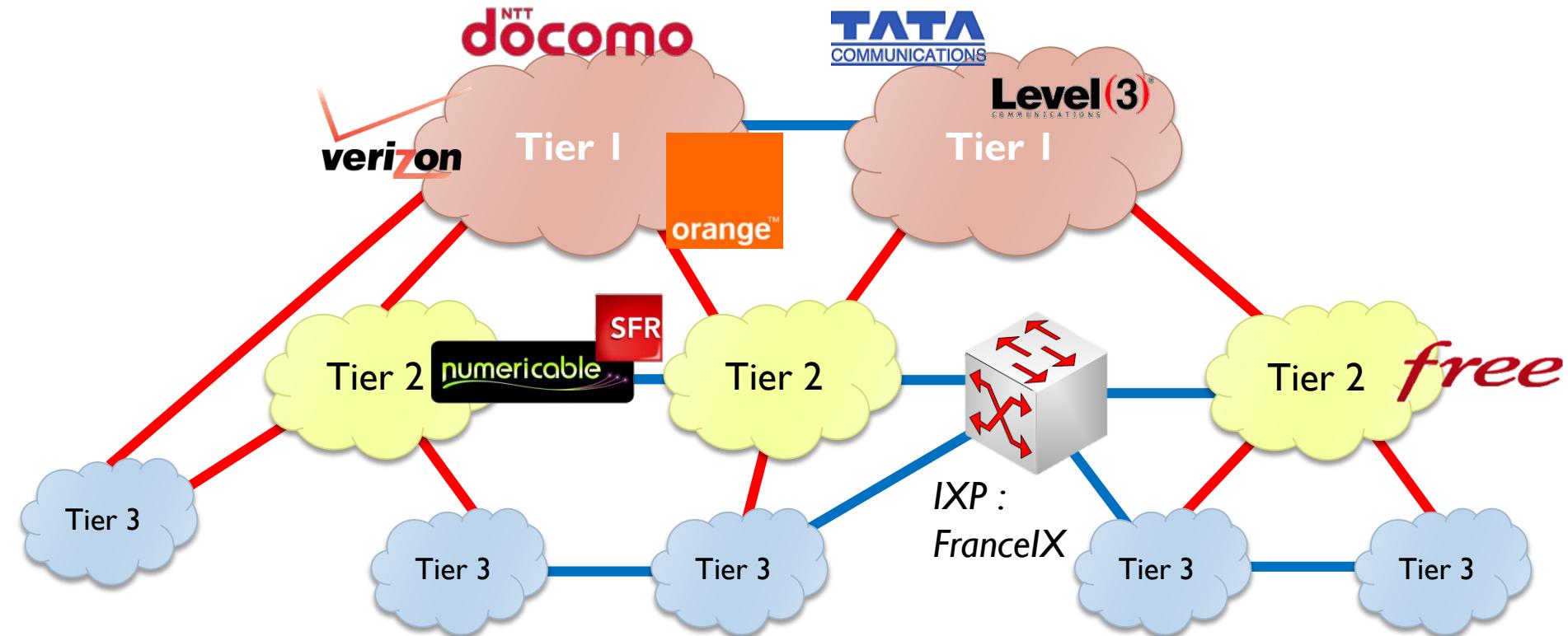
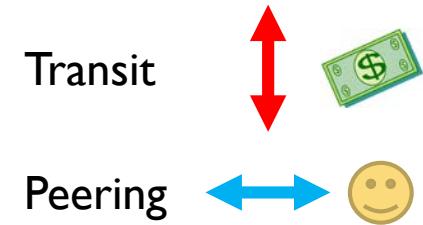
Exemple OVH <http://www.ovh.com/fr/apropos/reseau.xml>



Les réseaux numériques

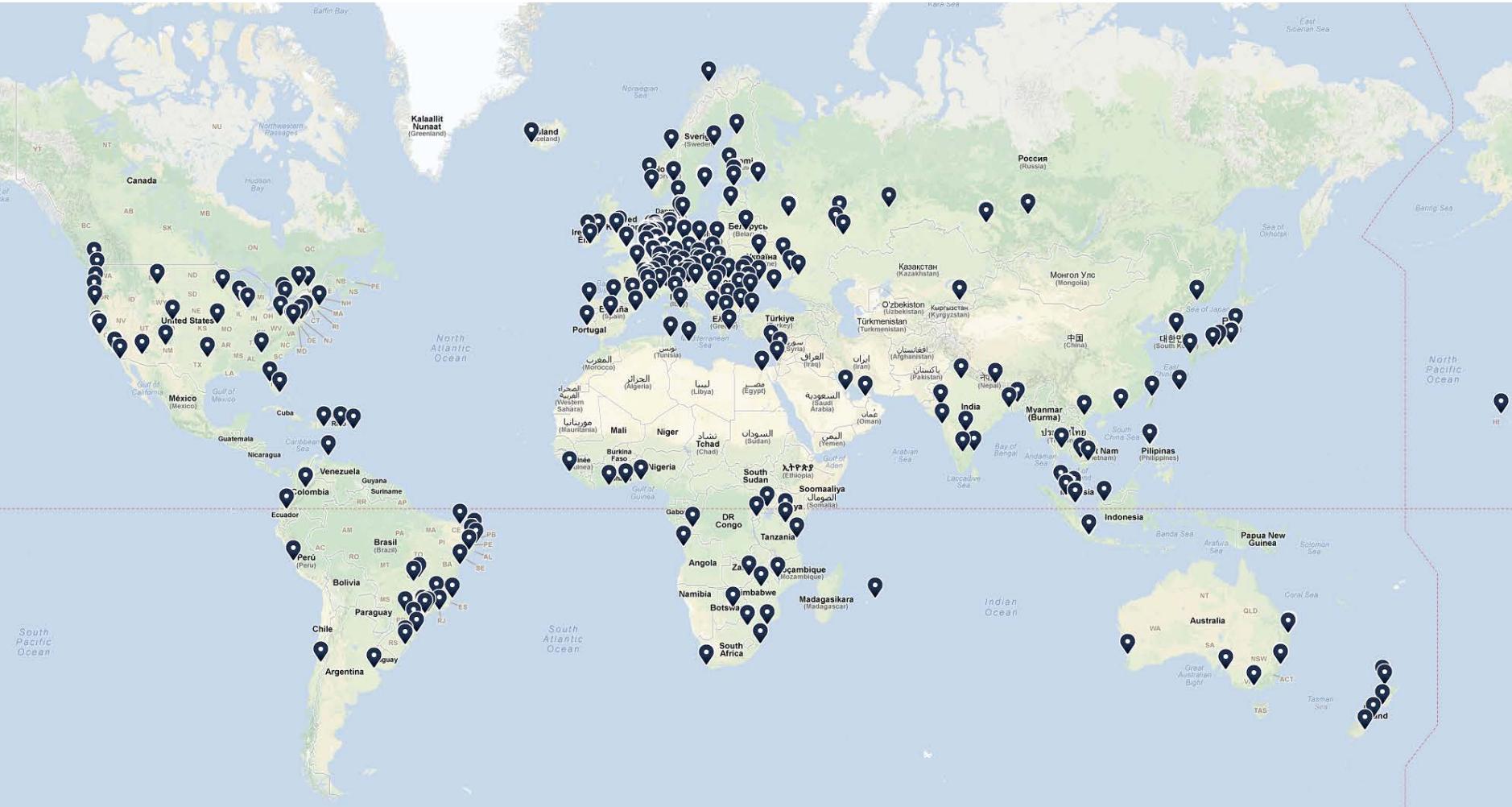
Réseaux WAN d'interconnexion

- Relations entre les opérateurs Tier 1/2/3



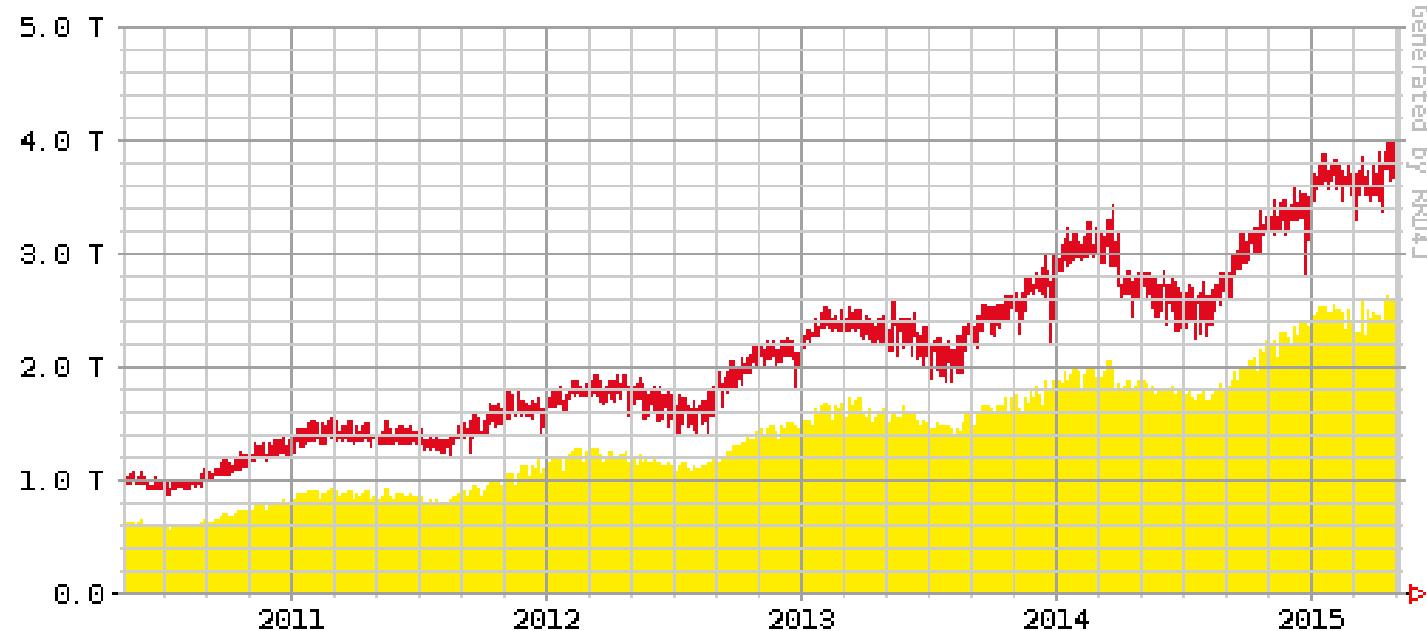
Les réseaux numériques

Points d'échange Internet : eXchange



Les réseaux numériques

Points d'échange Internet : eXchange – DE-CIX



Current 2588.9 G

Averaged 1327.5 G

Graph Peak 4005.4 G

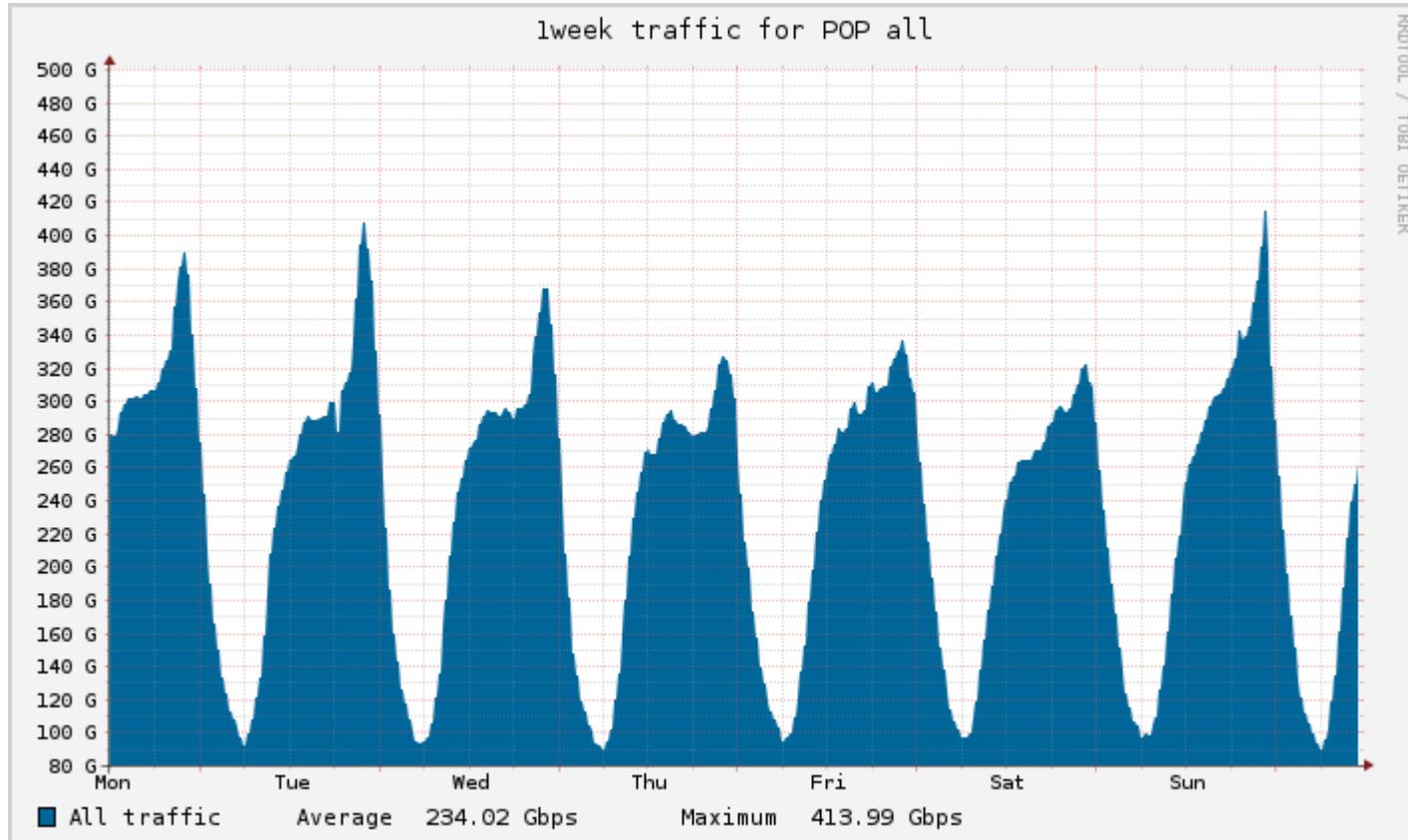
DE-CIX All-Time Peak 4005.44 G - reached at 2015-04-28T20:50+02:00

Created at 2015-05-04 09:12 UTC

Copyright 2015 DE-CIX Management GmbH

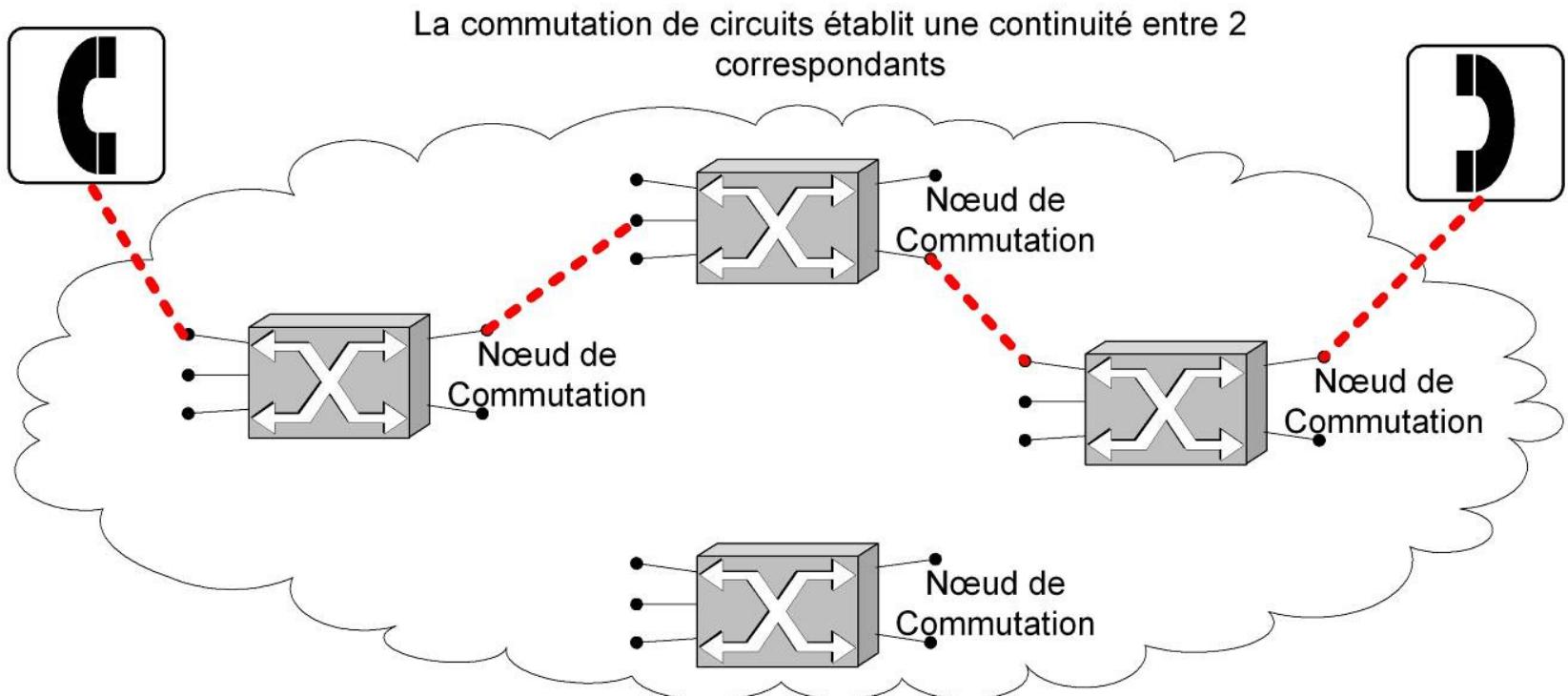
Les réseaux numériques

Points d'échange Internet : eXchange – FranceIX



Mécanismes de transfert

Commutation de circuits



Mécanismes de transfert

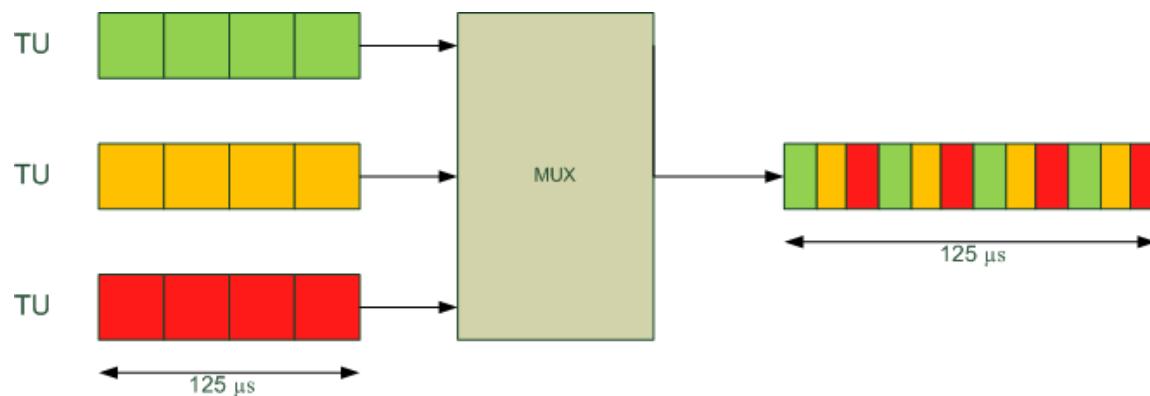
Commutation de circuits



Mécanismes de transfert

Commutation de circuits

- ▶ Réservation d'un circuit physique
 - ▶ Simple.
 - ▶ Ressources garanties.
 - ▶ Sous optimisation lors des 'silences' de transmission.
 - ▶ Cher
- ▶ Multiplexage temporel



Mécanismes de transfert

Commutation de paquets

- ▶ Pas de réservation de ressources
 - ▶ Optimisation générale de l'infrastructure
 - ▶ Mode « Best-effort ».
 - ▶ Mécanismes de Qualité de Service peuvent être nécessaires.

- ▶ Mode non connecté



Routage

- ▶ Chaque paquet est routé indépendamment dans le réseau
 - ▶ Chaque paquet possède les informations de routage
 - ▶ Paquets à réordonner à l'arrivée.

- ▶ Mode connecté : Circuits virtuels



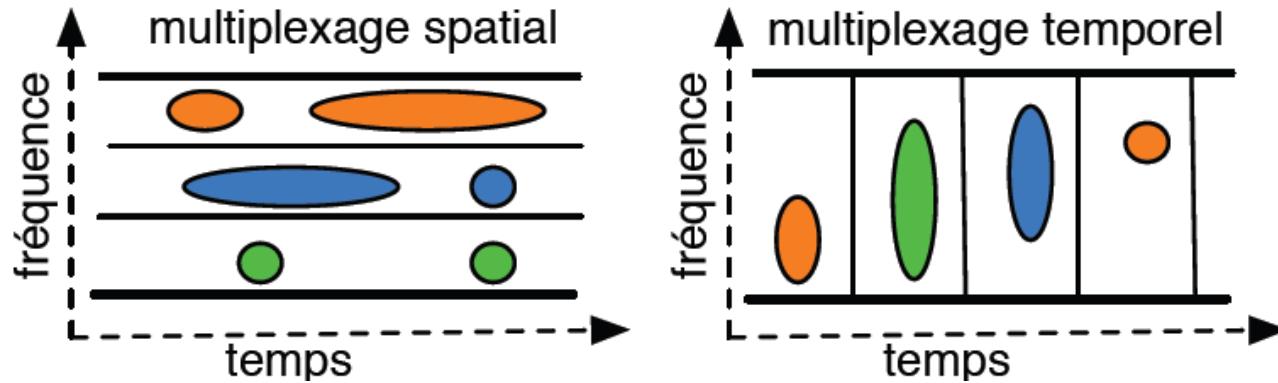
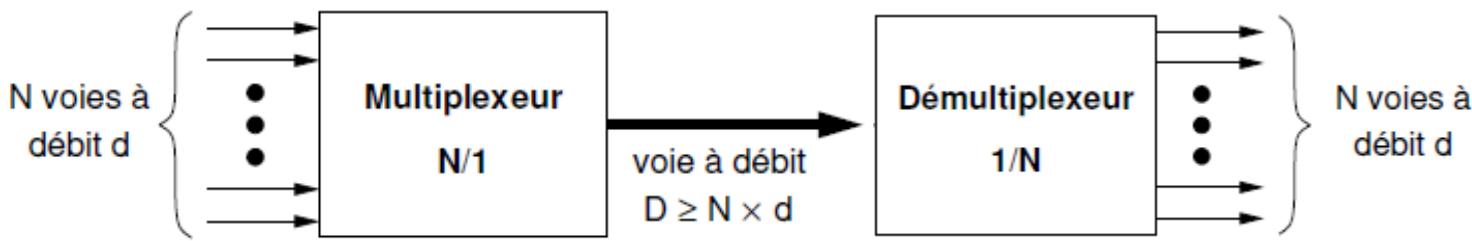
Commutation

- ▶ Séquence préalable de connexion.
 - ▶ Les paquets contiennent l'information de circuit virtuel.

Mécanismes de transfert

Multiplexage

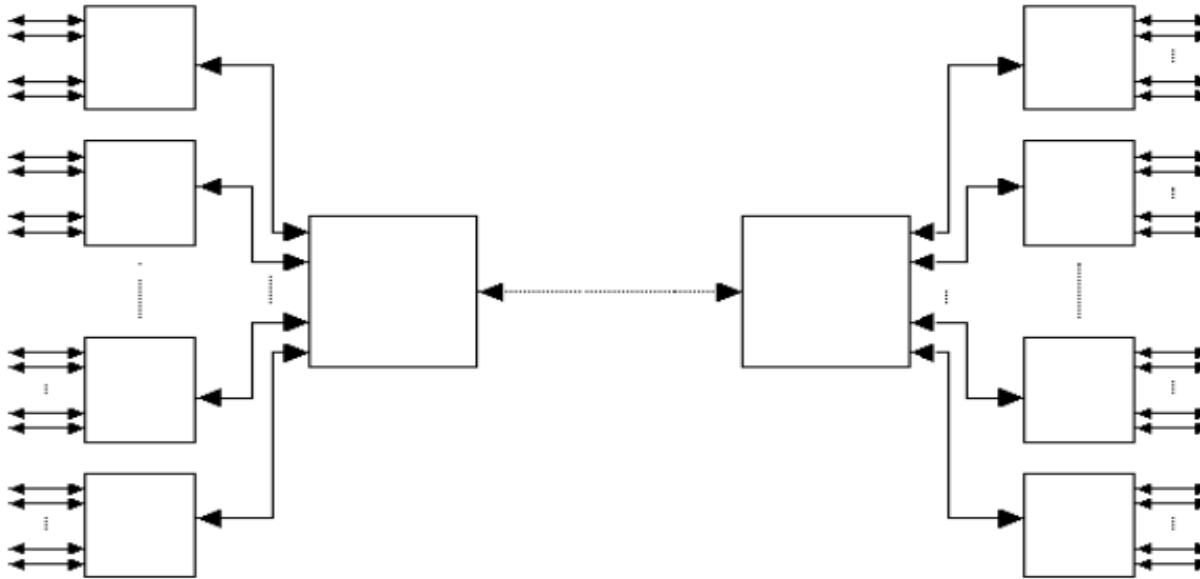
- ▶ Mélanger l'information provenant de plusieurs entrées sur une seule ligne de sortie.
- ▶ **Multiplexeur et Démultiplexeurs**



Mécanismes de transfert

Multiplexage

- ▶ Le multiplexage/démultiplexage est souvent **hiérarchique**.



- ▶ L'extraction d'un canal multiplexé peut être complexe.
- ▶ Le multiplexage/demultiplexage intervient aussi dans les circuits virtuels. Ex. :TCP

Mécanismes de transfert

Adressage

- ▶ Adresse : identifiant de la machine sur le réseau.
 - ▶ Communication entre une adresse source et une adresse destination
 - ▶ Permet au réseau de choisir le meilleur chemin
-
- ▶ Adressage hiérarchique
 - ▶ Adresse postale
 - Pays
 - Ville + code postal
 - Rue
 - Bâtiment
 - Boite aux lettres (nom de la personne)
 - ▶ Le réseau n'a pas besoin de connaître toutes les adresses, seul ses adresses et les pointeurs 'Pays' sont nécessaires.
 - ▶ Adressage linéaire/plat. Ex. Adresses MAC
 - ▶ Le réseau doit savoir joindre toutes les adresses.

Les Réseaux

ENSAM

Karim Boudjemaa

Études et Projets – RENATER

Karim.boudjemaa@renater.fr

Cours n°2

Plan du cours 2

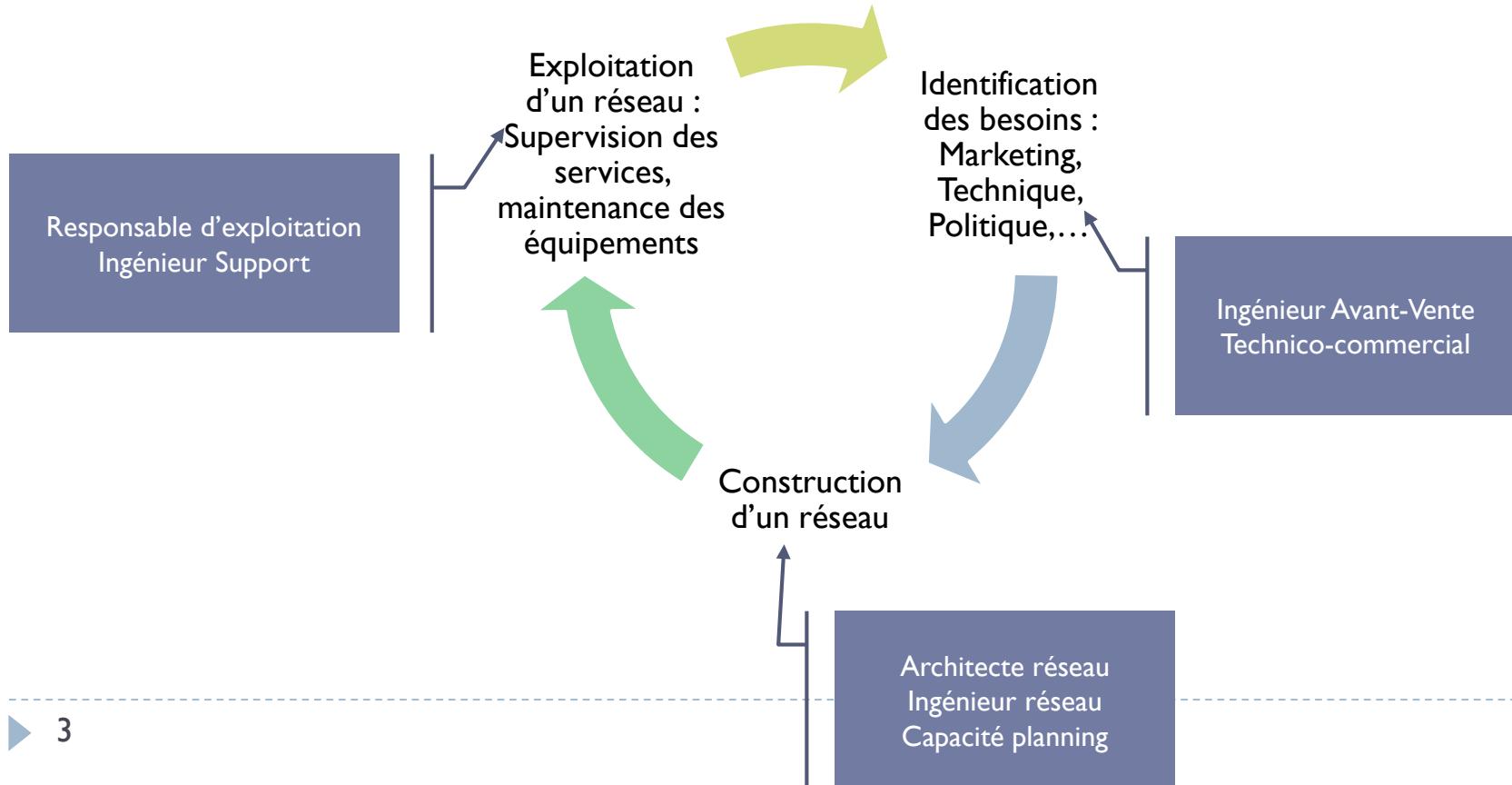
I. Retour sur le Cours I

2. Modèle en couches

- ▶ Généralités
- ▶ Couche 1 – Physique
 - ▶ Objectifs
 - ▶ Notion de signaux
 - ▶ Transmission bande de base ou large bande
 - ▶ Bande passante d'un support
 - ▶ Modulation
 - ▶ Débit
 - ▶ Différents types de transmission
 - ▶ Facteurs limitants
 - ▶ Exemples de supports de transmission
- ▶ Couche 2 – Liaison
 - ▶ Objectifs
 - ▶ Spécification des trames – exemples
 - ▶ Délimitations
 - ▶ Détection et correction d'erreurs
 - ▶ Gestion des échanges – flux
 - ▶ Focus sur Ethernet
 - Ethernet partagé
 - Ethernet commuté
 - Notion de Vlans
 - ▶ Notion d'architecture matériels

Retour sur le Cours 1

- ▶ Qu'est ce qu'un opérateur ?
- ▶ <https://www.youtube.com/watch?v=z0KfIEg9xng>



Modèles en couches

Généralités

- ▶ Modèle OSI (1984)
 - ▶ Le modèle OSI (de l'anglais Open Systems Interconnection) est un standard de communication, en réseau, de tous les systèmes informatiques. C'est un modèle de communications entre ordinateurs proposé par l'ISO (International Standard Organisation) qui décrit les fonctionnalités nécessaires à la communication et l'organisation de ces fonctions. (source wikipedia)
 - ▶ 7 couches
 - ▶ Rigoureux, utilisé pour certaines applications critiques, ou pour ses fonctionnalités permettant de garantir une qualité de service.
- ▶ Modèle TCP/IP (1976)
 - ▶ Approche modulaire
 - ▶ 4 ou 5 couches

Modèle OSI

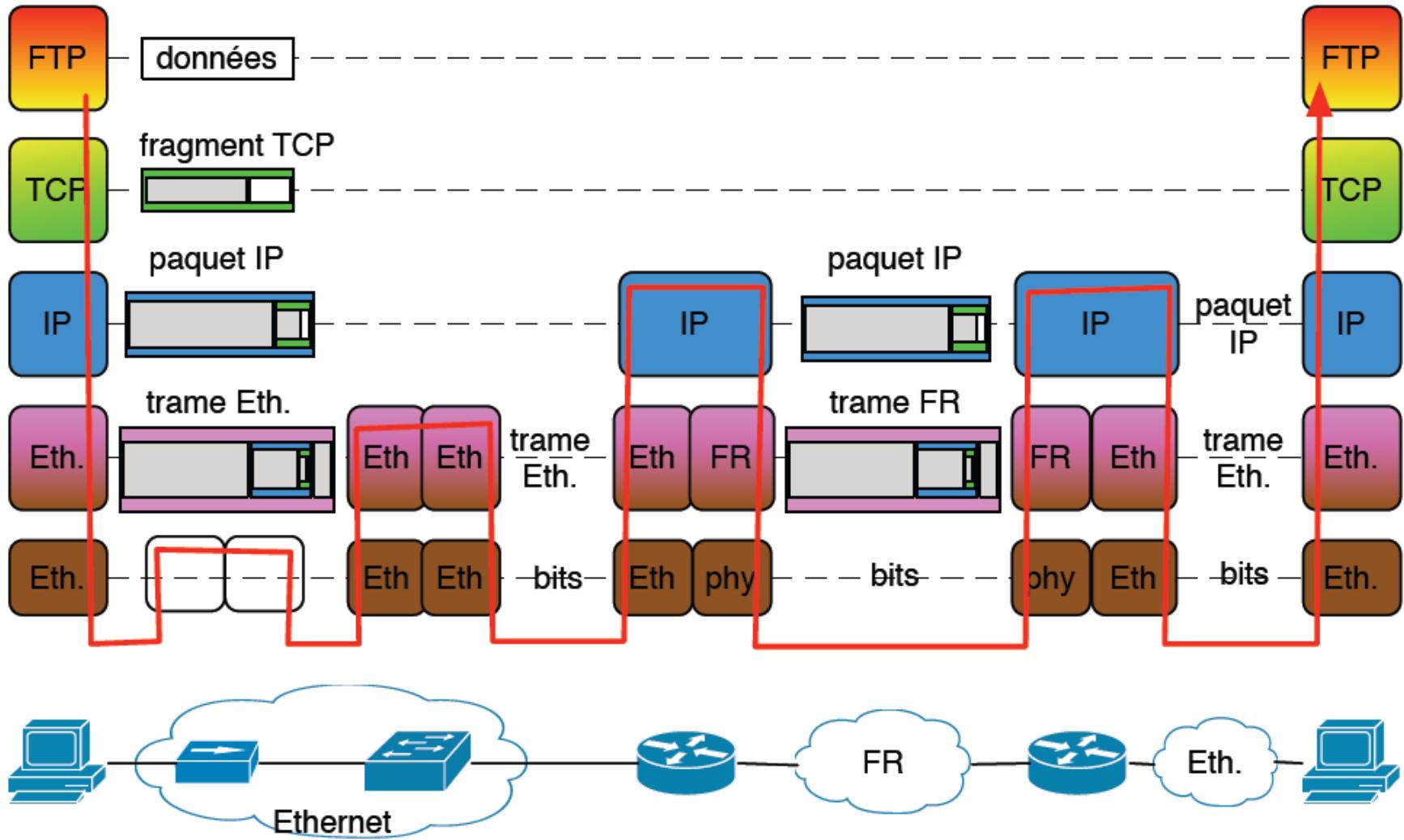
	Type de données	Couche	Fonction	Exemple de protocole ou de mécanisme
Couches hautes « Application »	Données	7. Application	Point d'accès aux services réseaux	HTTP, FTP, SMTP, SSH, SIP ...
		6. Présentation	Gère le chiffrement et le déchiffrement des données, convertit les données machine en données exploitables par n'importe quelle autre machine	SMB, ASCII, ASN.I, AFP,...
		5. Session	Communication Interhost, gère les sessions entre les différentes applications	AppleTalk NetBios, ...
	Segment	4. Transport	Connexion bout à bout, connectabilité et contrôle de flux. Intervient la notion de port.	TCP, UDP,
		3. Réseau	Détermine le parcours des données et l'adressage logique.	IPv4, IPv6, NetBEUI, IPX, OSPF, ISIS, BGP
		2. Liaison	Adressage physique	Ethernet, X25, FrameRelay, ATM, MPLS (2,5)
Couches Basses « Matériielles »	Bit	1. Physique	Transmission des signaux sous forme binaire	Codage NRZ, Manchester, 100BaseT, ADSL, SDH, DWDM

Modèle TCP/IP

	Type de données	Couche	Fonction	Exemple de protocole ou de mécanisme
Couches hautes « Application »	Données	5-7. Application	Non défini par TCP/IP	
	Segment	4. Transport	Connexion bout à bout, connectabilité et contrôle de flux. Intervient la notion de port.	TCP, UDP, ICMP
Couches basses « Matérielles »	Paquet	3. Réseau	Détermine le parcours des données et l'adressage logique.	IPv4, IPv6
	Trame	2. Liaison	Adressage physique	Ethernet, X25, FrameRelay, ATM, MPLS (2,5)
	Bit	1. Physique	Transmission des signaux sous forme binaire	Codage NRZ, Manchester, 100BaseT, ADSL, SDH, DWDM

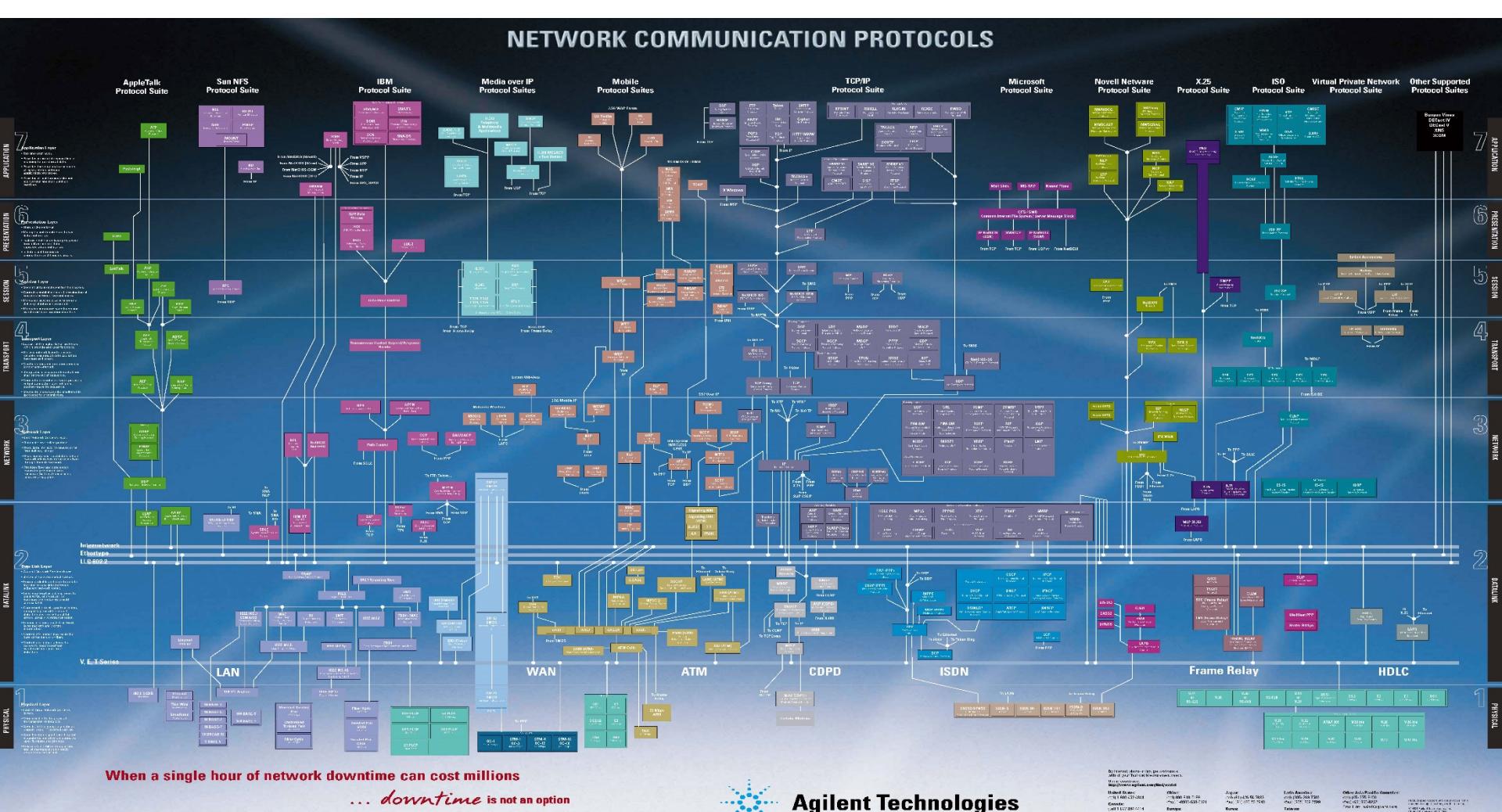
Modèles en couches

Généralités



Modèles en couches

Généralités



When a single hour of network downtime can cost millions

... downtime is not an option

www.agilent.com/comms/opennetworks



Agilent Technologies

**Deutschlands größte
Mitspieler und Kooperationspartner.**

Couche 1 – Physique

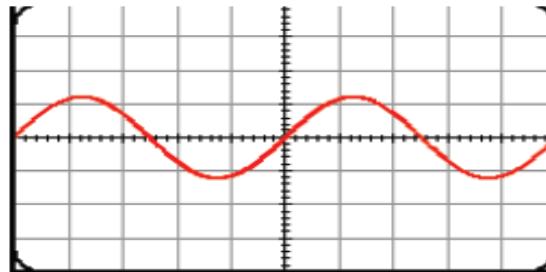
Objectifs

- ▶ Cette couche permet :
 - ▶ Le raccordement de deux points d'un réseau indépendamment des contraintes liées au support de transmission : atténuation, bruit,...
 - ▶ L'adaptation du flux binaire selon le support physique
 - ▶ Fournit un premier niveau de qualité.
- ▶ De multiples types de transmission existent :
 - ▶ selon le besoin en modulation :
 - ▶ Bande de base
 - Signal pas ou peu modulé
 - ▶ Large bande
 - Signal modulé
 - ▶ selon l'exploitation de la liaison :
 - ▶ Synchrone/asynchrone
 - ▶ Symétrique/asymétrique
 - ▶ Simplex/half/full duplex
- ▶ L'entité de cette couche : **le bit**
- ▶ Matériels concernés : Modem, Hub, amplificateurs/répéteurs, câbles, connecteurs,...

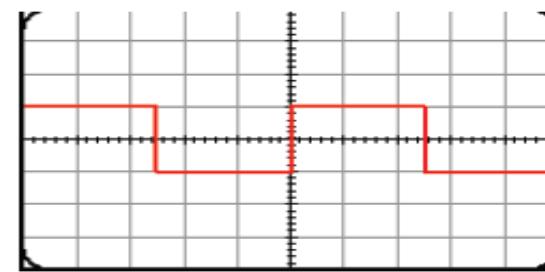
Couche 1 – Physique

Notions de signaux

- ▶ Définition : un **signal** est une information qui transite à travers un canal de communication. Il permet de transmettre une donnée brute entre deux machines de manière adaptée au support de communication.
 - ▶ Un signal est **analogique** lorsque sa forme est sinusoïdale et son amplitude évolue de manière continue dans le temps,
 - ▶ Un signal est **numérique** lorsque son amplitude prend des valeurs fixes à des intervalles de temps



signal analogique



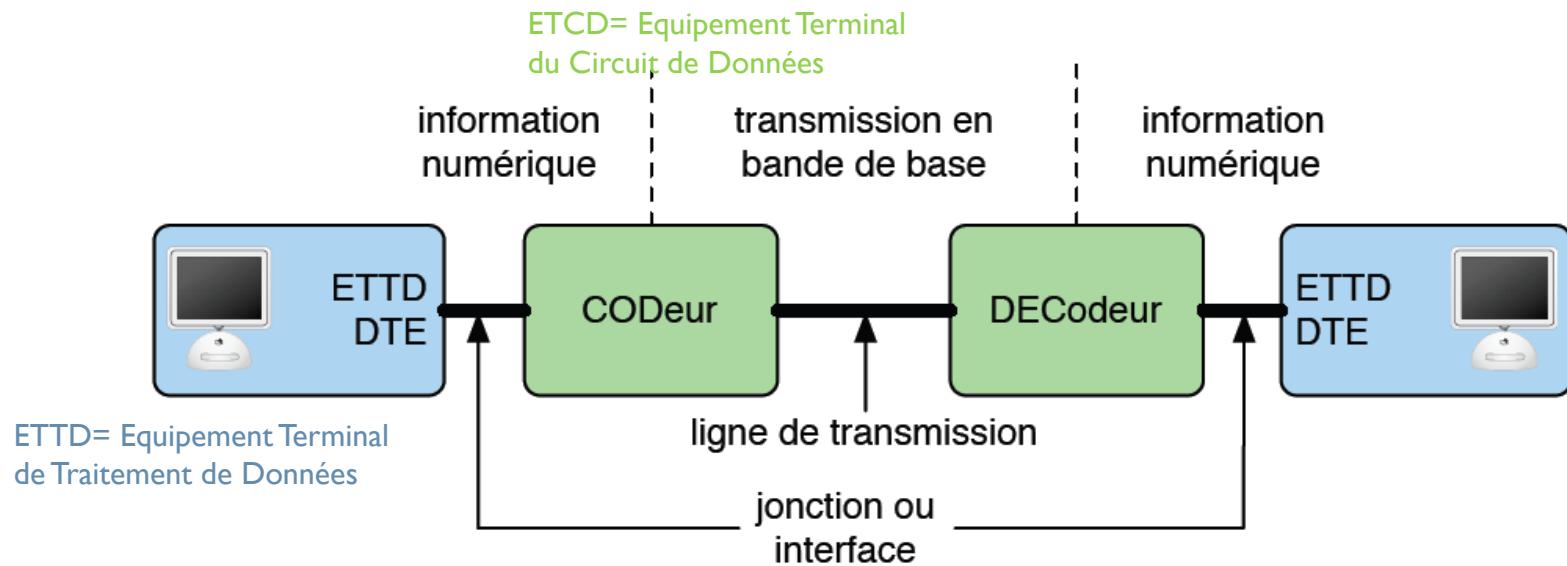
signal numérique

- ▶ Interprétation d'un signal : effectuée selon la tension électrique, l'impulsion lumineuse, l'onde électromagnétique.

Couche 1 – Physique

Transmission bande de base

- ▶ La transmission en **bande de base** consiste à modifier légèrement (on dit **transcoder**) le signal émis par l'ETTD. Ce mode de transmission est peu adapté aux longues distances.

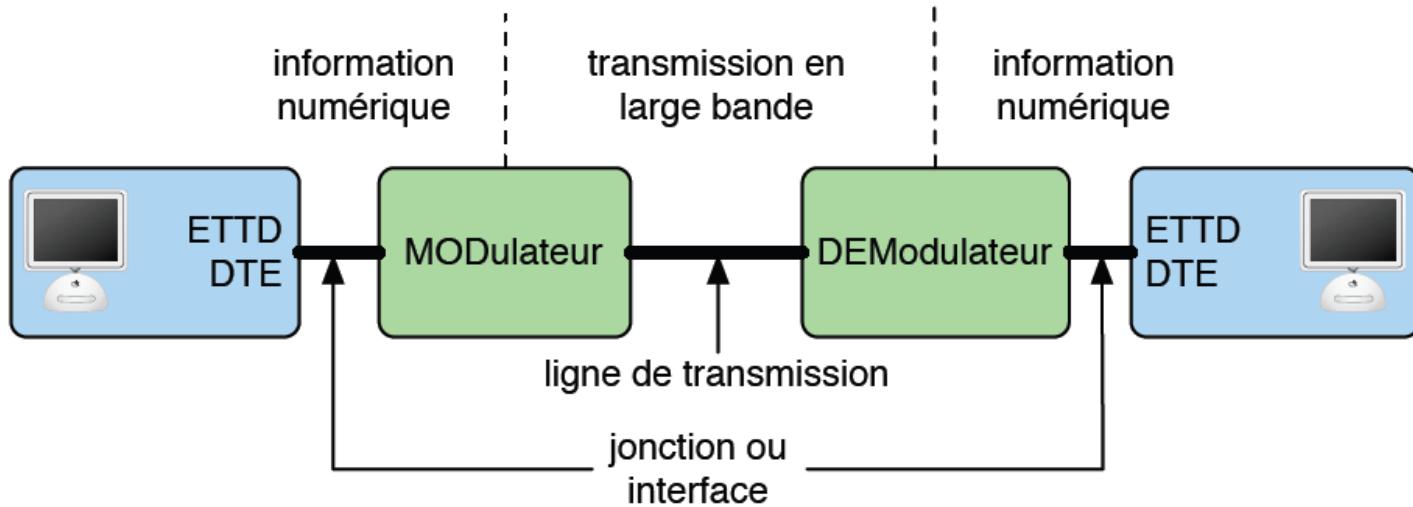


- ▶ L'ETCD est un **codeur/décodeur**. Il a essentiellement pour objet de coder le signal pour supprimer les composantes continues et de maintenir la synchronisation de l'horloge de réception.

Couche 1 – Physique

Transmission large bande

- ▶ La transmission **large bande** translate le spectre du signal à émettre dans une bande de fréquence mieux admise par le système de transmission.
- ▶ On utilise une **porteuse** analogique modulée par le signal à transmettre

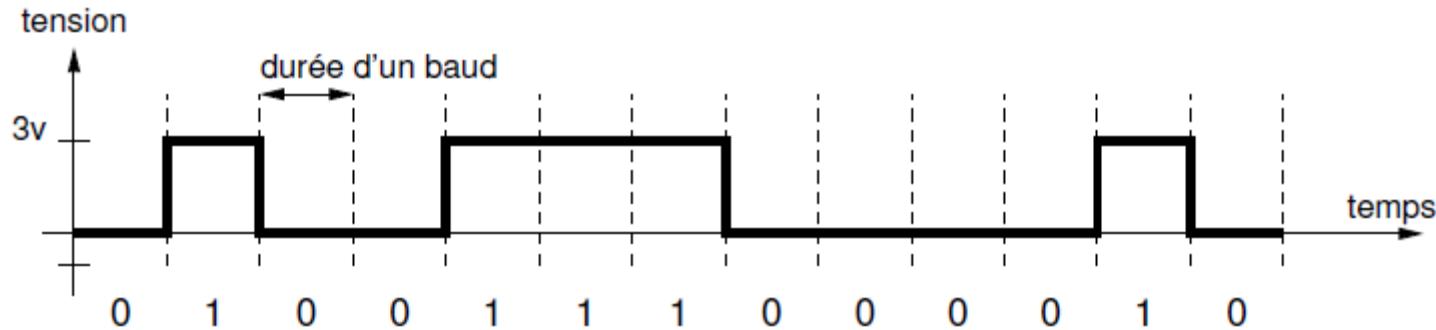


- ▶ L'ETCD est un **modulateur/démodulateur**. Il transforme le signal numérique en un signal sinusoïdal modulé (par fréquence/amplitude/phase) plus résistant que le signal en bande de base. Il permet donc d'atteindre des distances plus importantes. De plus, une transmission en large bande permet le multiplexage spatial.

Couche 1 – Physique

Transmission bande de base

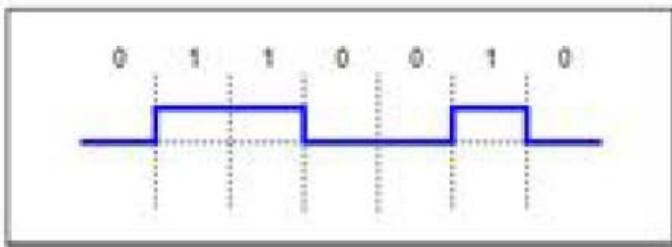
- ▶ Se dégrade rapidement avec la distance :
 - ▶ Besoin de répéteurs pour ré amplifier / régénérer le signal.
- ▶ Dans le cas du code RZ, impossibilité de distinguer une suite de 0 et l'absence d'information.



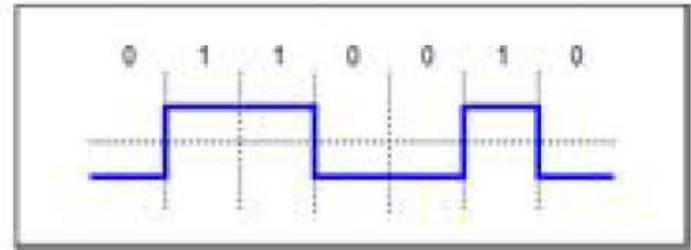
- ▶ Utilisation limitée de la bande spectrale → Plus sensible aux perturbations.

Couche 1 – Physique

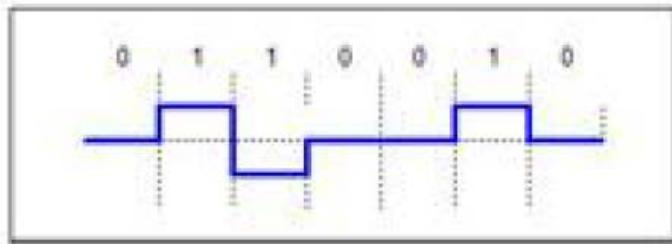
Transmission en bande de base - codage



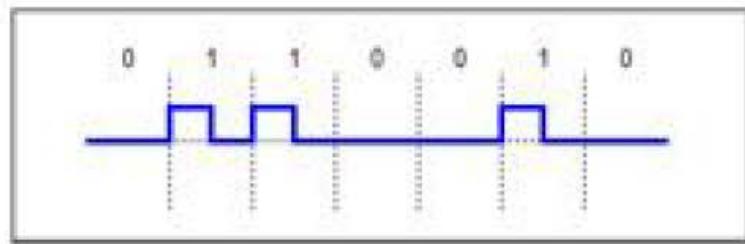
tout ou rien



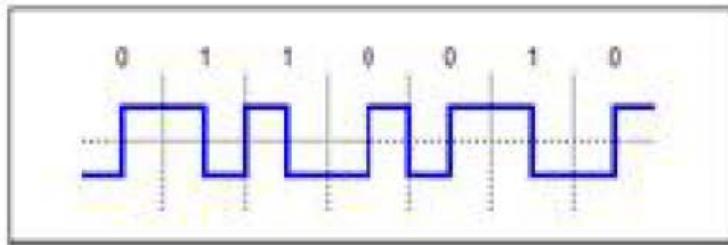
NRZ



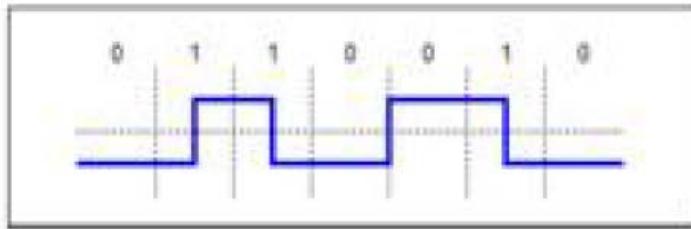
bipolaire



RZ



Manchester



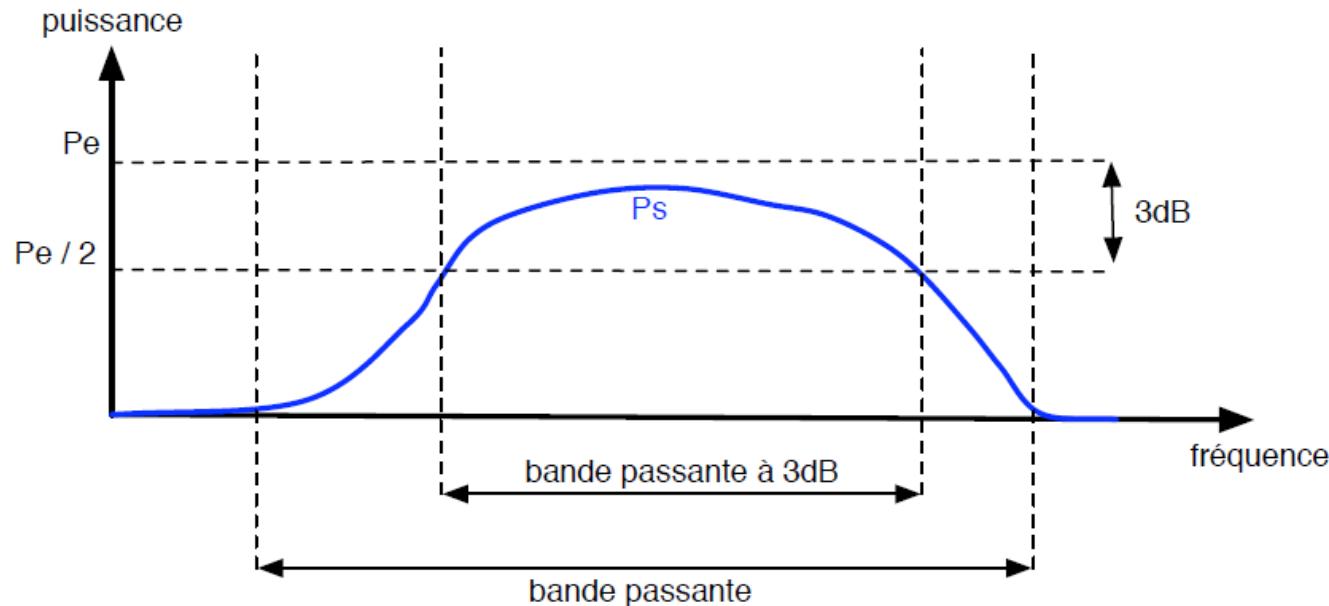
Miller

Couche 1 – Physique

Le support - Bande Passante

On caractérise un support de transmission par sa **bande passante à 3dB** :

- ▶ C'est la plage de fréquence dans laquelle les signaux appliqués à l'entrée du support subissent un affaiblissement inférieur à 3dB.



- ▶ L'affaiblissement \mathcal{A} (dB) d'un signal est donné par la formule suivante :

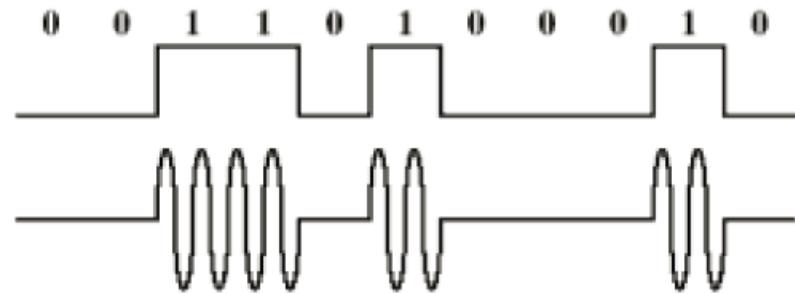
$$\mathcal{A} = 10 \cdot \log_{10} P_e/P_s$$

▶ Pour que $\mathcal{A} < 3\text{dB}$, il faut donc que $P_s > P_e/2$.

Couche 1 – Physique

Modulation d'un signal numérique

- ▶ Modulation d'amplitude
ASK Amplitude Shift Keying.



Modulation en Amplitude

- ▶ Modulation de fréquence
FSK Frequency Shift Keying



Modulation en Fréquence

- ▶ Modulation de phase
PSK Phase Shift Keying

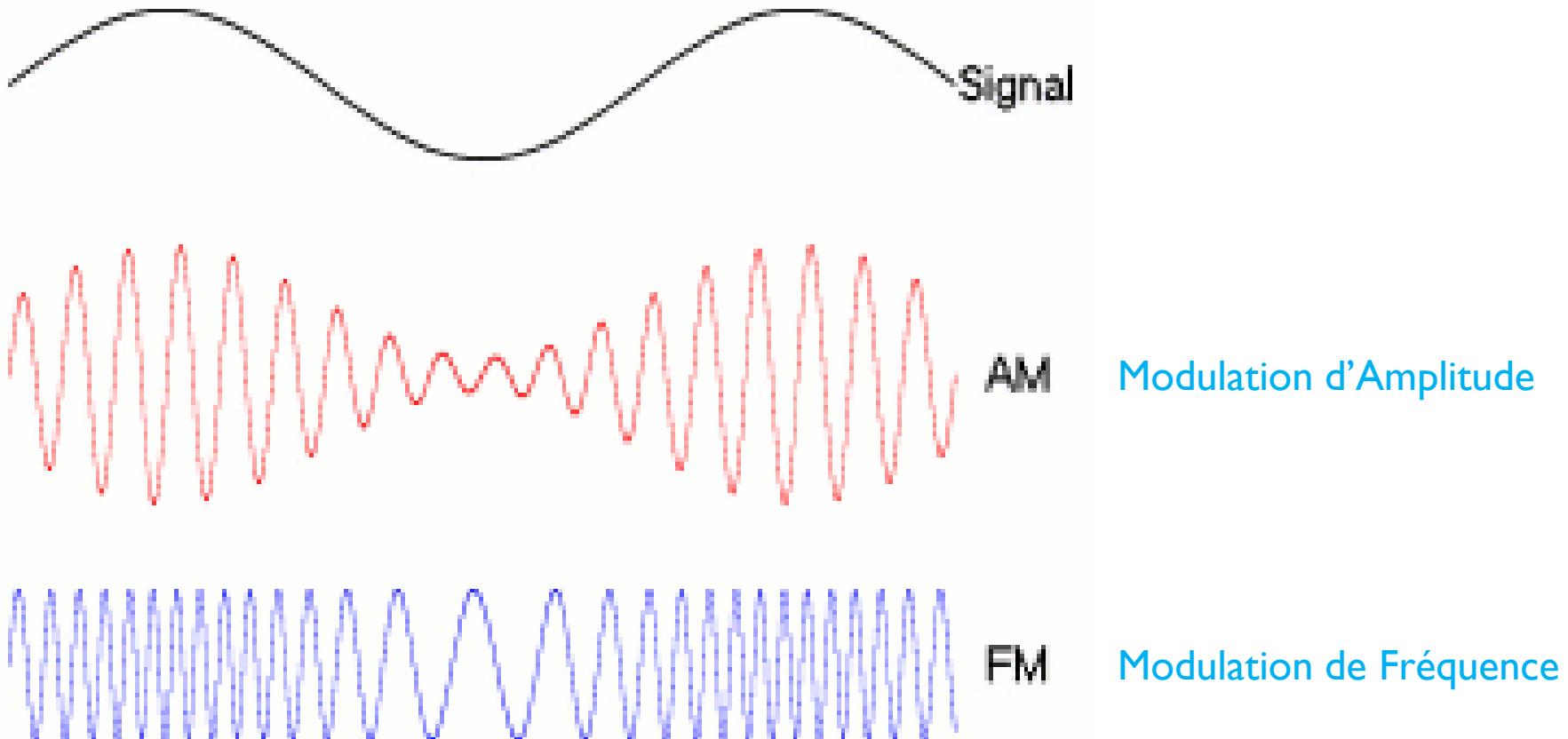


Modulation en Phase

- ▶ Les différentes techniques de modulation peuvent être **combinées** :
 - ▶ Exemple = Modulation QAM (Quadrature Amplitude Modulation)

Couche 1 – Physique

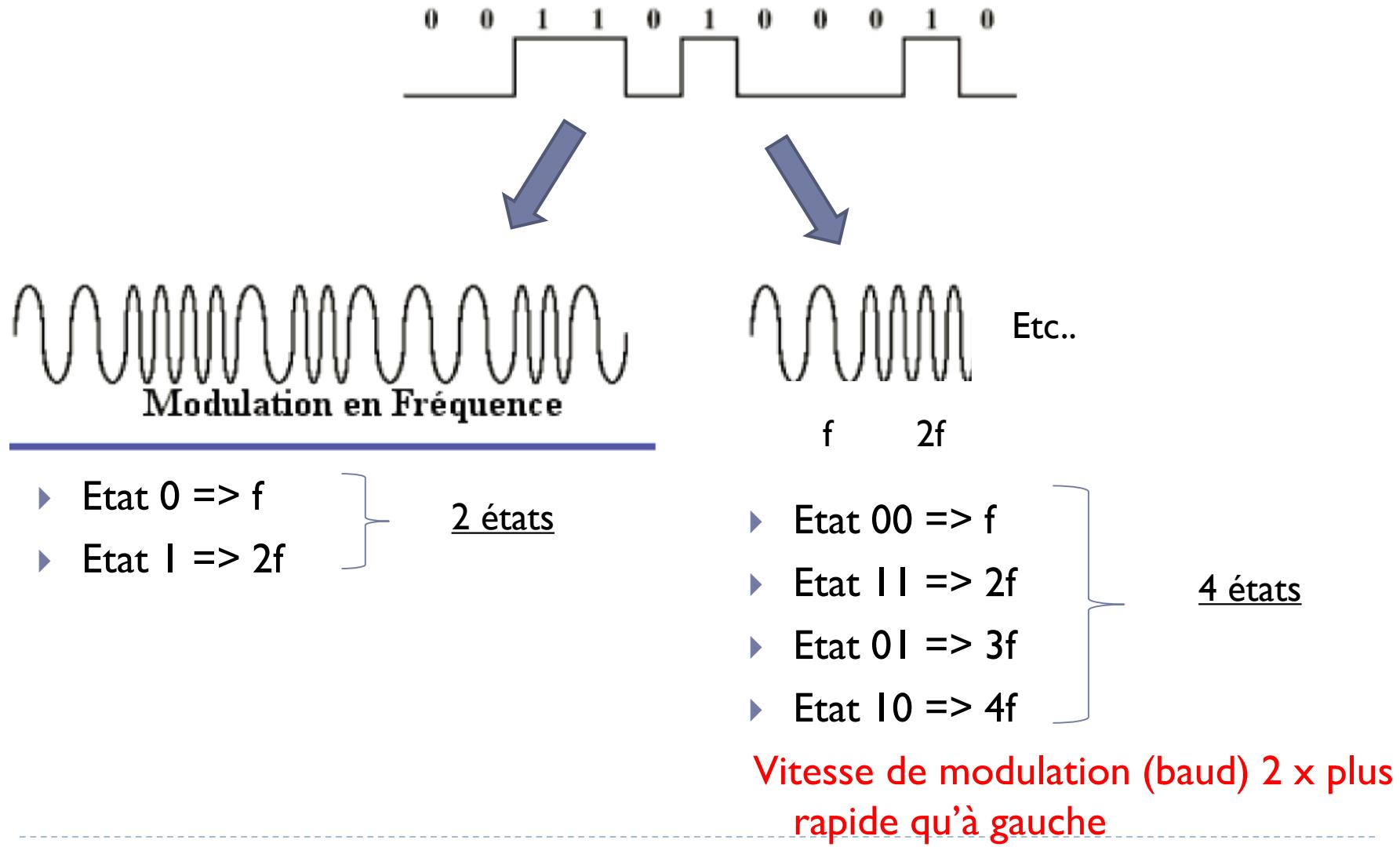
Modulation d'un signal analogique



Source wikipedia

Couche 1 – Physique

Modulation – Notion d'états



Couche 1 – Physique

Valence et rapport signa/bruit

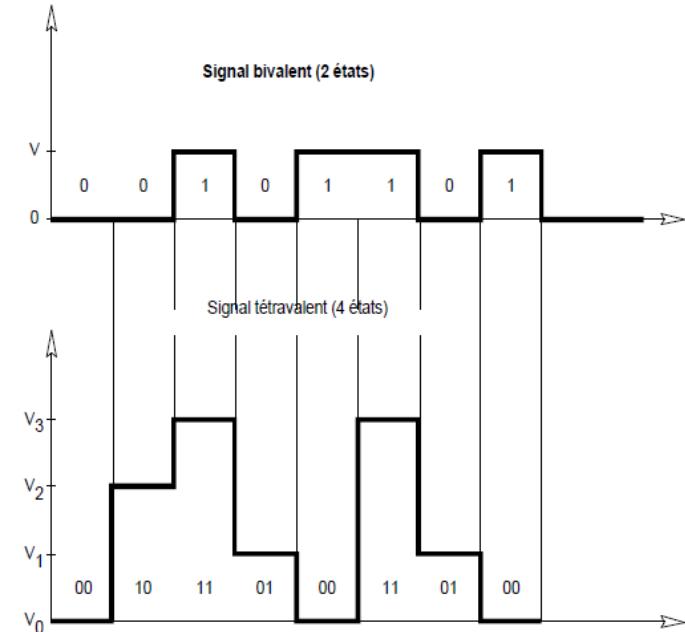
- ▶ **Valence** : c'est le nombre de symboles (états) discernables dans le signal. On le note \mathcal{V} .

Le nombre de bits codés par symbole est noté $q = \log_2 \mathcal{V}$ bits.

- ▶ Le rapport entre la puissance (S) du signal transmis et la puissance (B) du bruit s'appelle le **rapport signal sur bruit**. $S/B_{\text{dB}} = 10 \log_{10} S/B$

- ▶ Relation de Shannon : **valence maximale** $\mathcal{V}_{\max} = \sqrt{1 + S/B}$.

- ▶ **Capacité** : débit binaire maximal $\mathcal{D}_{\max} = 2 \cdot \text{BP} \log_2 \sqrt{1 + S/B}$.



Couche 1 – Physique

Rapidité de modulation

- ▶ Le nombre maximal de modulation (i.e. de changement d'états) d'un signal par unité de temps est lié à la bande passante du support de transmission par le **critère de Nyquist** :

$$\mathcal{M}_{\max} \leq 2 \cdot \text{BP} \text{ (cas d'une ligne non bruité)}$$

- ▶ Exemple : une ligne téléphonique a une bande passante comprise entre 300 et 3400 Hz.

$$\mathcal{M}_{\max} = 2 \cdot (3400 - 300) = 6200 \text{ bauds.}$$

Couche 1 – Physique

Débit

- ▶ **Débit binaire** : c'est le nombre de bits transmis par seconde, soit

$$D = q \cdot M$$



Limité par la modulation

Limité par la bande passante
du support

Compromis !

- ▶ Exemple :

- ▶ avec 16 valeurs d'amplitude (= 16 états / valence $\nu = 16$), on peut coder 0001,0010,0011...1111, soit 4 bits par changement d'amplitude $q = \log_2 16 = 4$
- ▶ $M_{\max} = 2 \cdot (3400 - 300) = 6200$ bauds
- ▶ Le débit binaire est dans ce cas le quadruple de la rapidité de modulation $D = 4 \cdot 6200 = 24\,800$ soit 24,8 k bit/s
- ▶ **Débit max** : $D_{\max} = 2 \cdot \text{BP} \log_2 \nu$ (*cas d'une ligne non bruitée*)
- ▶ **Débit max** : $D_{\max} = 2 \cdot \text{BP} \log_2 \sqrt{1 + S/B}$.

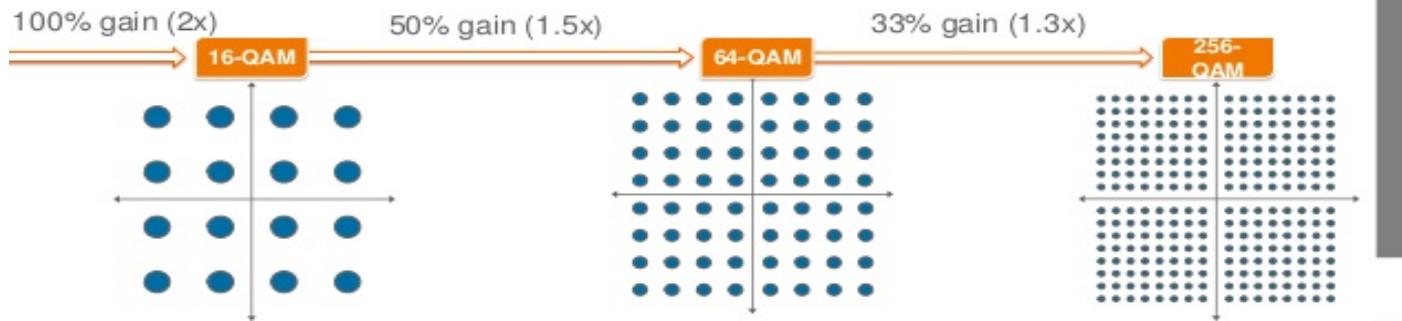
Couche 1 – Physique

Modulation - Limite



256-QAM

- Improves efficiency by 33%
- Adds complexity, requires higher SNR
- Efficiency gain from modulation does not increase linearly



- ▶ Mais augmenter le nombre d'états pour augmenter le débit implique :
 - ▶ Avoir un bon rapport signal/bruit
 - ▶ Demande d'importantes ressources processeurs.

Couche 1 – Physique

Transmission : Bilan

- ▶ Critères de choix d'un codage
 - ▶ Adapter le spectre du signal à la bande passante du canal
 - ▶ Codage NRZ mal adapté (coupure des basses fréquences)
 - ▶ Limitation de la bande passante utilisée ... et donc de la rapidité de modulation... et donc du débit
 - ▶ Réduire la sensibilité au bruit
 - ▶ Réduire la valence du signal et donc diminution du débit !
 - ▶ Déetecter, voire corriger les erreurs (notion de surdébit)
 - ▶ Diminution du débit effectif
 - ▶ Augmenter le débit
 - ▶ Augmenter la valence
 - ▶ Diminuer de la sensibilité au bruit
 - ▶ Augmenter la rapidité de modulation
 - ▶ Augmentation de la fréquence maximale du signal
 - ▶ Pas de méthode parfaite ...

Couche 1 – Physique

Différents types d'exploitation de la transmission

Les caractéristiques des ETCD sont liées à l'organisation fonctionnelle et physique des échanges. Il faut prendre en compte :

- ▶ le sens de transmission : **unidirectionnelle** (simplex), **alternatif** (half duplex) ou **bidirectionnelle** (full duplex).
 - ▶ Exemples : TV, Talkie/Walkie, Téléphonie
- ▶ le type de transmission : **transmission parallèle** (efficace mais problèmes de diaphonie et de propagation non homogène entre canaux – adapté aux très courtes distances) ou **transmission série** (qui est plus adaptée aux longues distances).
 - ▶ Exemples liaison parallèle : liaisons pour les anciennes imprimantes
- ▶ le type de synchronisation des horloges : une transmission correcte des données nécessite la synchronisation de l'horloge du récepteur sur celle de l'émetteur. Deux possibilités, la transmission **synchrone** ou **asynchrone** :
 - ▶ Synchrone : émetteur et récepteur ont leur propre horloge donnant le même signal d'horloge,
 - ▶ Asynchrone : l'envoi d'une série de bits est précédé par des fanions permettant d'informer le récepteur que la transmission a commencé
- ▶ le mode de transmission de débit : **asymétrique** ou **symétrique**.
 - ▶ Débit différent selon le sens de transmission : download et upload.
 - ▶ Exemples : ADSL, SDSL

Couche 1 – Physique

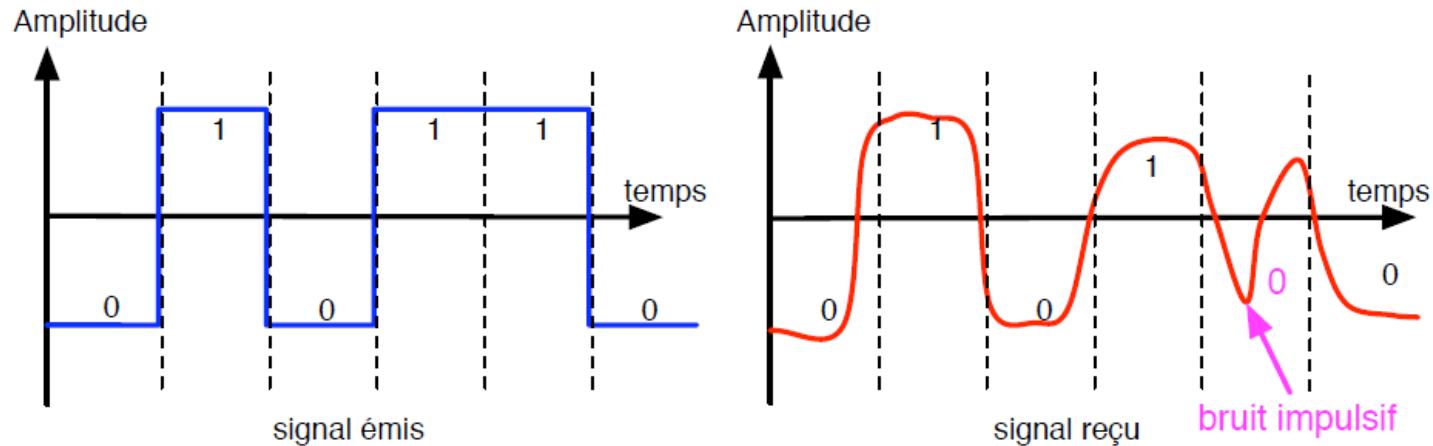
Facteurs limitants

- ▶ Atténuation et distorsion du signal (limitées par le choix du support, des connectiques).
- ▶ Bruit : perturbations extérieures (variation thermique, interférences électromagnétique) et diaphonie (due aux champs magnétiques des autres conducteurs d'un câble).
- ▶ Collision : des ordinateurs émettent en même temps sur le même support.
- ▶ Gigue : fluctuation du signal numérique dans le temps ou en phase due aux retards dans les transmissions dû aux composants intermédiaires.
- ▶ Horloges des émetteurs et récepteurs non synchronisées.

Couche 1 – Physique

Facteurs limitants - Bruit et distorsions

- ▶ La **distorsion/atténuation** du signal peut affecter ce signal jusqu'a le rendre non reconnaissable par le récepteur.
- ▶ Les bruits impulsionnels sont une perturbation brève provenant de l'extérieur. D'intensité élevée, ils peuvent générer des erreurs de transmission.



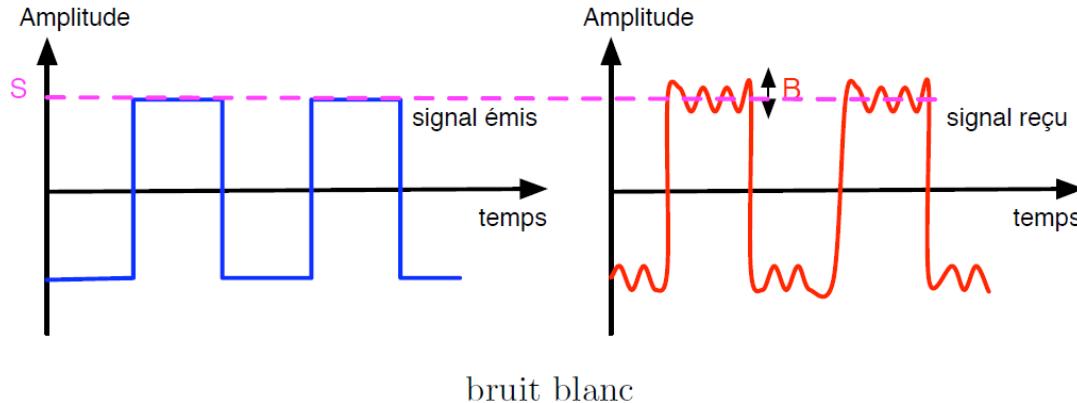
Distorsion, atténuation et bruit impulsif

- ▶ Ces phénomènes peuvent être limités par le choix du support de transmission

Couche 1 – Physique

Facteurs limitants - Bruit et distorsions

- Le bruit blanc provient de l'agitation thermique des électrons. Il est généralement d'amplitude faible et est peu gênant pour les transmissions.

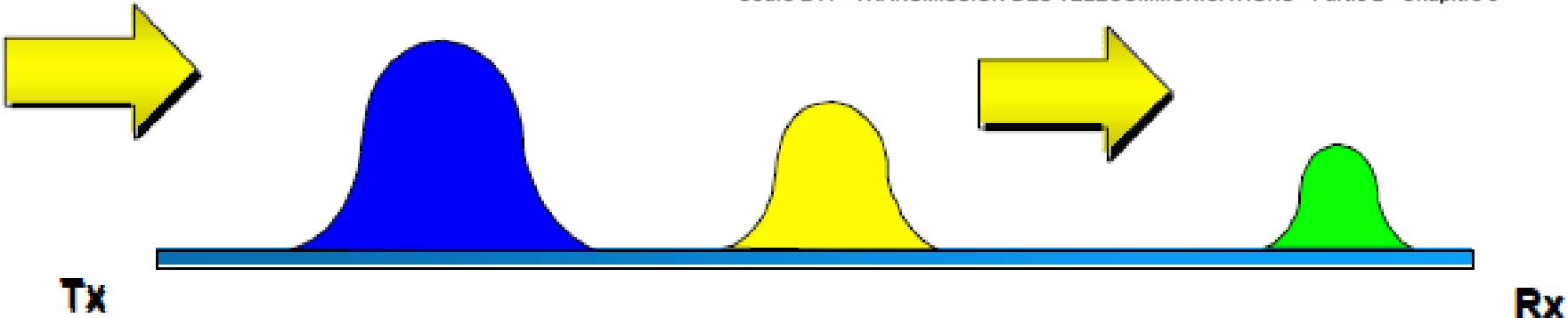
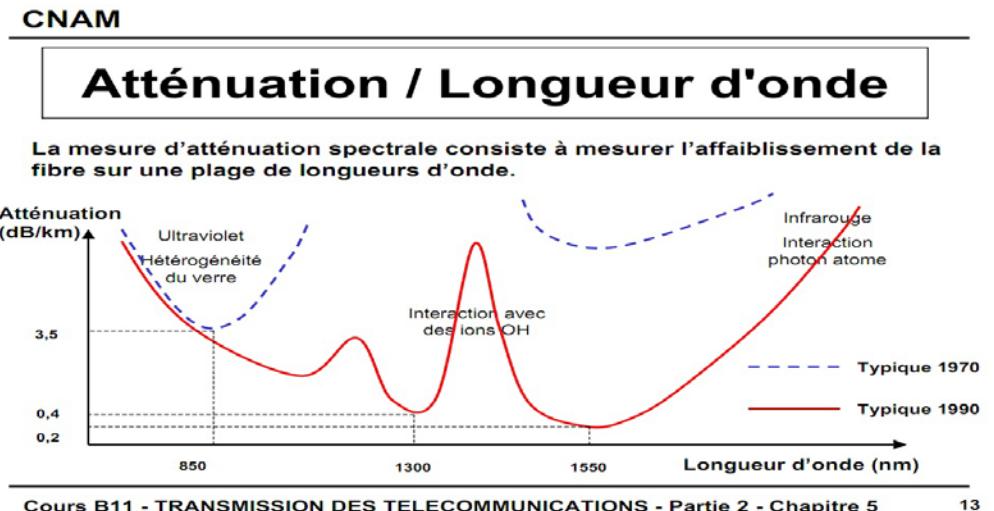


- Le rapport entre la puissance (S) du signal transmis et la puissance (B) du bruit s'appelle le rapport signal sur bruit. $S/B_{\text{dB}} = 10 \log_{10} \cdot S/B$
- Relation de Shannon : valence maximale $\nu_{\max} = \sqrt{1 + S/B}$.
- Capacité : débit binaire maximal $\mathcal{D}_{\max} = 2 \cdot \text{BP} \log_2 \cdot \sqrt{1 + S/B}$.

Couche 1 – Physique

Facteurs limitants - Atténuation

- ▶ Perte de puissance du signal
- ▶ S'exprime en dB
- ▶ L'atténuation augmente avec
 - ▶ La distance
 - ▶ La fréquence



Couche 1 – Physique

Facteurs limitants – Atténuation : exemple de bilan de liaison

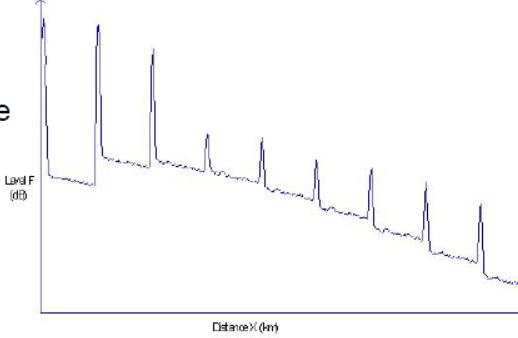
2007-04-19 Liaisons optiques v5.pdf - Adobe Acrobat Pro

Fichier Edition Affichage Fenêtre Aide

Budget optique 1/2

- Perte de puissance lumineuse sur un lien.
- Calculé en utilisant un OTDR (Optical Time Domain Reflectometer), à partir de
 - La longueur de la fibre
 - L'atténuation des différentes sections de fibre
 - Caractéristiques d'atténuation de la fibre
 - La localisation des connecteurs, épissures, défauts du câble



Distance X (km)

19 avril 2007

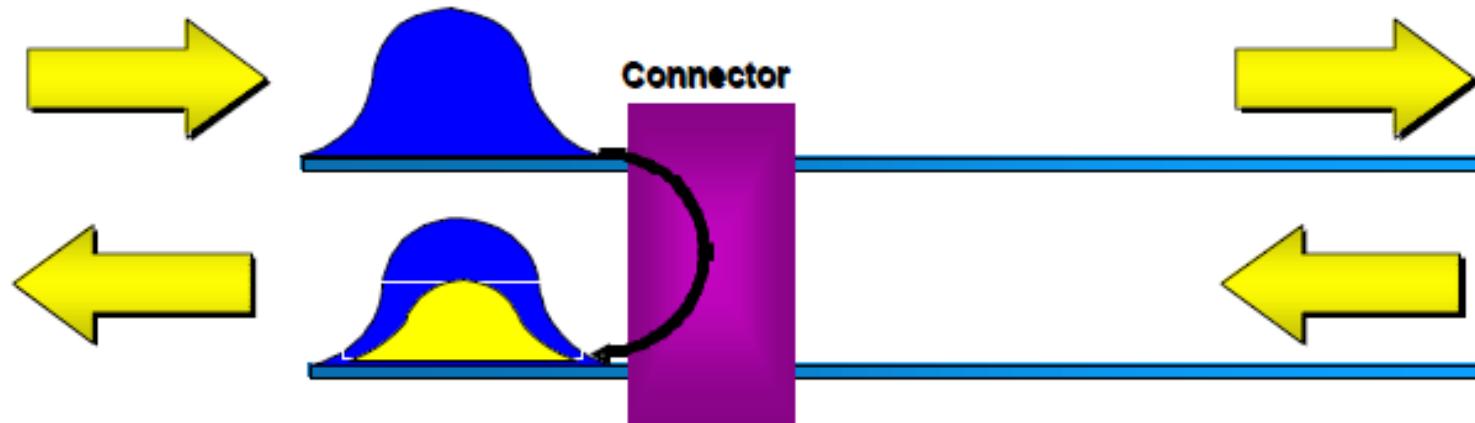
Liaisons optiques - E.Camisard

5

Couche 1 – Physique

Facteurs limitants - Paradiaphonie

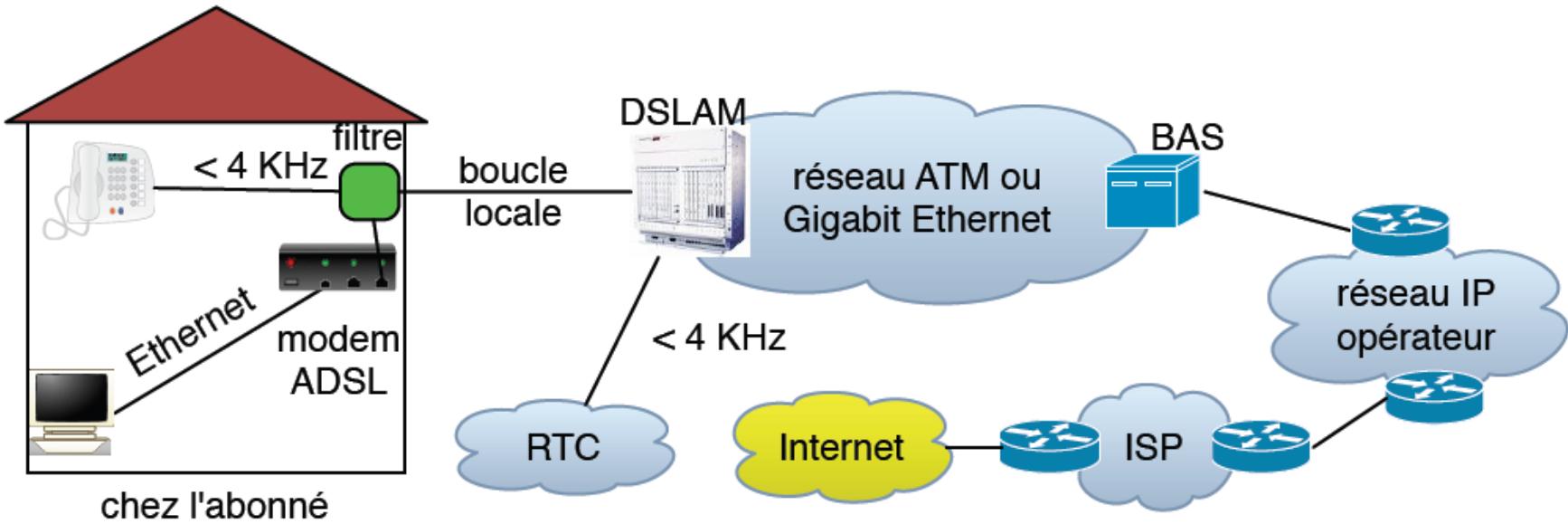
- ▶ Couplage entrées/sorties
- ▶ S'exprime en dB (on recherche des valeurs élevées)
- ▶ Augmente avec la fréquence
- ▶ Affectée par :
 - ▶ La construction du câble (blindage, torsade non régulière...)
 - ▶ La qualité de l'installation (points de branchement).



Couche 1 – Physique

Exemples de supports de transmission : Cuivre

▶ Architecture ADSL



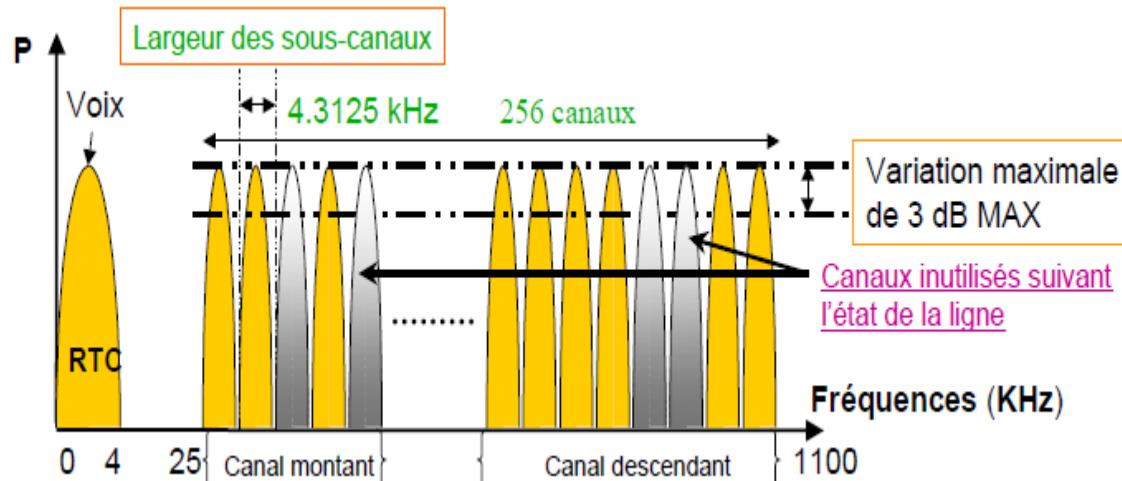
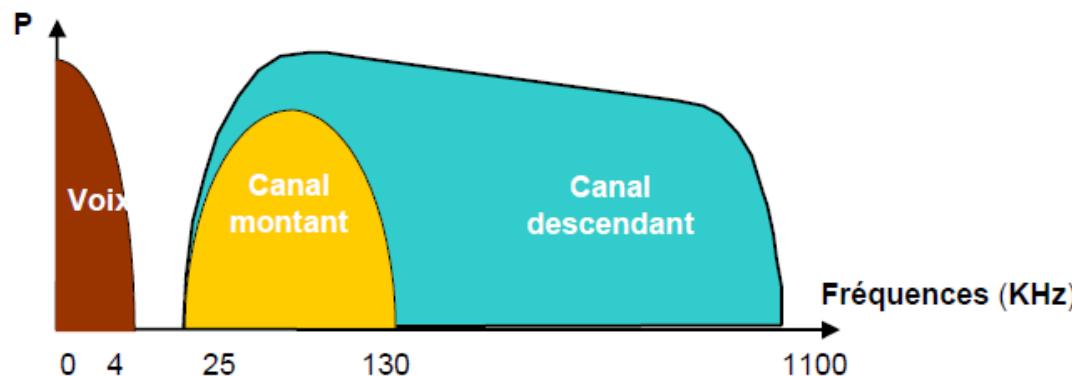
Couche 1 – Physique

Exemples de supports de transmission : Cuivre

▶ Technologie ADSL :

Modulation DMT = Discrete MultiTone

- ▶ Canaux indépendants entre eux,
- ▶ Modulation QAM des sous canaux,
- ▶ Optimisation individuellement et en temps réel en fonction du rapport S/N.

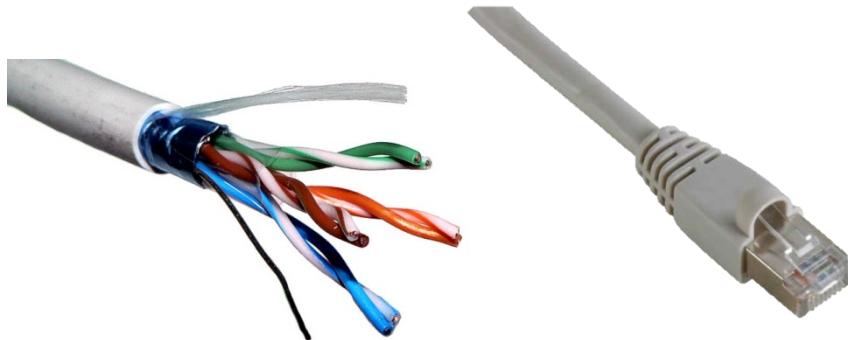


Couche 1 – Physique

Exemples de supports de transmission : Cuivre

▶ Câbles en cuivre

- ▶ Paire bifilaire torsadée
 - ▶ peu coûteux,
 - ▶ pertes élevées, débit limité.



- ▶ Paire coaxiale
 - ▶ pertes faibles,
 - ▶ bande passante (débit) élevée.

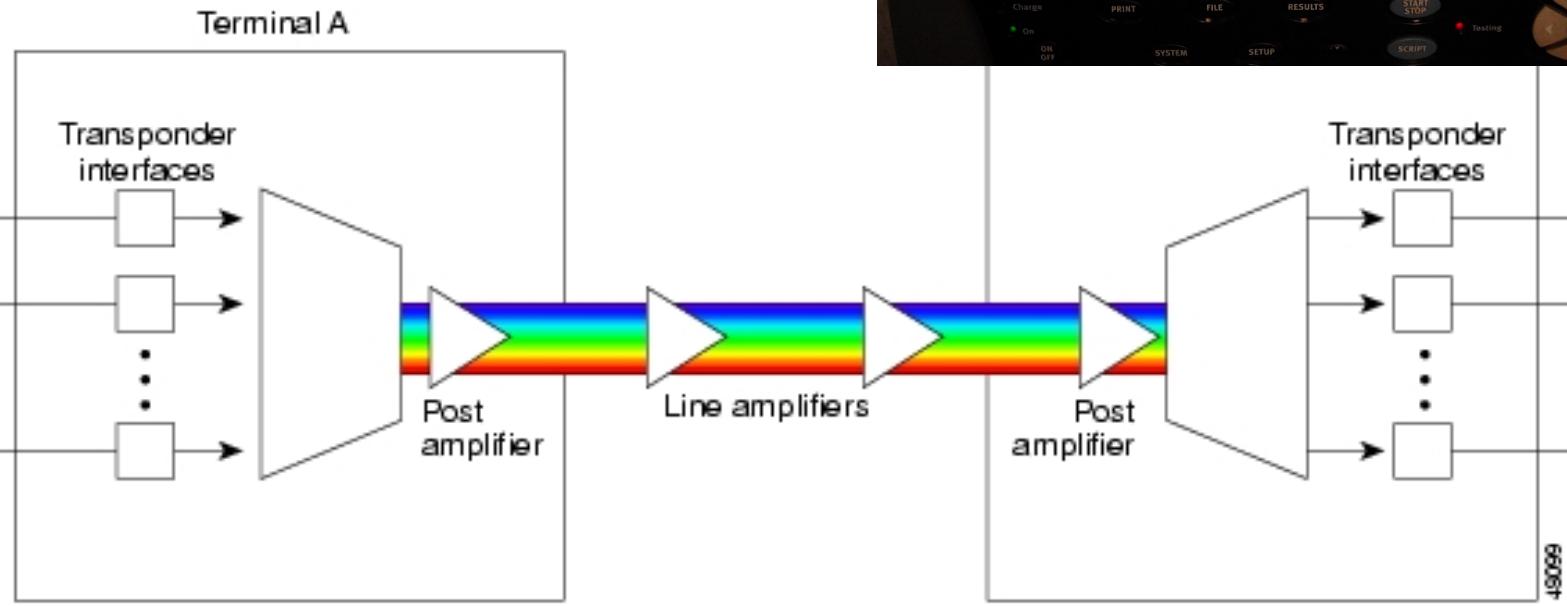


Couche 1 – Physique

Exemples de supports de transmission : Fibre Optique

▶ Dense Wavelength Division Multiplexing (DWDM)

- ▶ 1λ optique
- ▶ Modulation d'amplitude



Couche 1 – Physique

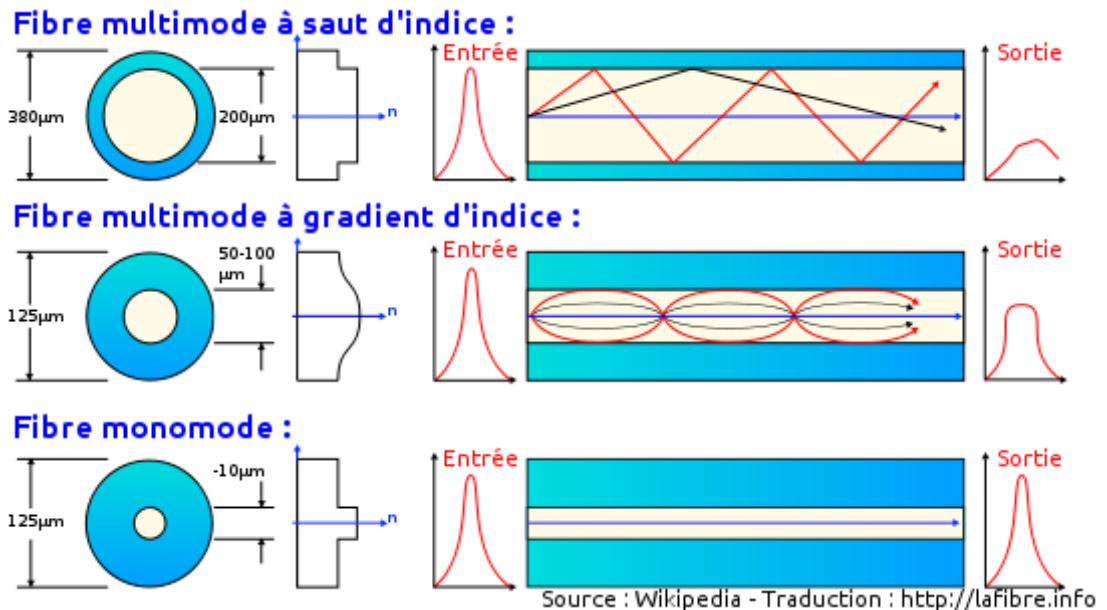
Exemples de supports de transmission : Fibre Optique

▶ Fibre optique

- ▶ pertes faibles à très faibles,
- ▶ immunité au bruits,
- ▶ bande passante (débit) très élevée



▶ Fibre multi-mode



▶ Fibre monomode

- ▶ mise en œuvre délicate : <https://www.youtube.com/watch?v=64TDjeFodzQ>

Couche 1 – Physique

Exemples de supports de transmission : Fibre Optique

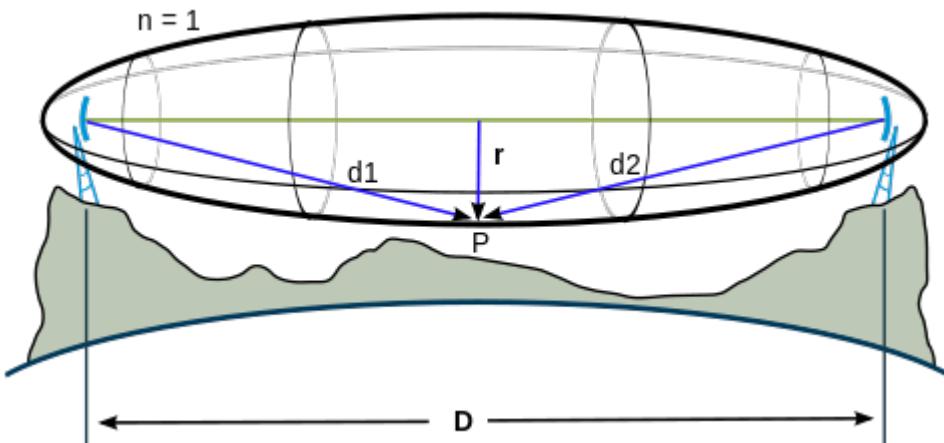
- ▶ Réseau de câbles sous-marin :
 - ▶ <http://www.submarinecablemap.com/#/>

Couche 1 – Physique

Exemples de supports de transmission : Air

▶ Faisceaux hertziens

- ▶ spectre disponible limité,
- ▶ bande passante limitée,
- ▶ propagation linéaire (à vue) en H.F.
- ▶ Interférences
- ▶ Utilisés dans les pays émergents, dans les vallées.



- ▶ Ellipsoide de Fresnel



Couche 1 – Physique

Exemples de supports de transmission : Air

- ▶ Spectre Hertzien :

Couche 1 – Physique

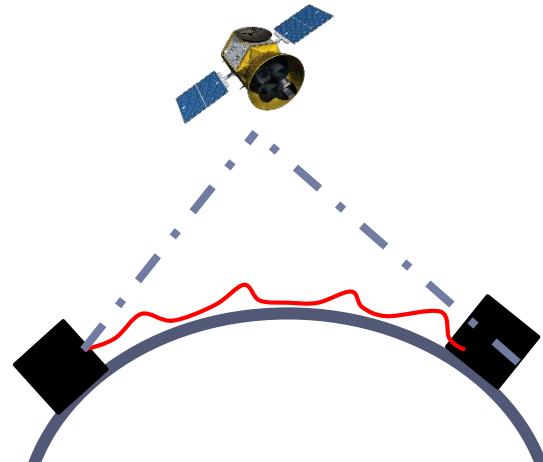
La transmission dans l'actualité

- ▶ Transmission sur fibre optique
 - ▶ Câbles sous-marins :
 - ▶ http://www.lemondeinformatique.fr/actualites/lire-les-sous-marins-russes-pres-des-cables-transatlantiques-inquietent-les-americains-62773.html?utm_source=mail&utm_medium=email&utm_campaign=Newsletter
- ▶ Transmission Hertzienne :
 - ▶ <http://www.lemondeinformatique.fr/actualites/lire-project-loon-google-pret-a-lacher-ses-milliers-de-ballons-internet-60904.html>

Couche 1 – Physique

Cas pratique- Calcul de délai de propagation

- ▶ Comparaison de la propagation entre deux points distants de 600 km
 - ▶ Transmission sur fibre optique :
 - $V = 200000 \text{ km/s}$
 - ▶ Transmission via un satellite géostationnaire :
 - $V = 200000 \text{ km/s}$
 - ▶ Transmission sur fibre optique :
 - $T = 3 \text{ ms}$
 - ▶ Transmission via un satellite :
 - $T = 0,36 \text{ s}$



Plan du cours 2

- ▶ Couche 2 – Liaison
 - ▶ Objectifs
 - ▶ Spécification des trames – exemples
 - ▶ Délimitations
 - ▶ Détection et correction d'erreurs
 - ▶ Gestion des échanges – flux
 - ▶ Focus sur Ethernet
 - ▶ Ethernet commuté
 - ▶ Notion d'architecture matériels

Couche 2 – Liaison Objectifs

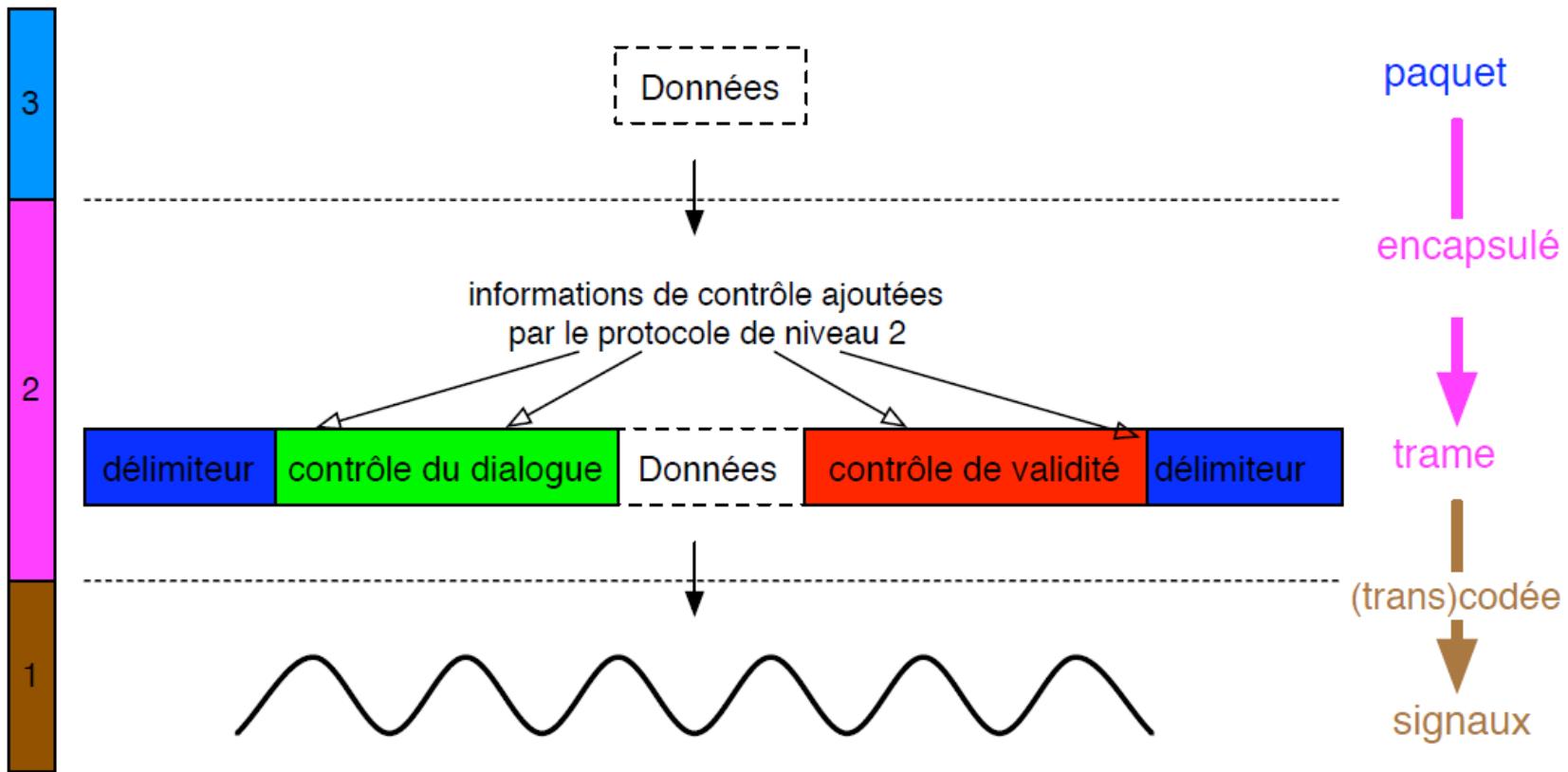
- ▶ Les protocoles de liaison de données supervisent et définissent des règles pour assurer la fiabilité des échanges
- ▶ L'entité de cette couche : **la Trame**
- ▶ Ces règles définissent une structure type de la trame avec :
 - ▶ La délimitation des différentes trames
 - ▶ Le contrôle de la validité des trames
 - ▶ L'envoi de commandes de supervision
- ▶ Ces règles permettent aussi la gestion du dialogue entre extrémités :
 - ▶ procédure de reprise sur erreur
 - ▶ contrôle du flux de données entre les extrémités
 - ▶ gestion des acquittements des trames

Couche 2 – Liaison

La Trame

- ▶ **Trame** : paquet (données provenant de la couche 3) + informations de contrôle.
On dit que le paquet est **encapsulé** dans la trame.

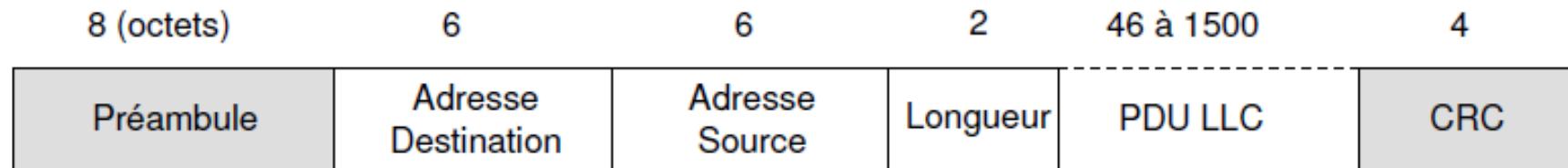
couches OSI



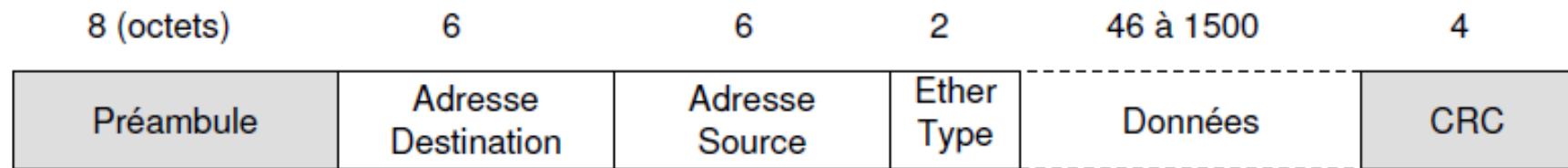
Couche 2 – Liaison

Exemple de trames

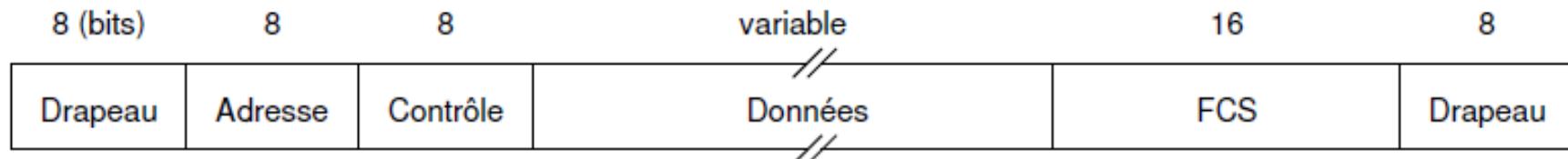
IEEE 802.3 :



Ethernet V2 :



HDLC (*High-Level Data Link Control*) et LAP-B (*Link Access Procedure Balanced*) :



Couche 2 – Liaison

Délimitation de la trame par fanion

- ▶ Cas : HDLC/PPP
- ▶ Une séquence de bits spécifiques, appelée **fanion**, est ajoutée au début et à la fin des



- ▶ Afin d'interpréter correctement la trame, un mécanisme de **transparence** doit être mis en œuvre par le protocole sur l'ensemble de la trame hors fanions. On peut utiliser par exemple la méthode du **bit stuffing** : ajout d'un bit à 0 après n bits à 1.
- ▶ Exemple :

Données 011011110011101001

- ▶ Ajout Fanions : 0111110 011011110011101001 0111110

- ▶ Sans mécanisme de transparence la trame est mal interprétée : 011
- ▶ Avec mécanisme de transparence : 0111110 011011110100111010010111110
- ▶ => 01101111010011101001
- ▶ => 011011110011101001

Couche 2 – Liaison

Délimitation de la trame par transmission de la longueur des données

- ▶ Cas : Ethernet
- ▶ Un champs en entête indique **la longueur des données** utiles de la trame (en octet, mot ou double mot). Ce champs est généralement précédé d'un délimiteur de trame.



- ▶ Ce mécanisme induit une taille de trame maximale. De plus les données utiles doivent avoir une longueur multiple d'un octet, d'un mot ou d'un double mot suivant le cas.

Couche 2 – Liaison

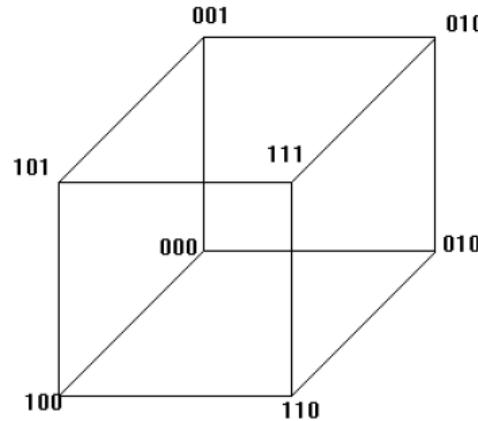
Détection et correction d'erreurs

- ▶ Il existe principalement deux possibilités :
 - ▶ Par redondance : pour permettre la détection et la correction d'erreurs
 - ▶ Par utilisation d'un code de détection et demande d'une retransmission
- ▶ En fonction de la qualité de la transmission, l'une ou l'autre des méthodes peut être utilisée
- ▶ Aujourd'hui, la qualité de la transmission (meilleur câblage, meilleur code,...) et le type d'application cible rendent la méthode par redondance peu efficace et peu utilisée.
 - ▶ Cas d'usage de la méthode par redondance :
 - ▶ liaisons satellites pour ne pas saturer les mémoires tampons des récepteurs

Couche 2 – Liaison

Détection et correction d'erreurs issus de la couche 1

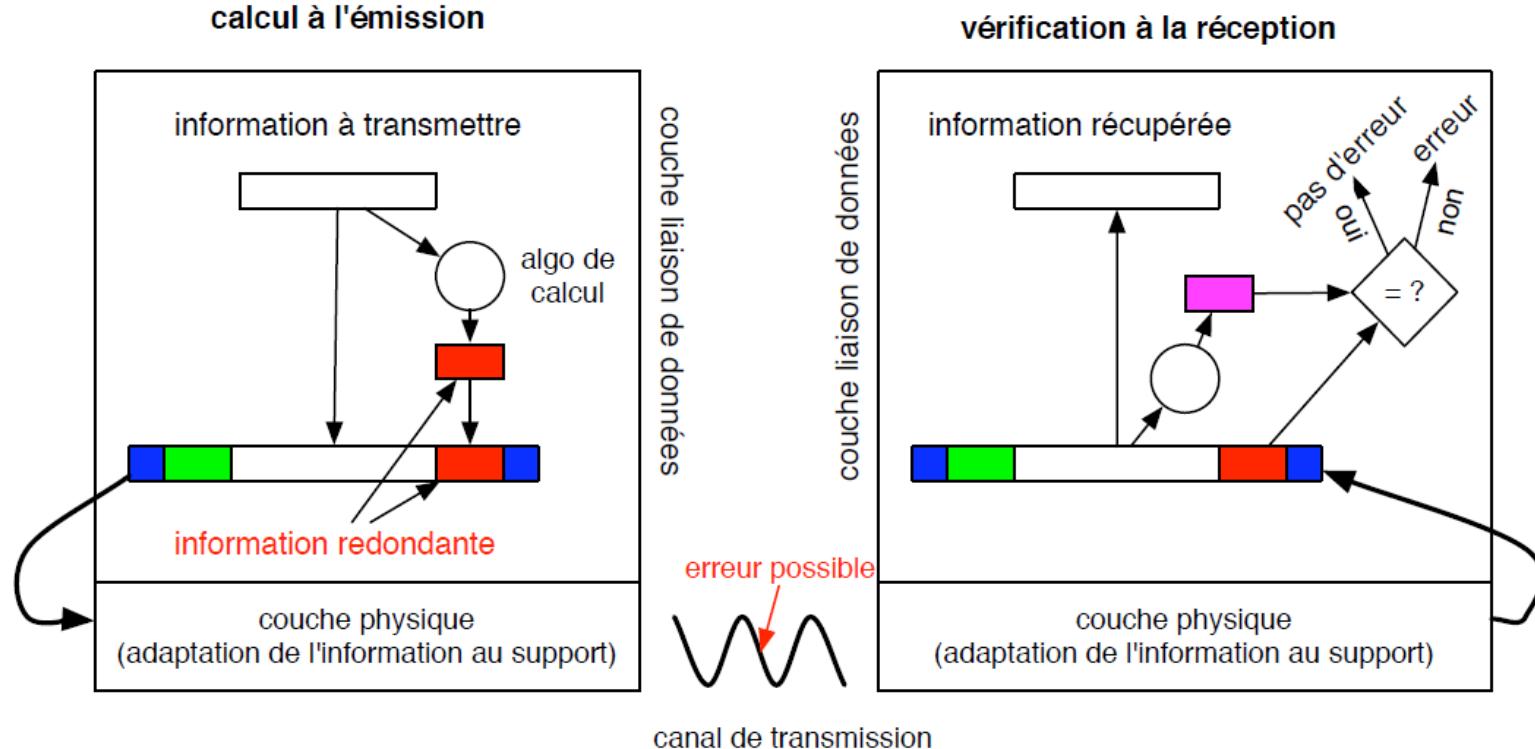
- ▶ **Bit de parité :**
 - ▶ Tous les n bits, on place le bit $n+1$ à 0 ou à 1 selon que la séquence est paire ou impaire.
 - ▶ Permet de détecter des erreurs de transmissions mais pas de les corriger.
 - ▶ Ne détecte pas les erreurs paires...
- ▶ **Code auto-correcteur :** La distance de Hamming entre deux mots binaires est égale au nombre de bits de rang identique qui sont différents.
On utilise une valence importante pour transmettre une information plus réduite.
 - ▶ Exemple : la valence $v = 8 = 2^3$
On choisit deux mots de code
 $0 \rightarrow 000$ et $1 \rightarrow 111$.
 - ▶ Les mots reçus avec deux 0 seront corrigés en 000 (0). Les mots reçus avec deux 1 seront corrigés en 111 (1)
- ▶ Ce code auto-correcteur nécessite une redondance très importante et n'est plus adaptée aux supports de transmission moderne aux taux d'erreur faible.



Couche 2 – Liaison

Détection d'erreurs par clé

- ▶ On ajoute aux trames transmises une redondance qui est une information de contrôle calculée par un algorithme spécifié dans le protocole.
- ▶ Le calcul est effectué sur les **données utiles**.



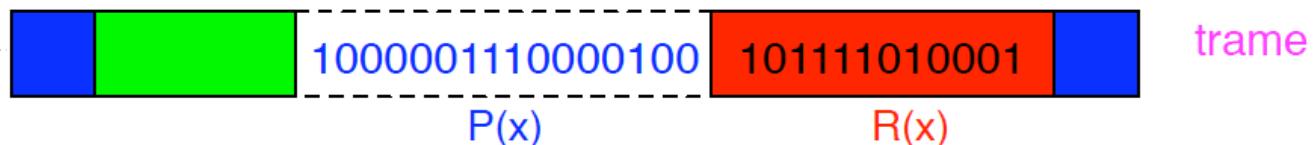
Couche 2 – Liaison

Exemple d'algorithme de détection d'erreurs : CRC

- ▶ **Cyclic Redundancy Check (CRC)** : appelé aussi contrôle polynomial, il est très utilisé dans les protocoles modernes car il permet de détecter des erreurs sur plusieurs bits.
- ▶ Cette méthode utilise une division euclidienne entre un polynôme représentatif des données à transmettre et un polynôme de contrôle.
- ▶ Exemple : Soit **1000001110000100** l'information à transmettre. Le polynôme correspondant est :

$$P(x) = x^{15} + x^9 + x^8 + x^7 + x^2$$

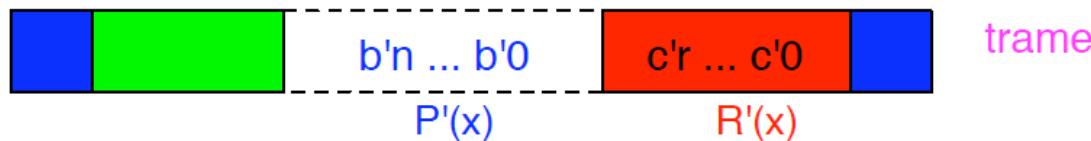
- ▶ Soit le polynôme de contrôle de degrés 12 suivant :
$$Q(x) = x^{12} + x^{11} + x^3 + x^2 + x + 1$$
- ▶ La division euclidienne de $P(x)$ par $Q(x)$ donne le polynôme reste :
$$R(x) = (x^{12} \cdot P(x)) \bmod Q(x) = x^{11} + x^9 + x^8 + x^7 + x^6 + x^4 + 1$$
- ▶ L'information redondante à ajouter en fin de trame est donc : **101111010001**.
- ▶ La trame envoyée contient donc : **1000001110000100 101111010001**.



Couche 2 – Liaison

Exemple d'algorithme de détection d'erreurs : CRC

- Le protocole de liaison de données du côté destinataire reçoit donc une trame du type :



- Pour vérifier la validité des données, il faut effectuer le quotient suivant :
$$(x^r \cdot P'(x) + R'(x))/Q(x)$$
- Si le reste est nul alors on suppose qu'il n'y a pas eu d'erreur de transmission.
- Si le reste n'est pas nul, alors il y a eu une erreur de transmission et il faut demander la réémission de la trame.

Couche 2 – Liaison

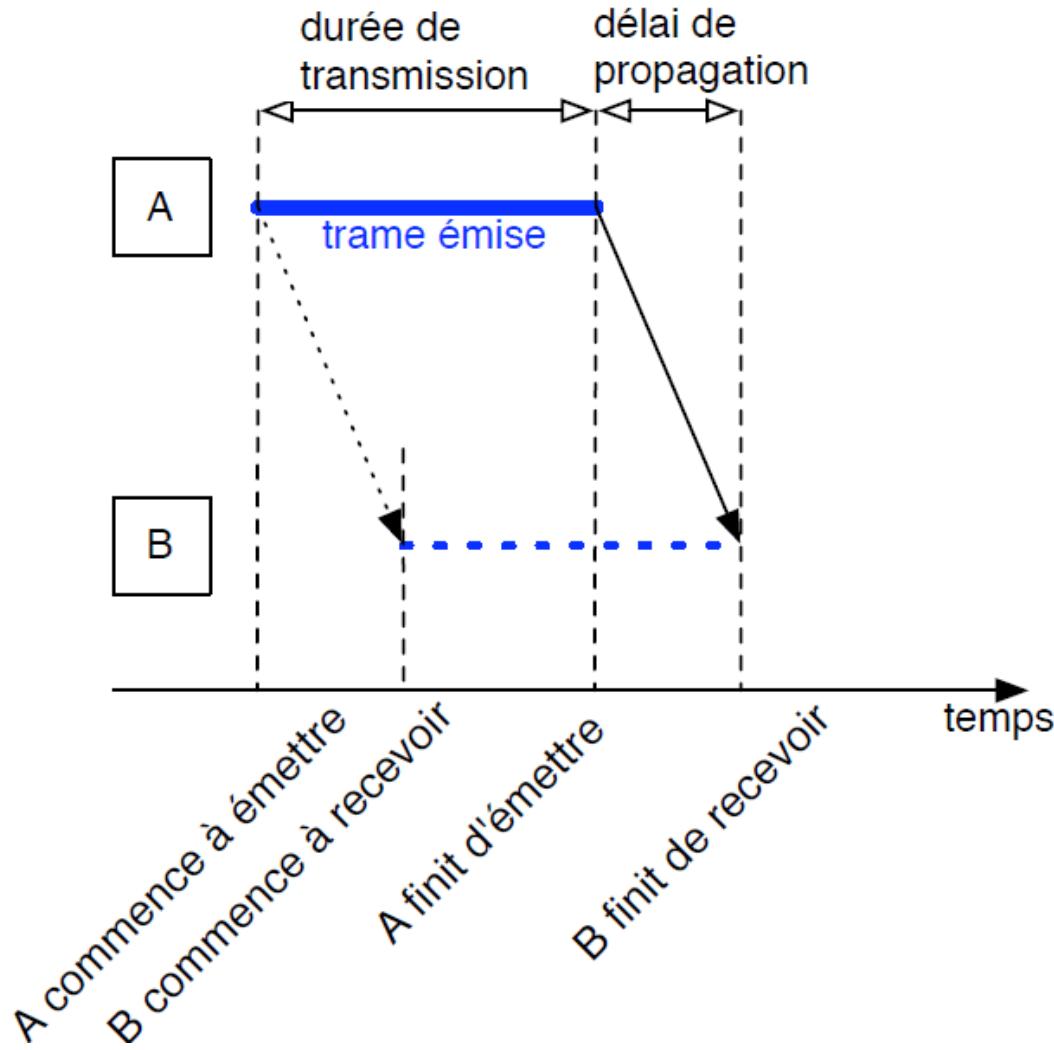
Modes d'exploitation d'une liaison de données

- ▶ Le mode d'exploitation d'une liaison de données peut être :
 - ▶ **simplex** : l'échange de données se fait dans **un seul sens** ;
 - ▶ **half-duplex** : l'échange de données se fait **alternativement** dans les deux sens. Ce mode d'exploitation nécessite souvent des règles supplémentaires d'accès au support pour éviter la contention.
 - ▶ **full-duplex** : l'échange de données se fait dans les deux sens **simultanément**.
- ▶ **Remarque** : le mode d'exploitation d'une liaison de données peut différer de celui du circuit de données. Par exemple, un circuit de données permettant des communications en half-duplex peut être exploité seulement en simplex par le protocole de liaison.



Couche 2 – Liaison

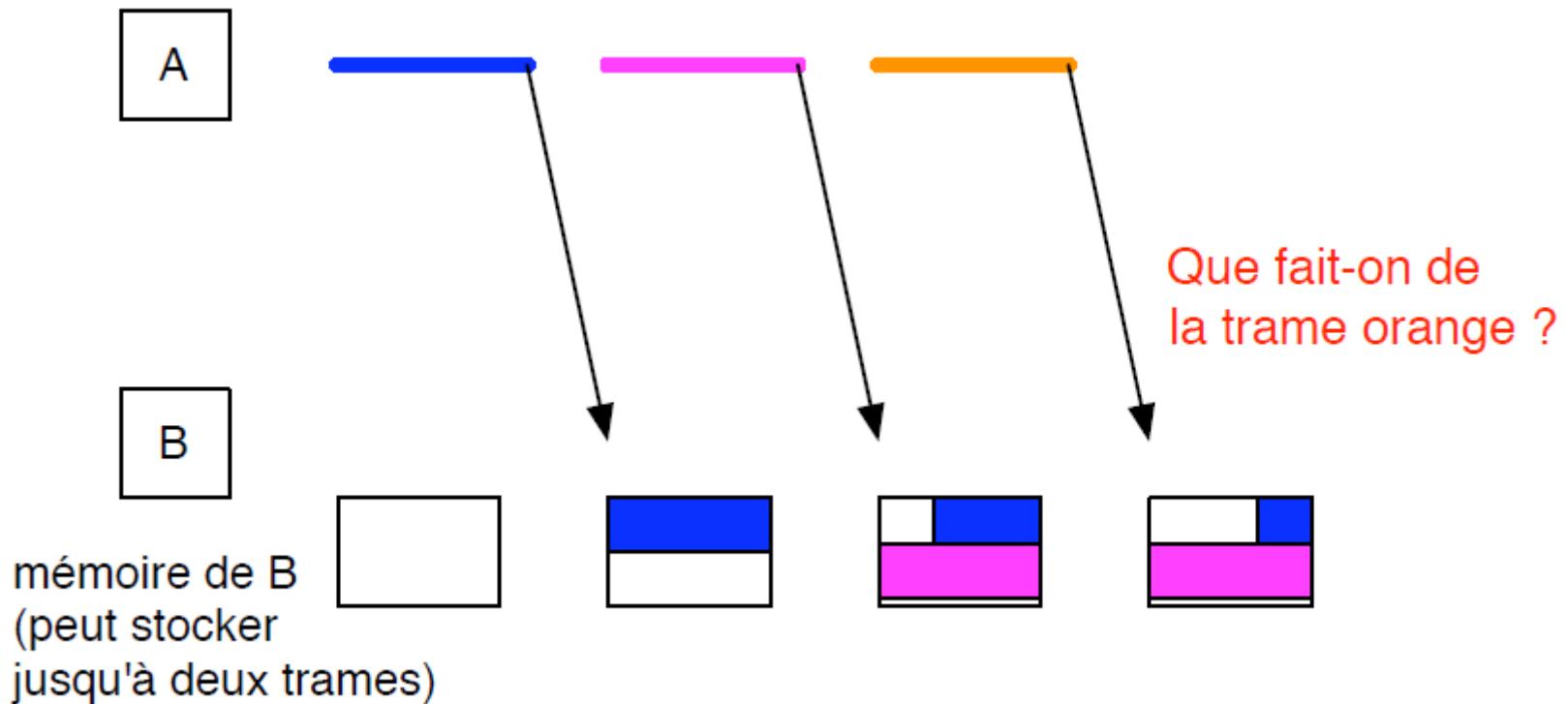
Représentation des échanges de données



Couche 2 – Liaison

Contrôle de flux

- ▶ Mécanisme de contrôle du rythme d'envoi des informations vers le récepteur.



Couche 2 – Liaison

Contrôle de flux

- ▶ Mécanisme de **contrôle du rythme d'envoi** des informations vers le récepteur.
- ▶ Plusieurs politiques d'acquittements possibles :
 - ▶ Acquittement à chaque trame reçu,
 - ▶ Acquittements accumulés pour être envoyés tous en même temps,
 - ▶ Acquittements transmis dans les trames du sens opposé,
 - ▶ Seule la trame erronée est retransmise,
 - ▶ Toutes les trames, à partir de celle erronée, sont retransmises

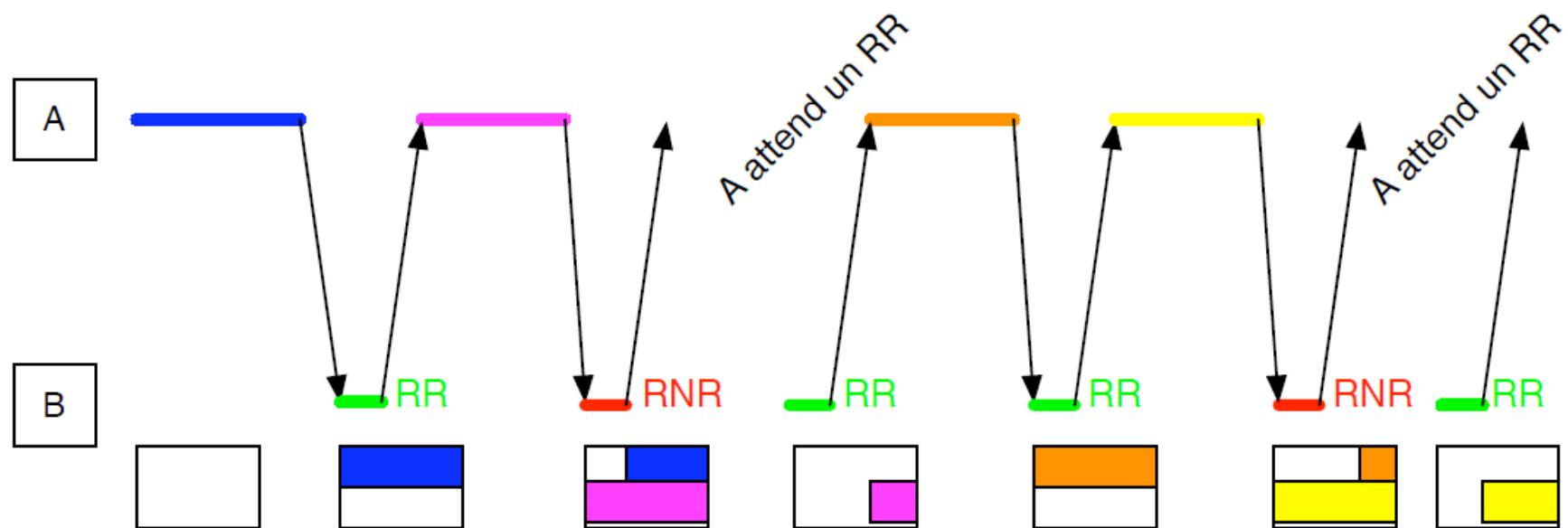
Couche 2 – Liaison

Contrôle de flux – trames de supervision

- ▶ Trames de supervision : RR (Receiver Ready) et RNR (Receiver Not Ready).



Nécessite une taille de mémoire satisfaisante....

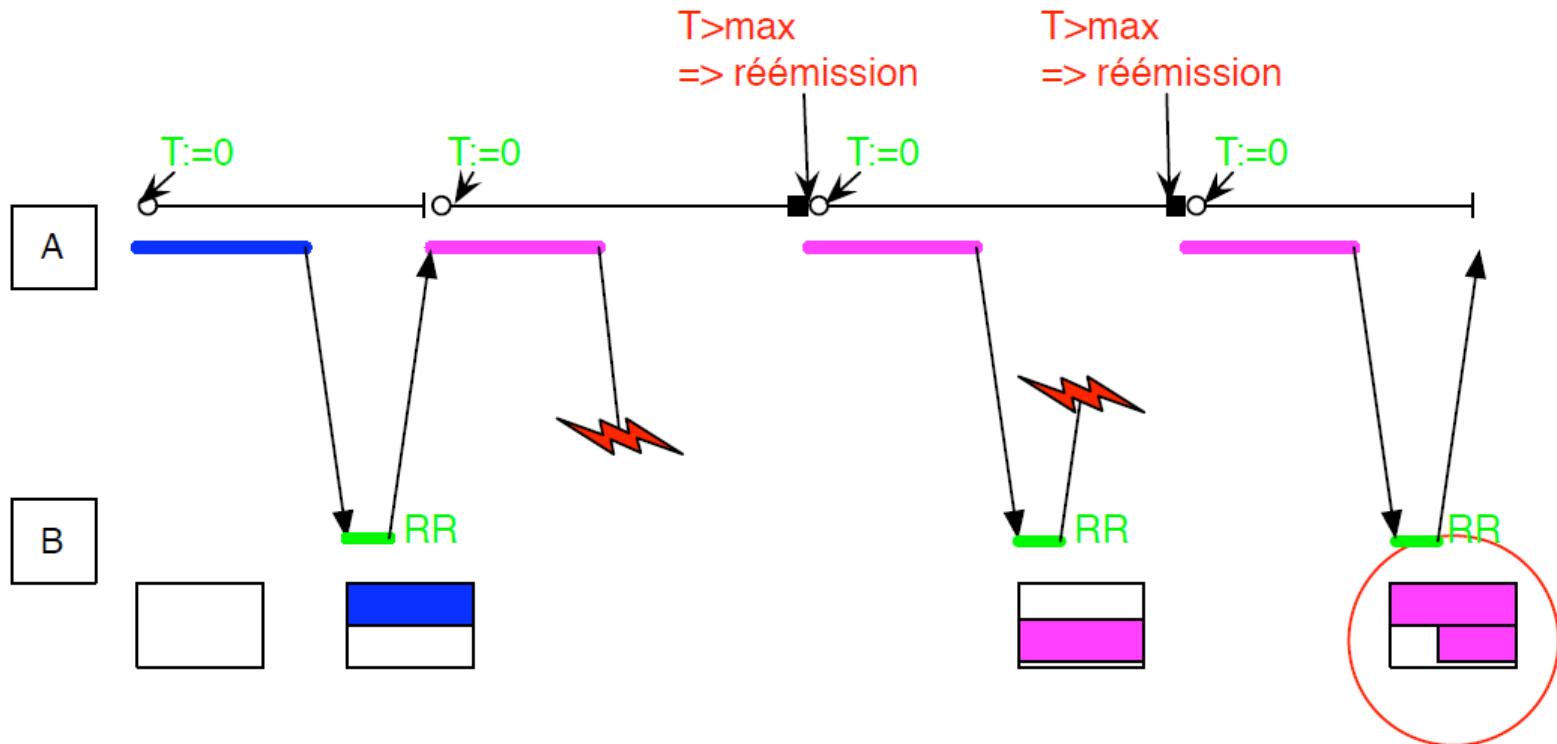


Exemple sur un canal exempt d'erreur

Couche 2 – Liaison

Gestion des acquittements

- ▶ Les trames de supervision peuvent aussi servir d'acquittement afin de gérer les erreurs de transmission. Cela nécessite l'utilisation d'un temporisateur.

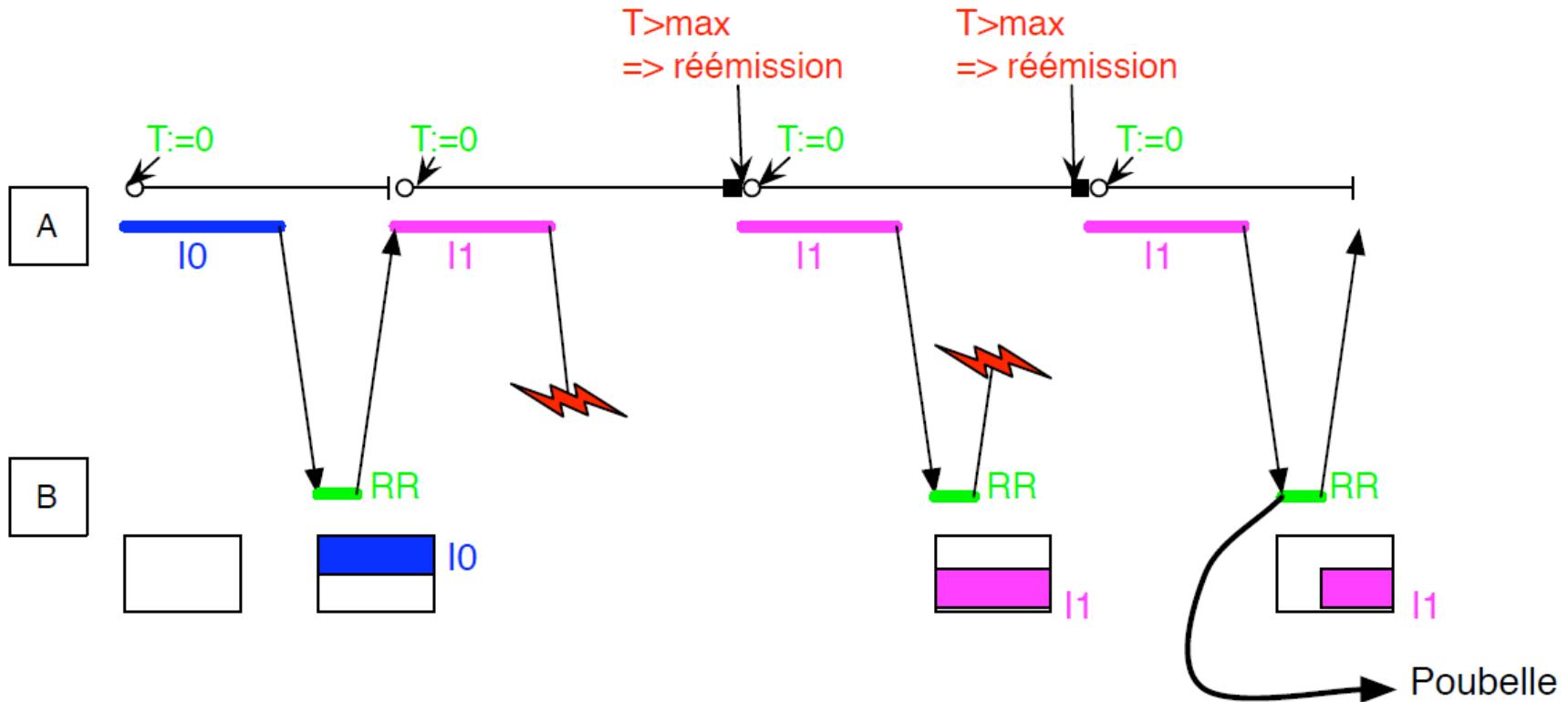


Pb de duplicité : nécessite une identification de la trame...

La même trame
est reçue deux fois !

Couche 2 – Liaison

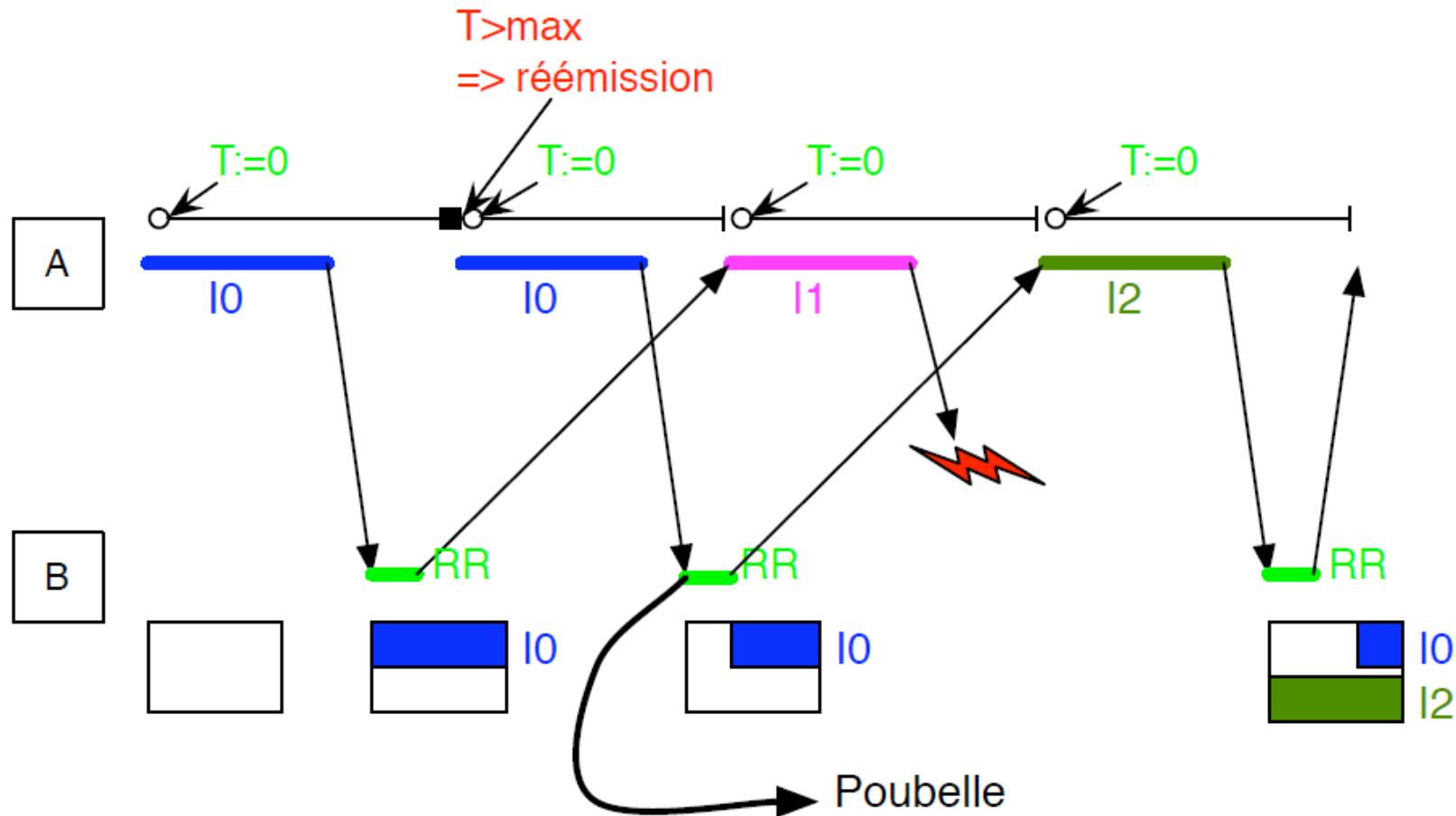
Numérotation des trames d'information



Le choix de la temporisation a-t-elle une influence sur la gestion du dialogue ?

Couche 2 – Liaison

Numérotation des trames d'information – problèmes de temporisation

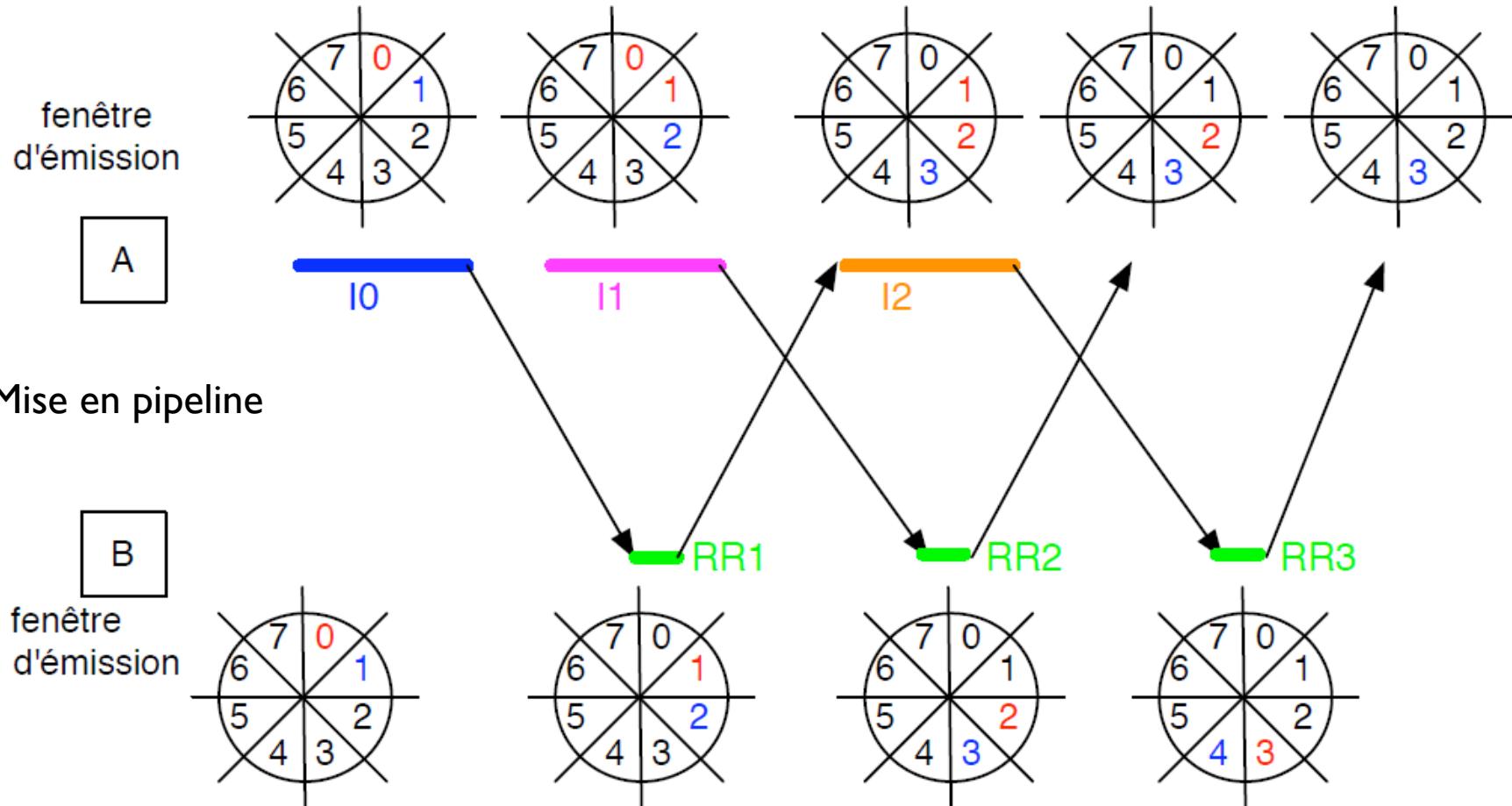


La tempo. doit être paramétrée en fct du débit et de liaison

Nécessite une identification de l'acquittement...

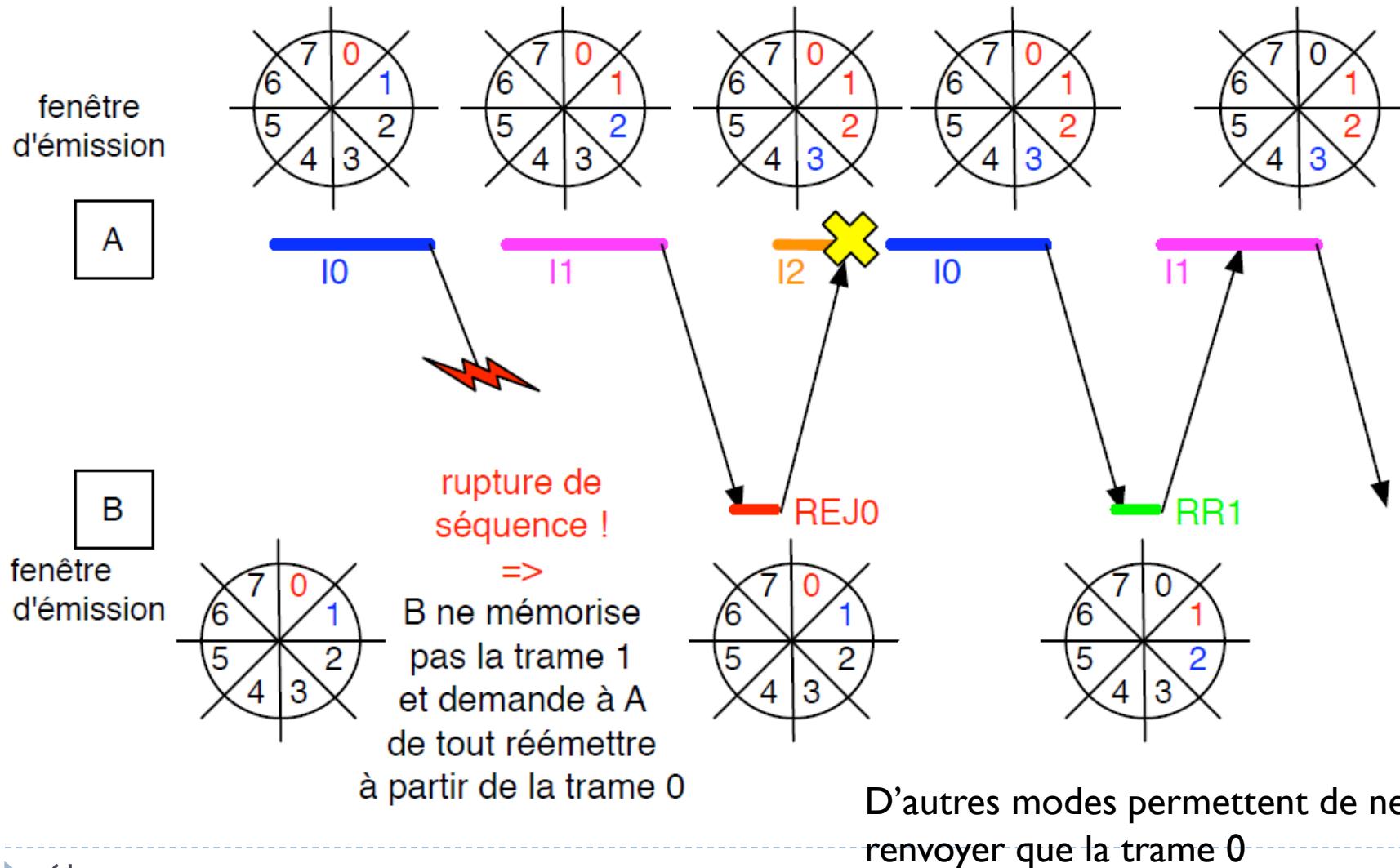
Couche 2 – Liaison

Fenêtre d'anticipation – exemple avec une fenêtre de 3 envoi max.



Couche 2 – Liaison

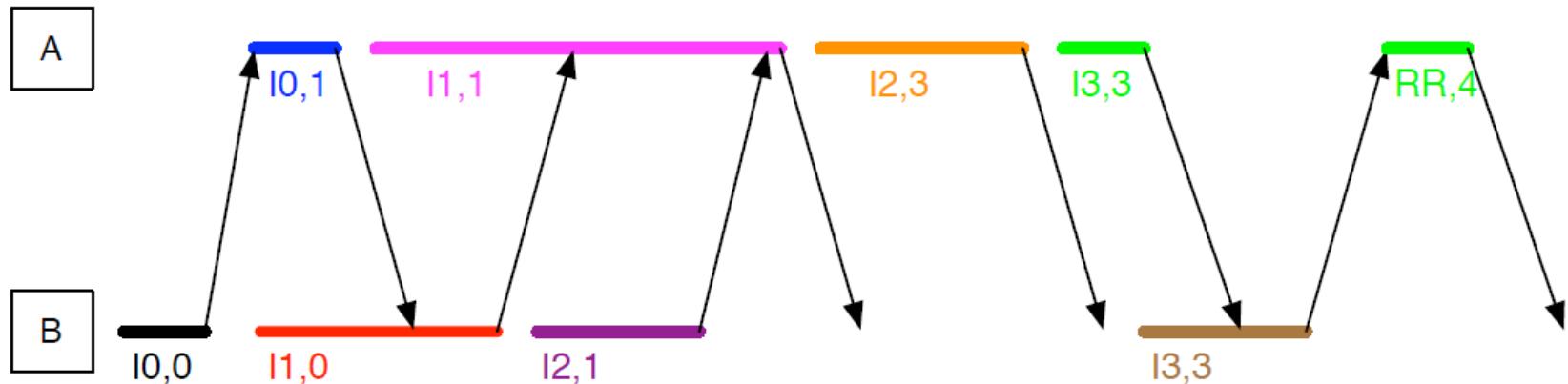
Fenêtre d'anticipation – Go Back N



Couche 2 – Liaison

Piggy Backing

- ▶ Supposons que l'échange soit bidirectionnel. Dans ce protocole, les trames d'information vont aussi jouer le rôle de trames de supervision. Pour cela, il suffit d'ajouter un champs supplémentaire acquittant les trames émises dans le sens opposé :



Avec une fenêtre d'anticipation égale à 3.

Couche 2 – Liaison Ethernet

« À l'origine, Ether est un dieu primordial de la mythologie grecque, personnifiant les parties supérieures du ciel, ainsi que sa brillance ...» [wikipedia](#)

Historiquement présent dans les LANS, c'est le protocole de couche 2 le plus largement répandu aujourd'hui (LAN, MAN, WAN).

Les SAN, réseaux de Stockage de données sont les derniers à passer sur Ethernet.

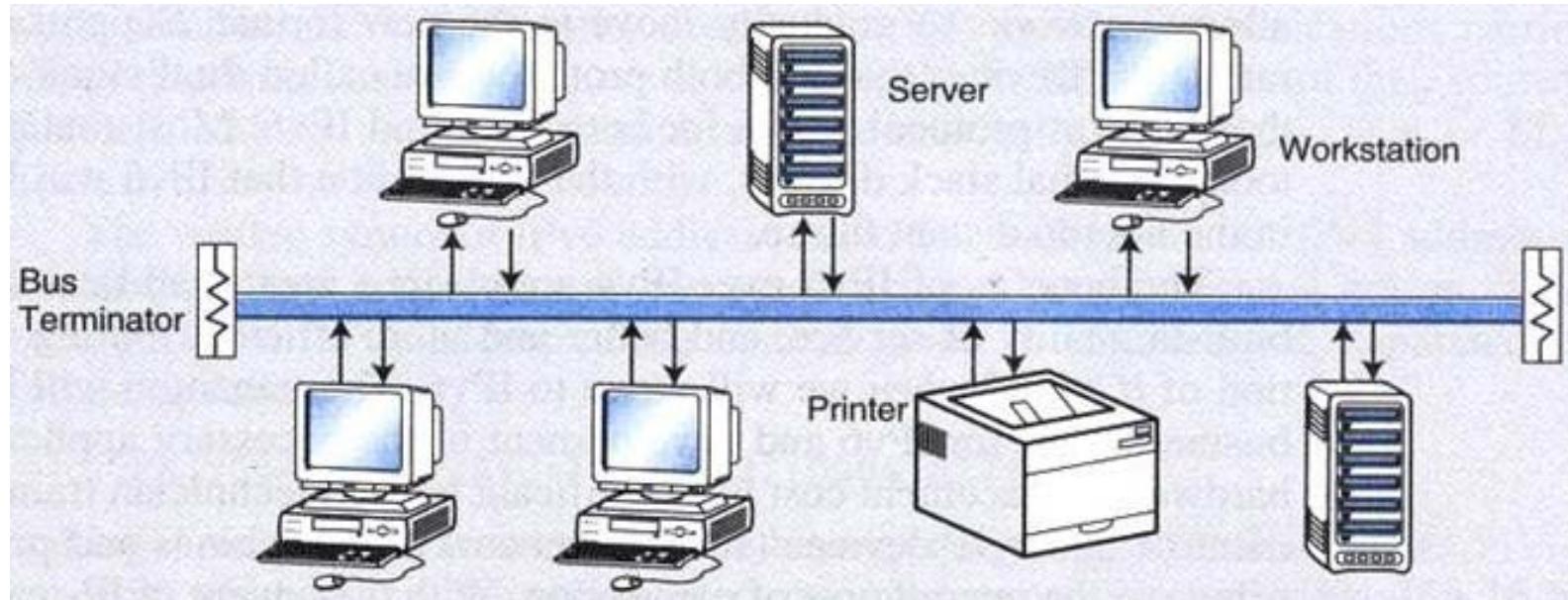
Année	Norme IEEE	Ethernet
1983	802.1 – 802.3	CSMA/CD à 10Mbit/s
1986	802.3c	Hub segmentation
1990	802.1D	Switched Ethernet
1995	802.3u	Fast Ethernet 100Mbit/s
1997	802.3x	Full Duplex
1998	802.3z	Gigabit Ethernet
2000	802.3ad	Link aggregation
2002	802.3ae	10 Gigabit Ethernet
2010	802.3ba	100 Gigabit Ethernet
2020	...	Terabit Ethernet

Couche 2 – Liaison

Méthodes d'accès au média - MAC

Réseau à **diffusion**, contrôle **des collisions** : exemple Ethernet (1983)

Algorithme de contrôle CSMA/CD (Collision Detection)



Mode quasiment obsolète dans les réseaux filaires

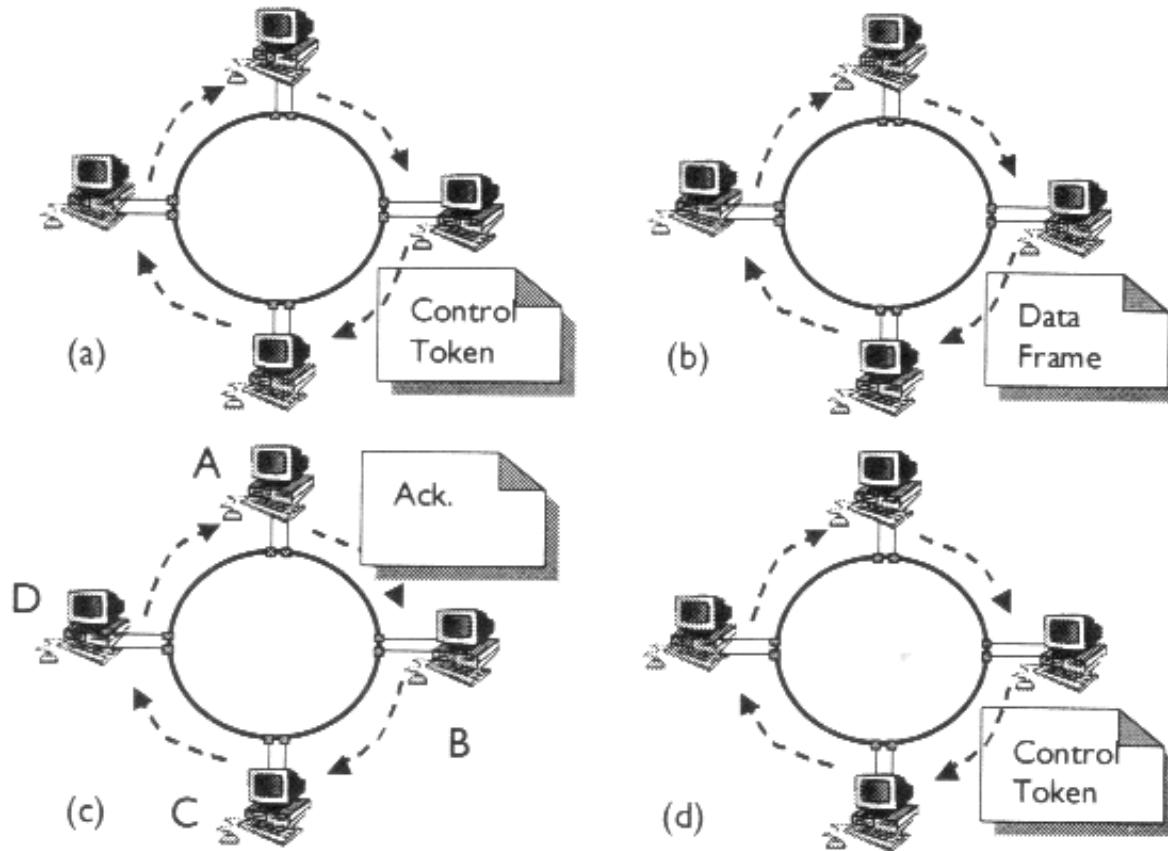
Mais reste assez proche de celui existant sur le WIFI : CSMA/CA (Collision Avoidance)

Couche 2 – Liaison

Méthodes d'accès au média - MAC

Réseau à **diffusion**, contrôle **centralisé** : exemple le Token Ring (IBM 1980)

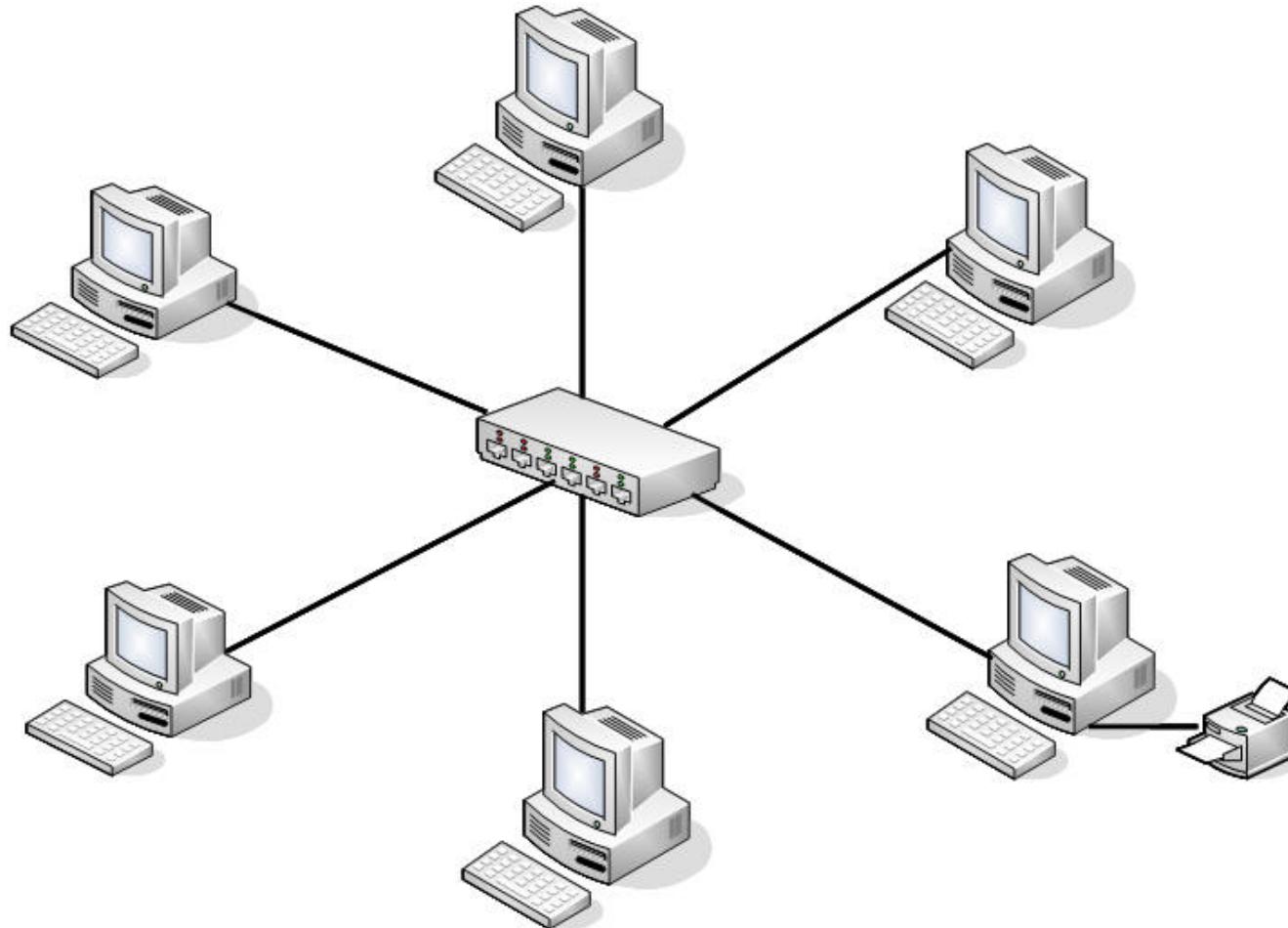
Obsolète



Couche 2 – Liaison

Méthodes d'accès au média - MAC

Réseau **commuté** : aujourd'hui



Couche 2 – Liaison

Trame Ethernet v2

8 (octets)	6	6	2	46 à 1500	4
Préambule	Adresse Destination	Adresse Source	Ether Type	Données	CRC

- ▶ Taille minimale 64 octets (512bits)
- ▶ Taille maximale 1500 octets (>9000 en jumbo frame)
- ▶ Adresses Source et Destination : adresse MAC

Que manque t'il ???

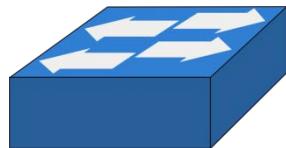
- ▶ Ethernet ne s'occupe pas du contrôle du dialogue... Il laisse ce travail aux protocoles de couche supérieure

Couche 2 – Liaison Adresses MAC

- ▶ Adresse unique pour chaque interface
- ▶ Adresse Ethernet MAC = Medium Access Control ou
Adresse physique
- ▶ 6 octets soit 48 bits :
 - ▶ ID Constructeur ; N° de série
 - ▶ Adresses multicast : premier bit à 1
 - ▶ Adresse broadcast : tous les bits à 1, FF:FF:FF:FF:FF:FF.
- ▶ Notation en hexadécimal 00:11:22:AA:BB:CC

Couche 2 – Liaison Adressage MAC

- ▶ Diffusion des adresses Ethernet (@) en broadcast dans un domaine de diffusion
- ▶ Chaque machine enregistre les adresses reçues dans une mémoire : **table de commutation**.



Adresse MAC	Interface physique
00:11:22:33:44:55	Giga Ethernet 0/1
00:11:22:33:44:AA	Giga Ethernet 0/2
00:22:33:55:44:AA	Giga Ethernet 0/3
00:AA:BB:CC:DD:AA	Ten Giga Ethernet 1/1
00:AA:BB:CC:DD:AB	Ten Giga Ethernet 1/1
00:AA:BB:CC:DD:AC	Ten Giga Ethernet 1/1
00:AA:BB:CC:DD:AD	Ten Giga Ethernet 1/1

Couche 2 – Liaison Adressage MAC

- ▶ Plus le réseau est étendu :
 - ▶ Plus de risque d'inondation de broadcast
 - ▶ Plus la taille de la table de commutation est importante. Risque de saturation des mémoires :
 - ▶ @Ethernet sur 48bits : 2^{48} @ possibles
- ▶ Besoin de segmenter les réseaux

Couche 2 – Liaison

Cas pratique

- ▶ Trouver l'adresse MAC de votre PC :
- ▶ Trouver le fabricant de cette carte :
- ▶ Aller sur : http://www.coffer.com/mac_find/

Couche 2 – Liaison Ethernet – méthode d'accès CSMA/CD

Origine du protocole : ALOHAnet à Hawaï (radio)

CSMA/CD : Carrier Sense Multiple Access / Collision Detection

Lorsqu'un ordinateur veut envoyer de l'information, il obéit à l'algorithme suivant :

1. Si le média n'est pas utilisé, commencer la transmission, sinon aller à l'étape 4 ;
2. *[transmission de l'information]* Si une collision est détectée, continuer à transmettre jusqu'à ce que le temps minimal pour un paquet soit dépassé (pour s'assurer que tous les postes détectent la collision), puis aller à l'étape 4 ;
3. *[fin d'une transmission réussie]* Indiquer la réussite au protocole du niveau supérieur et sortir du mode de transfert ;
4. *[câble occupé]* Attendre jusqu'à ce que le fil soit inutilisé ;
5. *[le câble est redevenu libre]* Attendre pendant un temps aléatoire, puis retourner à l'étape 1, sauf si le nombre maximal d'essais de transmission a été dépassé ;
6. *[nombre maximal d'essais de transmission dépassé]* Annoncer l'échec au protocole de niveau supérieur et sortir du mode de transmission.

Couche 2 – Liaison CSMA/CD

Ecouter avant de parler

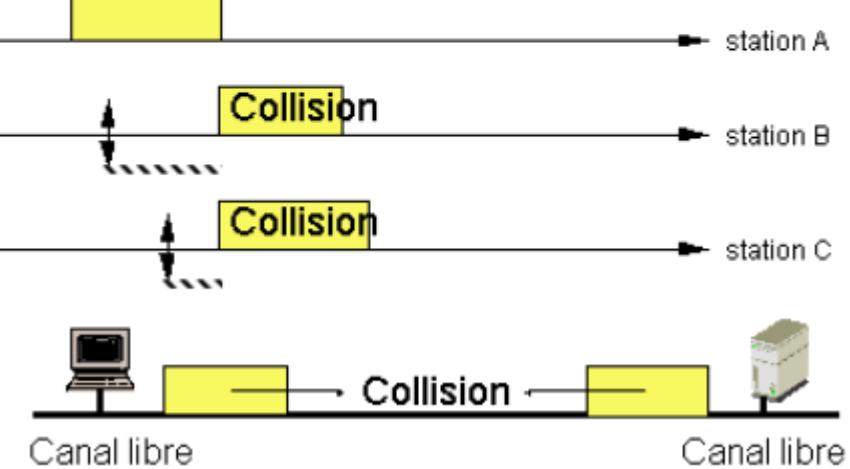
- ▶ Si canal libre : émettre
- ▶ Si canal occupé : attendre



Collisions encore possibles

- ▶ Entre deux stations
- ▶ Entre deux stations qui croient que le media est libre.

Problème lié au temps de propagation.



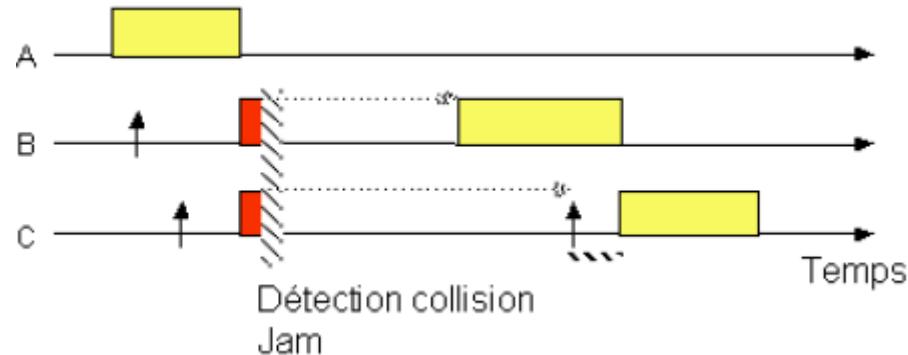
Couche 2 – Liaison CSMA/CD

Il faut donc détecter les collision

- ▶ La station continue à écouter pendant qu'elle émet

Si détection collision

- ▶ Interruption de la transmission
- ▶ Emission jam (signal de brouillage)
- ▶ Délai de retransmission aléatoire tiré dans $[0,2n[T]$
 - ▶ $n = \text{nb de collisions successives}$ (on garde 10 max)
 - ▶ $T = \text{temps d'émission de 512 bits (51,2 } \mu\text{s à 10Mbps)}$.
 - ▶ Algorithme de ralentissement en cas de congestion.



Couche 2 – Liaison

CSMA/CD – Limitations de distance

Taille minimale d'une trame 64 octets.

→ TRTD \leq 512 temps bit

Plus le débit augmente, plus la distance maximale entre les stations diminue :

- ▶ 51,2 µs à 10Mbps \rightarrow 5,12km
- ▶ 5,12 µs à 100Mbps \rightarrow 512m
- ▶ 0,512 µs à 1Gbps \rightarrow 5,12m

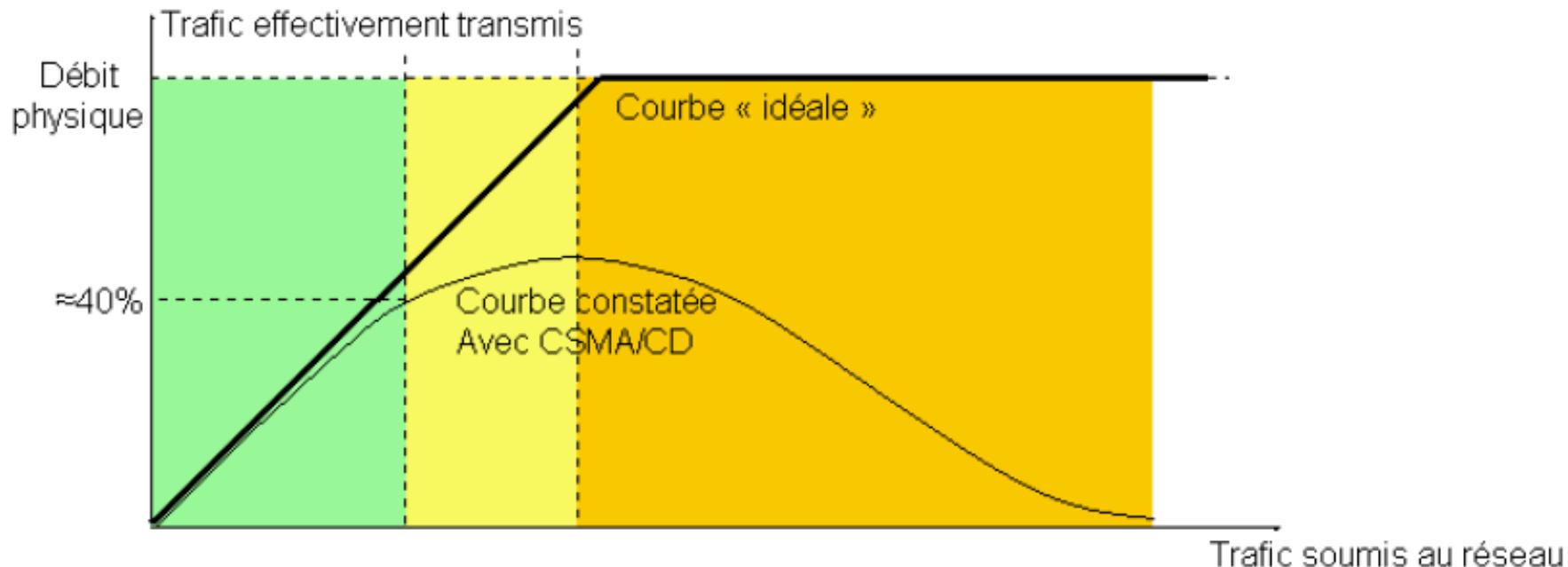
*Vitesse de propagation C = 200.000 km/s

Détermine le domaine de collision

Couche 2 – Liaison CSMA/CD – tenue à forte charge

Plus le trafic augmente, plus il y a de collisions

- ▶ Les collisions encombrent le réseau
- ▶ Plus il y a de collisions, plus il y a de collisions...
- ▶ A forte charge, le réseau finit par s'effondrer.



Couche 2 – Liaison

Bilan

- ▶ Les collisions ont un gros impact sur les performances
- ▶ Il faut segmenter le réseau, les espaces de collisions, par des matériels actifs ‘intelligents’.
 - ▶ Ponts : segmentent les domaines de collisions
 - ▶ Commutateurs :
 - ▶ 1 prise 1 machine : Plus d'espace de collisions.
 - ▶ Routeurs : Segmentation du **domaine de diffusion**.
- ▶ Bilan

Avantages :

- Réduction des collisions,
- Pas de contraintes de distance,

Inconvénients :

- nécessite un contrôle des flux pour ne pas saturer les mémoires présentes dans les commutateurs.
- plus onéreux.

Couche 2 – Liaison Ethernet commuté

▶ Problème des boucles

- ▶ Le rôle des équipements de commutation est de répéter les trames jusqu'à la machine de destination.
- ▶ Dans une boucle, les trames peuvent tourner à l'infini.



➔ Mécanismes de coupure de boucle (Spanning Tree) par extinction de ports ou de suppression des trames déjà vues (plus utilisé).

Couche 2 – Liaison

Notions de Vlans

- ▶ Limite la propagation des diffusions
- ▶ Renforce la sécurité
- ▶ Pour donner de la flexibilité à l'administration réseau
 - ▶ Dépasser les limites physiques (géographiques) d'un site
 - ▶ Création de vlan par type de service dans une entreprise :
 - Commercial,
 - Technique,
 - Direction

Couche 2 – Liaison

Notions de Vlans

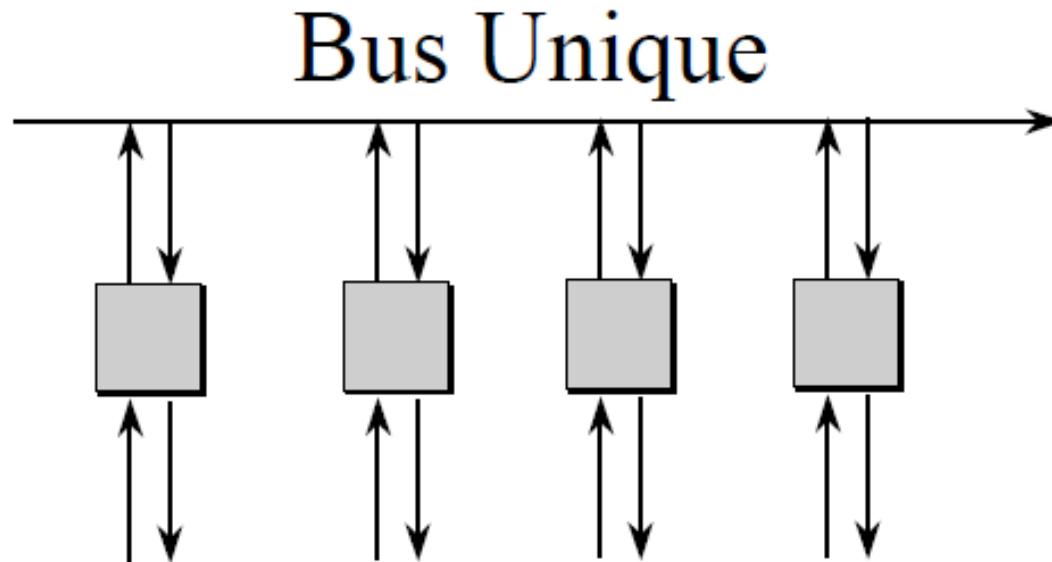
Trame ethernet modifiée [[modifier](#) | [modifier le code](#)]

adresse MAC dst.	adresse MAC src.	Tag (inséré)	Taille de la trame/EtherType	Data	FCS (modifié)
------------------	------------------	---------------------	------------------------------	------	----------------------

Le champ FCS est recalculé après l'insertion de la balise de VLAN.

- ▶ Plusieurs critères de création de Vlans :
 - ▶ par ports
 - ▶ Par adresse MAC
 - ▶ Par sous-réseau (niv. 3)
 - ▶ Par application
- ▶ Vlans peuvent être assimilés au VPN

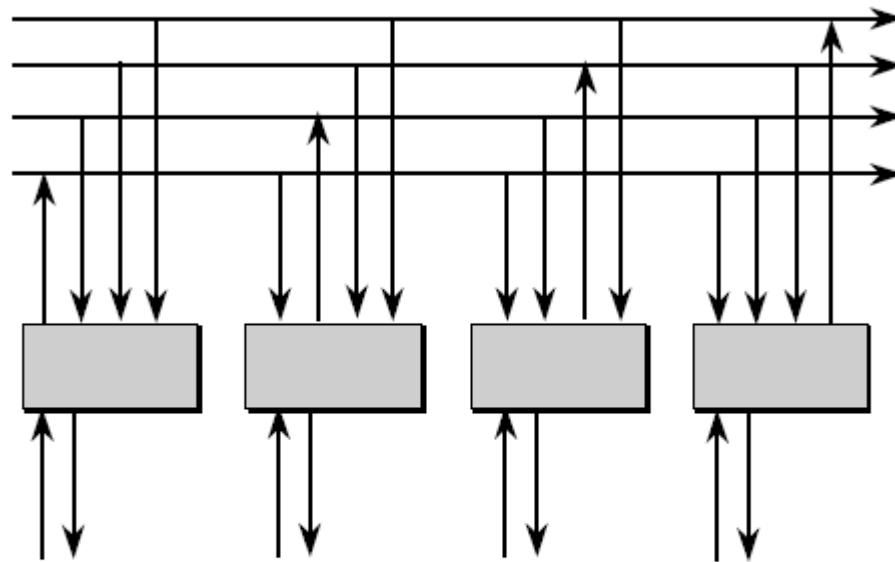
Couche 2 – Liaison Commutateurs Ethernet – Structure



- Le plus simple
- 1–10 Gbps
- Multicast facile
- Blocage si over-subscription du bus

Couche 2 – Liaison Commutateurs Ethernet - Structure

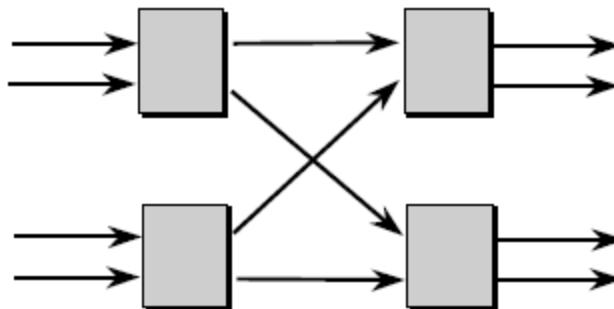
Bus Multiple



- Contrôle du blocage plus complexe
- Vitesse du Bus généralement supérieure au débit des portes
- Débit comparable au bus unique—10 Gbps
- Multicast facile

Couche 2 – Liaison Commutateurs Ethernet - Structure

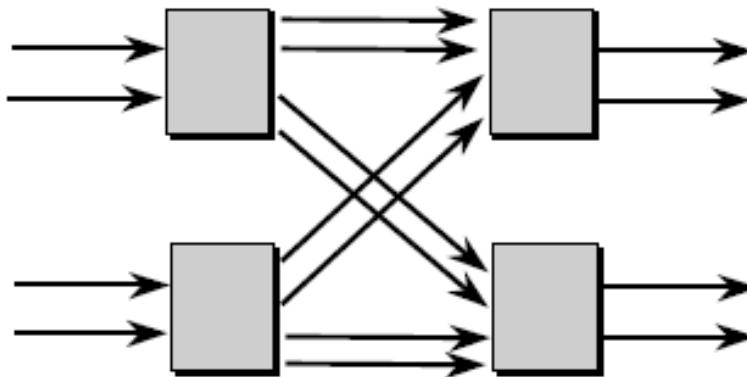
Commutation (Blocante)



- Circuiterie plus complexe
- Généralement basé sur ASICs
- Multicasts par copie de trame
- La matrice interne fonctionne à la vitesse des entrées
- Probabilité élevée de blocage
- Jusqu'à 200 Gbps

Couche 2 – Liaison Commutateurs Ethernet - Structure

Matrice non blocante



- Circuiterie plus complexe
- Généralement basé sur ASICs
- Multicasts par copie de trame
- La matrice interne fonctionne généralement à une vitesse supérieure à celle des entrées
- Faible probabilité de blocage

Couche 2 – Liaison

Commutateurs Ethernet – Files d'attente

Files d'attentes internes

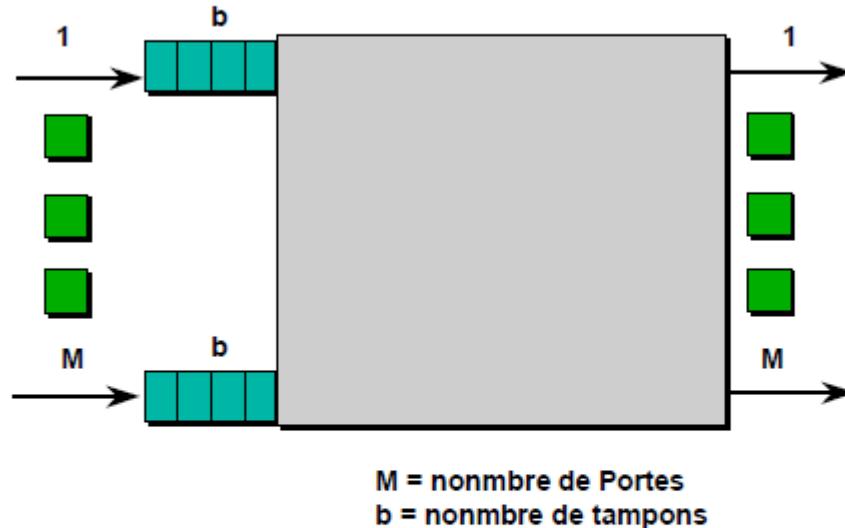


$M = \text{ombre de Portes}$

- Evolutivité facile
- Difficulté d'implémentation
 - Priorités des files d'attente
 - Taille des tampons
 - Multicast

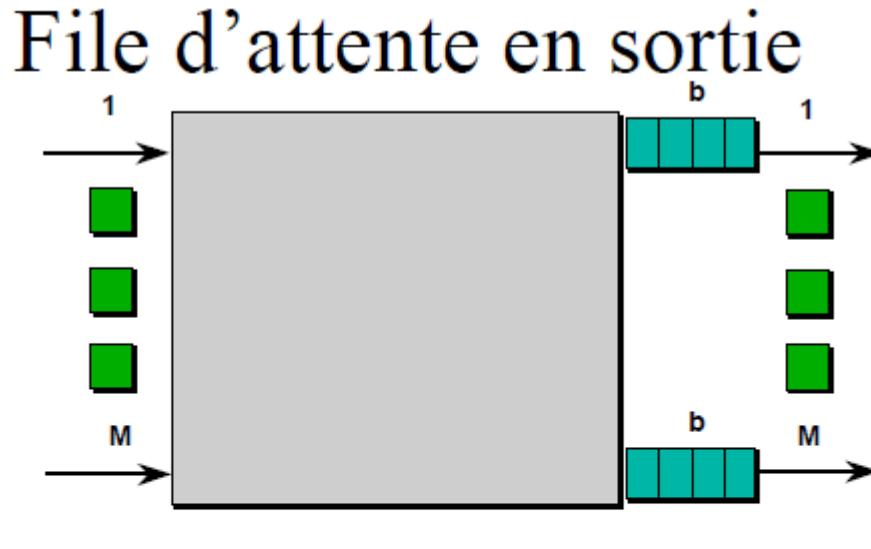
Couche 2 – Liaison Commutateurs Ethernet – Files d'attente

Files d'attente en entrée



- Simple à implémenter
- Blocage potentiel en entrée
- Limitation possible à 50–60% de la vitesses des portes

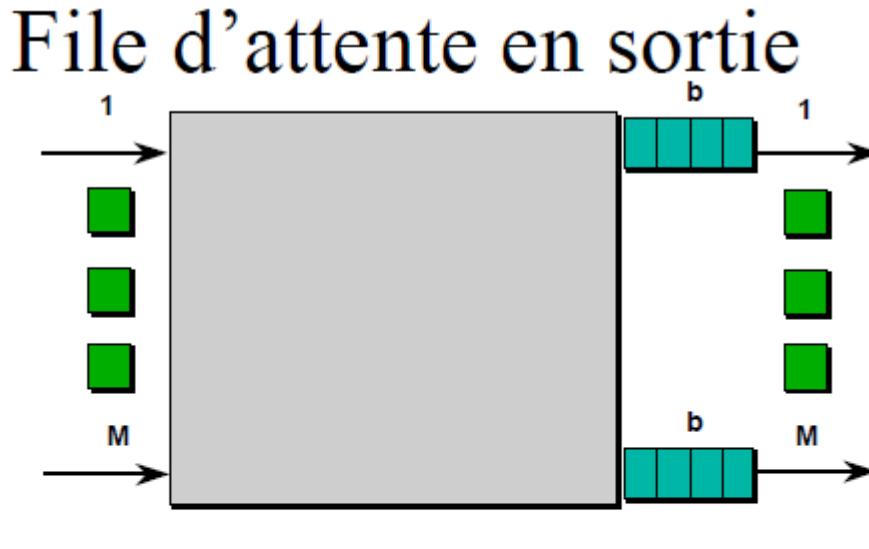
Couche 2 – Liaison Commutateurs Ethernet – Files d'attente



M = nombre de Portes
b = nombre de tampons

- Pas de blocage en entrée
- Risque de blocage des tampons sur surcharge des tampons (bouffées de trafic)

Couche 2 – Liaison Commutateurs Ethernet – Files d'attente

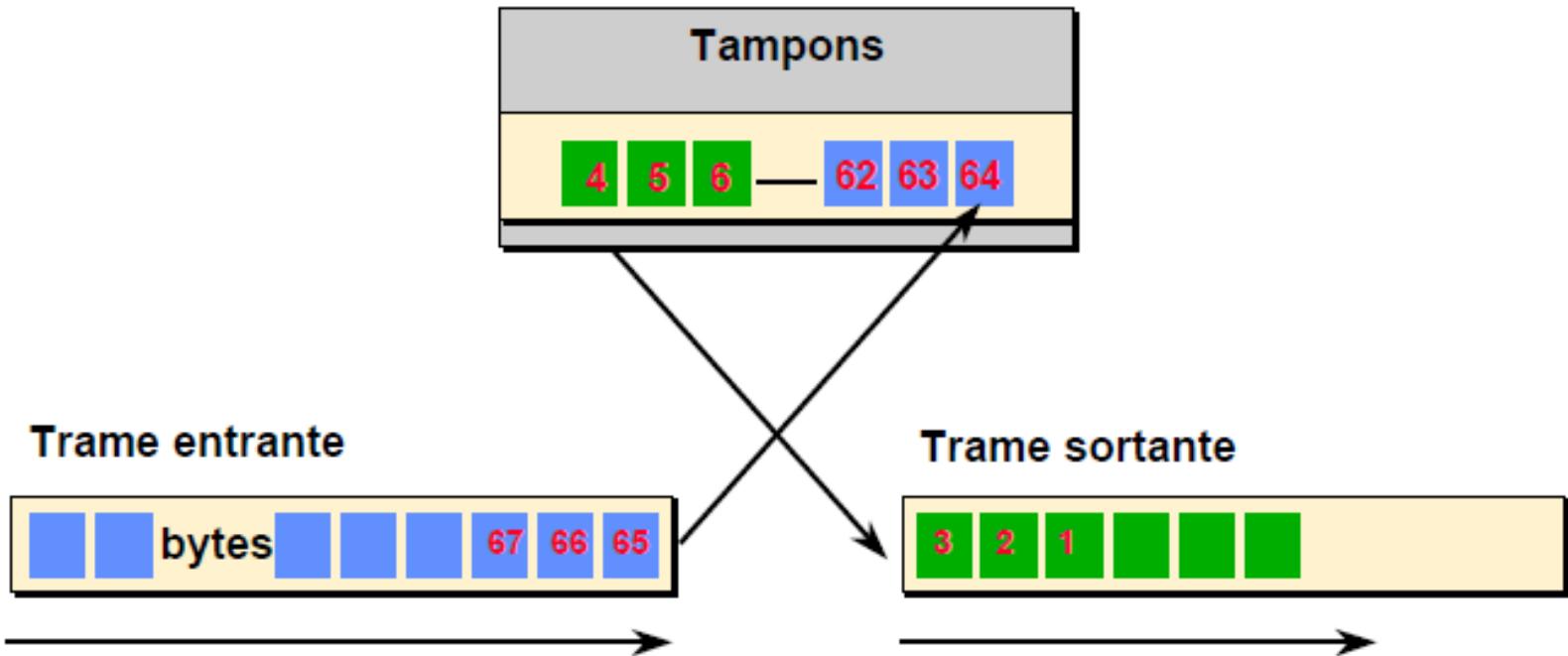


M = nombre de Portes
b = nombre de tampons

- Pas de blocage en entrée
- Risque de blocage des tampons sur surcharge des tampons (bouffées de trafic)

Couche 2 – Liaison Commutateurs Ethernet – Gestion des files

Cut-Through



Couche 2 – Liaison Commutateurs Ethernet – Gestion des files

- ▶ **Cut-Throught**
 - ▶ Très faible latence
 - ▶ Transmission des fragments résultants de collisions
 - ▶ Transmissions des trames en erreurs
 - ▶ Bilan : Excellent quand les contraintes temporelles sont plus importantes que le contrôle d'erreur.

- ▶ **Store & Forward**
 - ▶ Stockage de la trame entière avant commutation
 - ▶ Avantage : Contrôle des erreurs
 - ▶ Inconvénient : Latence augmentée

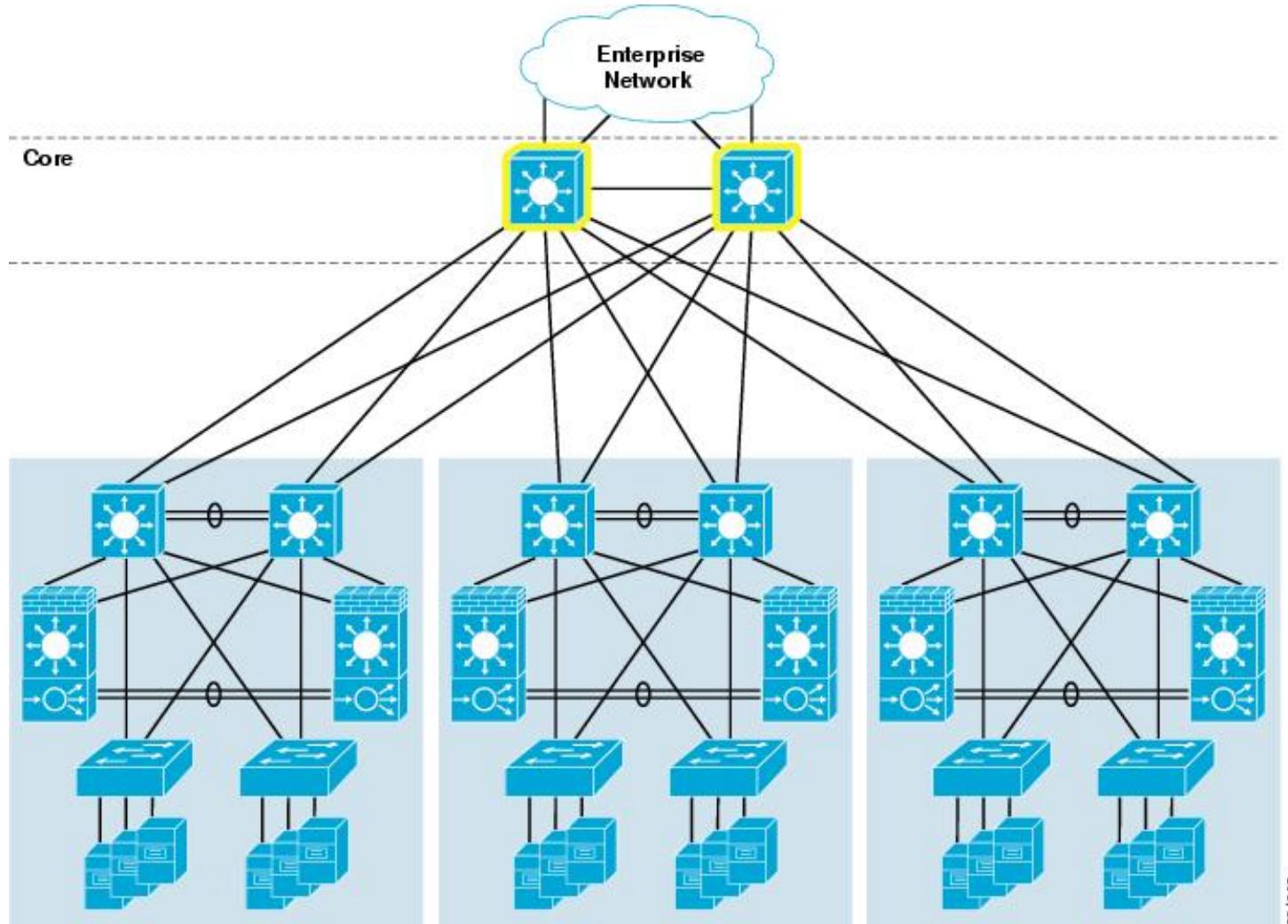
Couche 2 – Liaison

Exemple d'équipements

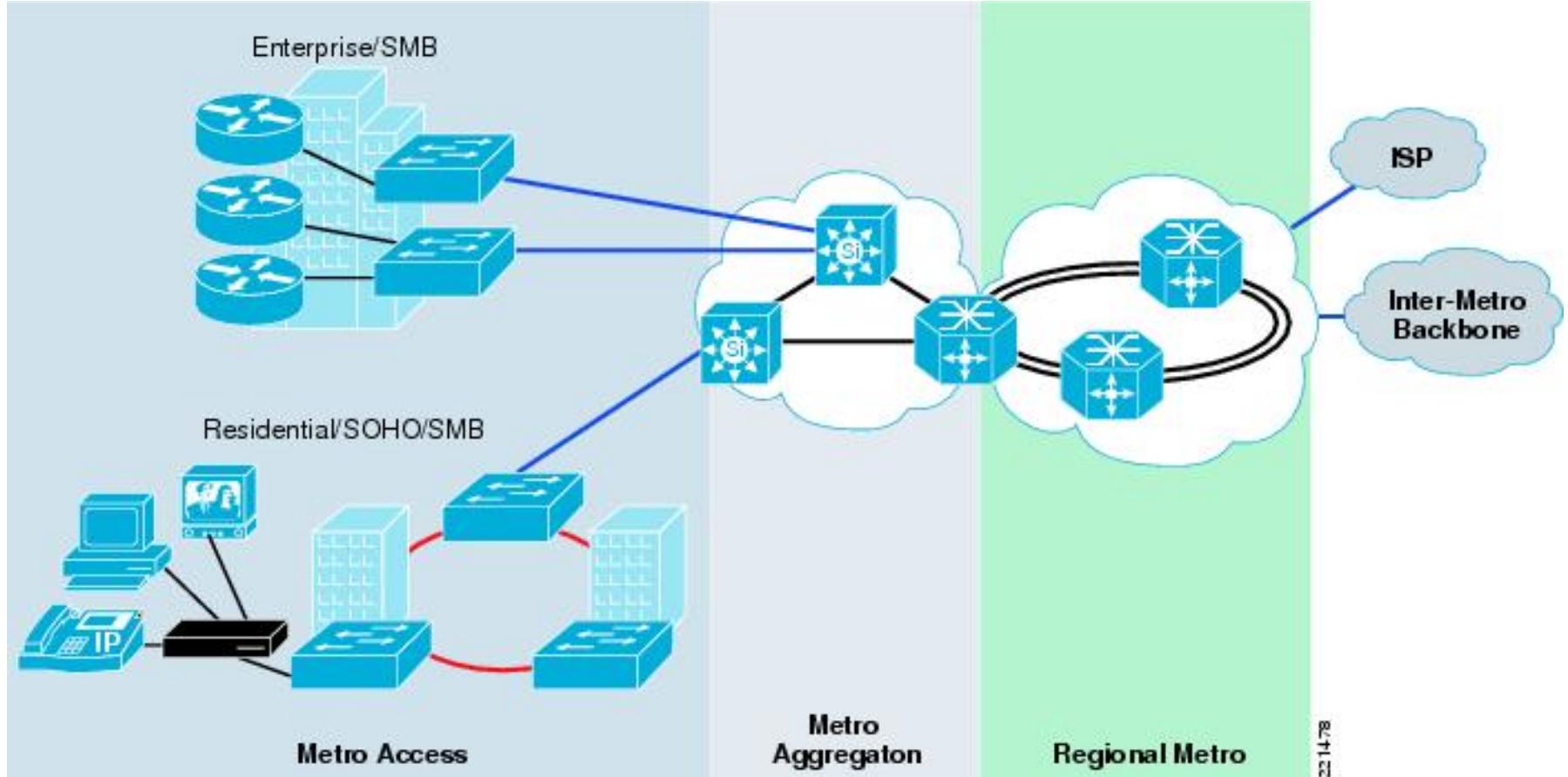


Couche 2 – Liaison

Architectures LAN – exemple datacenter



Couche 2 – Liaison Architectures WAN



Cours n°2

Questions ?

Les Réseaux

ENSAM

Karim Boudjemaïa

Études et Projets – RENATER

Karim.boudjemaia@renater.fr

Cours n°3

Plan du cours 3

- ▶ **Couche 3 - Réseaux**
 - ▶ Objectifs
 - ▶ Présentation IP
 - ▶ Routage et relayage
 - ▶ Notions d'interconnexion
 - ▶ Adressage IP
 - ▶ Sous-réseau, classes
 - ▶ Cas pratique
 - ▶ Protocole IP
 - ▶ Routage
 - ▶ Catégorisation
 - ▶ Routage interne
 - Type de algorithme de routage
 - OSPF
 - Cas pratique
 - ▶ Routage externe
 - BGP
 - Cas pratique
- ▶ **Mécanismes IP**
 - ▶ ARP
 - ▶ DHCP
 - ▶ DNS
 - ▶ NAT
- ▶ **Notion de Qualité de Services QoS**
 - ▶ Besoins
 - ▶ Approche par dimensionnement (DiffServ)
- ▶ **MPLS**
- ▶ Conclusion
- ▶ **Couche 4 – Transport**
 - ▶ TCP
 - ▶ Mécanisme de fenêtre glissante
 - ▶ UDP

Couche 3 – Réseaux Objectifs

- ▶ Le rôle de la couche 3 permet notamment de :
 - ▶ Acheminer les paquets vers leur destination,
 - ▶ Jouer un rôle sur la gestion des flux,
 - ▶ Jouer le rôle de passerelle entre réseaux,
- ▶ L'entité est le : **paquet**
- ▶ Matériels concernés : routeurs, switch/routeur

Couche 3 – Réseaux Objectifs

- ▶ Il existe plusieurs types de protocoles intervenant sur la couche 3. Exemples :
 - ▶ IPv4,
 - ▶ IPv6,
 - ▶ X25 : protocole crée par France Telecom et permettant de transporter les données du Minitel. Depuis 2012, ce protocole n'est plus utilisé.
- ▶ Dans le cadre de ce cours seul le **protocole IPv4**, sera présenté.

Couche 3 – Réseaux Internet Protocol - IP

- ▶ IP est un protocole qui se charge de l'acheminement des paquets pour des protocoles « clients » :
 - ▶ TCP : mode connecté,
 - ▶ UDP : mode non connecté
- ▶ Il fournit un système de remise de données optimisé sans connexion.
 - ▶ La fonctionnalité de somme de contrôle du protocole ne confirme que l'intégrité de l'entête IP.
 - ▶ Ainsi, seuls les protocoles de niveau supérieur sont responsables des données contenues dans les paquets IP (et de leur ordre de réception).
 - ▶ les paquets émis par le niveau 3 sont acheminés de manière autonome (datagrammes), sans garantie de livraison.

Couche 3 – Réseaux

Routage et relayage

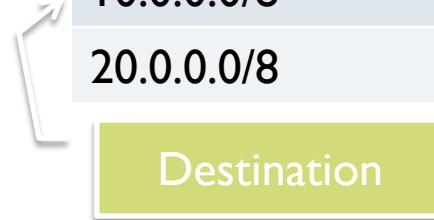
- ▶ Dans un réseau, acheminer les informations signifie assurer le transport des unités de données de leur point d'entrée vers un point de sortie du réseau désigné par son adresse.
 - ▶ Ce processus nécessite l'élaboration de techniques permettant de décider de l'itinéraire à suivre. L'ensemble de ces techniques constitue le **routage**.
- ▶ En pratique, chaque nœud recevant un paquet va décider localement vers quel nœud suivant le paquet sera transféré. Ainsi, de proche en proche, le transfert du paquet sera assuré de la source jusqu'au destinataire.
 - ▶ Cela s'appelle le **relayage** (forwarding).
- ▶ Informations nécessaires à chaque nœud pour prendre la « bonne » décision :
 - ▶ chaque paquet doit contenir une information précisant son destinataire;
 - ▶ des **table de routage et de relayage** enregistrées sur le nœud, construites à partir d'un **algorithme de routage**.

Couche 3 – Réseaux Routage et relayage

- ▶ Table de routage (Control Plane - CPU)

Adresse Internet	Nœud suivant (next hop)	coût
10.0.0.0/8	Routeur A	10
20.0.0.0/8	Routeur B	100

Destination

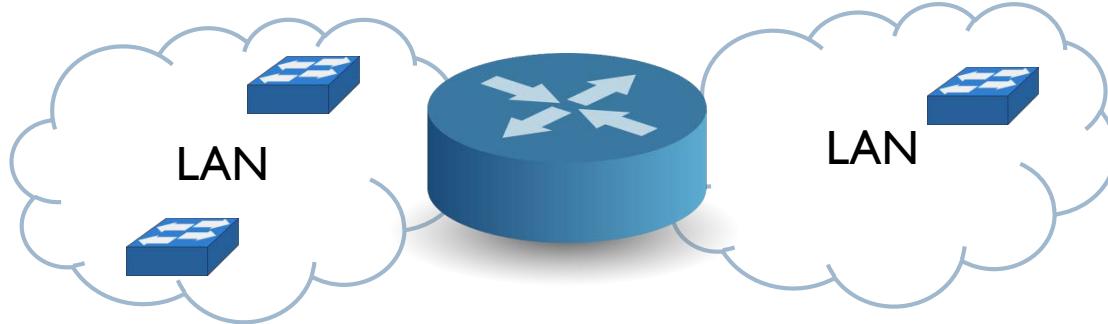


- ▶ Table de relayage (Forwarding Plane - ASICS)

Nœud	Adresse Internet	Adresse physique
Routeur A	10.0.0.1/8	00:11:22:33:44:55
Routeur B	20.0.0.1/8	00:AA:BB:CC:DD:AA

Couche 3 – Réseaux

Notions d'interconnexion réseaux



- ▶ Chaque LAN connaît ses propres adresses et commute les trames entre les machines :
 - ▶ On parle de **routage direct** (cf. protocole ARP)
- ▶ L'interconnexion entre ces réseaux est effectuée par un équipement de couche 3 qui sait **acheminer** le trafic entre les différents réseaux :
 - ▶ On parle de **routage indirect**

Couche 3 – Réseaux

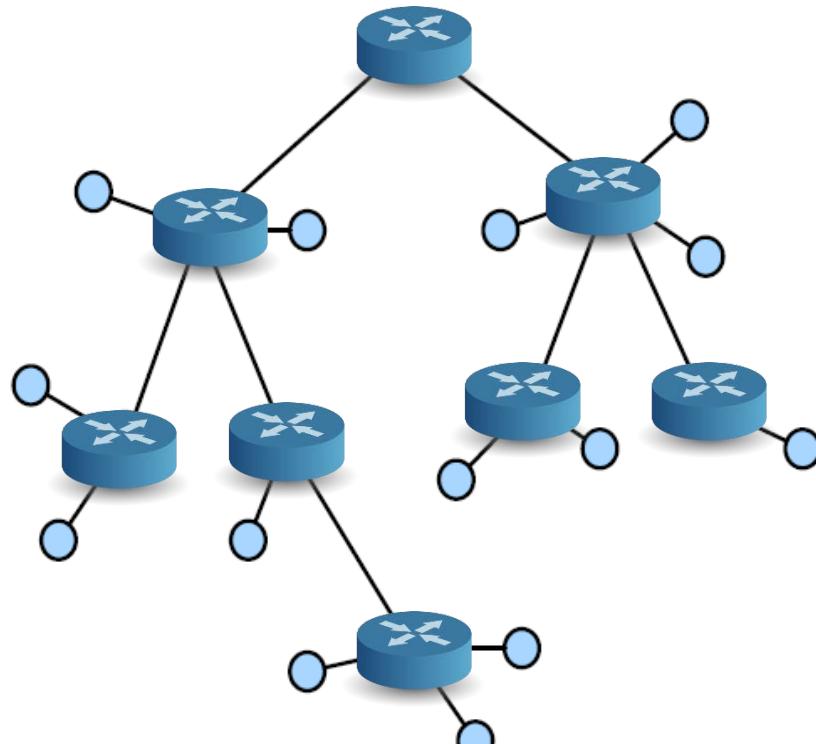
Notions d'interconnexion réseaux



- Le rôle du **routeur** est de connaître les adresses des réseaux auxquels il est connecté et d'orienter le trafic entre ces réseaux.

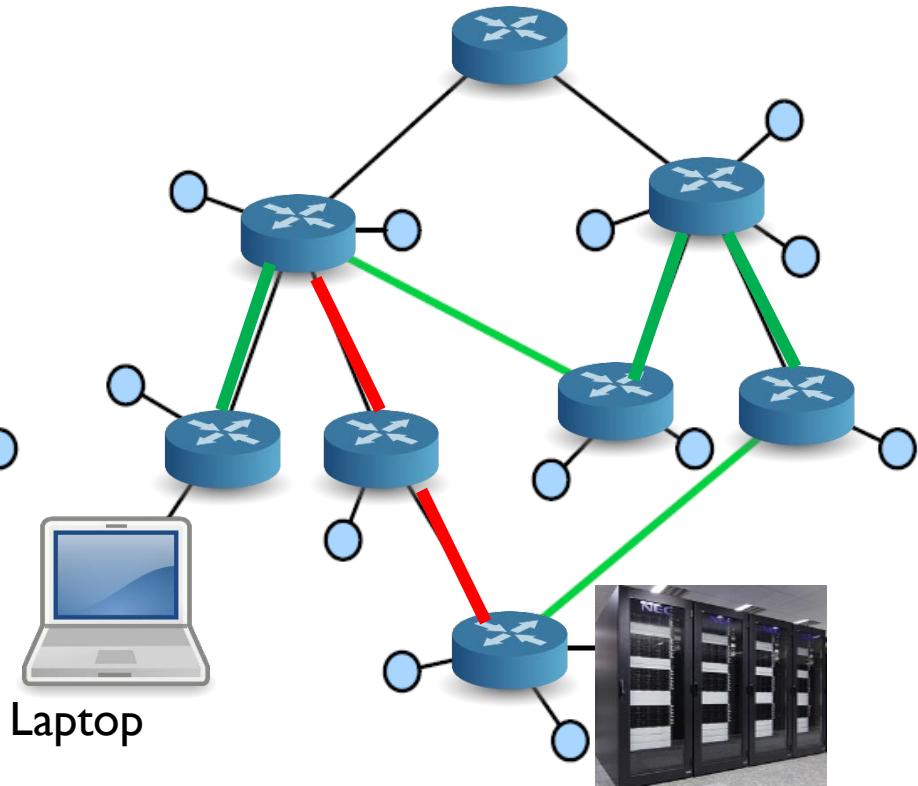
Couche 3 – Réseaux

Notions d'interconnexion réseaux



réseau arborescent
(hiérarchique)

Un seul chemin entre deux noeuds



Laptop

réseau maillé

Serveurs

Eventuellement plusieurs chemins
entre deux noeuds

Couche 3 – Réseaux Adressage IPv4

Une adresse IPv4 (notation décimale à point)

172 . 16 . 254 . 1



10101100 . 00010000 . 11111110 . 00000001



1 octet = 8 bits

32 bits ($4 * 8$), ou 4 octets

Couche 3 – Réseaux Sous-Réseau

- ▶ Un identificateur de réseau (NET-ID)
- ▶ Un identificateur d'hôte (HOST-ID).

NET-ID + HOST-ID = une adresse IP **unique** sur le réseau.

- ▶ Comment trouver l'adresse du sous réseau (Net-id) ?
 - ▶ Nécessite une info. supplémentaire : masque de réseau
 - ▶ Par ex.: 172.16.254.1/24
- ▶ Quel est l'adresse de broadcast (diffusion) ?

Couche 3 – Réseaux Sous-réseau

- ▶ Adresses particulières pour un réseau
 - ▶ 1^{ère} adresse → adresse du réseau : 172.16.254.0
 - ▶ Dernière adresse → adresse de broadcast dans le réseau : 172.16.254.255
 - ▶ Masque de sous réseau



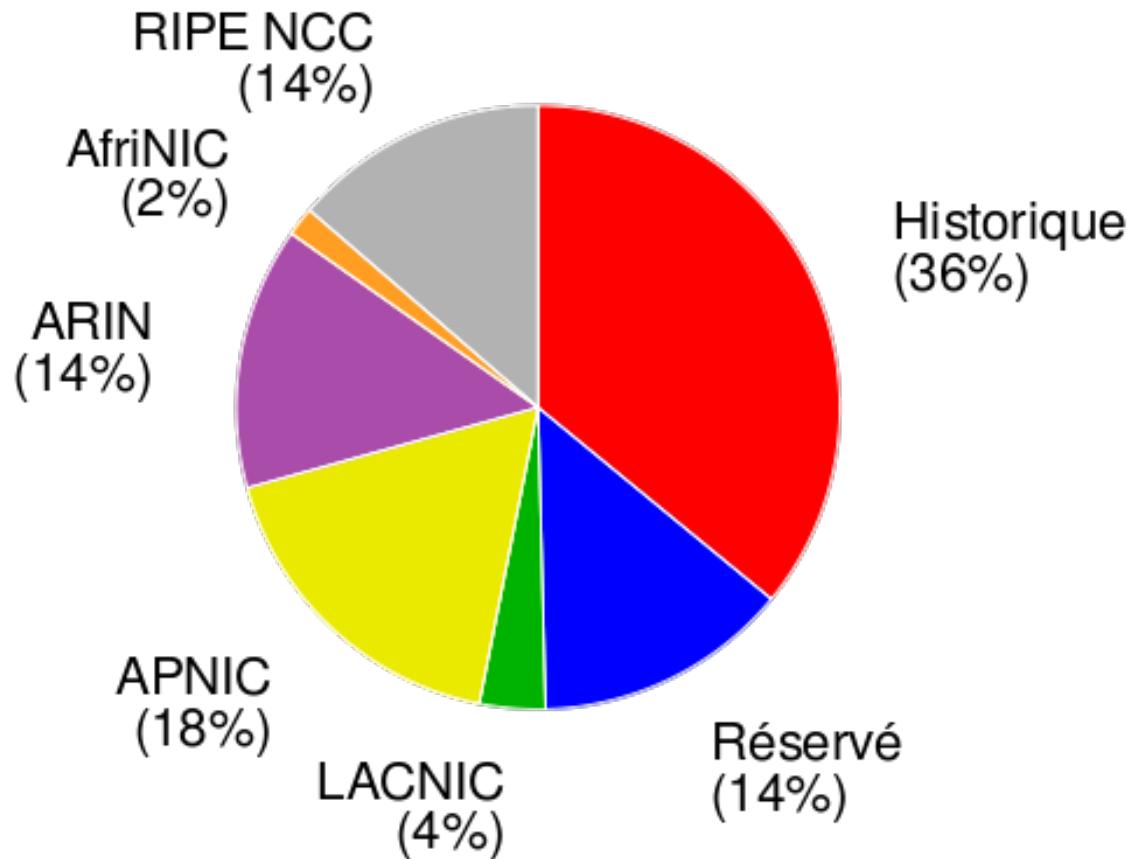
Feuille de calcul
Microsoft Excel

- ▶ Classless Inter-Domain Routing – CIDR :
 - ▶ Suppression des classes organisées par octet
 - ▶ Classe A = premier octet
 - ▶ Classe B = deuxième octet
 - ▶ Etc...
 - ▶ Utilisation de masque variable afin d'optimiser la répartition des adresses IPv4.
 - ▶ Possibilité de créer des sous-réseaux via un découpage d'une plage réseaux.
 - ▶ Agrégation de plage réseaux plus efficace

Couche 3 – Réseaux

Gestion des adresses IP

- ▶ Attribution des adresses par des organismes internationaux.
 - ▶ Les opérateurs achètent des blocs d'adresses.



Couche 3 – Réseaux

Adressage particulier

- ▶ Adressage Public
 - ▶ ROUTÉ sur Internet
 - ▶ Limite d'adressage « atteinte »
- ▶ Adressage Privé : cf. RFC1918
 - ▶ 10.0.0.0 à 10.255.255.255 : 10.0.0.0/8
 - ▶ 172.16.0.0 à 172.31.255.255 : 172.16.0.0/12
 - ▶ 192.168.0.0 à 192.168.255.255 : 192.168.0.0/16
- ▶ permet aux entreprises/particuliers de disposer d'un grand nombre d'adresses.
- ▶ NON ROUTÉ sur Internet
- ▶ Nécessite un mécanisme de 'Translation d'adresse' vers une IP publique pour sortir sur Internet.

Couche 3 – Réseaux

Cas pratique

- ▶ **Cas pratique :**
 - ▶ Trouver votre adresse IP :
 - ▶ Traduisez cette adresse en binaire :
 - ▶ De quel type est elle ?
- ▶ **Traduction binaire à décimal**
 - ▶ 11001010.10011100.00110111.00001111
 - ▶ 01010111.11100001.01010101.11110000
 - ▶ 11111111.11111111.11111111.11111111
- ▶ **Traduction décimal vers binaire**
 - ▶ 12.125.42.18
 - ▶ 224.0.0.9
- ▶ **Trouver votre adresse sous-réseau :**

Couche 3 – Réseaux

Cas pratique

- ▶ En tant qu'administrateur réseau d'une PME, vous êtes en charge de construire le réseau informatique. Votre PME compte 92 salariés répartis en plusieurs services :
 - ▶ 50 personnes au service production
 - ▶ 30 personnes au service commercial
 - ▶ 10 personnes au service des ressources humaines
 - ▶ 2 personnes à la Direction
- ▶ D'après la stratégie décidée par la Direction de l'entreprise, l'entreprise doit connaître une augmentation de son personnel pour accueillir jusqu'à 110 personnes au maximum.
 - ▶ A partir du bloc d'adresses vues précédemment (172.16.254.1/24) :
 - ▶ Définir une adresse de sous-réseau pour l'entreprise
 - Pour le service prod
 - Pour le service commercial
 - Pour les RH
 - Pour la Direction

Couche 3 – Réseaux Constat d'épuisement d'adresses IPv4 (1/2)

- **IPv4**

32bits : 4 294 967 296.

Derniers blocs d'adresses
allouées en 2012...

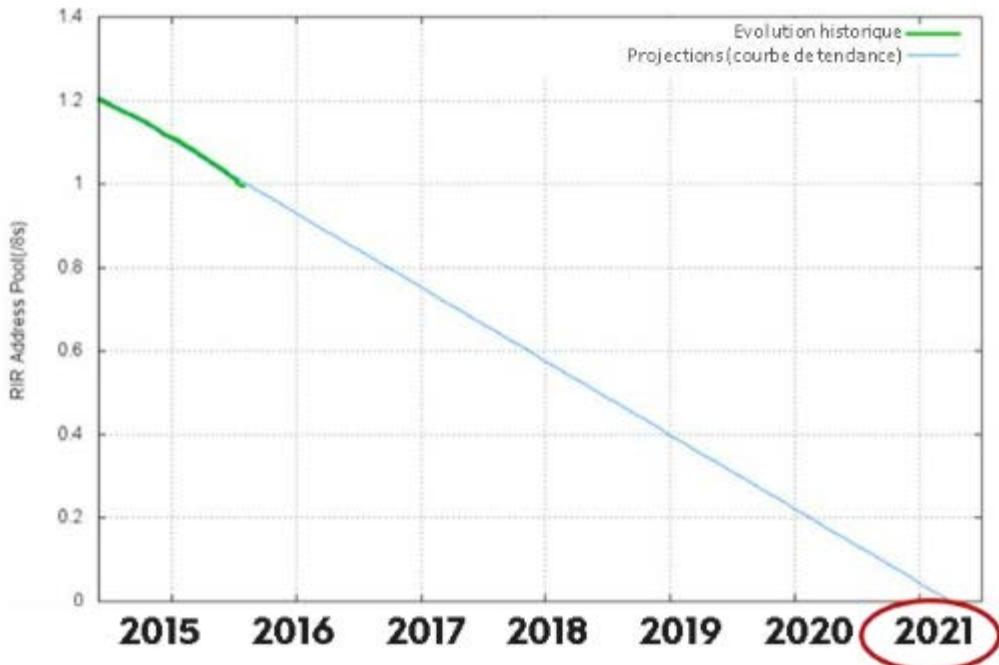


Figure 3 : Projection de l'épuisement des adresses IPv4 dans la région RIPE-NCC

Source : ARCEP

Couche 3 – Réseaux

Constat d'épuisement d'adresses IPv4 (2/2)

- Face à cette pénurie, les opérateurs ont eu d'abord recours à des solutions de contournement ou « workaround »
 - NAT : Network Address Translation

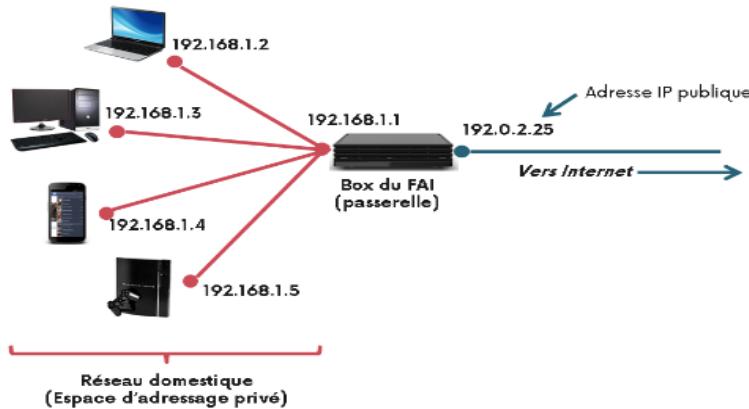


Figure 4 : Utilisation du NAT sur un réseau local

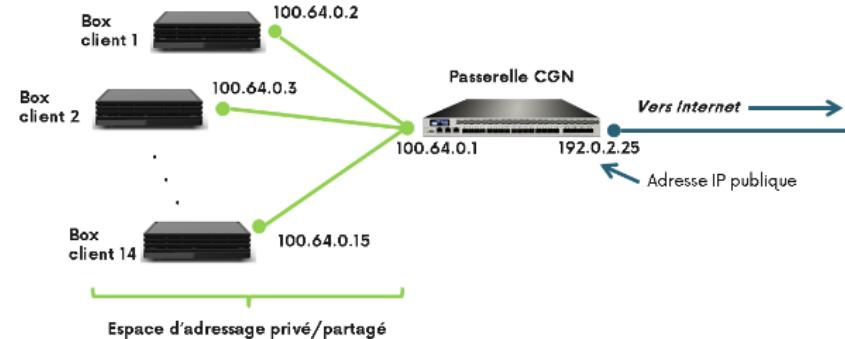


Figure 5 : Utilisation du CGN pour mettre plusieurs box derrière une passerelle

Inconvénients :

- Ajout d'un équipement passerelle : coût supplémentaire, maintenance
- Dysfonctionnement de certaines applications

Source : ARCEP

Couche 3 – Réseaux Vers IPv6

- ▶ IPv6
 - ▶ 128bits : $3,4 \cdot 10^{38}$:
 - ▶ Soit 667 millions de milliards d'adresses IP disponibles par mm² de la surface de la Terre
 - ▶ Répond à tous les besoins actuels et futurs (IoT)
- ▶ IPv6 « embarque » nativement des fonctionnalités supplémentaires (*corrigées depuis pour IPv4*) en matière de :
 - ▶ Qualité de service,
 - ▶ Sécurité,
 - ▶ Routage

Couche 3 – Réseaux Adressage IPv6

An IPv6 address (in hexadecimal)

2001:0DB8:AC10:FE01:0000:0000:0000:0000

↓ ↓ ↓ ↓ ↴
2001:0DB8:AC10:FE01:: Zeroes can be omitted

1000000000001:0000110110111000:1010110000010000:1111111000000001:
0000000000000000:0000000000000000:0000000000000000:0000000000000000

Couche 3 – Réseaux IPv6 : frein à l'adoption

- Multiplicité des acteurs impliqués,
- Compatibilité IPV6 d'un grand nombre d'équipements le long d'un grand nombre de réseaux traversés
- Lecture peu commode à l'homme

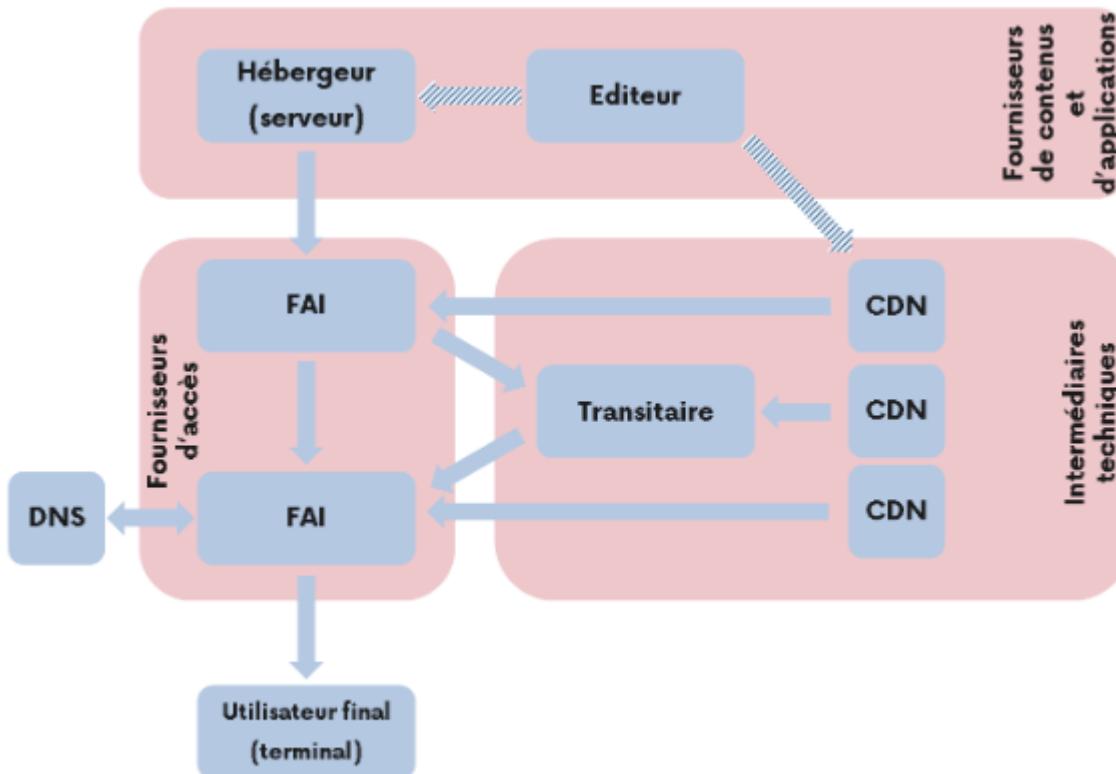


Figure 6 : Chaîne technique d'acheminement du trafic sur internet

Source : ARCEP

Couche 3 – Réseaux IPv6 : frein à l'adoption

En attendant IPV6...

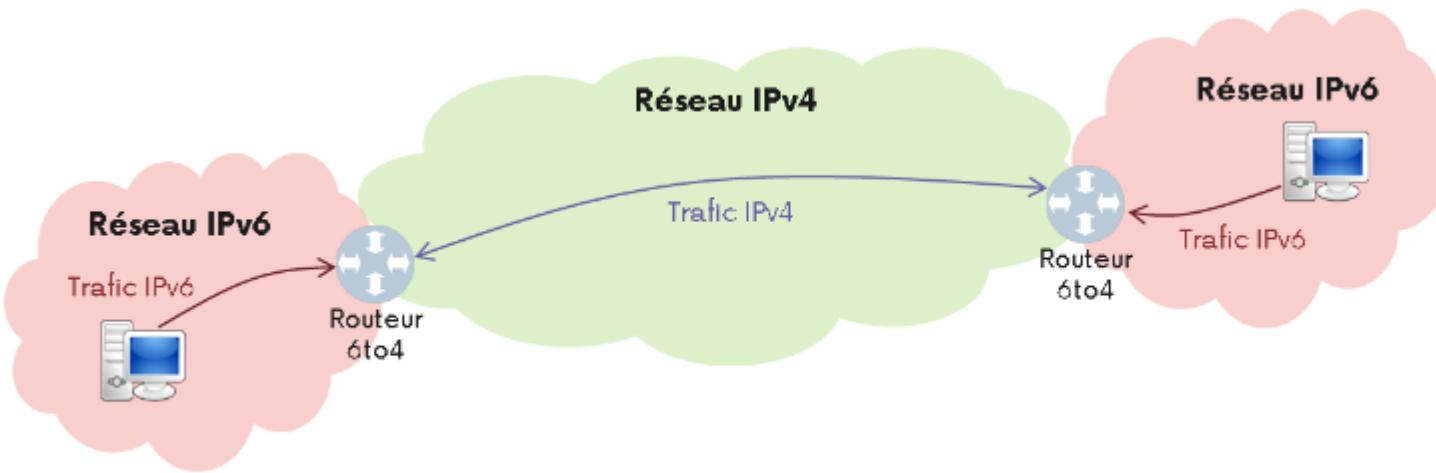
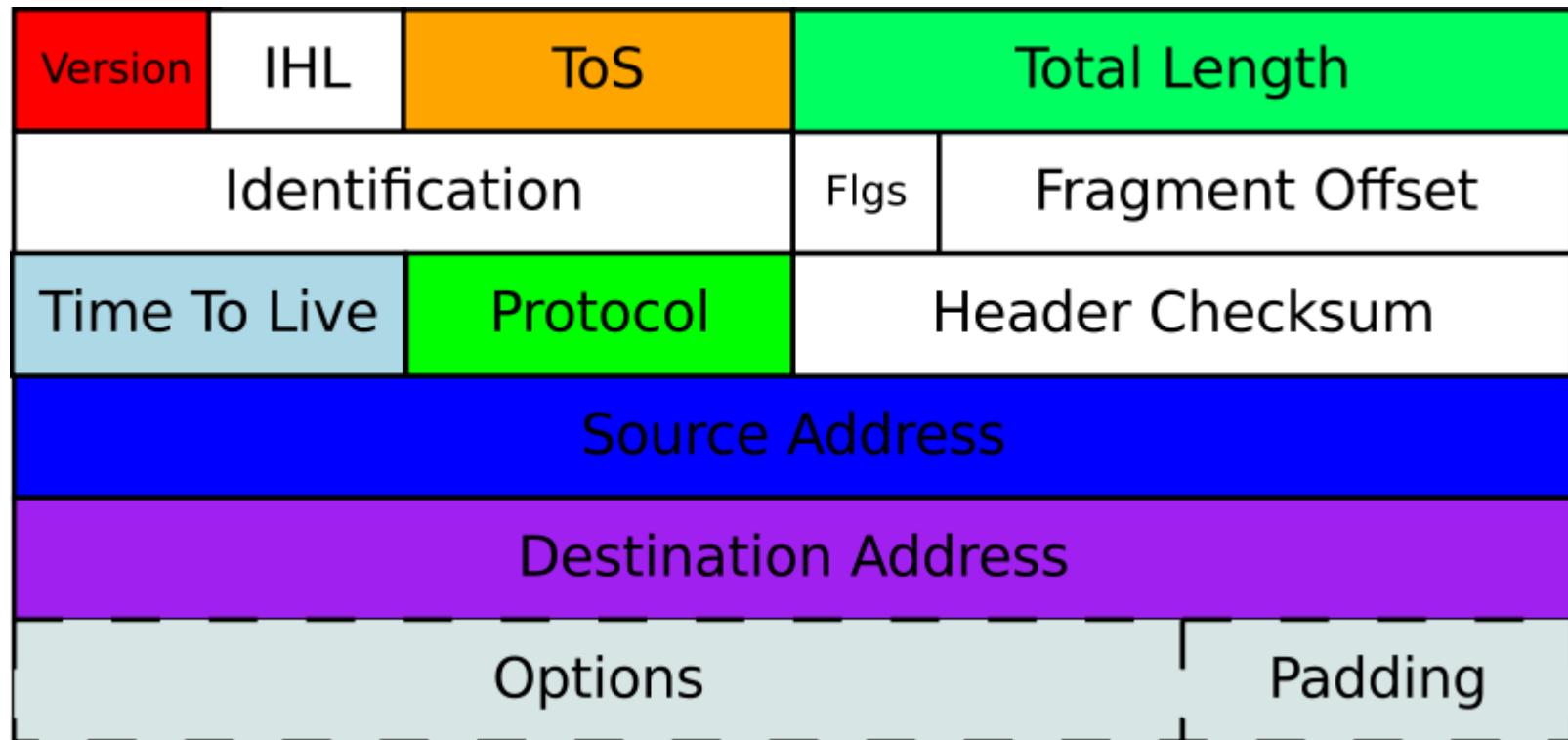


Figure 7 : Conversion en IPv4 lors d'une communication IPv6

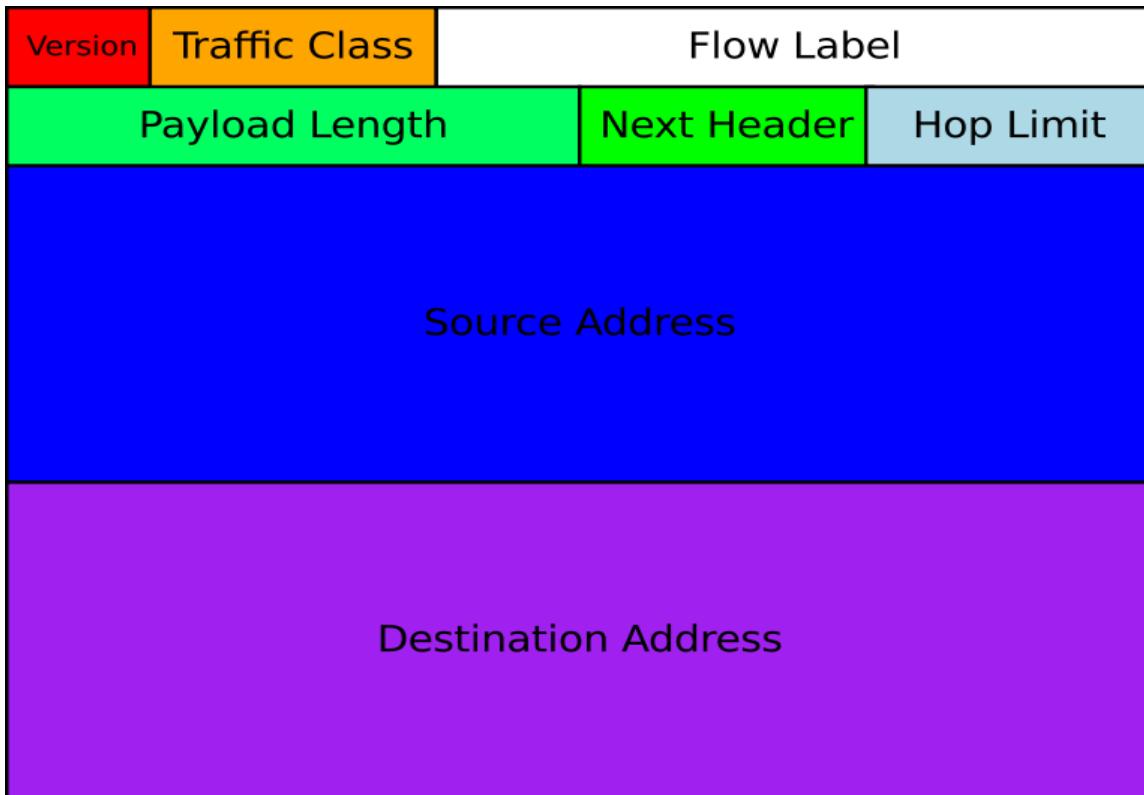
Source : ARCEP

Couche 3 – Réseaux

Protocole IPv4 – En tête



Flgs/Fragment offset: 16 bits, offset 20. Total length: 16 bits, offset 12. Header checksum: 16 bits, offset 40. Source/Destination address: 32 bits each, offset 48/56. Options: variable length, offset 64. Padding: variable length, offset 64 + Options length.



Couche 3 – Réseaux Protocole IPv6 - En tête

- Version = V6
- Traffic class : indique la qualité de service
- Flow label permet de nommer des flux dès la source et pouvant recevoir un traitement spécifique
- Payload length = Total length en v4
- Next header = Protocol en v4
- Hop limit = TTL
- Pas d'information sur la fragmentation

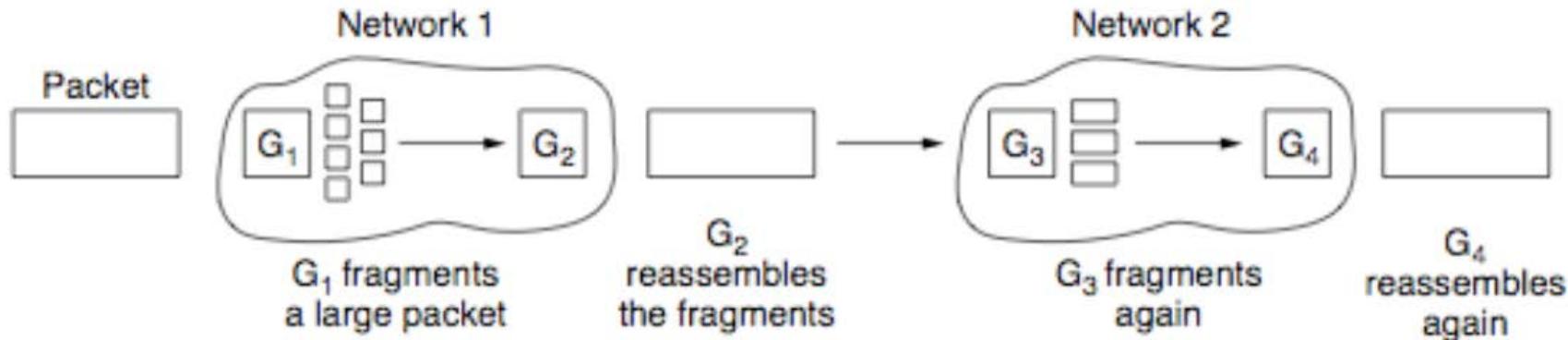
Couche 3 – Réseaux

Adaptation de la taille des données

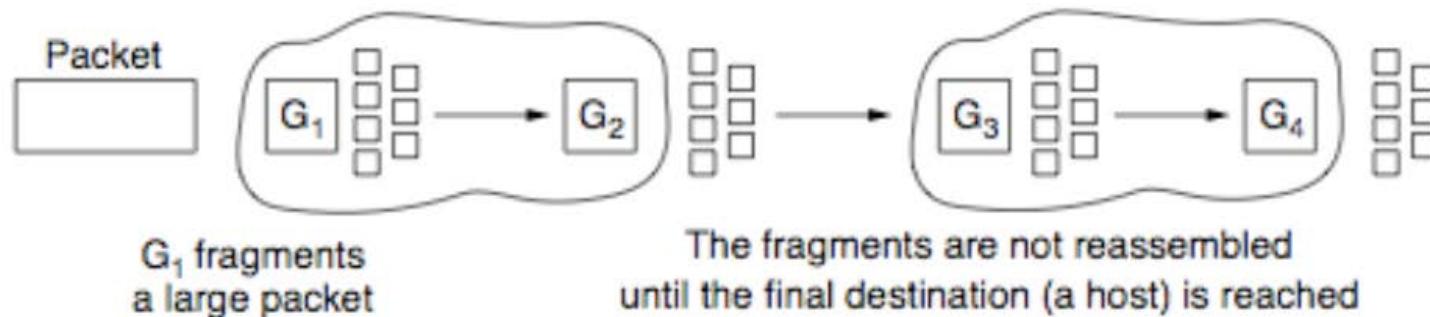
- ▶ Comme vu précédemment, Internet est un réseau de réseaux. Chaque réseau impose une taille maximale de trames M.T.U. (Maximum Transmission Unit) :
 - ▶ du matériel,
 - ▶ des protocoles utilisés,
 - ▶ ou pour limiter
 - ▶ les erreurs de transmission et les retransmissions
 - ▶ l'utilisation du canal par un paquet.
- il faut alors **fragmenter** les paquets

Couche 3 – Réseaux

Adaptation de la taille des données



(a)

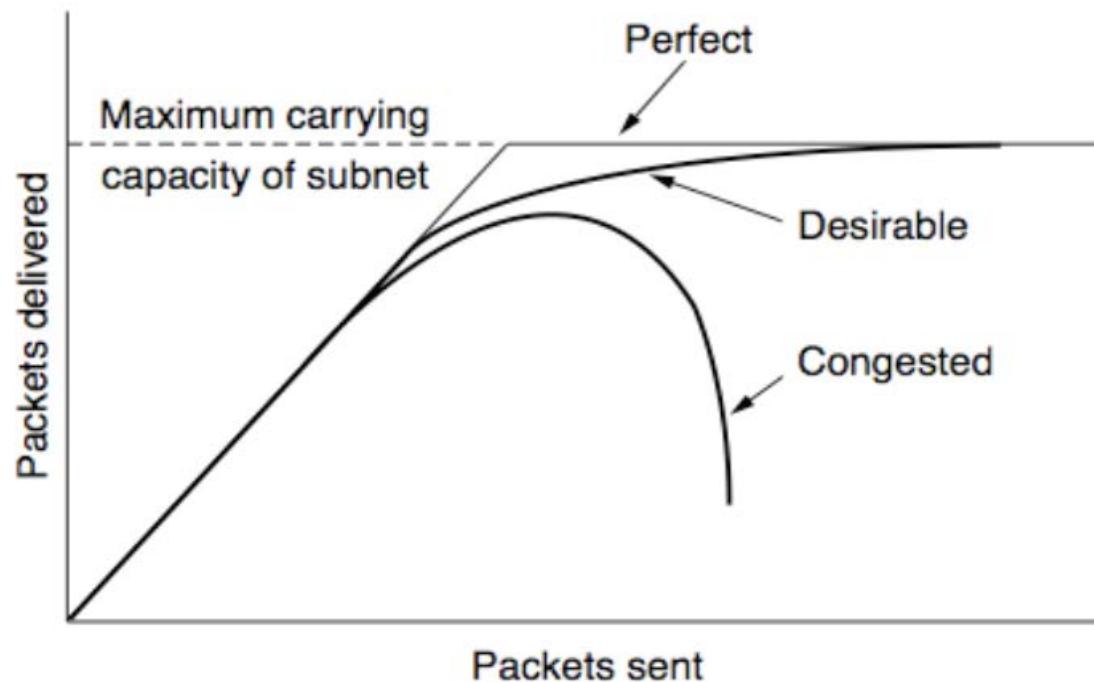


(b)

fragmentation transparente (a) et non transparente (b)

Couche 3 – Réseaux Congestion

- ▶ Lorsque trop de fragments circulent sur le réseau (ou une portion de ce réseau) :
 - ▶ Le risque de perte de fragment est augmenté
 - ▶ Les performances peuvent se dégrader : **phénomène de congestion :**



Couche 3 – Réseaux Routage - Généralités

► Analogie routière



Couche 3 – Réseaux Routage IP

- ▶ Le routage consiste à calculer les tables utilisées par les nœuds pour acheminer les paquets dans les réseaux.
- ▶ Les règles utilisées par les routeurs et les types d'informations échangées par les routeurs pour l'établissement des tables constituent le protocole de routage.
- ▶ Pour construire ces tables, l'opération de routage peut prendre en compte :
 - ▶ la topologie du réseau
 - ▶ d'autres paramètres tels que la latence, le débit,... caractérisant le coût.
- ▶ Le choix d'un chemin se fera donc le plus souvent sur un critère de coût minimal.
- ▶ La qualité d'un algo. de routage sera jugée :
 - ▶ Dans la prise en compte des modifications de l'état du réseau dues à :
 - ▶ des pannes,
 - ▶ un trafic élevé,
 - ▶ Dans l'efficacité/la qualité des informations échangées pour maintenir à jour les tables

Couche 3 – Réseaux

Routage - Catégorisation

- ▶ On distingue deux types selon la manière de mettre à jour les tables de routage :

I- Le routage centralisé ou routage statique

- ▶ Les tables de routage sont configurées de façon définitive dans chaque nœud ou dans un nœud (dans le cas centralisé) par l'administrateur réseaux.
- ▶ Maîtrise plus fine du réseau : le séquencement des paquets est garanti, pas de doute sur l'algorithme de routage.
- ▶ Mais :
 - Difficulté de mise en œuvre en raison de la taille du réseau
 - Le site central représente une fragilité....

Peu ou pas utilisé aujourd'hui.

Mais, avec les puissances de calcul mises en œuvre pour le Cloud, il est possible que ce type de routage devienne à l'avenir en vogue....

Couche 3 – Réseaux Routage - Catégorisation

2- Le routage distribué

- ▶ Basé sur un algorithme distribué sur chaque nœud et itératif
- ▶ Les tables de routage évoluent en fonction de l'état courant du réseau (topologie, charge, nœud en panne, ...).

Très courant. Permet un routage plus résilient

Mais nécessite une maîtrise des informations de contrôles transmises dans le réseau pour ne pas alourdir le transport de l'information

Couche 3 – Réseaux

Routage IP

- ▶ Distinction entre les zones couvertes par le protocole de routage :
 - ▶ **Interne** (I.G.P.) : pour le réseau d'une même entité administrative et technique. Exemples :
 - ▶ OSPF (entreprise); IS-IS (Opérateurs).
 - ▶ Dans ce cas, on parle d'I.G.P. : Interior Gateway Protocol et la zone couverte s'appelle un A.S. (Autonomous System). Le numéro d'AS est délivré par les mêmes entités que pour les adresses IP (RIPE NCC).
- ▶ **Externe** : Routage entre les réseaux.
 - ▶ On parle d'E.G.P. : Exterior Gateway Protocol. Exemple :
 - ▶ B.G.P. (Border Gateway Protocol)

Couche 3 – Réseaux

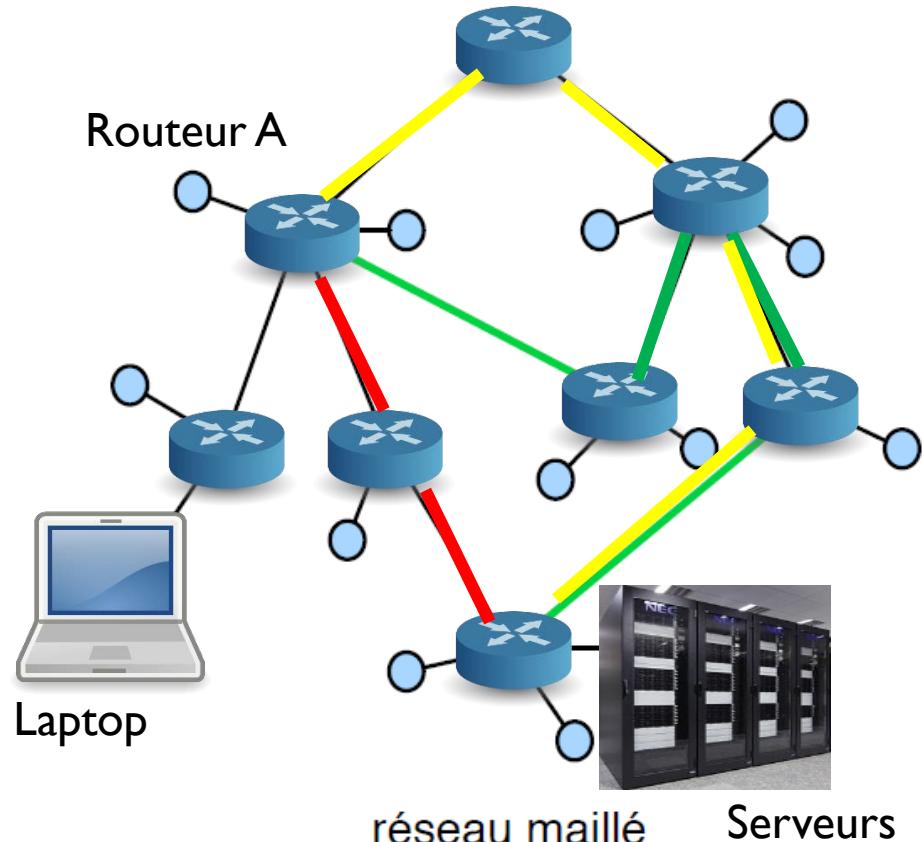
Routage – Vecteur distance

- ▶ Chaque nœud calcule le plus court chemin vers les autres nœuds de son réseau (Algorithme de Dijkstra).
 - ▶ La notion de coût entre deux nœuds est prise en compte :
 - ▶ Débit
 - ▶ Temps A/R
 - ▶ Distance administrative
 - ▶ Coût (€€€)
 - ▶ Etc...
- ▶ Utilisé par tous les algorithmes de routage (hors inondation).

Couche 3 – Réseaux Routage –Vecteur distance

- ▶ Pour aller du laptop au Serveurs, le routeur A connaît trois chemins possibles :

- ▶ Vert
 - ▶ coût = 4
- ▶ Jaune
 - ▶ coût = 4
- ▶ Rouge
 - ▶ coût = 2



- ▶ Le routeur A ne retient qu'une route : rouge

Couche 3 – Réseaux

Routage vecteur distance

- ▶ Chaque nœud communique ensuite cette distance (route) au nœud voisin.
- ▶ Les tables de routage sont construites de proche en proche
 - ▶ Temps de convergence fonction de la taille du réseau
 - ▶ Le « poids » de transmission des données de routage est lourd car toutes les tables sont transmises
 - ▶ Mais peut être amoindri si seulement les modifs de routage sont envoyées
 - ▶ Exemples : RIP, EIGRP

Couche 3 – Réseaux

Routage - états des liens

Phase de découverte du réseau :

- ▶ Chaque nœud découvre ses routeurs voisins directs et la qualité des liens environnants (débit, délai,...) :
 - ▶ Echange périodique de messages périodiques : « hello! » (ttes les 10s. par exemple)
 - ▶ Envoi d'un message rapport partageant ses infos avec tous les nœuds d'un réseau

Phase de calcul du chemin :

- ▶ Transmission du coût d'acheminement de A vers les autres routeurs
 - ▶ Construction d'une table des plus courts chemins depuis la matrice élaborée grâce aux paquets reçus des autres routeurs.

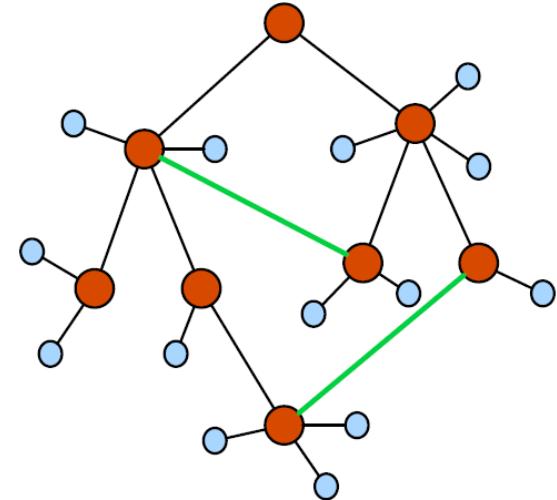
 - ▶ Convergence initiale longue (découverte de l'architecture)
 - ▶ Très bonne résilience aux changement de topologie.

 - ▶ Exemples : OSPF, IS-IS
-

Couche 3 – Réseaux

Routage par inondation

- ▶ Chaque nœud envoie le message reçu sur toutes ses lignes sauf celle d'où provient le message.
 - ▶ Très simple
 - ▶ Très robuste
 - ▶ La destination est toujours trouvée.
 - ▶ Peu de latence
 - ▶ Mais :
 - ▶ Surcharge inutile du réseau
 - ▶ Bouclage, paquets reçus plusieurs fois à éliminer
 - ▶ Entraine des réémissions lorsque le chemin optimal n'est pas trouvé (cf. cours 2 sur les tempo. dans les équipements de niveau 2)

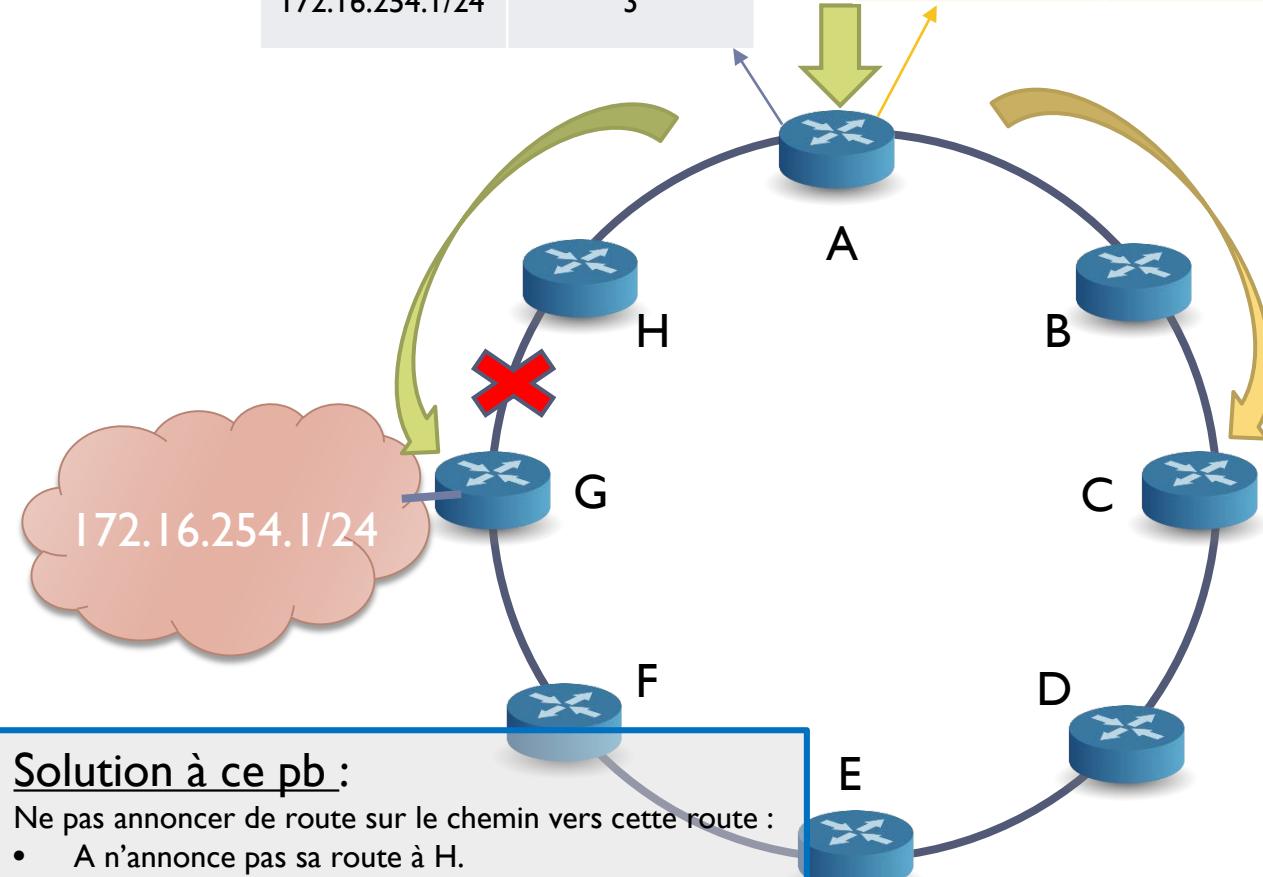


Annonce de A

Dest.	Coût
172.16.254.1/24	3

Nouvelle annonce de A

Dest.	Coût
172.16.254.1/24	7



Solution à ce pb :

Ne pas annoncer de route sur le chemin vers cette route :

- A n'annonce pas sa route à H.

Ou

- Annoncer les routes en donnant le prochain routeur :

« Next hop router »

Couche 3 – Réseaux Notion de convergence à l'infini

- Le lien H-G tombe
- H détecte et augmente la métrique vers G (1000 par ex.)
- Mais :
- A lui annonce *toujours* une route avec un coût à 3
- H met donc sa table à jour avec un coût de 4 et efface sa route avec un coût à 1000...
- A remet ensuite sa table à jour avec un coût de 5
- Etc...
- Jusqu'à bascule par B

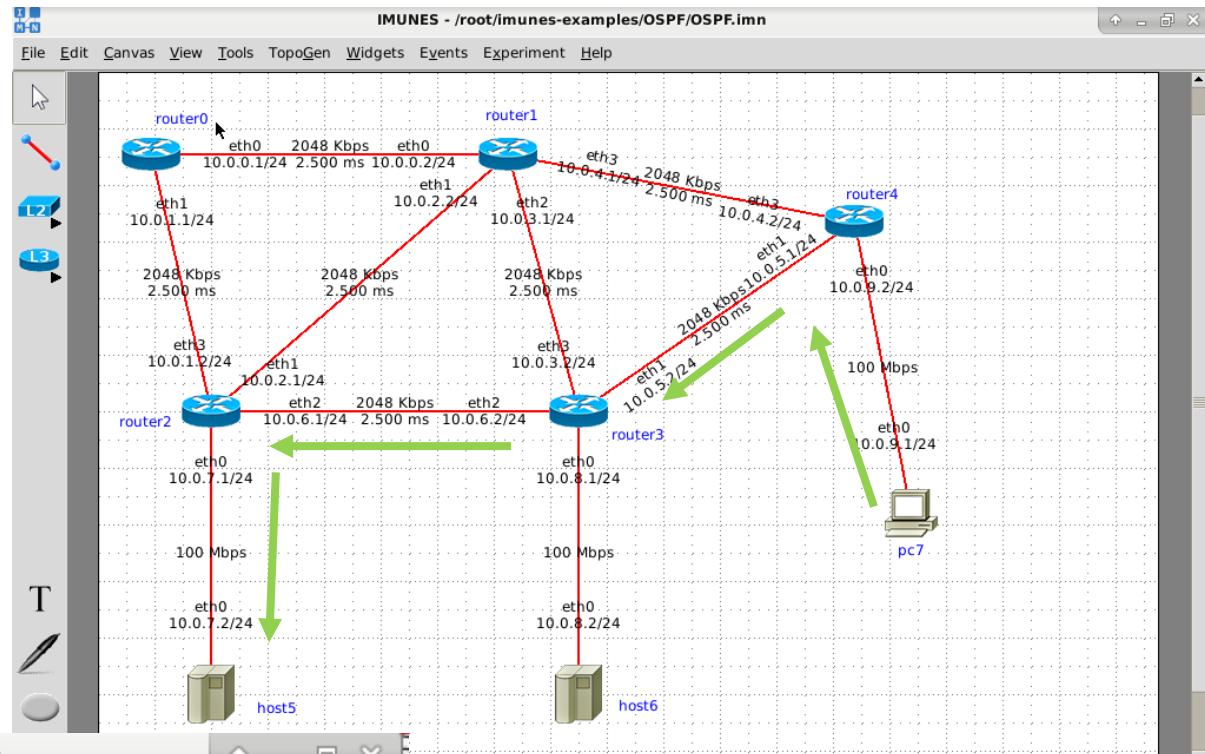
Couche 3 – Réseaux

Cas pratique – PING

Ping est le nom d'une commande informatique permettant de tester l'accessibilité d'une autre machine à travers un réseau IP.



WIKIPÉDIA
L'encyclopédie libre



IMUNES: pc7 (console) sh

```
# ping 10.0.7.2
PING 10.0.7.2 (10.0.7.2): 56 data bytes
64 bytes from 10.0.7.2: icmp_seq=0 ttl=61 time=16.000 ms
64 bytes from 10.0.7.2: icmp_seq=1 ttl=61 time=17.967 ms
64 bytes from 10.0.7.2: icmp_seq=2 ttl=61 time=16.993 ms
64 bytes from 10.0.7.2: icmp_seq=3 ttl=61 time=21.965 ms
64 bytes from 10.0.7.2: icmp_seq=4 ttl=61 time=18.914 ms
64 bytes from 10.0.7.2: icmp_seq=5 ttl=61 time=16.937 ms
64 bytes from 10.0.7.2: icmp_seq=6 ttl=61 time=18.941 ms
^C
```

Temps aller-retour

Nombre de routeurs traversés sur le retour

Couche 3 – Réseaux

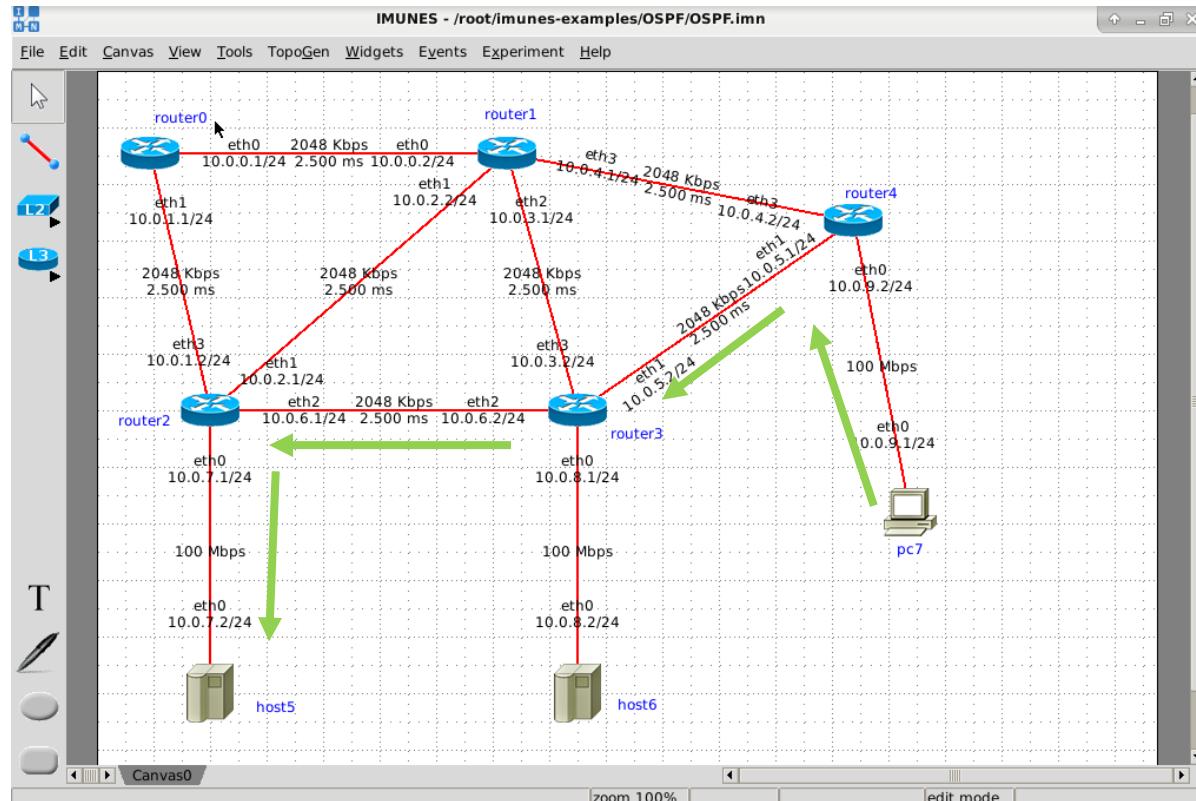
Cas pratique - TRACEROUTE

traceroute (ou tracert sous Windows) est un programme utilitaire qui permet de suivre les chemins

qu'un paquet de données (paquet IP) va prendre pour aller de la machine locale à une autre machine connectée au réseau IP. Il a été conçu au sein du Laboratoire national Lawrence-Berkeley.



WIKIPÉDIA
L'encyclopédie libre



IMUNES: pc7 (console) sh

```
# traceroute 10.0.7.2
traceroute to 10.0.7.2 (10.0.7.2), 64 hops max, 40 byte packets
1  10.0.9.2 (10.0.9.2)  1.052 ms  1.217 ms  2.097 ms
2  10.0.8.1 (10.0.8.1)  7.910 ms  7.607 ms  7.401 ms
3  10.0.2.1 (10.0.2.1)  17.841 ms  13.319 ms  13.782 ms
4  10.0.7.2 (10.0.7.2)  18.544 ms  15.608 ms  15.549 ms
```

Adresse IP de l'interface
du routeur traversé

Délai entre chaque routeur
traversé

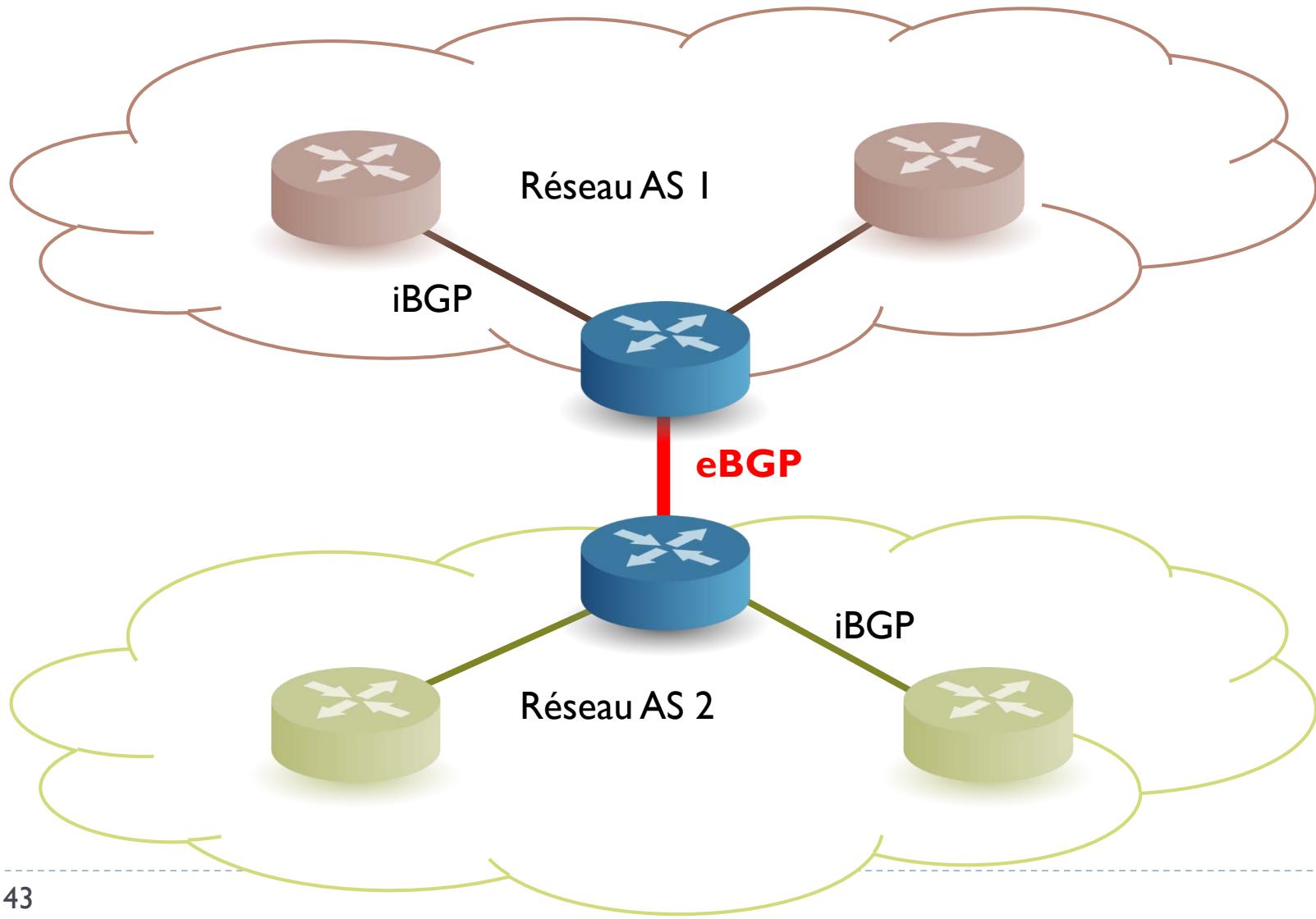
Couche 3 – Réseaux

Cas pratique – Simulateur de réseau

- ▶ IMUNES
 - ▶ Création d'une topologie
 - ▶ Activation du routage OSPF
 - ▶ Mise en place d'un évènement et observation du comportement du réseau
 - ▶ Analyse des trames à l'aide de Wireshark



Couche 3 – Réseaux Routage externe - BGP



Couche 3 – Réseaux BGP

- ▶ Transmission des routes
 - ▶ iBGP : AS identique
 - ▶ eBGP : AS différent
- ▶ Toutes les routes de l'internet IPv4 : 512.000 routes
- ▶ Alléger la mémoire des routeurs : Réflecteurs de routes ou route par défaut
- ▶ Choix du meilleur chemin BGP
 - ▶ AS PATH : liste les AS traversés sur un chemin
 - ▶ LOCAL PREF : permet de relayer les infos iBGP à l'intérieur d'un AS
 - ▶ MED : permet d'appliquer une stratégie sur les préfixes issus d'interco. différentes
 - ▶ COMMUNITIES : permet de préciser la stratégie autour de communautés

Couche 3 – Réseaux BGP – Cas pratique

- ▶ Discutons avec l'Australie ! ☺
- ▶ Suivre un paquet depuis Paris vers : 202.158.196.129
- ▶ Observer les réseaux traversés
- ▶ Observer la stratégie d'interconnection

- ▶ Protocole de portée Mondiale ! Exemple : PakistanTelecom – Fév. 2008



Couche 3 – Réseaux

Diffusion des adresses IP

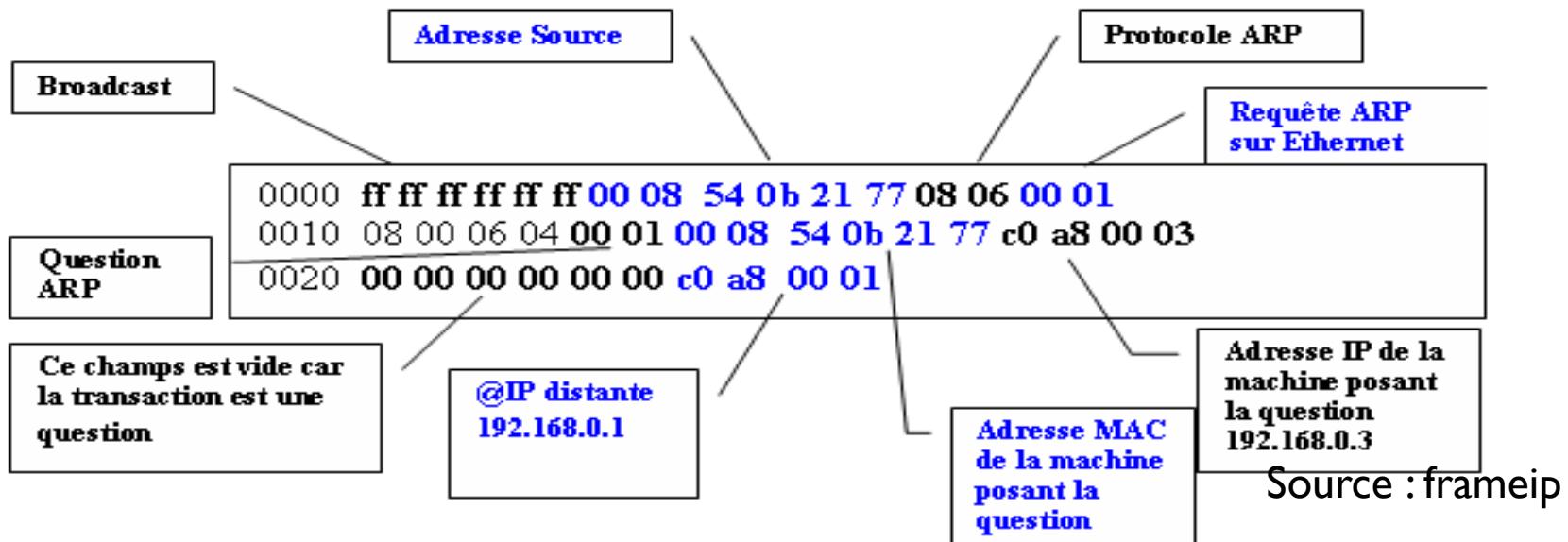
- ▶ ARP : Address Resolution Protocol
 - ▶ Chaque carte réseau possède son adresse physique MAC et une adresse logique IP.
 - ▶ Sur un même espace de diffusion : ARP fait la correspondance directe entre @MAC et @IP et les machines peuvent se joindre directement
 - ▶ Sinon : l'@ IP du routeur ou de la passerelle est sélectionnée

Couche 3 – Réseaux

Diffusion des adresses IP

▶ ARP : Address Resolution Protocol

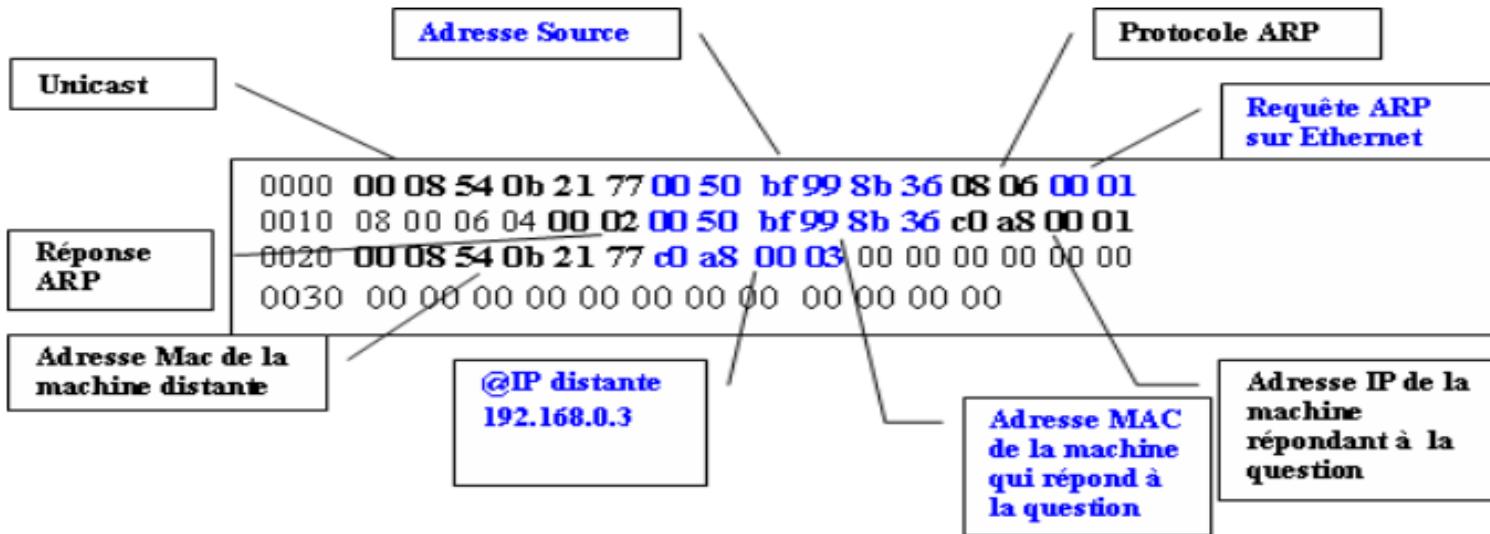
- ▶ Fonctionnement :
- ▶ ARP request : une machine doit envoyer un paquet à une @ IP dont elle ne connaît l'@ MAC correspondante.
- ▶ → Elle réalise un broadcast :



Couche 3 – Réseaux

Diffusion des adresses IP

- ▶ ARP : Address Resolution Protocol
 - ▶ Fonctionnement :
 - ▶ ARP reply : La machine se reconnaissant avec l'@ IP contenue dans la trame Ethernet répond avec son @ MAC :



- ▶ La commande pour connaître le cache : arp -a

Couche 3 – Réseaux

Dynamic Host Configuration Protocol

- ▶ Dynamic Host Configuration Protocol (DHCP) est un protocole réseau dont le rôle est d'assurer la configuration automatique des paramètres IP d'une station, notamment en lui affectant automatiquement une adresse IP et un masque de sous-réseau. DHCP peut aussi configurer l'adresse de la passerelle par défaut et des serveurs de noms DNS.
- ▶ Evite les erreurs humaines et la lourdeur d'administration
- ▶ Optimise l'utilisation des adresses IP en ne les affectant que sur les machines le nécessitant

Couche 3 – Réseaux

DHCP - Processus

▶ Processus

- ▶ Une machine sans @ IP envoie un message « DHCP discover » en diffusion IP avec son adresse MAC
- ▶ Le serveur répond sur l'adresse MAC avec une offre d'@ IP et l'@ IP du serveur
- ▶ L'ordinateur diffuse une réponse « DHCP request » avec son @ IP pour que d'autres serveurs DHCP éventuels s'en aperçoivent

Couche 3 – Réseaux

DNS - Relation adresse IP/nom de domaine

- ▶ Les adresses IP sont faites pour les machines, pas pour les humain.

- ▶ Protocole et architecture Domain Name System DNS.
 - ▶ Chaque réseau déclare le nom ‘humain’ pour les adresses des machines.
 - ▶ Hiérarchie mondiale de serveurs DNS
 - ▶ 13 serveurs racine

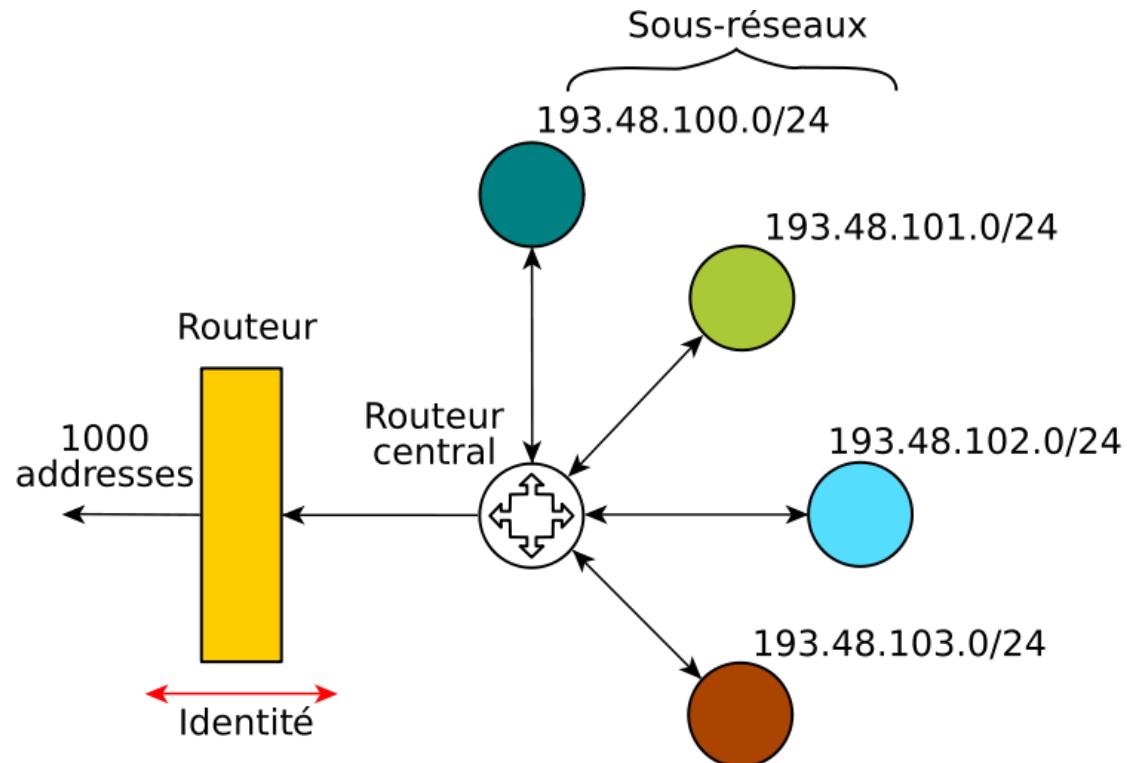
- ▶ Cas pratique :
 - ▶ A qui appartient l'adresse IP : 91.198.174.225

Couche 3 – Réseaux

Network Address Translation - NAT

- ▶ Les adresses IP publiques sont chères. On utilise le plus souvent l'adressage privé pour les LAN. (Pour les mobiles également).

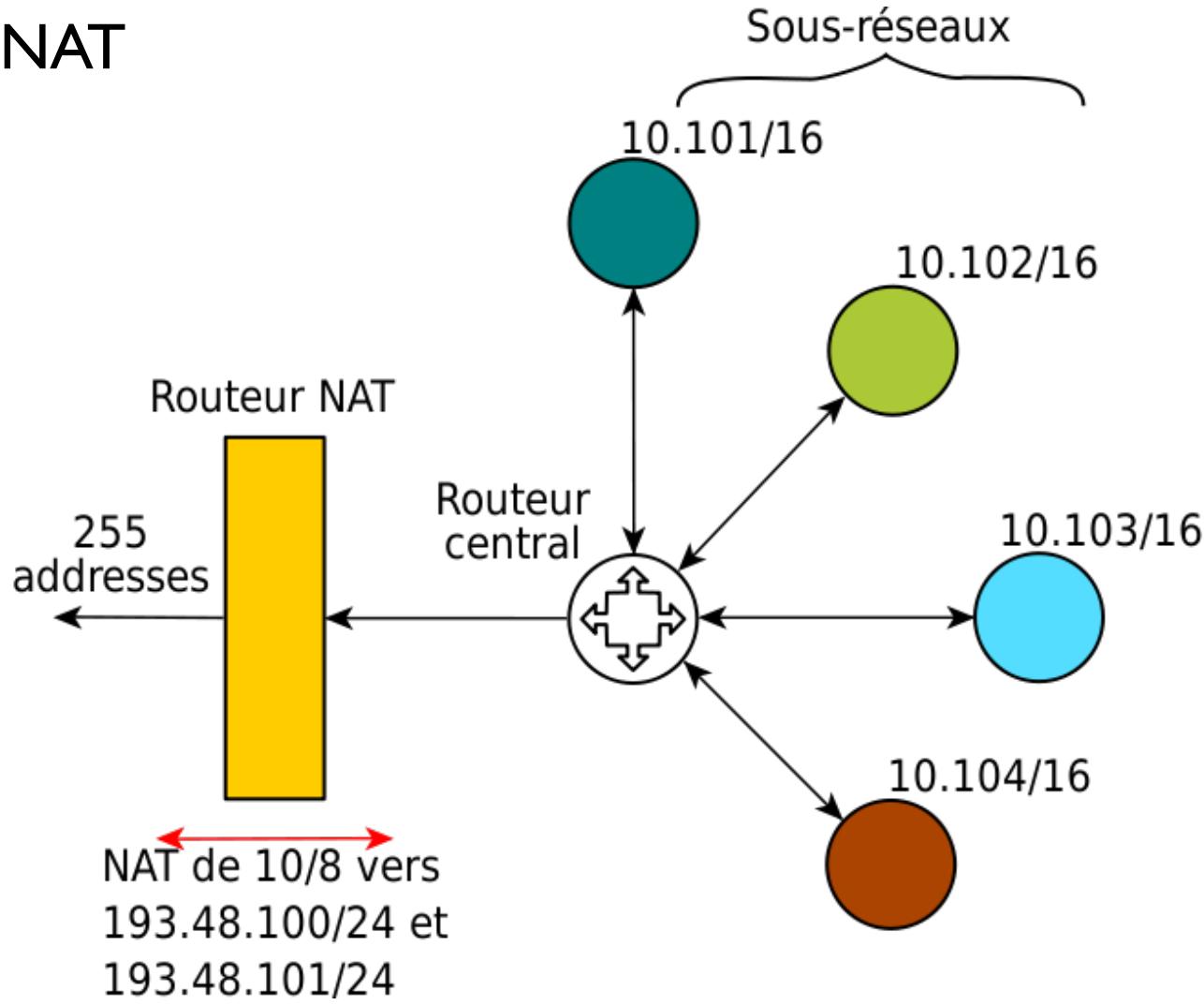
- ▶ Sans NAT :



Couche 3 – Réseaux

Network Address Translation - NAT

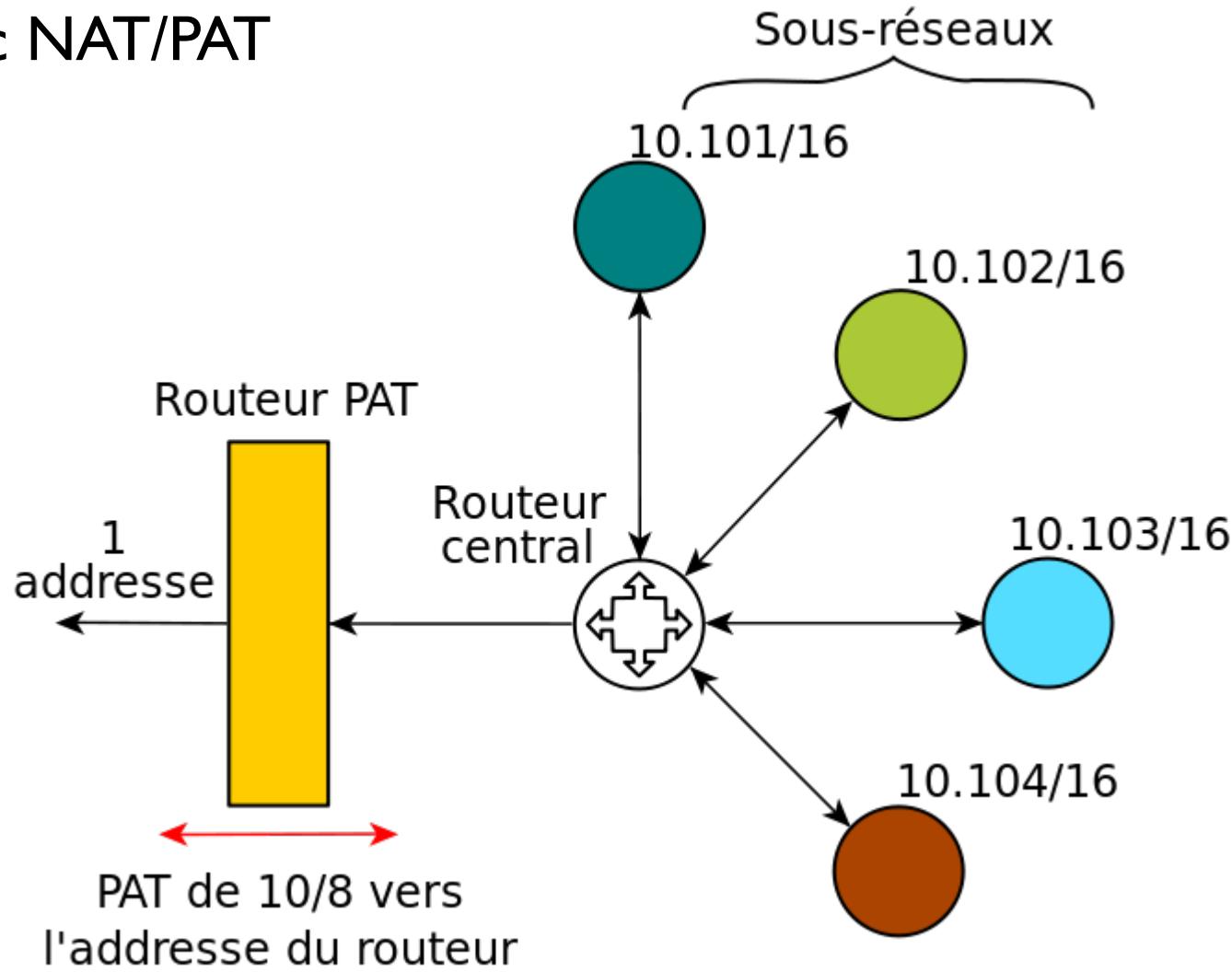
► Avec NAT



Couche 3 – Réseaux

Network Address Translation – NAT // PAT

► Avec NAT/PAT



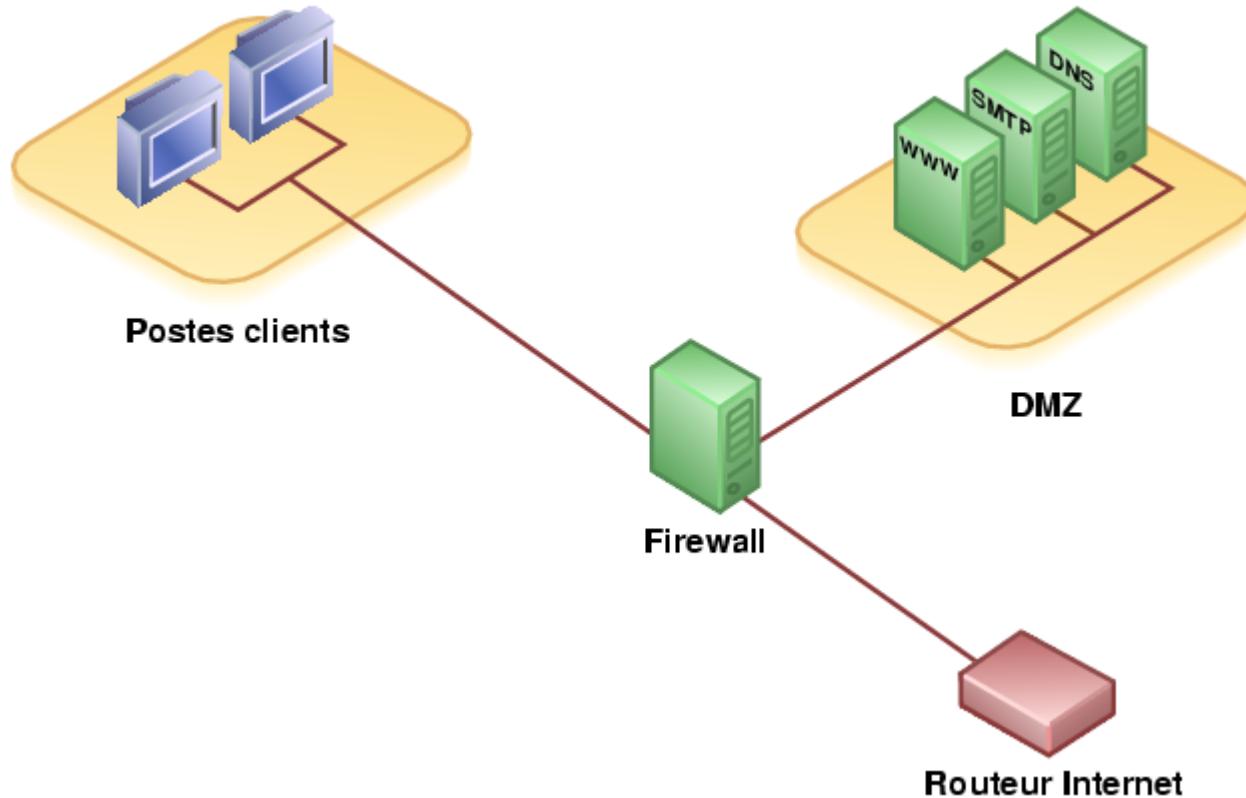
Couche 3 – Réseaux

Network Address Translation - NAT

- ▶ Avantages :
 - ▶ Disparition du problème de manque d'adresses.
 - ▶ Plus de sécurité → Les machines ne sont pas directement adressable, il faut passer par un élément intermédiaire.
 - ▶ Emplacement privilégié pour ajouter des éléments de sécurité : Firewall

- ▶ Inconvénients :
 - ▶ Moins flexible qu'un adressage direct car dépendant de l'équipement NAT.

Couche 3 – Réseaux NAT et DMZ



Les Réseaux

ENSAM

Karim Boudjemaïa

Études et Projets – RENATER

Karim.boudjemaia@renater.fr

Cours n°3

Plan du cours 3

- ▶ **Couche 3 - Réseaux**
 - ▶ Objectifs
 - ▶ Présentation IP
 - ▶ Routage et relayage
 - ▶ Notions d'interconnexion
 - ▶ Adressage IP
 - ▶ Sous-réseau, classes
 - ▶ Cas pratique
 - ▶ Protocole IP
 - ▶ Routage
 - ▶ Catégorisation
 - ▶ Routage interne
 - Type de algorithme de routage
 - OSPF
 - Cas pratique
 - ▶ Routage externe
 - BGP
 - Cas pratique
- ▶ **Mécanismes IP**
 - ▶ ARP
 - ▶ DHCP
 - ▶ DNS
 - ▶ NAT
- ▶ **Notion de Qualité de Services QoS**
 - ▶ Besoins
 - ▶ Approche par dimensionnement (DiffServ)
- ▶ **MPLS**
- ▶ Conclusion
- ▶ **Couche 4 – Transport**
 - ▶ TCP
 - ▶ Mécanisme de fenêtre glissante
 - ▶ UDP

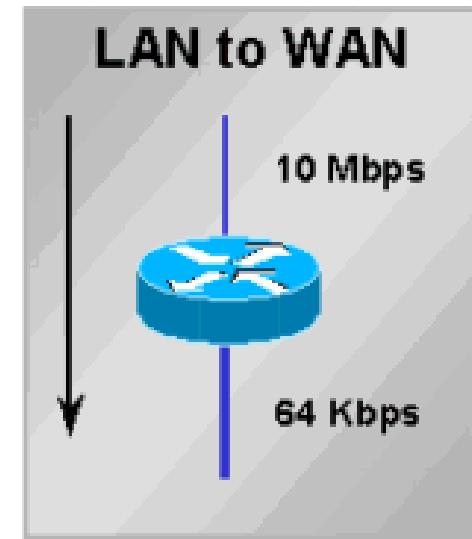
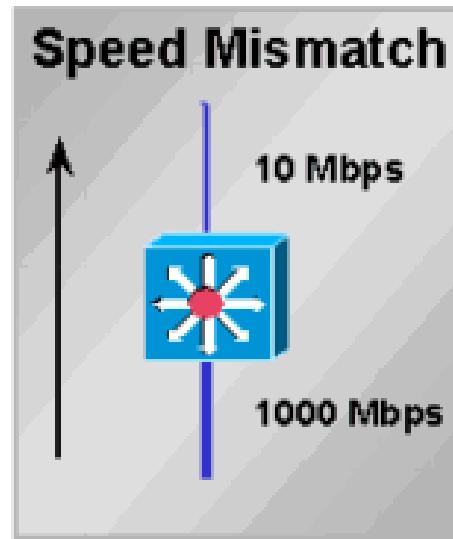
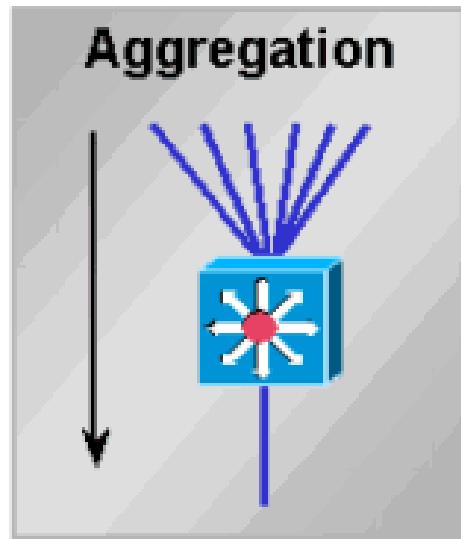
Couche 3 – Réseaux

Notion de qualité de service - QoS

- ▶ Diverses applications transportées par les réseaux :
 - ▶ Temps réel : gaming, visio. Conférence,
 - ▶ Streaming,
 - ▶ Transfert de fichiers, email,
- ▶ **Mais tous ces flux convergent vers le même réseau IP et ce réseau n'achemine les paquets que dans un mode B.E. (Best Effort)**
- ▶ Plusieurs approches :
 - ▶ Flux par flux :
 - ▶ Complexé et alourdi les tables de routages car cela s'ajoute aux infos du routage classique
 - ▶ Dimensionnement
 - ▶ classification du trafic et traitement en fonction (IP Diffserv)
 - ▶ réservation en excès (over-provisionning) :
 - méthode très efficace, mais très coûteuse
 - ▶ Par ingénierie de trafic : réservation de ressources à la création d'un Circuit Virtuel (type MPLS) qui ne repose pas sur le même algorithme de routage

Couche 3 – Réseaux Congestion

- ▶ Facteurs pouvant provoquer une congestion :
 - ▶ flux entrant dans un routeur trop important
 - ▶ processeurs trop lents
 - ▶ débits des lignes trop faibles.



Couche 3 – Réseaux Congestion

- ▶ Tous ces problèmes génèrent un dépassement de mémoire dans les routeurs

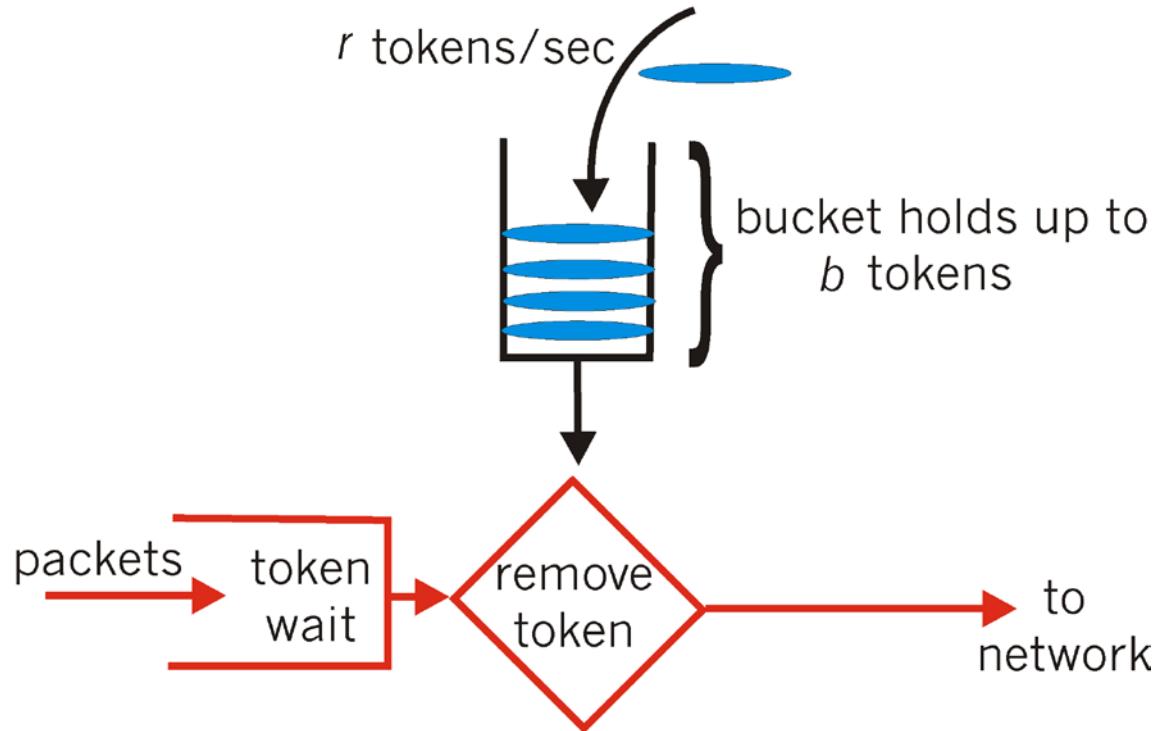
- ▶ Choix de la quantité de mémoire dans les routeurs :
 - ▶ trop de paquets sont perdus si la mémoire est insuffisante
 - ▶ trop de paquets sont retransmis si la mémoire est trop grande

- ▶ Dans les deux cas :
- ➔ effondrement des performances et congestion

Couche 3 – Réseaux

Contrôle d'accès- régulation du trafic

- ▶ Sceau percé

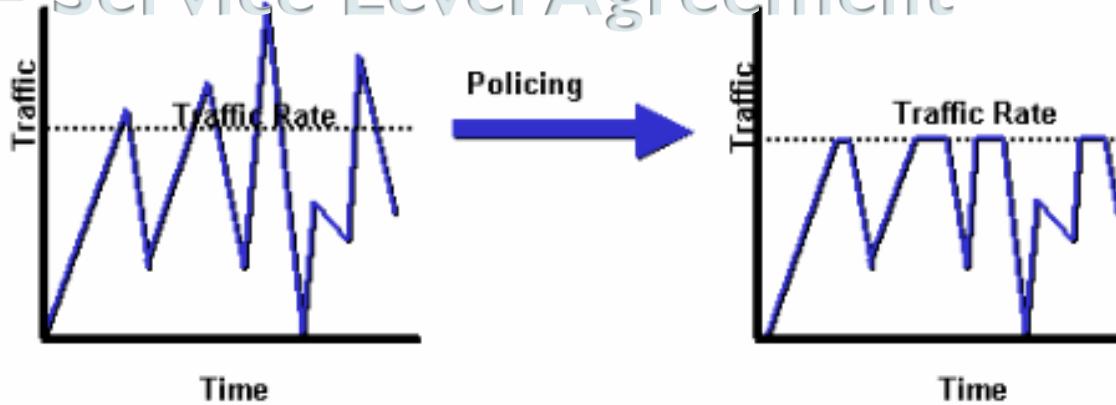


Permet la facturation

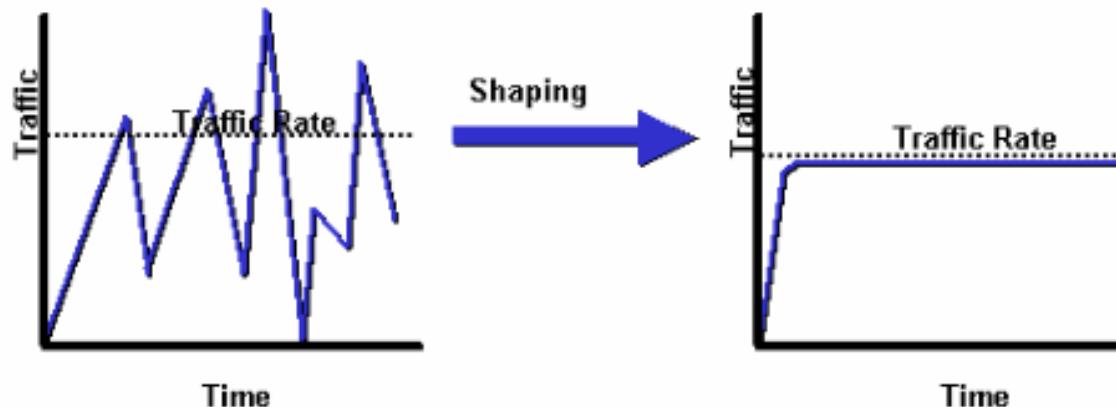
Couche 3 – Réseaux

Contrôle d'admission – Policing & Shaping

SLA = Service Level Agreement



Drop de paquets dès que la limite est atteinte



Ralentissement des envois jusqu'à atteindre une limite

Couche 3 – Réseaux DiffServ

- ▶ Trois classes sont définies selon le Per Hop Behavior (PHB) :
 - ▶ Best Effort : BE
 - ▶ Expedited Forwarding : EF
 - ▶ Assured Forwarding : AF
- ▶ On parle de marquage.
- ▶ Ce marquage peut avoir lieu :
 - ▶ soit directement par l'application émettrice,
 - ▶ soit par le (les) premier(s) routeur(s) en bordure : Access List

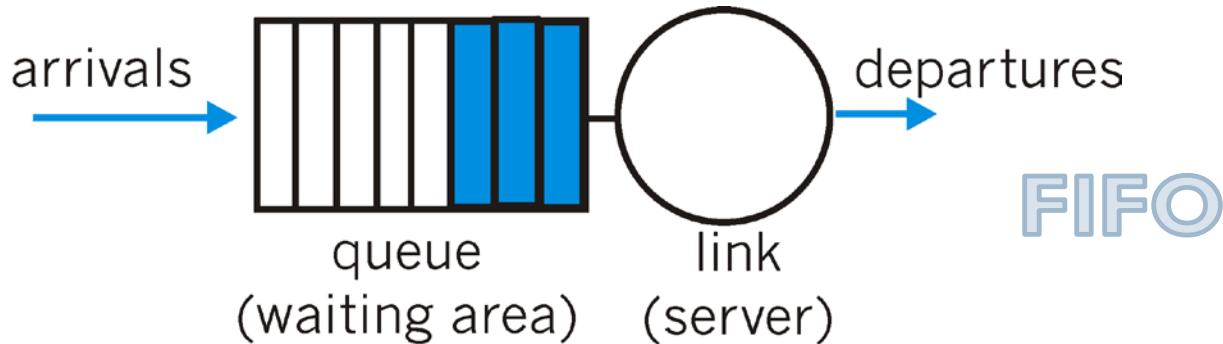


Version	IHL	ToS	Total Length	
Identification		Flags	Fragment Offset	
Time To Live	Protocol	Header Checksum		
Source Address				
Destination Address				
Options			Padding	

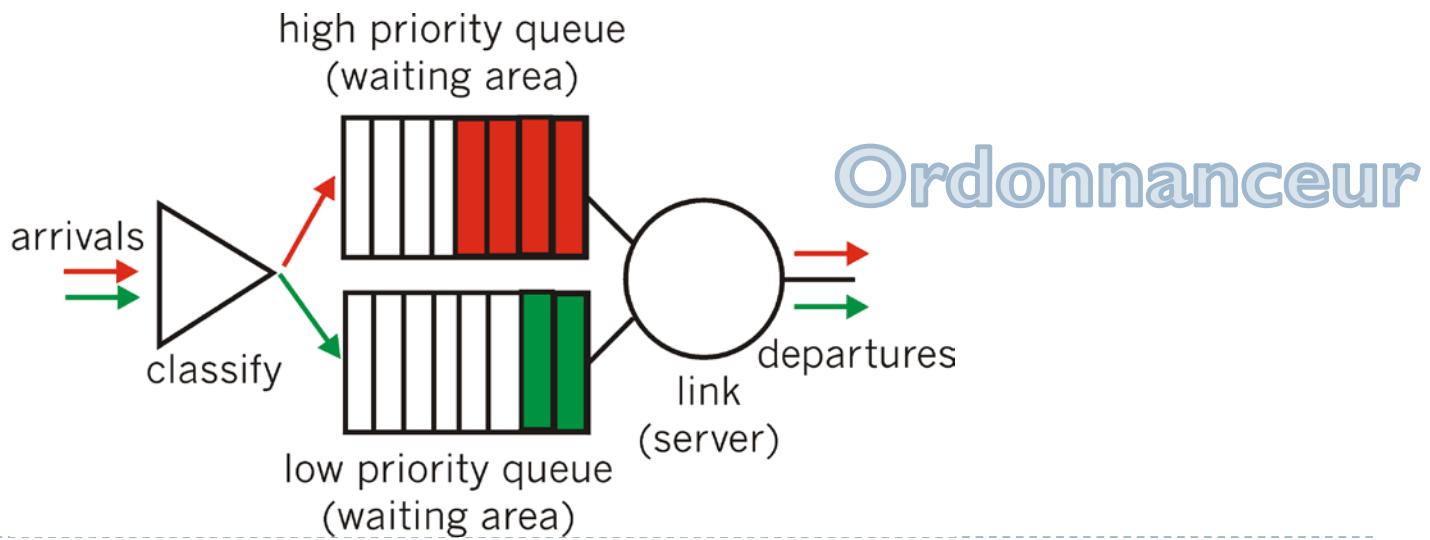
Couche 3 – Réseaux

Classification du trafic

- ▶ Une seule classe de trafic



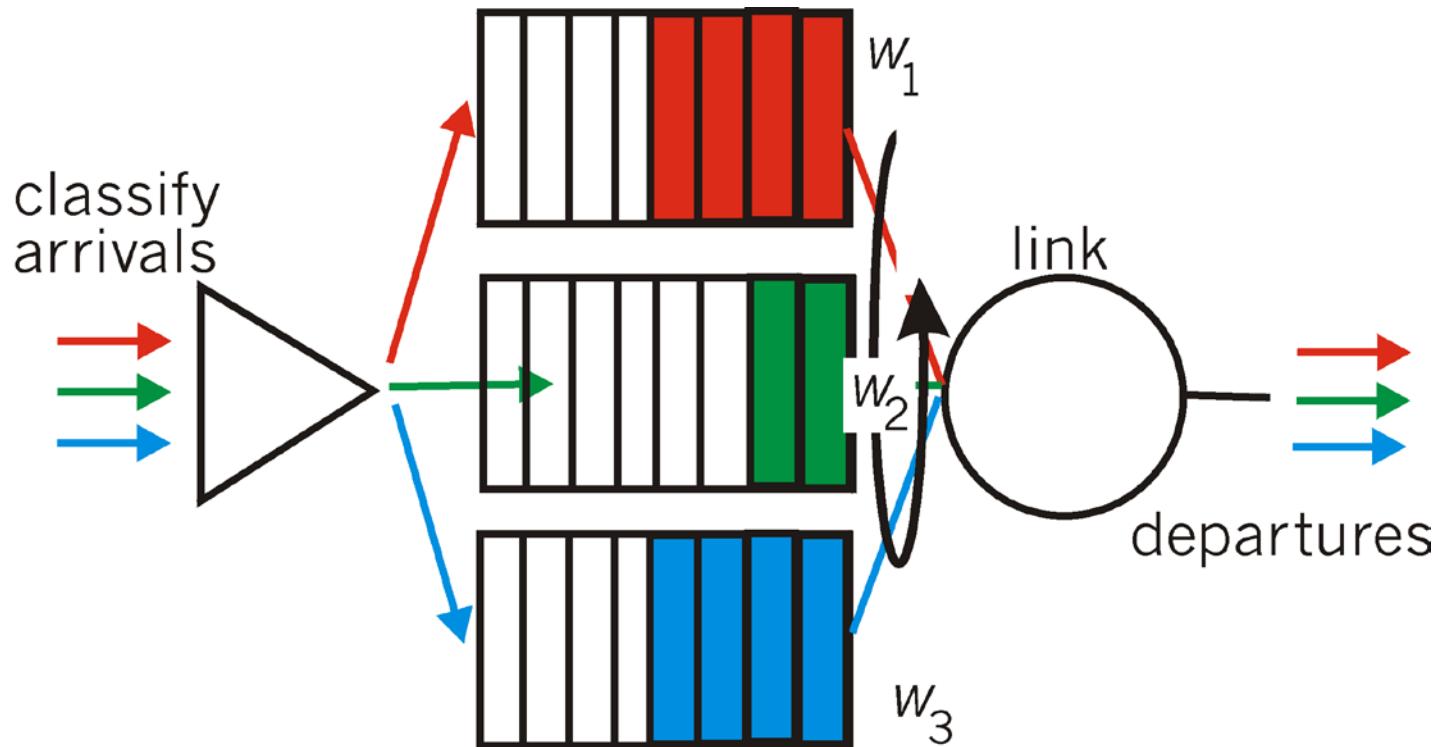
- ▶ 2 Classes



Couche 3 – Réseaux

Classification du trafic

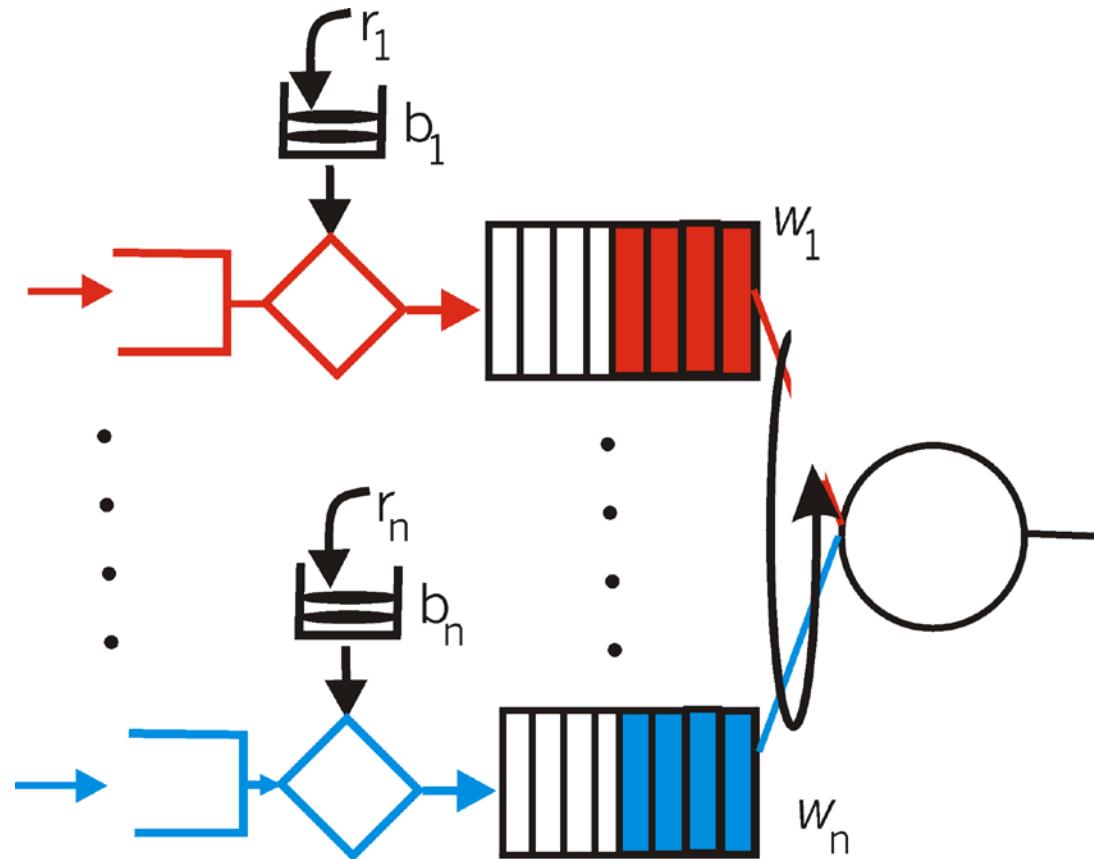
- ▶ N classes pondérées WFQ :Weighted Fair Queueing



Couche 3 – Réseaux

Régulation du trafic

- ▶ Sceau percé + WFQ

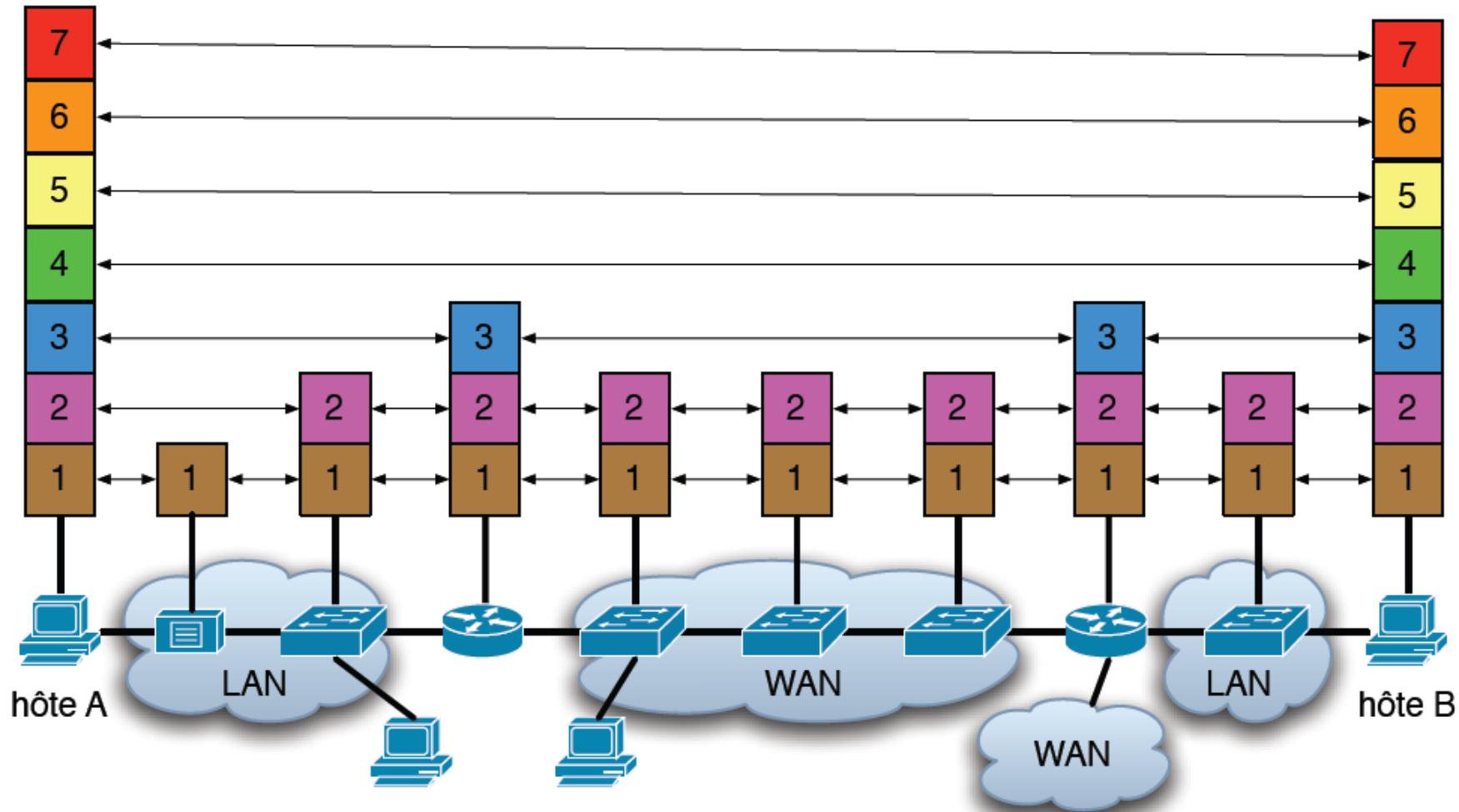


Couche 3 – Réseaux

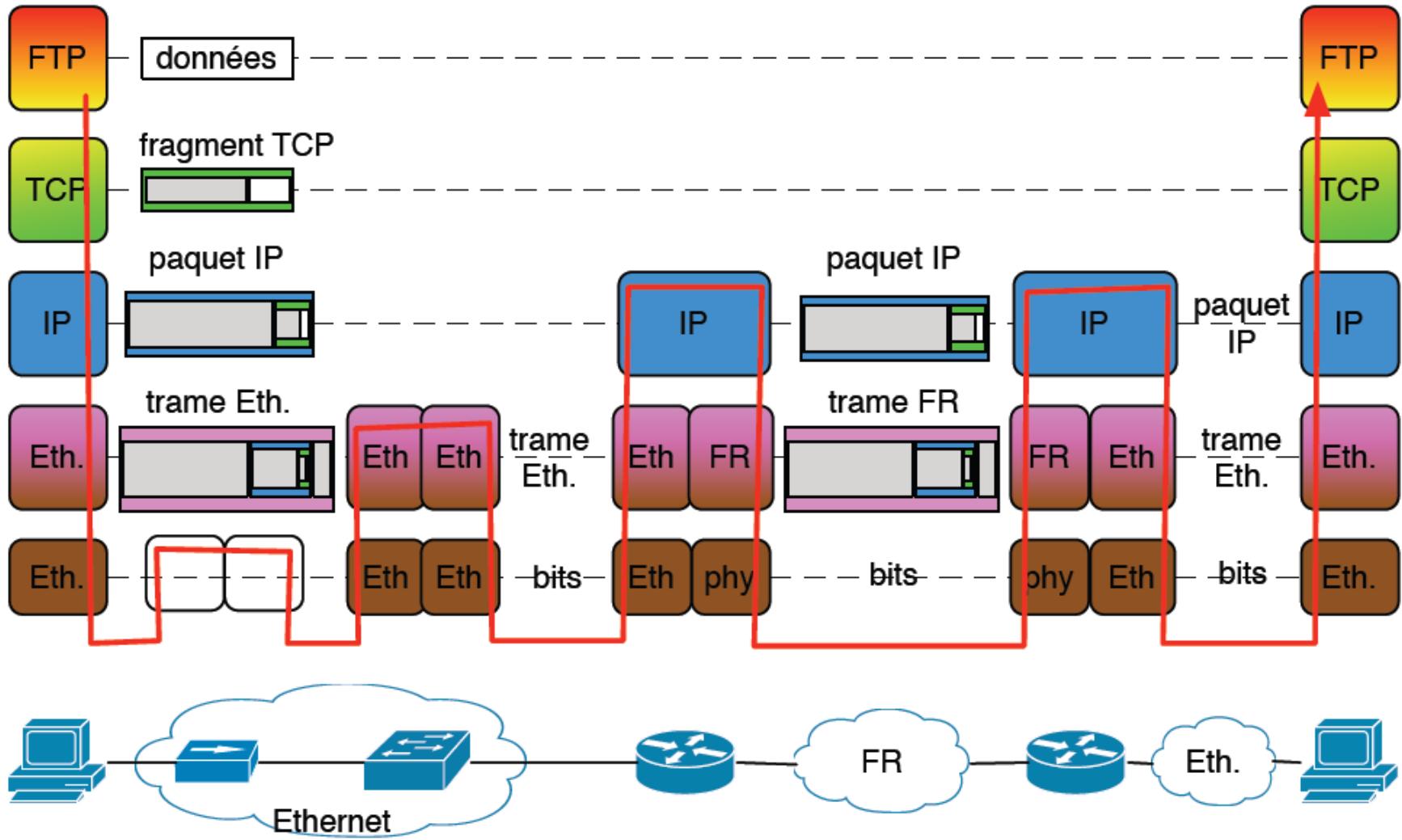
QoS - Bilan

- ▶ La gestion de la qualité des services est complexe car on veut faire transiter une grande diversité de qualité de trafic sur un réseau. C'est le défi de l'ingénieur réseau de pouvoir transporter tous ces flux différents sur un même réseau IP.
- ▶ Elle repose sur les protocoles de routage et donc sollicite encore plus la capacité de calcul des routeurs

Couche réseaux



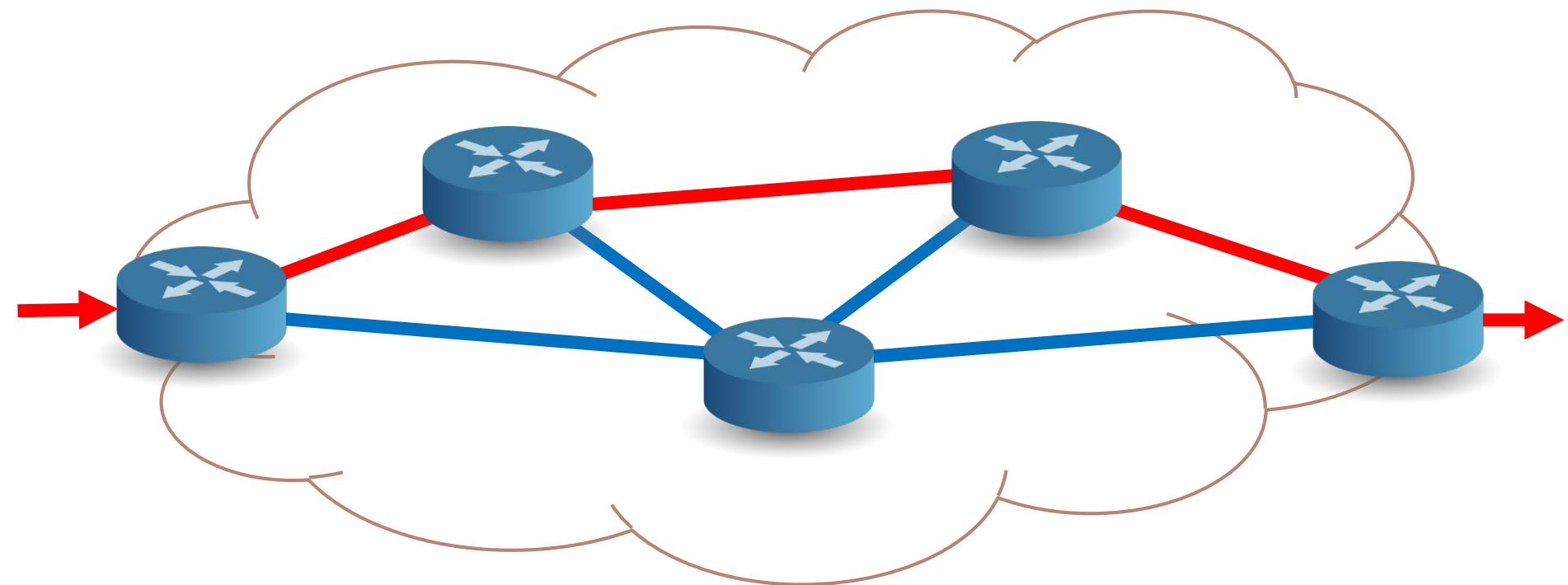
Couche réseaux



Couche 2,5 – Réseaux/Commutation

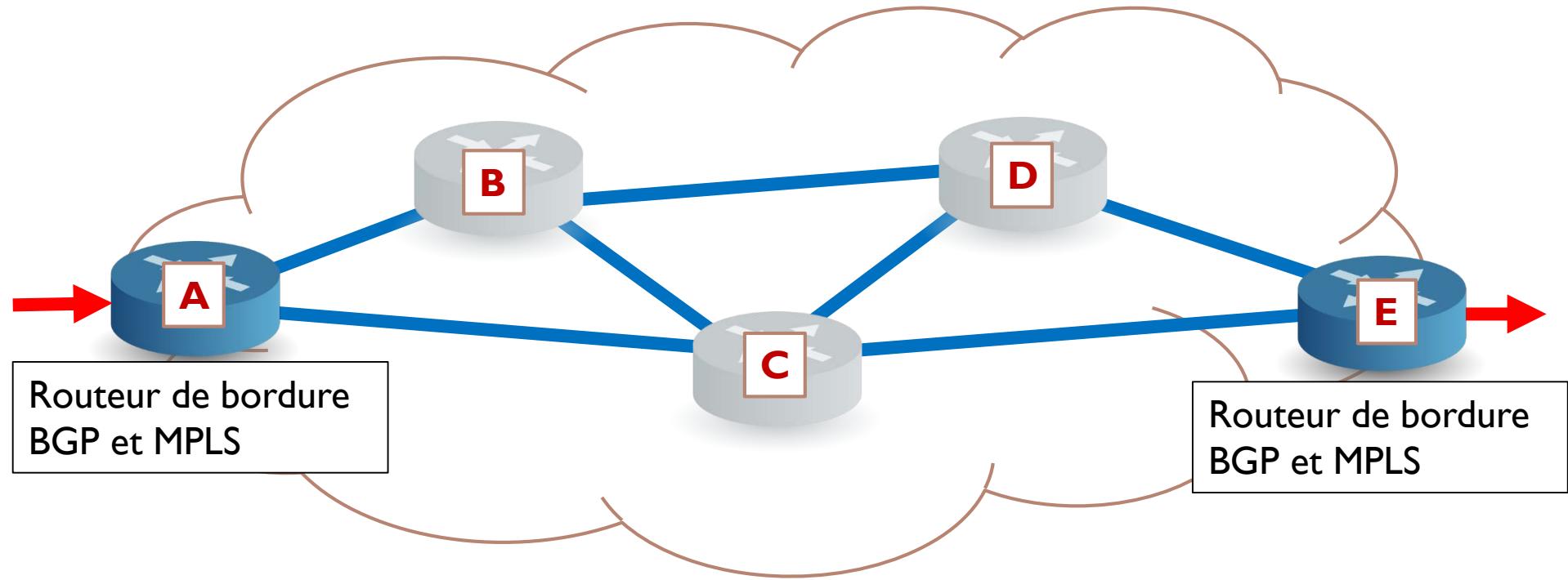
Multi Protocol Label Switching - MPLS

- ▶ Constat pour un réseau d'opérateur :
 - ▶ Au sein d'un même AS, beaucoup de trafic transite d'un nœud de bordure vers un autre nœud de bordure pour rejoindre un autre AS
- ▶ Quelle est alors l'utilité de router ce trafic à chaque nœud ?



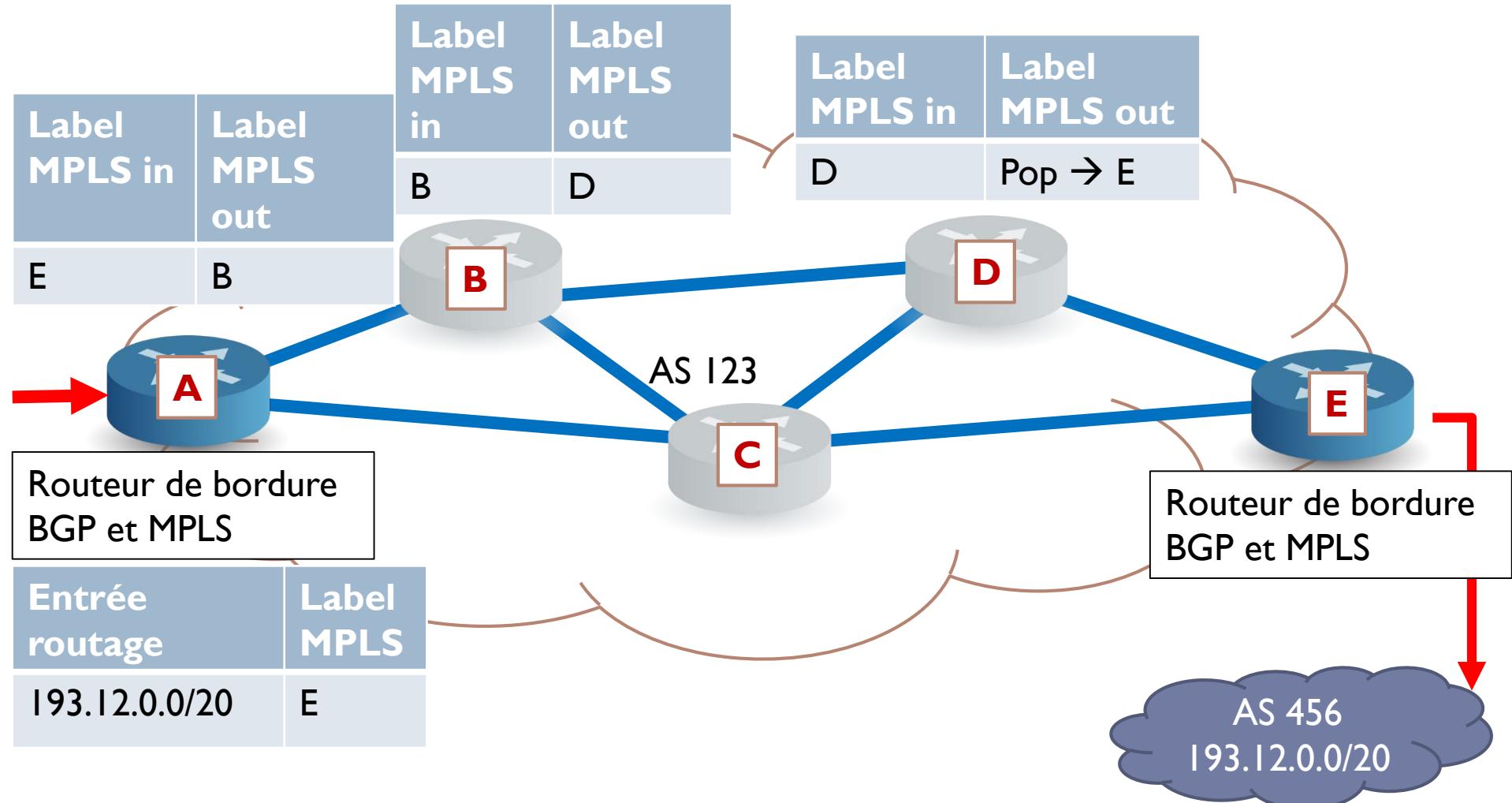
Couche 2,5 – Réseaux/Commutation

Multi Protocol Label Switching - MPLS



Couche 2,5 – Réseaux/Commutation

Multi Protocol Label Switching - MPLS



Couche 3 – Réseaux

Conclusion sur IP

- ▶ Services d'IP
 - ▶ Interconnexion de réseaux aux couches 2 différentes
 - ▶ Acheminement de datagrammes à des hôtes IP
 - ▶ Adaptation aux MTU des réseaux grâce à la fragmentation
 - ▶ Durée de vie limitée des datagrammes par le biais du TTL
 - ▶ Détection d'erreurs sur l'en-tête
 - ▶ Signalisation de certaines erreurs via ICMP
- ▶ Limitation d'IP
 - ▶ Pas d'adressage des applications (client/serveur Web, FTP, SMTP, etc.)
 - ▶ Livraison de datagrammes non garantie, Best Effort
 - ▶ Duplication de datagrammes possible -> faiblesse de la sécurité
 - ▶ Dé séquencement possible
 - ▶ Erreur possible sur les données

Couche 4 – Transport

Objectifs

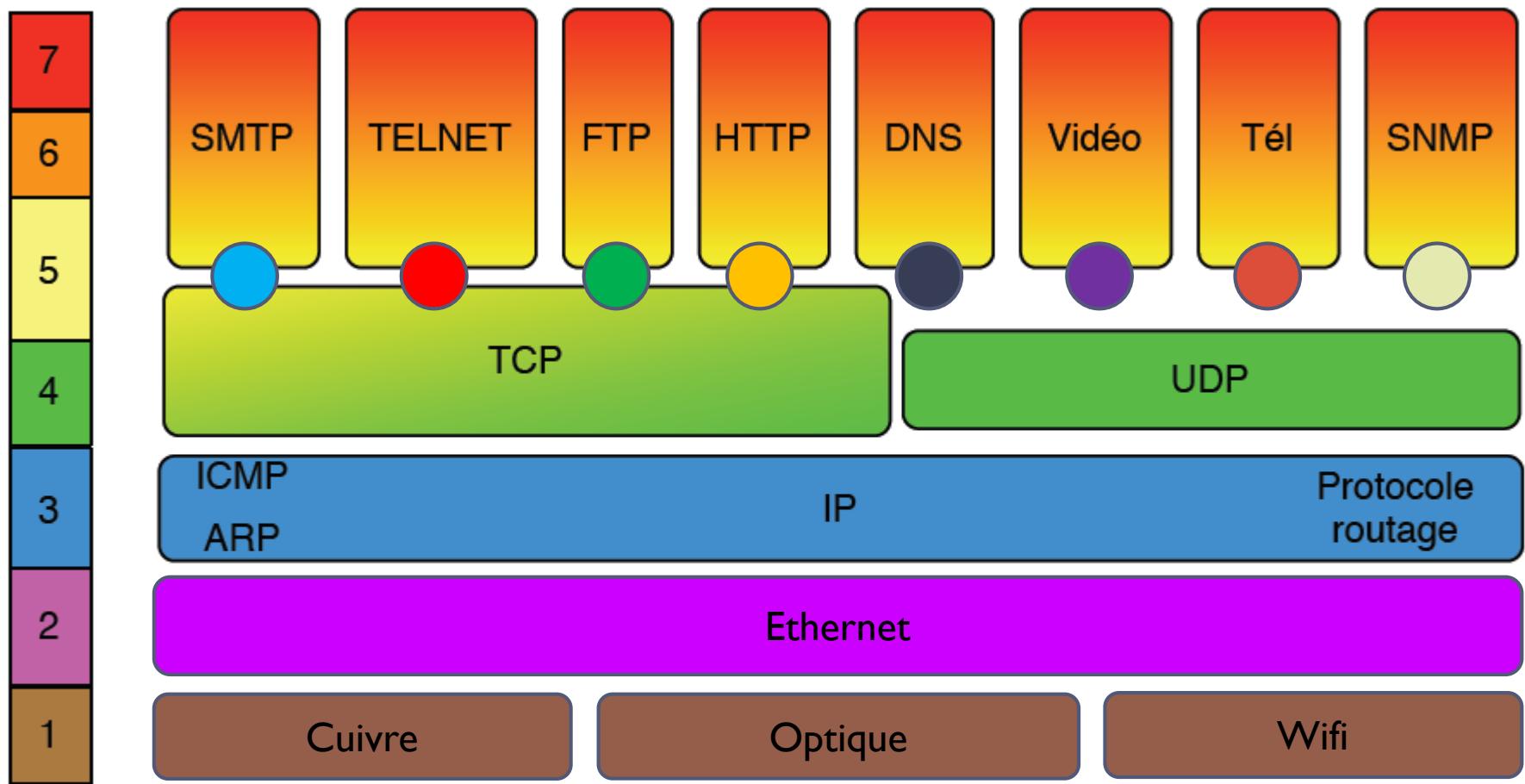
- ▶ Les objectifs de la couche transport sont :
 - ▶ Transport de bout en bout
 - ▶ Peu importe le découpage sous réseau en dessous
 - ▶ Sélectionner la qualité de service
 - ▶ Délai, taux d'erreurs,...
 - ▶ Transparence
 - ▶ Transparence au format des données : codage,...
- ▶ L'entité est le : **message**

Couche 4 – Transport

Objectifs

- ▶ Les objectifs de la couche transport sont :
 - ▶ Aller au-delà des limites d'IP
 - ▶ Assurer si nécessaire la correction d'erreur
- ▶ 2 protocoles disponibles dans TCP/IP
 - ▶ UDP (User Datagram Protocol) : transport rapide, non connecté, permettant la multidiffusion
 - ▶ TCP (Transmission Control Protocol) : transport fiable en mode connecté, point à point.
- ▶ Ces deux protocoles distinguent les applications au sein d'un même hôte par un « port » d'application.
 - ▶ Notation : Adresse IP de l'hôte : numéro de port
 - ▶ Exemple : 195.97.235.122:80
 - ▶ Cf. <http://www.frameip.com/liste-des-ports-tcp-udp/affichage-liste-des-ports-tcp-udp.php?plage=1>

Couche 4 – Transport



modèle
OSI

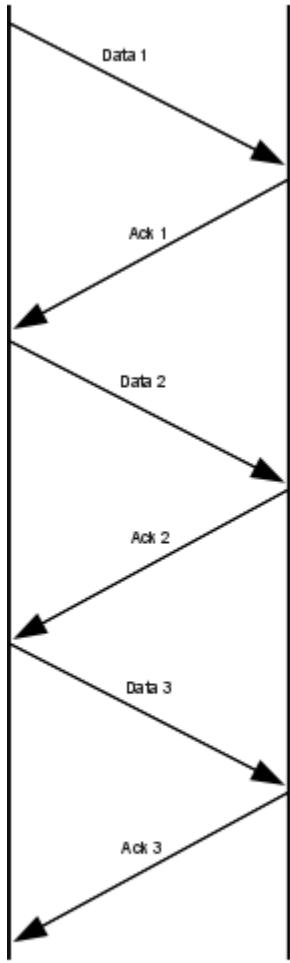
modèle
TCP/IP

Couche 4 – Transport

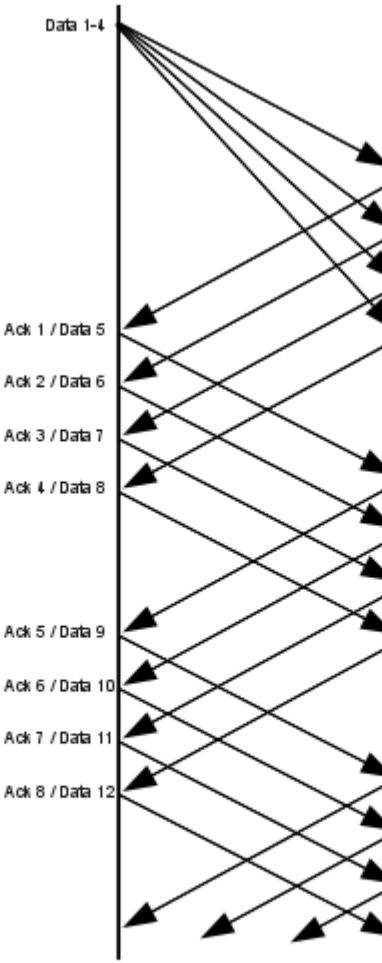
TCP – Transmission Control Protocol

- ▶ Les applications ont besoin d'échanger des volumes de données de manière fiable.
- ▶ Avant d'échanger des données, TCP établit une session entre les deux machines :
 - ▶ Etablissement de la session
 - ▶ Négociation de la qualité de service,...
 - ▶ Transfert des données
 - ▶ Libération de la session
- ▶ TCP s'occupe de :
 - ▶ Remettre les données dans l'ordre
 - ▶ Valider l'intégrité des données et de confirmer la bonne réception à l'émetteur.
 - ▶ Optimiser la vitesse de transmission : contrôle de flux et de congestion
 - ▶ Multiplexage
 - ▶ Eclatement
 - ▶ Mécanisme de fenêtre glissante à taille variable à l'aide du RTT (Round Trip Time)

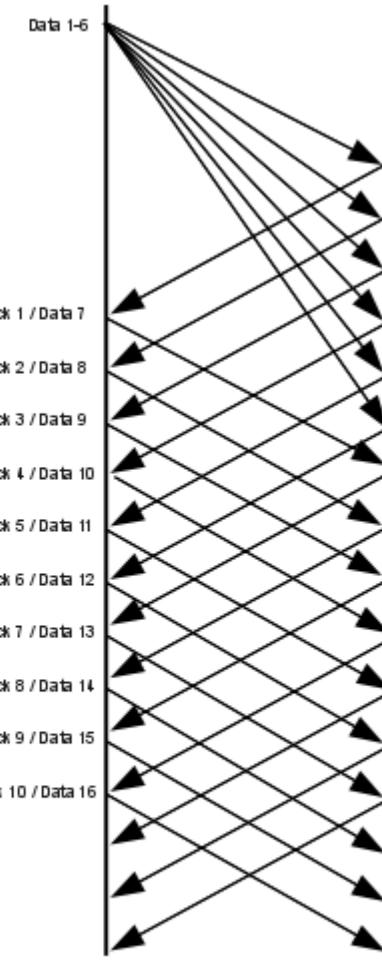
Couche 4 – Transport TCP – Fenêtre de transmission



WinSize = 1



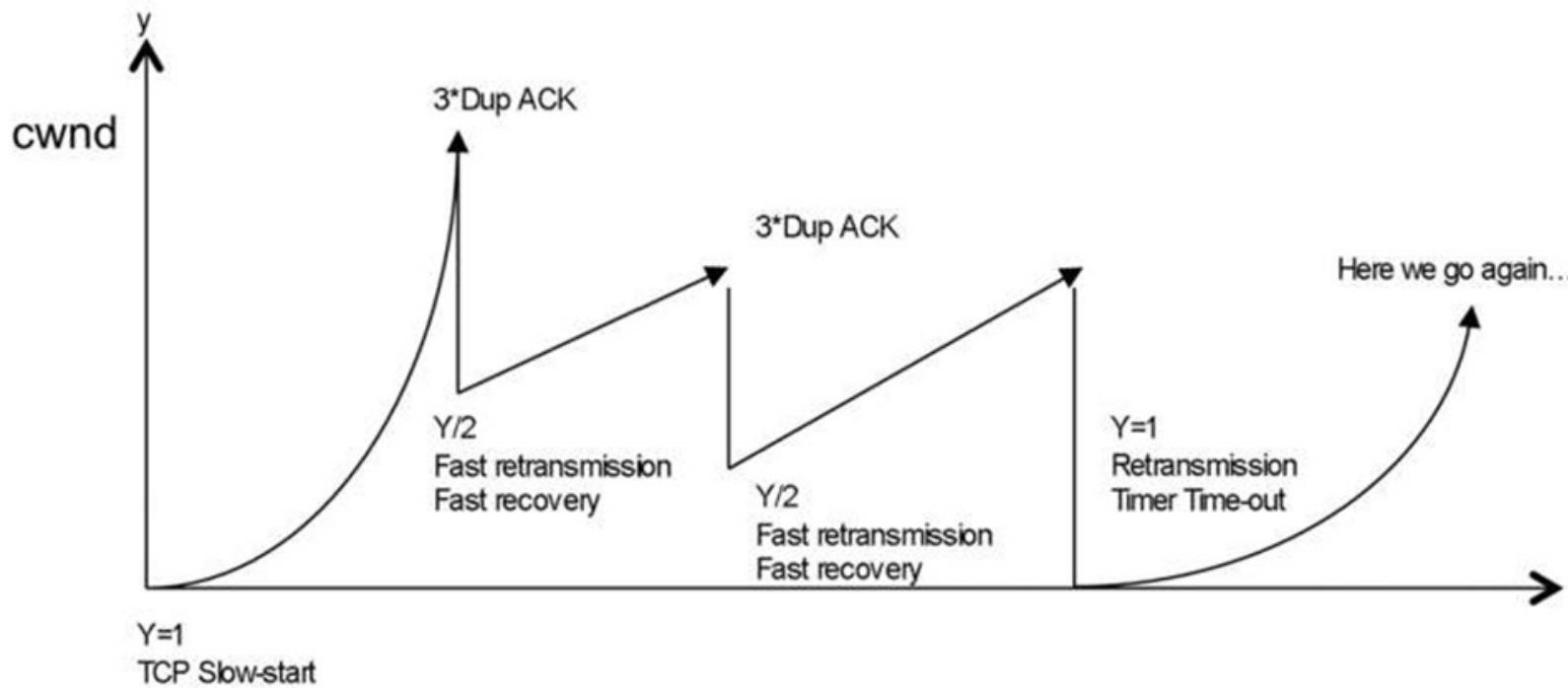
WinSize = 4



WinSize = 6

Sliding Windows, bandwidth 6 packets/RTT

Couche 4 – Transport TCP – Contrôle de la congestion



Convergence de TCP vers la meilleure fenêtre pour la connexion.

Couche 4 – Transport

User Datagram Protocol - UDP

- ▶ Utilise IP pour acheminer les messages entre les hôtes.
- ▶ Services UDP
 - ▶ Adressage des applications par n° de port
 - ▶ Mux/Demux des numéros de port
 - ▶ Contrôle facultatif de l'intégrité des données
- ▶ Même problèmes que pour IP
 - ▶ Possibilité de pertes, duplication, dé séquencement des messages
 - ▶ Pas de régulation de flux

Une application qui utilise UDP doit gérer elle-même ces problèmes !

- ▶ Exemples de service
 - ▶ Service de temps : N.T.P. = Network Time Protocol qui distribue une référence horaire dans un réseau
 - ▶ D.N.S.
 - ▶ D.H.C.P.
 - ▶ Vidéo à la demande
 - ▶ Téléphonie
 - ▶ Visioconférence
- ▶ Modèles de service applicatif Client / Serveur :
 - ▶ Un serveur démarre un service applicatif associé à un port UDP et écoute.
 - ▶ Un client envoie une requête à l'adresse du serveur : port

Les Réseaux

ENSAM

Karim Boudjemaïa

Études et Projets Réseaux – RENATER

Karim.boudjemaia@renater.fr

Cours n°4

Plan du cours 4

I. Notion de sécurité des réseaux

1. Objectifs
2. Exemples de menaces
3. Parades

2. Applications réseaux

1. VPNs
2. Client-Serveur
3. Pairs à pairs

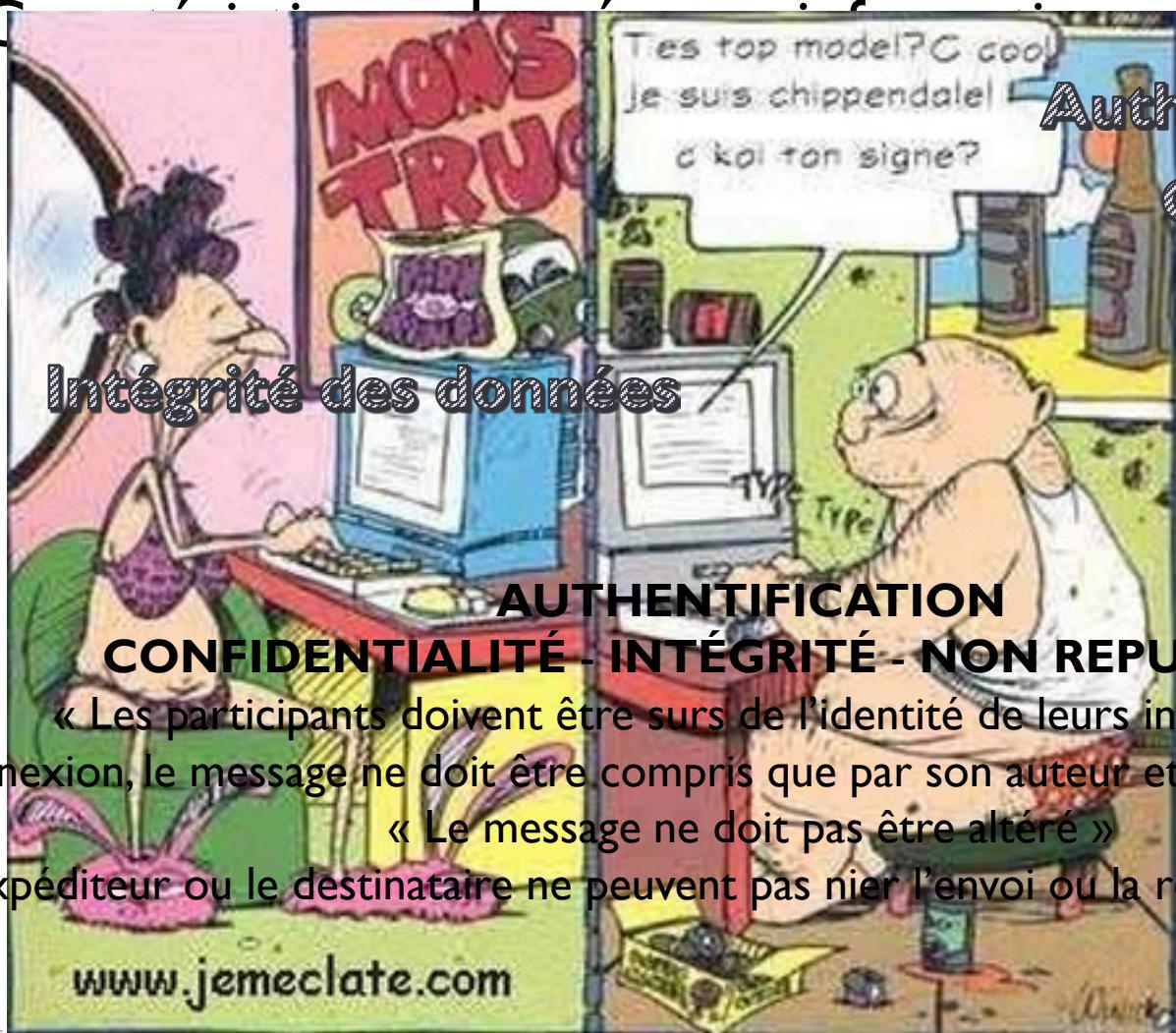
3. Et demain

1. Le Cloud
2. Software Defined Network (SDN)
3. Internet of Things (IoT)

Sécurité dans les réseaux

Contexte

- ▶ Confidentialité : Chiffrement
- ▶ Intégrité : Integrity
- ▶ Non Répudiation : Non Repudiation



« Les participants doivent être sûrs de l'identité de leurs interlocuteurs »

« La connexion, le message ne doit être compris que par son auteur et son(ses) destinataire(s) »

« Le message ne doit pas être altéré »

« L'expéditeur ou le destinataire ne peuvent pas nier l'envoi ou la réception du message »

Sécurité dans les réseaux

Généralités

- ▶ La sécurité se divise globalement en deux parties :
 - ▶ Sécurité de la communication
 - ▶ Sécurité des infrastructures réseaux
- ▶ La sécurité n'a pas été prévue dès l'origine des réseaux. Elle fait l'objet d'efforts depuis env. 20 ans pour apporter une solution. (ex. histoire de l'automobile)
- ▶ Les parades se jouent autant au niveau **humain** que **technique**

Sécurité dans les réseaux

Exemples de menaces sur la communication

▶ Capture et rejet de mot de passe

- ▶ Visuelle
- ▶ Electronique
- ▶ Cheval de troie :
 - ▶ <https://www.youtube.com/watch?v=wa1>
- ▶ Force brute (crack, dictionnaires)
- ▶ Deviner
 - ▶ mot de passe par défaut
 - ▶ mot de passe simple
- ▶ Ingénierie sociale
 - ▶ <https://www.youtube.com/watch?v=Z2JhHpjK6RU>

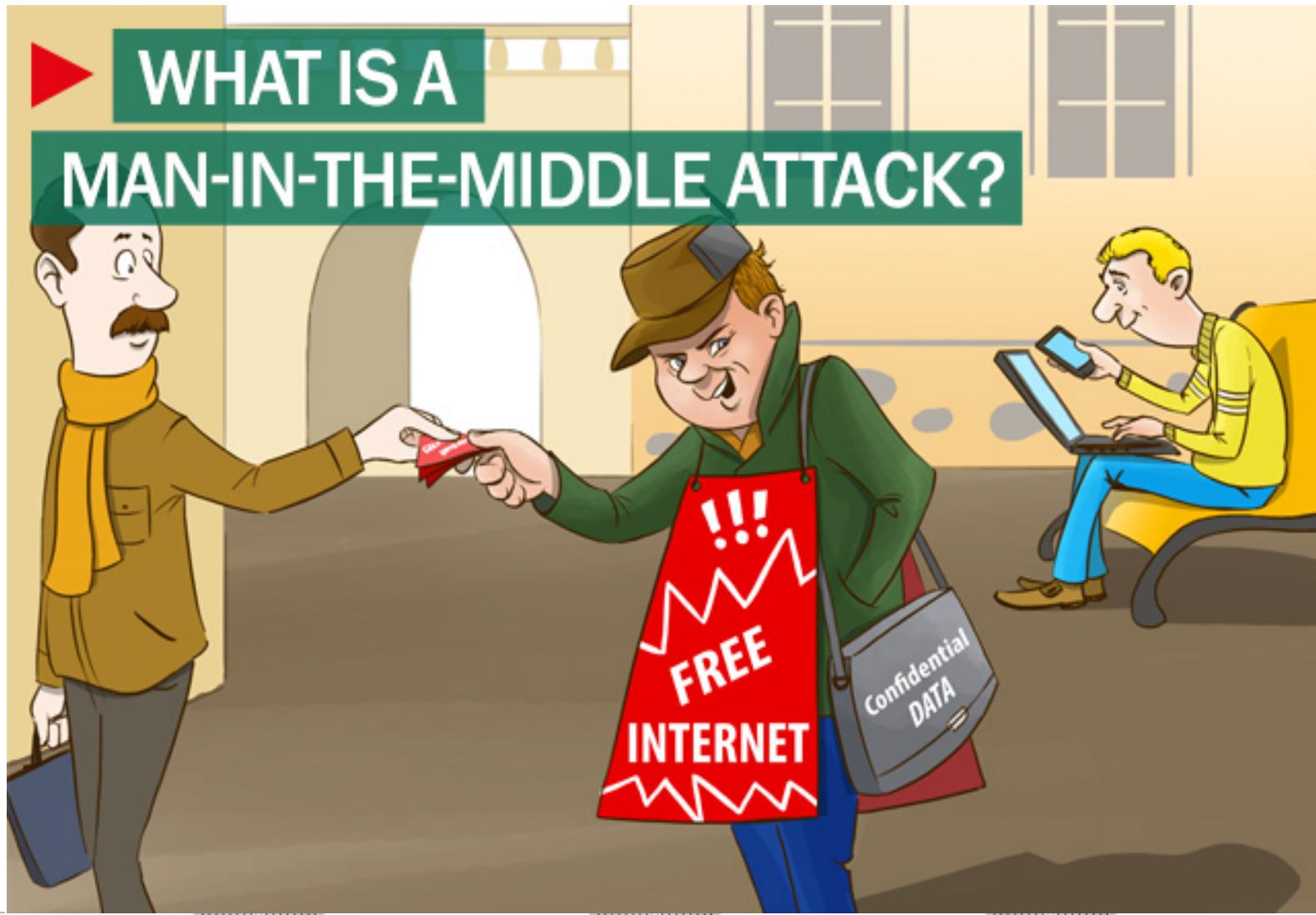


Sécurité dans les réseaux

Exemples de menaces sur la communication

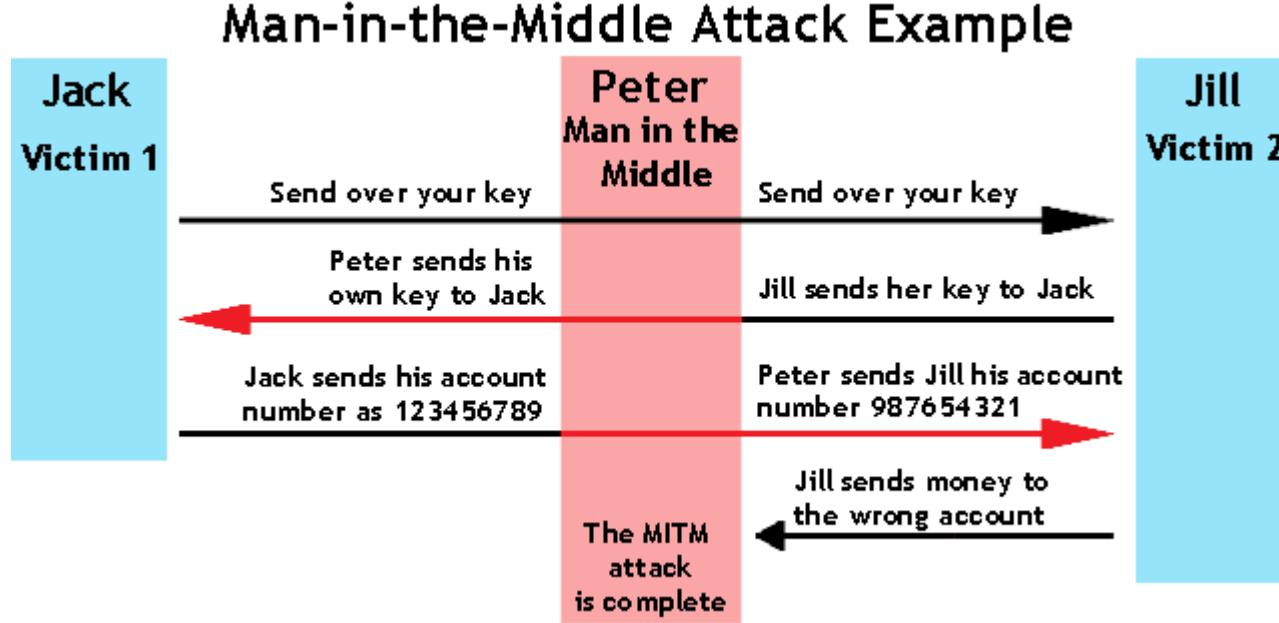


► WHAT IS A MAN-IN-THE-MIDDLE ATTACK?



Sécurité dans les réseaux

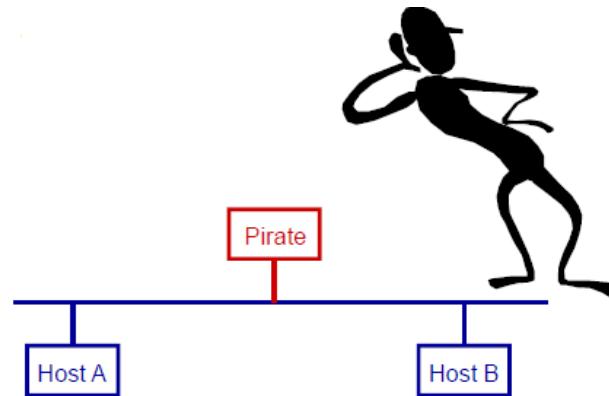
Exemples de menaces sur la communication



Sécurité dans les réseaux

Exemples de menaces sur la communication

- ▶ Opérations d'écoutes passives
 - ▶ Ecoute physique



- ▶ Ecoute Logique

- Spoofing de @ MAC, @ IP, port TCP, de séquence TCP, de numéro de fragments... :
 - Permet de ne pas être reconnu
 - Permet de prendre la place d'une autre machine/ d'un autre flux et d'introduire un flux déjà authentifié



Sécurité dans les réseaux

Exemples de menaces sur les infrastructures

- ▶ **Exploitation de failles connues**
 - ▶ Avertissements CERT,
 - ▶ Exemple : bulletin CERT-Renater
 - ▶ Suivre les mises à jour éditeurs
 - ▶ Ou pas encore trop connues : ZeroD
- ▶ **Exploitation des faiblesses des protocoles**
 - ▶ W.E.P. = Wired Equivalent Protocol (remplacé par WPA2 = WIFI Protected Access)
 - ▶ Tous les protocoles sans authentification forte
- ▶ **Bugs de configuration**
 - ▶ Les règles d'administration des pare feu sont fragilisées au fil du temps.
- ▶ **Déni de service distribué**
 - ▶ DDoS :
 - ▶ <http://www.bbc.com/news/education-35043243>

Sécurité dans les réseaux

Exemples de menaces - Les virus

- ▶ Différents types de virus :

- ▶ Boot sector virus,
- ▶ File infected virus
- ▶ Polymorphic virus
- ▶ Stealth virus
- ▶ Encrypted virus
- ▶ Worms
- ▶ Cheval de Troie
- ▶ Time bomb virus
- ▶ Logical bombs

- ▶ Le marché des failles informatiques !

- ▶ http://www.lemonde.fr/pixels/article/2015/09/23/le-business-des-zero-day-ces-failles-inconnues-des-fabricants-de-logiciel_4768638_4408996.html

Sécurité dans les réseaux

Constat édifiant

Ces victoires, même provisoires, sont assez rares. Lors de la conférence BotConf 2015, qui a réuni 265 experts de 34 pays à Paris début décembre, l'ambiance était combative, mais pas très optimiste : les intervenants ont surtout insisté sur les progrès constants réalisés par les botmasters. Un **ingénieur sécurité français** employé par une société américaine résume la situation : « *L'innovation est menée par les attaquants, pas par les défenseurs. Quand un expert annonce qu'il a fait une découverte, ça signifie généralement qu'il a trouvé un fichier sur Internet, et repéré une erreur commise par un botmaster. Chaque année, nous organisons des conférences pour nous esbaudir sur les progrès incroyables réalisés par les attaquants au cours de l'année passée.* »

LeMonde.fr, 10 décembre 2015

- ▶ http://www.lemonde.fr/pixels/article/2015/12/10/sur-internet-la-lutte-sans-fin-contre-les-ordinateurs-zombies-des-botnets_4828887_4408996.html?xtmc=securite_informatique_decembre_2015&xtcr=2

Sécurité dans les réseaux

Concepts généraux

- ▶ Que protégez vous
 - ▶ Accès aux données, intégrité des transactions...
- ▶ De qui ?
 - ▶ Interne, Externe ?
- ▶ Quel est le niveau de sécurité requis ?
 - ▶ Périmètre de défense
 - ▶ Cœur vulnérable en cas d'intrusion
 - ▶ Sécurité en profondeur
 - ▶ Très sécurisé, mais ne passe pas à l'échelle.

Sécurité dans les réseaux

Concepts généraux

- ▶ Interdire sauf si autorisé
 - ▶ Meilleure sécurité, mise en place laborieuse
- ▶ Autorisé sauf si interdit
 - ▶ Mise en place plus simple
 - ▶ Mais ne peut s'améliorer qu'après avoir subi une attaque !
- ▶ Sécurité totale
 - ▶ Réseau débranché !!!
- ▶ Sécurité est donc une question de compromis

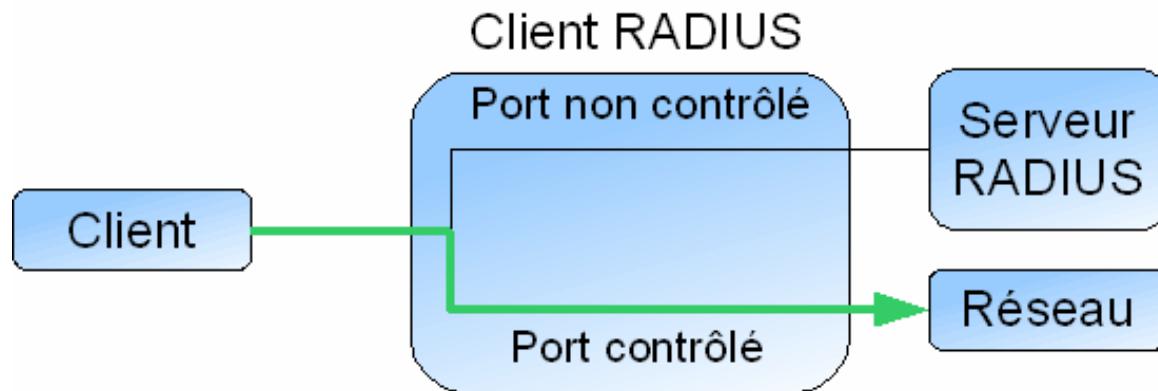
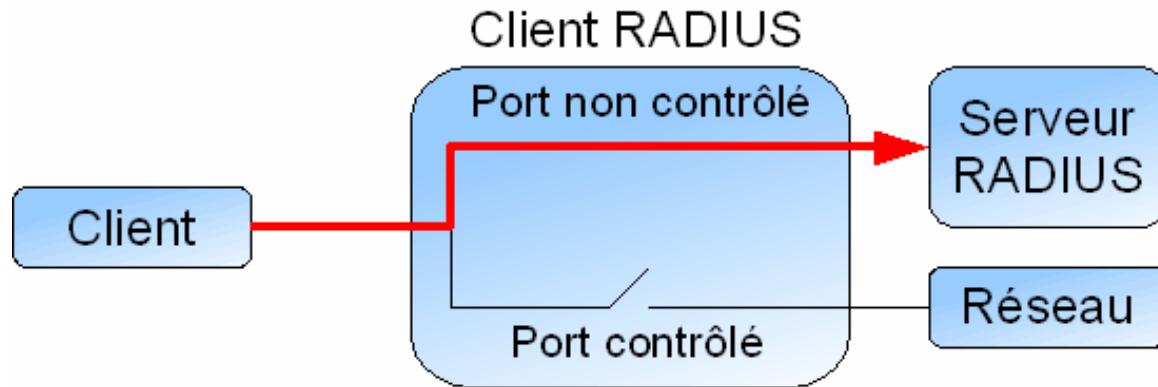
Sécurité dans les réseaux

Les parades

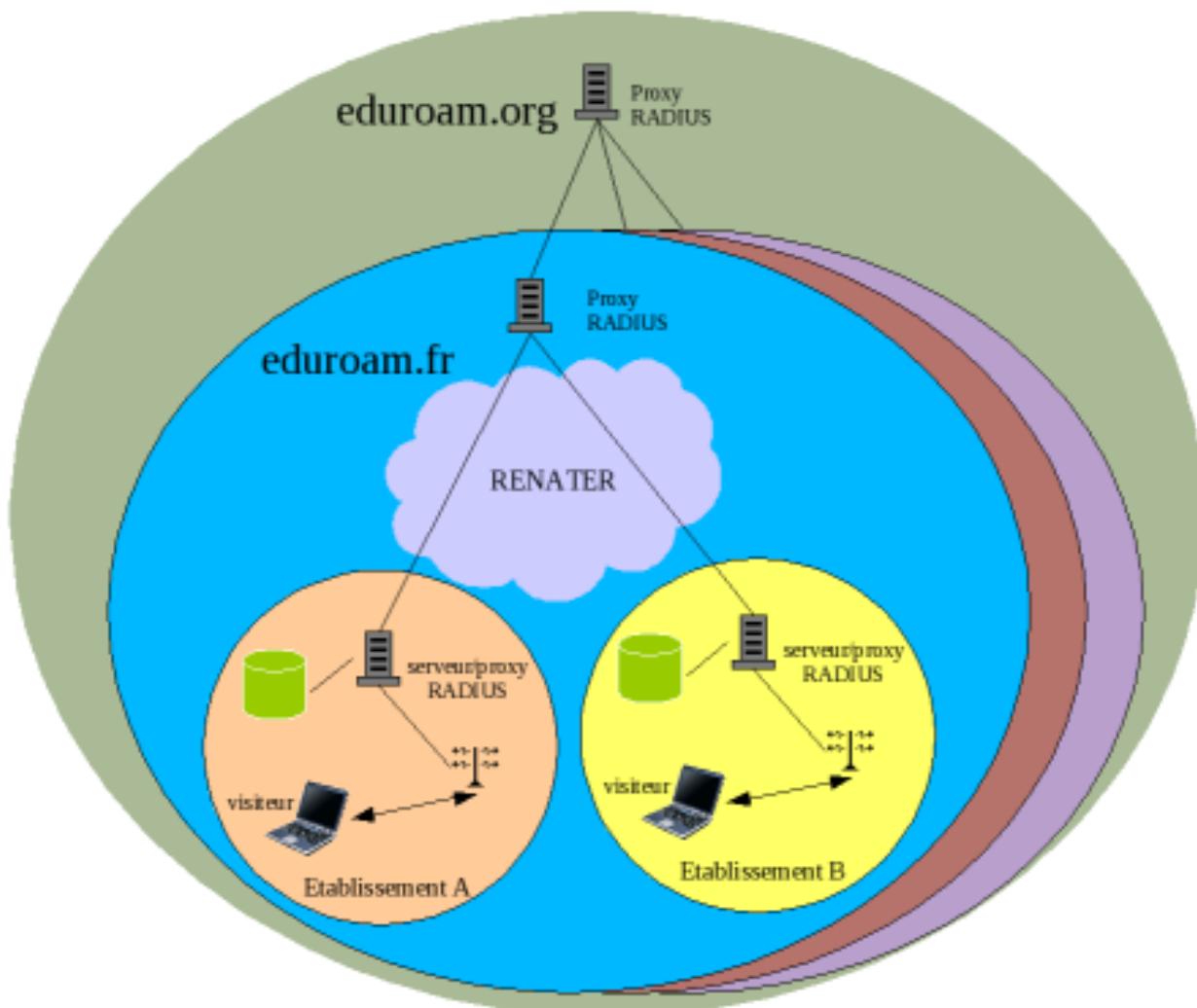
- ▶ **Authentification**
 - ▶ Authentification simple : concerne que l'utilisateur
 - ▶ Authentification mutuelle : concerne l'utilisateur et le serveur
 - ▶ Authentification forte : nécessite deux infra. complètement distinctes pour s'authentifier. Par ex. : Internet fixe + réseau mobile
- ▶ **Authentification par :**
 - ▶ Login/pwd
 - ▶ Code PIN
 - ▶ Biométrique
 - ▶ Etc...

Sécurité dans les réseaux

RADIUS et 802.1X



Sécurité dans les réseaux RADIUS et 802.1X



Sécurité dans les réseaux

Les parades

- ▶ L'intégrité des flux de données
 - ▶ But : S'assurer qu'aucun bit transmis n'a été modifié
 - ▶ Besoin d'une empreinte électronique
 - ▶ Peut prendre la forme d'une signature (Ex. : Checksum)
 - ▶ Intégrité + authentification
 - ▶ L'empreinte peut prendre la forme d'un chiffrement
 - ▶ Intégrité + authentification + confidentialité sont assurés
 - ▶ L'intégrité plus simplement peut être assurée par :
 - ▶ Un algorithme qui calcule une empreinte numérique, on parle de hachage
 - ▶ Un chiffrement est appliqué ensuite pour protéger le premier algorithme
 - ▶ Exemples :
 - MD5 (Message Digest #5) : empreinte de 128 bits,
 - SHA-1 (Secure Hash Algorithm) : empreinte de 160 bits, SHA-2

Sécurité dans les réseaux

Les parades

- ▶ **La non-répudiation :**
 - ▶ Empêcher un éventuel refus du récepteur d'effectuer une action suite à un démenti de réception (ex. : email)
 - ▶ Pouvoir tracer un email comme on peut tracer un appel téléphonique
 - ▶ Valeur juridique d'un message électronique ?

- ▶ **Solution :**
 - ⇒ Accusé de réception
 - ⇒ Tiers de confiance : Notaire électronique (ou email diffusé à une liste générale ?)

Sécurité dans les réseaux

Les parades

- ▶ La confidentialité :
 - ▶ Nécessite l'utilisation du chiffrement
 - ▶ Différents systèmes de chiffrement
 - ▶ Chiffrement symétrique
 - ▶ Chiffrement asymétrique
 - ▶ Mais, toutes les techniques de chiffrement sont à priori violables, tout est une question de moyen et de temps...

Sécurité dans les réseaux

Les parades

► Le chiffrement :

Texte en clair (‘Cleartext’)	Texte chiffré ou cryptogramme (‘Ciphertext’)	Texte en clair (‘Cleartext’)
---------------------------------	----------------------------------------------------	---------------------------------



Clé de chiffrement k_1
(‘Encryption Key’)

Clé de déchiffrement $k1$ ou $k2$
(‘Decryption Key’)

Sécurité dans les réseaux

Les parades

- ▶ **Chiffrement symétrique :**
 - ▶ La même clé est utilisée pour chiffrer et déchiffrer
 - ▶ Le déchiffrement se fait par transformation inverse du chiffrement
 - ▶ Chiffres en continu ou par bloc
- ▶ **Chiffres asymétrique (dit à clé publique) :**
 - ▶ Deux clés distinctes : une clé pour chiffrer, une clé pour déchiffrer :
 - ▶ Clé publique visible de tous,
 - ▶ Clé privée connue seulement de son propriétaire
 - ▶ Permet de réaliser des signatures digitales

Sécurité dans les réseaux

Les parades

- ▶ Exemples de chiffrement symétrique :
 - ▶ Chiffrement de césar
 - ▶ DES, 3 DES
 - ▶ A5/1 : fonction de chiffrement du GSM. Utilise des registres à décalage à rétroaction linéaire.
 - ▶ Facile à implémenter
 - ▶ Rapide (n'introduit pas de décalage dans la transmission)
 - ▶ Vulnérable depuis par la NSA selon Edward Snowden
 - ▶ RC4 (Rivest Code #4) : Jeu de permutation dans un tableau d'octets.
 - ▶ Populaire dans les applications des années 90.
 - ▶ Utilisé dans le wifi : WEP.
 - ▶ Longueur de Clé pouvant atteindre 2048 bits
 - ▶ Vulnérabilité démontrée en 2001. Toutes les valeurs chiffrées ne sont pas équiprobables : **attaque par collisions**.
 - ▶ AES (Advanced Encryption Standard)
 - ▶ Mécanisme de substitutions/permurations
 - ▶ 3 tailles de clés : 128, 192 et 256 bits
 - ▶ 1^{er} échange de clé risqué – moyen de sécurisation à ajouter.
 - ▶ Renouvellement périodique de la clé dans le flux chiffré.
 - ▶ Non cassé à ce jour.

Sécurité dans les réseaux

Les parades

- ▶ Exemples de chiffrement asymétrique :
 - ▶ RSA
 - ▶ 1977 : Ron Rivest, Adi Shamir, Leonard Adleman.
 - ▶ Libre de droits depuis 2003.
 - ▶ Considéré sûr avec des clés suffisamment longues : 1024bits à 4096bits.
 - ▶ Diffie-Hellman
- ▶ Basée sur une fonction mathématique à sens unique
 - ▶ Facile à calculer dans un sens
 - ▶ Difficile à inverser, sauf si l'on possède une information particulière, nommée : clé privée.
 - ▶ Produit de deux nombre $n = p * q$
 - ▶ p et q premiers, et très grand
 - ▶ Si on ne connaît pas p et q , factoriser n est difficile

Sécurité dans les réseaux

Les parades – Principe chiffrement asymétrique

I- Chiffrement avec
la clé publique
de Bob



2- Chiffrement avec
la clé privée d'Alice

3- Dechiffrement avec
la clé publique
d'Alice

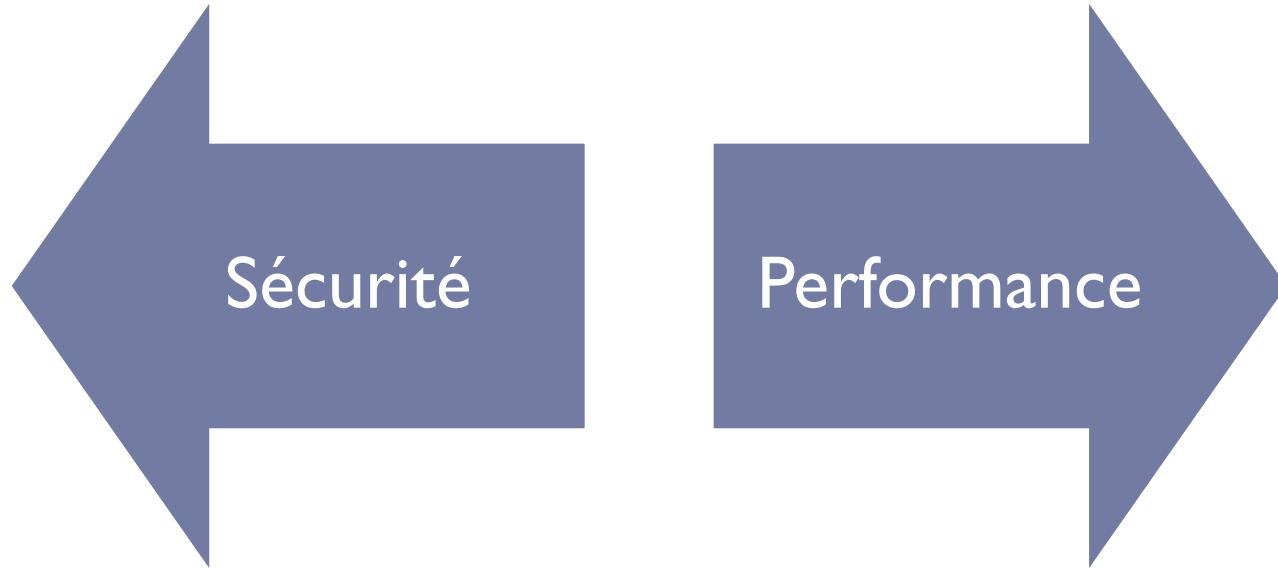


4- Dechiffrement avec
la clé privée de Bob

Sécurité dans les réseaux

Les parades

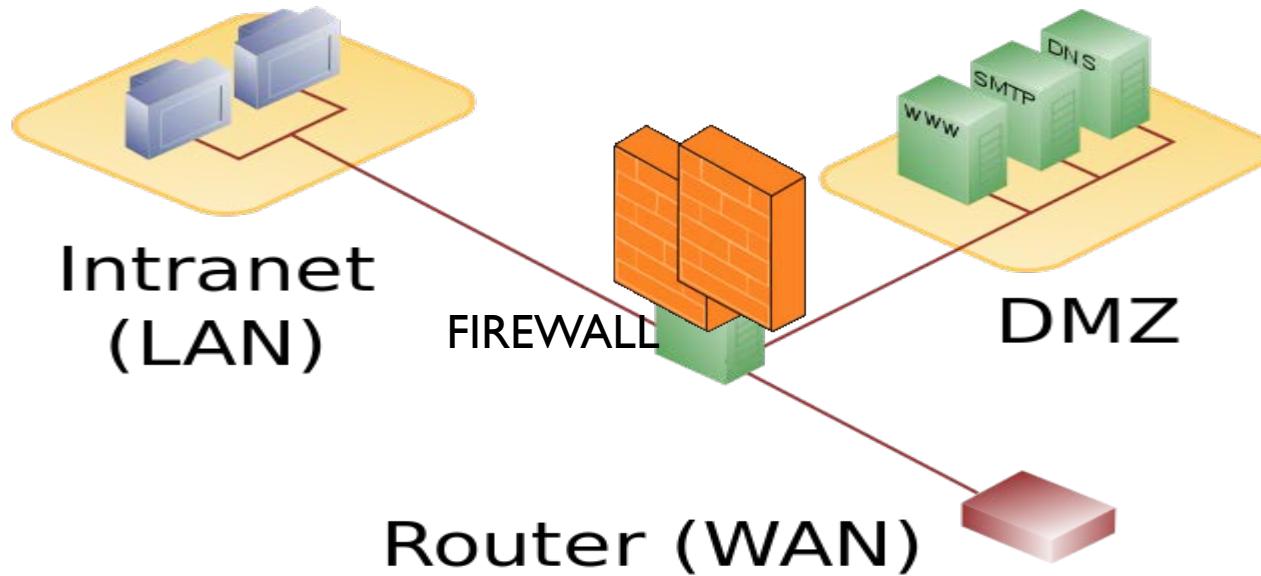
- ▶ Bilan sur le choix du chiffrement :
 - ▶ Compromis sécurité et rapidité de traitement à trouver :



Sécurité dans les réseaux

Les parades contre les virus

- ▶ Anti-virus
 - ▶ À jour
- ▶ Firewall



Sécurité dans les réseaux

Les parades contre les virus

▶ Firewall :

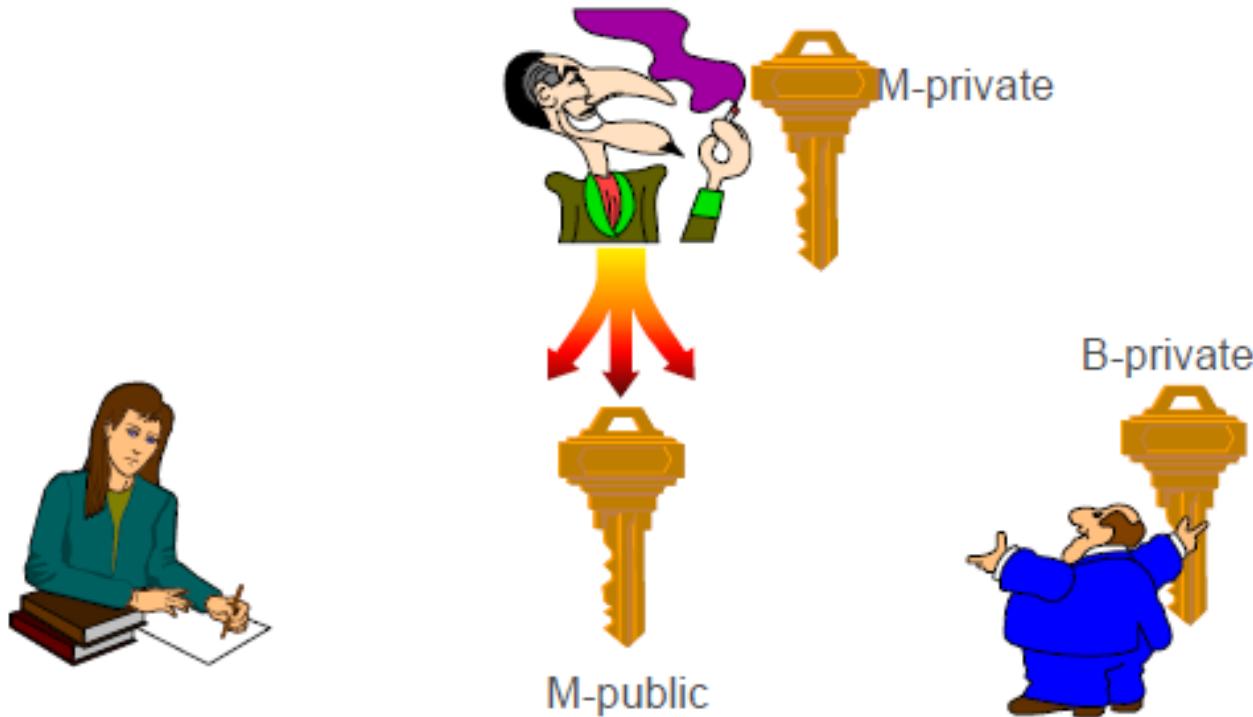
- ▶ D'une manière générale, un FW interdit tous les paquets sauf ceux d'une liste prédéterminée
- ▶ Un ensemble de règles de filtrage permet :
 - ▶ D'autoriser la connexion (allow) ;
 - ▶ De bloquer la connexion (deny) ;
 - ▶ De rejeter la demande de connexion sans avertir l'émetteur (drop).
- ▶ Exemple de règles :

Règle	Action	IP source	IP dest	Protocol	Port source	Port dest
1	Accept	192.168.10.20	194.154.192.3	tcp	any	25
2	Accept	any	192.168.10.3	tcp	any	80
3	Accept	192.168.10.0/24	any	tcp	any	80
4	Deny	any	any	any	any	any

Sécurité dans les réseaux

Certificats

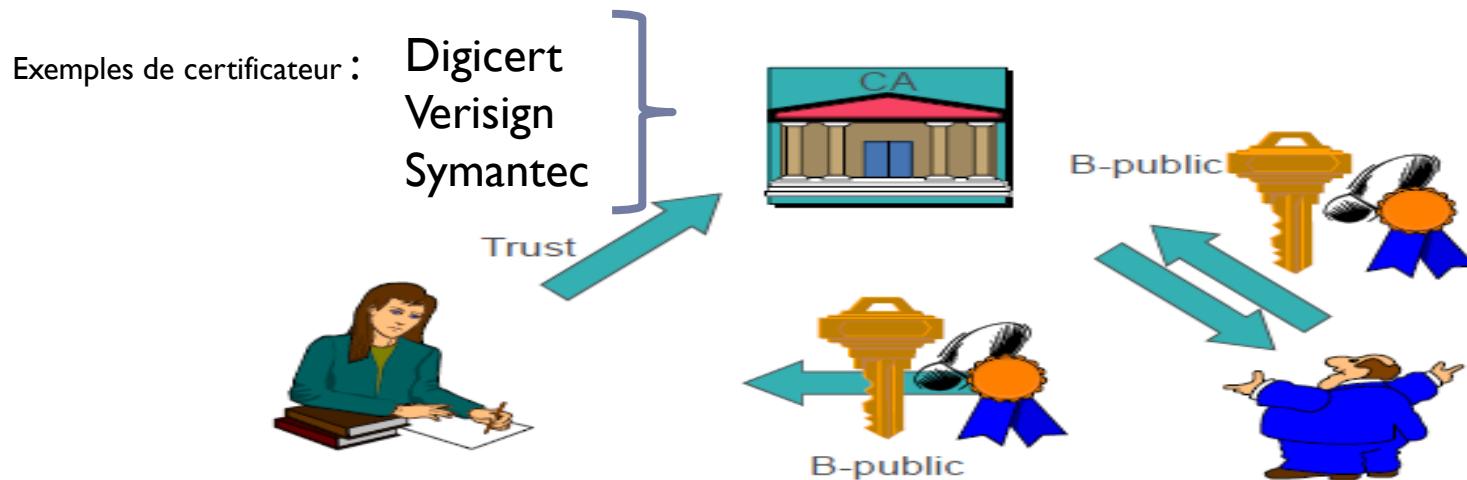
- ▶ Passage à l'échelle
- ▶ Attaque possible sur distribution de fausses clés



Sécurité dans les réseaux

Autorités de certification

- ▶ Nécessité d'une autorité de certification (PKI- Public Key Infrastructure) qui puisse valider l'identité du demandeur de certification
- ▶ Le demandeur fournit des informations sur son identité (coordonnées postales, téléphoniques,...) et une clé publique.
- ▶ En retour, création d'un certificat associé à cette clé publique.



Sécurité dans les réseaux

Certificat

The screenshot shows a web browser window with the URL <https://webmail.renater.fr>. A large blue arrow points from the top left towards a detailed certificate information dialog box.

Détails du certificat : *.renater.fr

Général [Détails]

Ce certificat a été vérifié pour les utilisations suivantes :

- Certificat client SSL
- Certificat serveur SSL

Émis pour

Nom commun (CN)	*.renater.fr
Organisation (O)	Reseau National de Télécommunication pour La Technologie, L'Enseignemen
Unité d'organisation (OU)	IT
Numéro de série	0C:8F:6A:B3:44:E7:09:8B:13:1A:B0:A8:2A:F9:63:FF

Émis par

Nom commun (CN)	TERENA SSL CA 3
Organisation (O)	TERENA
Unité d'organisation (OU)	<Ne fait pas partie du certificat>

Période de validité

Débute le	16/10/2015
Exire le	24/10/2018

Empreintes numériques

Empreinte numérique SHA-256	2A:36:0D:9B:BB:D7:3C:64:1F:EF:35:14:3C:E3:AD:C9:09:0A:35:45:75:1A:77:90:AF:6D:27:F9:F2:C7:7A:B8
Empreinte numérique SHA1	45:3E:25:79:AB:03:3A:F0:F5:E7:7A:91:D1:19:36:0B:B8:F9:E11

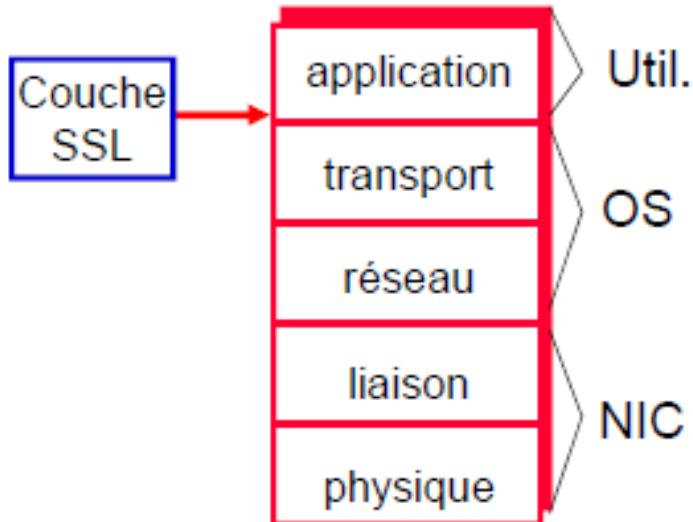
Fermer

Sécurité dans les réseaux

Protocoles de sécurité – SSL -> TLS

- ▶ Secure Sockets Layer -
Transport Layer Security

- ▶ Intervient à la couche 7
- ▶ Sécurisation application par application :
 - ▶ Htts



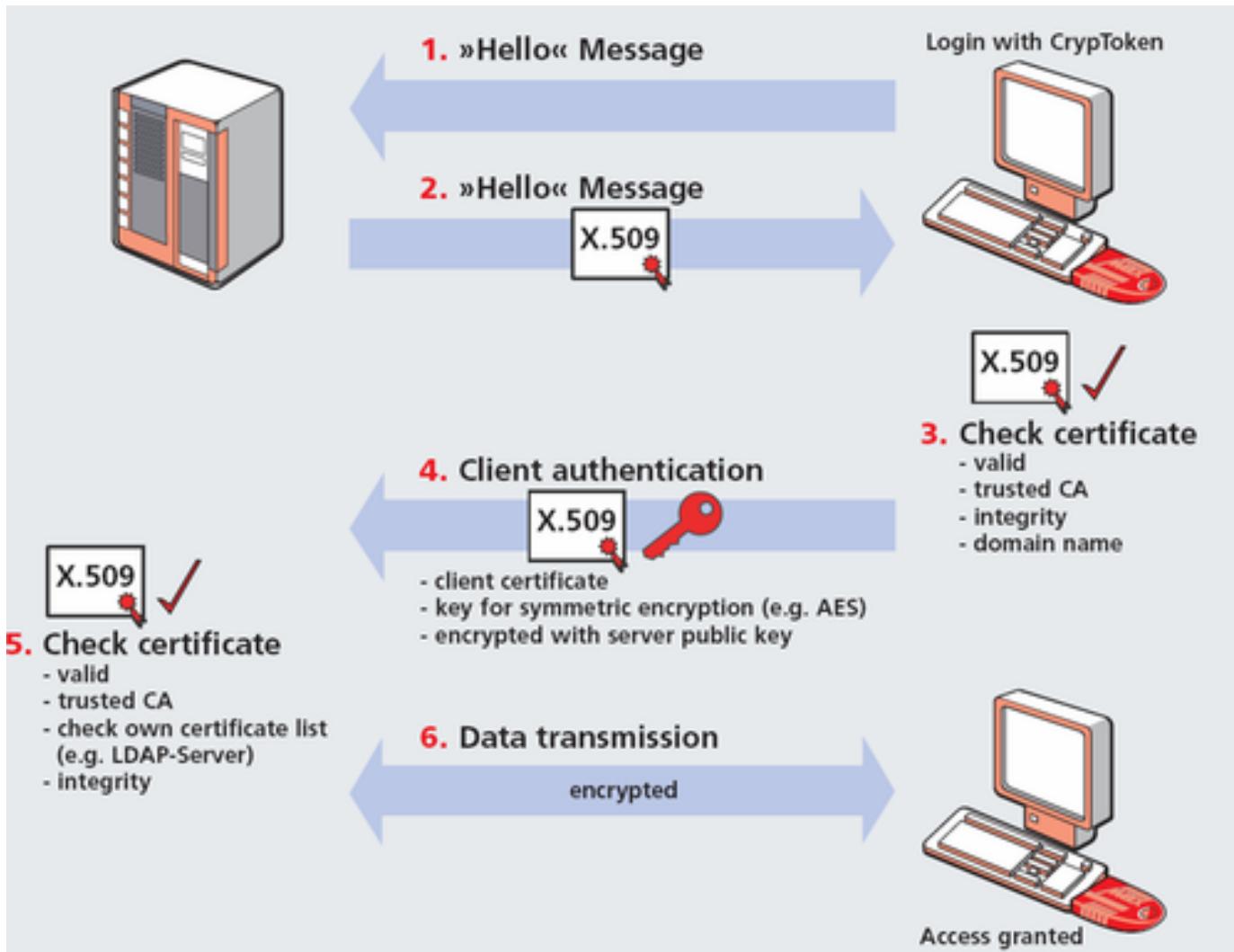
Sécurité dans les réseaux

Protocoles de sécurité – SSL -> TLS

- ▶ Protocole utilisé pour la plupart des transactions sur internet
 - ▶ failles dans l'implémentation SSL, pas dans le mécanisme (openSSL, windows ssl...)
 - ▶ Remplacé par TLS
- ▶ Exemple d'achat d'un livre sur fnac.com
 - ▶ On veut être sûr d'être connecté à fnac.com (authentification du site marchand).
 - ▶ Les informations de paiement (cb) doivent être protégées pendant leur transit (confidentialité, intégrité).
 - ▶ Tant que la banque confirme la transaction, le site marchand se moque de savoir qui vous êtes, pas d'authentification mutuelle.

Sécurité dans les réseaux

Protocoles de sécurité – SSL/TLS

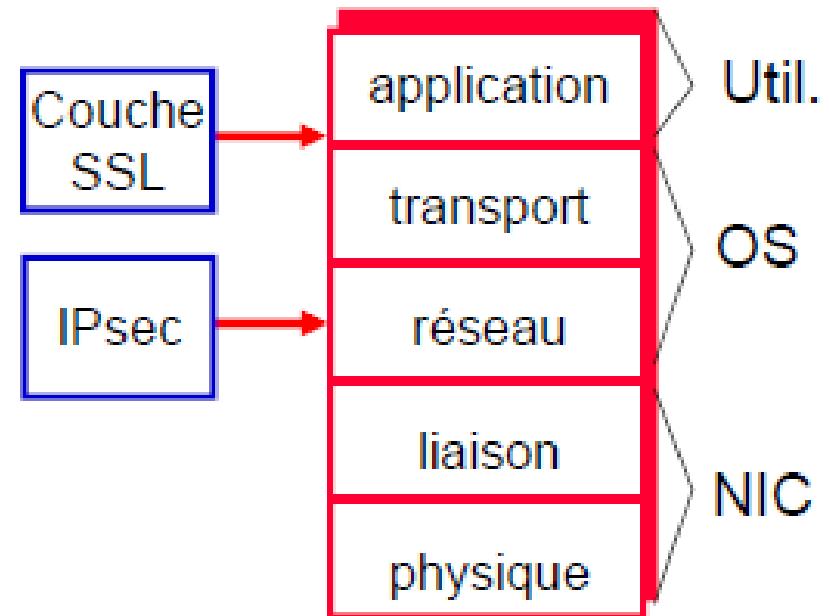


Sécurité dans les réseaux

Protocoles de sécurité – IPSec

IPsec fait partie de la couche réseau.

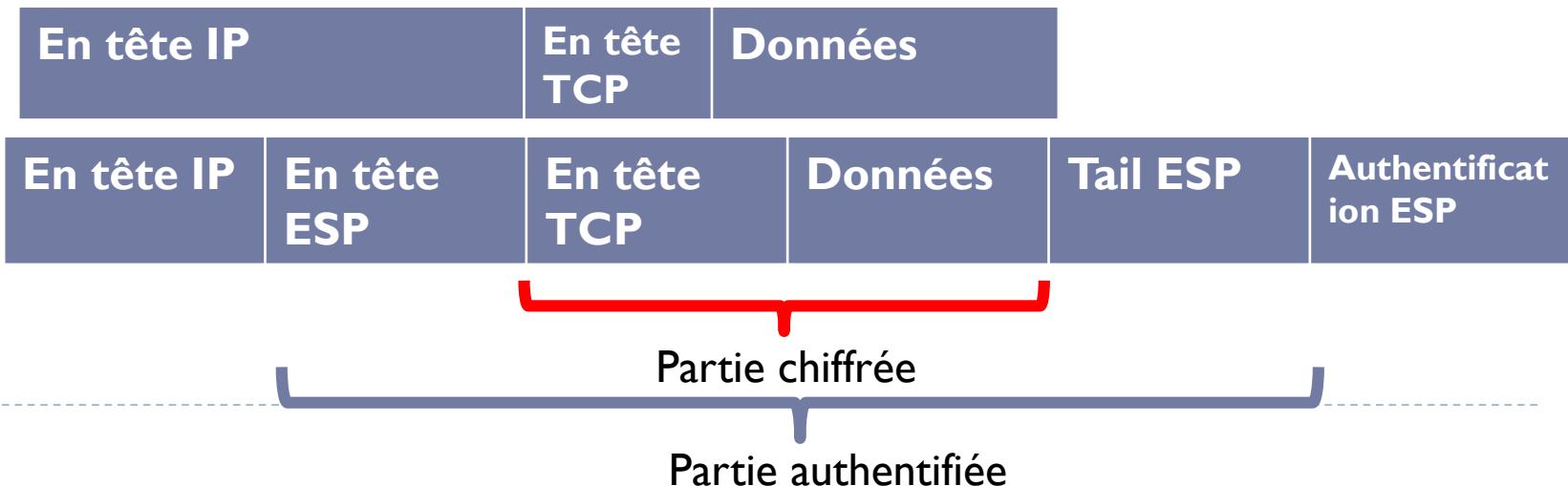
IPsec est transparent pour les applications



Sécurité dans les réseaux

Protocoles de sécurité – IPSec

- ▶ Nécessite de créer une association de sécurité spécifiant les paramètres à utiliser durant une connexion :
 - ▶ Type d'authentification
 - ▶ Type de chiffrement
 - ▶ Données de synchronisation ou d'initialisation
 - ▶ Durée de vie des clés
- ▶ ESP : Encapsulation Security Payload



Sécurité dans les réseaux

Bilan

- ▶ Un équilibre entre sécurité et performance :
 - ▶ Clés longues ou algorithme de chiffrement sûr versus
 - ▶ Augmentation de latence ou débit partiellement diminué
- ▶ Un équilibre « sociétal » entre :
 - ▶ Protection des données personnelles : désir de sécurité
 - ▶ Droit d'accès (en cas d'instruction juridique par exemple) : désir de liberté
- ▶ Course après les pirates informatiques pour maintenir efficace un système de sécurité

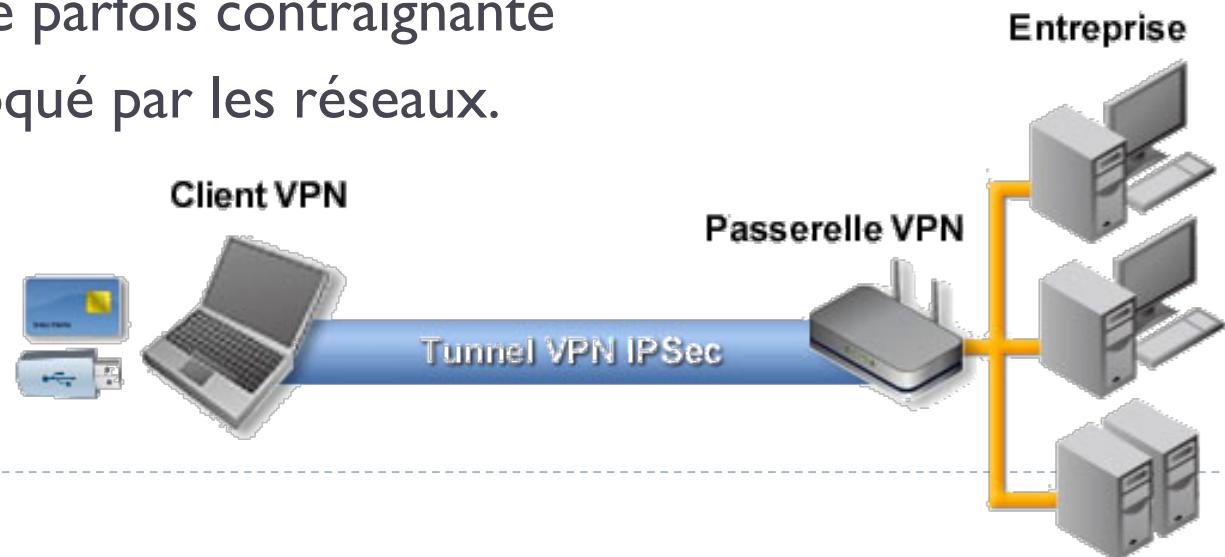


Services Réseau

Applications réseaux

VPN Entreprise – Utilisateurs

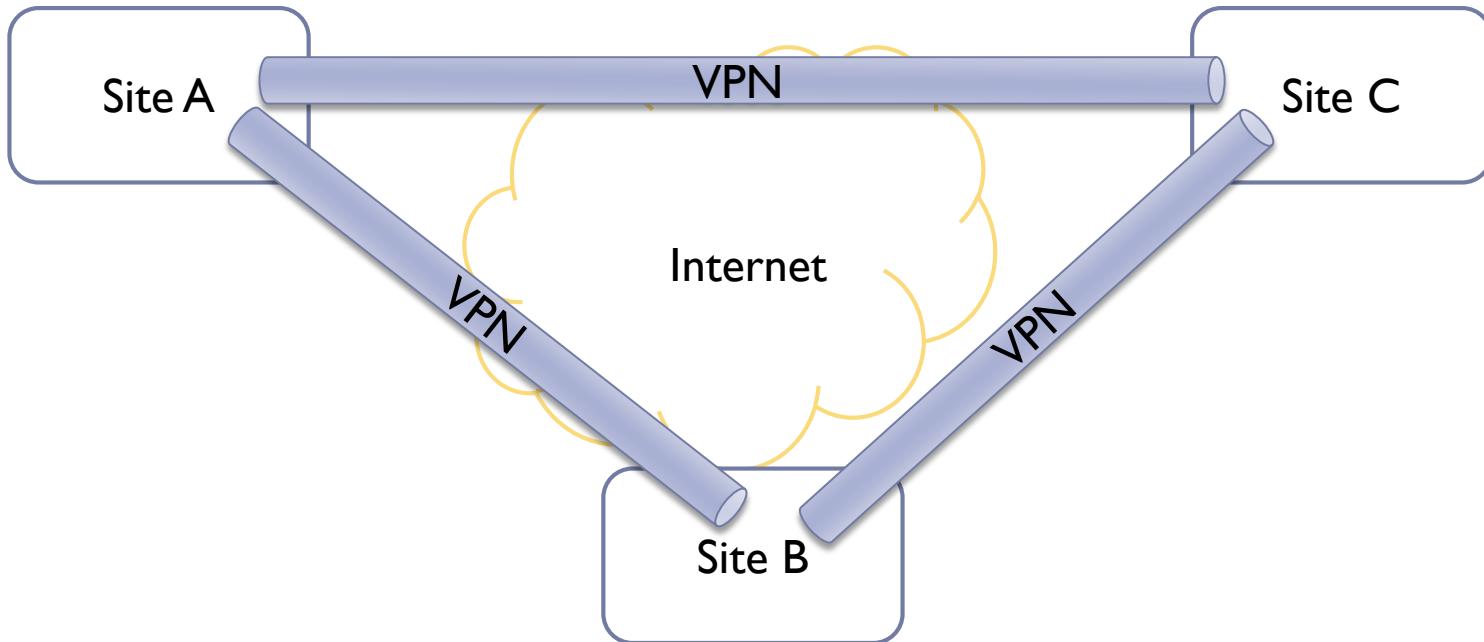
- ▶ Accès au réseau local depuis l'extérieur
- ▶ Chiffre les communications
- ▶ Avantages
 - ▶ Flexibilité
 - ▶ Protège de l'espionnage industriel
- ▶ Inconvénients
 - ▶ Mise en place parfois contraignante
 - ▶ Peut être bloqué par les réseaux.



Applications réseaux

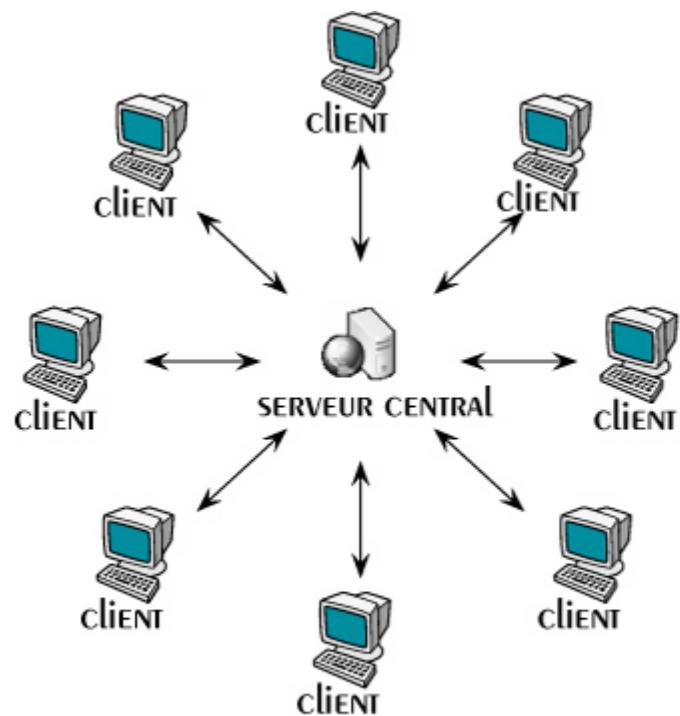
VPN Entreprise – Multi-site

- ▶ Interconnexion privée de sites distants à travers un opérateur de services réseaux (FAI).
- ▶ Point à point ; multipoint à multipoint
- ▶ Service IP ou Ethernet

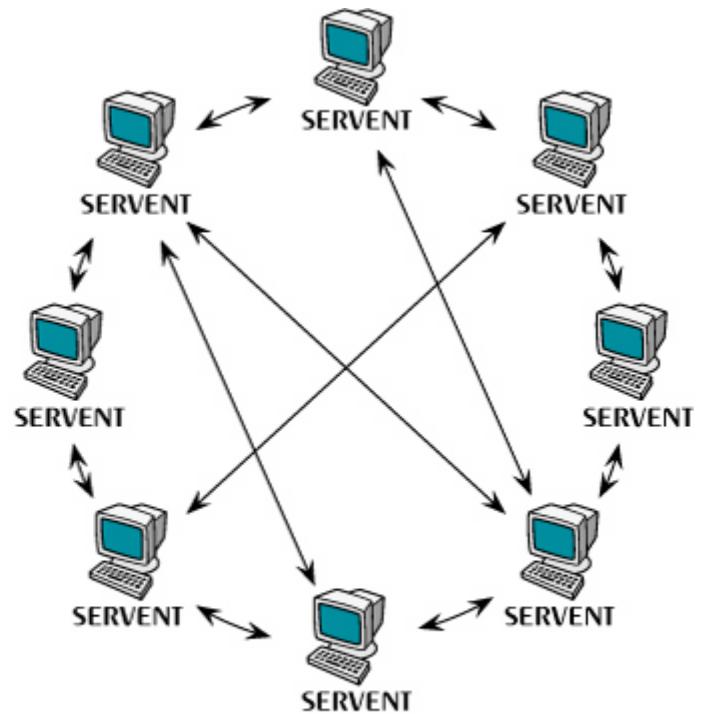


Applications réseaux

Client/Server (vs) P2P



ARCHITECTURE CLIENT-SERVEUR



ARCHITECTURE PAIR-À-PAIR

Applications réseaux

Client/Server (vs) P2P

- ▶ P2P utilisé pour les transferts de ‘fichiers’ entre internautes
- ▶ De plus en plus utilisé par les entreprises pour répartir leur trafic à destination de leurs clients
 - ▶ Mises à jour de jeu
 - ▶ Téléchargement multimédia
 - ▶ ...
- ▶ Utilisé par les entreprises informatiques innovantes
 - ▶ Facebook/Twitter mettent à jour leurs serveurs en un temps record.
 - ▶ Facebook : 1 minute.
 - ▶ Twitter : 12 secondes.
 - ▶ <https://blog.twitter.com/2010/murder-fast-datacenter-code-deploys-using-bittorrent>
 - ▶ <http://torrentfreak.com/facebook-uses-bittorrent-and-they-love-it-100625/>



Et demain...

Et demain...

Le 'Cloud'

- ▶ Le Cloud est une externalisation des moyens informatique.
- ▶ Infrastructure as a Service
IaaS
 - ▶ Location de serveurs
 - ▶ Location de temps de calcul
- ▶ Software as a Service
SaaS
 - ▶ Location d'une application : Mail, Compta, agendas, Bureautique...
- ▶ Network as a Service
NaaS
 - ▶ VPN
 - ▶ Bande passante à la demande



Et demain...

Le 'Cloud'

▶ Faiblesses

- ▶ Quid de la gouvernance de vos données ?
 - ▶ Services US soumis au Patriot Act...
- ▶ Pérennité ?
- ▶ Sécurité ?

▶ Forces

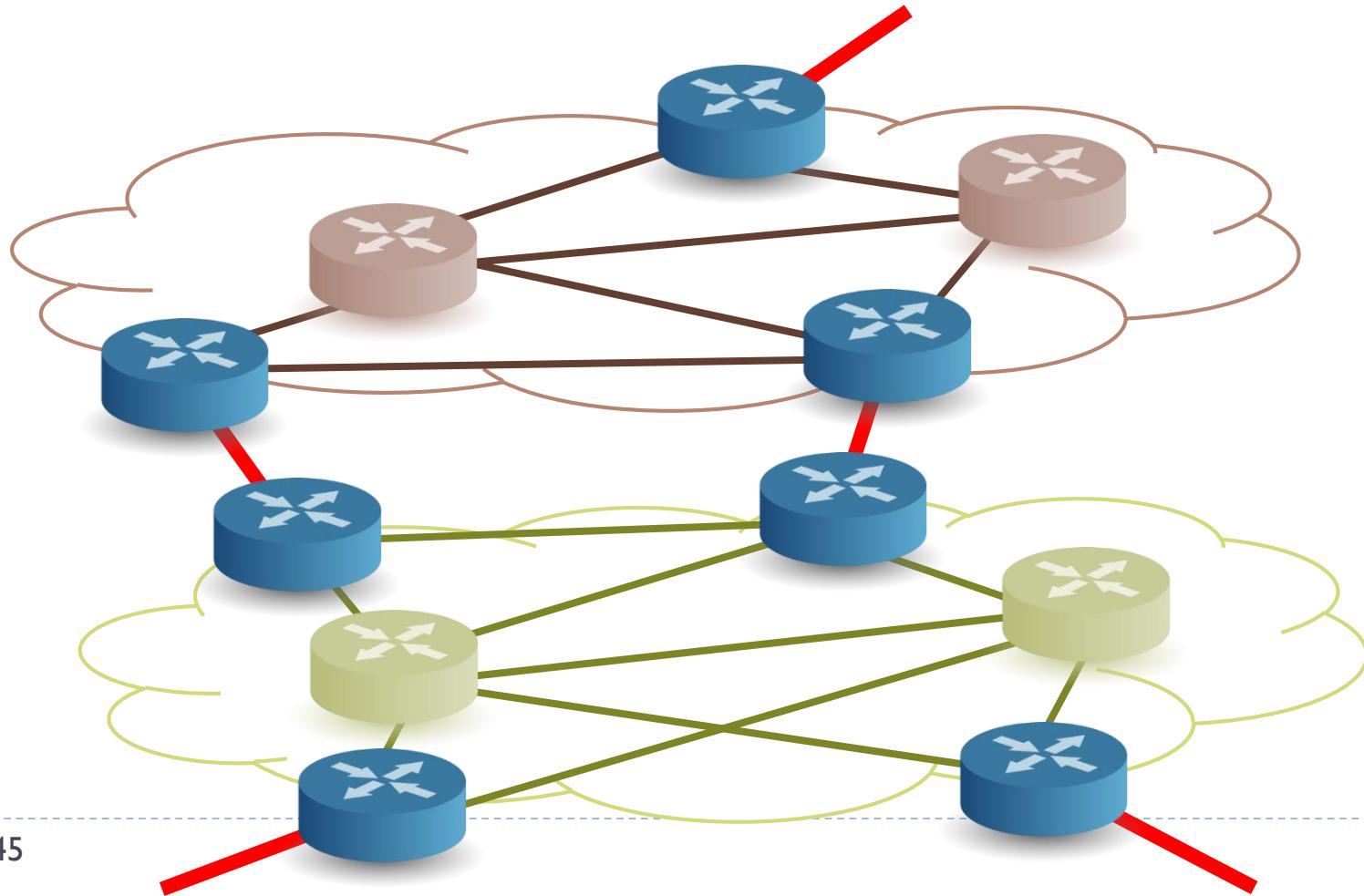
- ▶ Gains financiers,
- ▶ Meilleurs services,
 - ▶ Accès facilité à l'innovation,
- ▶ Meilleure efficience environnementale,



Et demain...

Software Defined Network – SDN

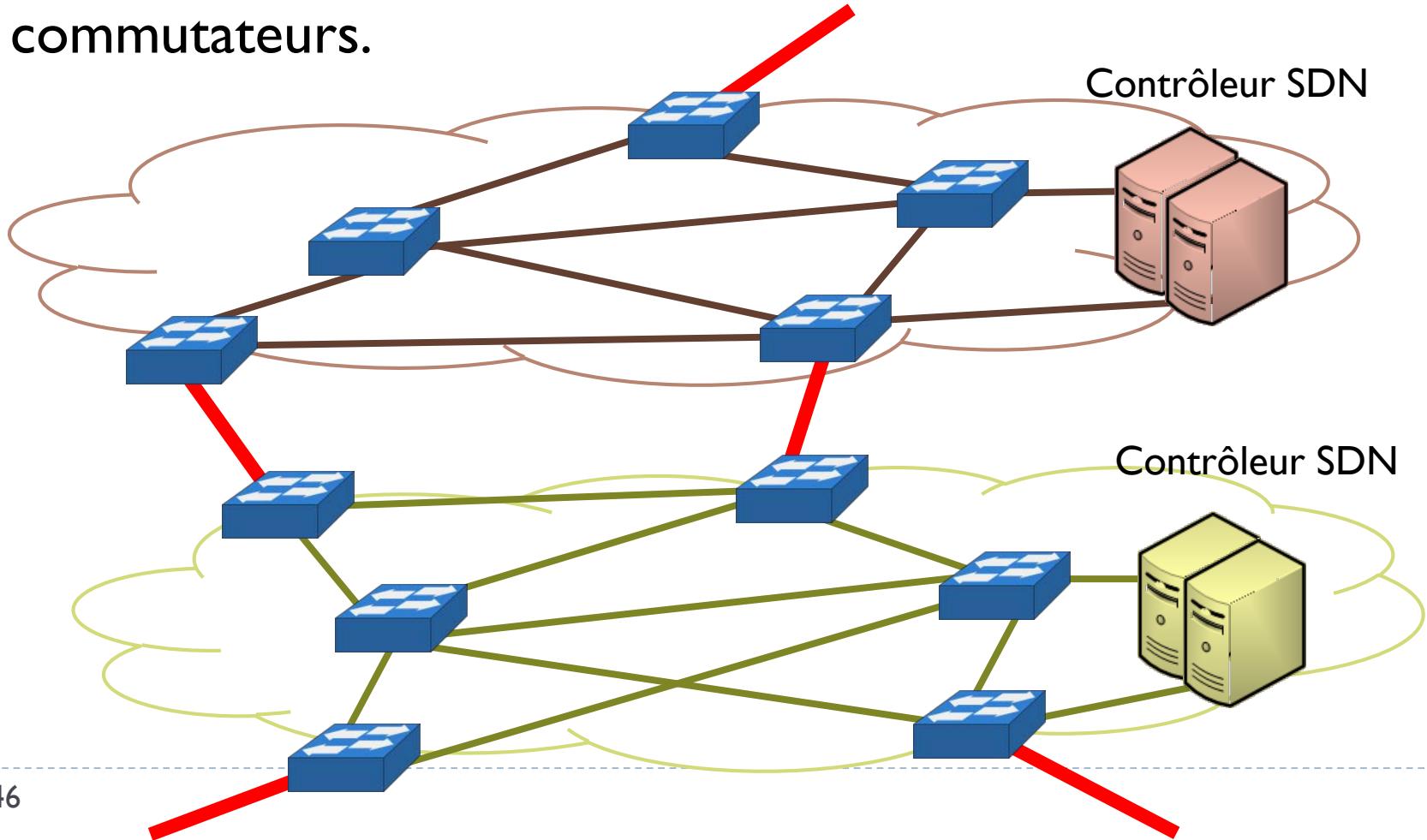
- ▶ Aujourd’hui, l’intelligence du réseau est contenu dans tous les nœuds du réseau



Et demain...

Software Defined Network – SDN

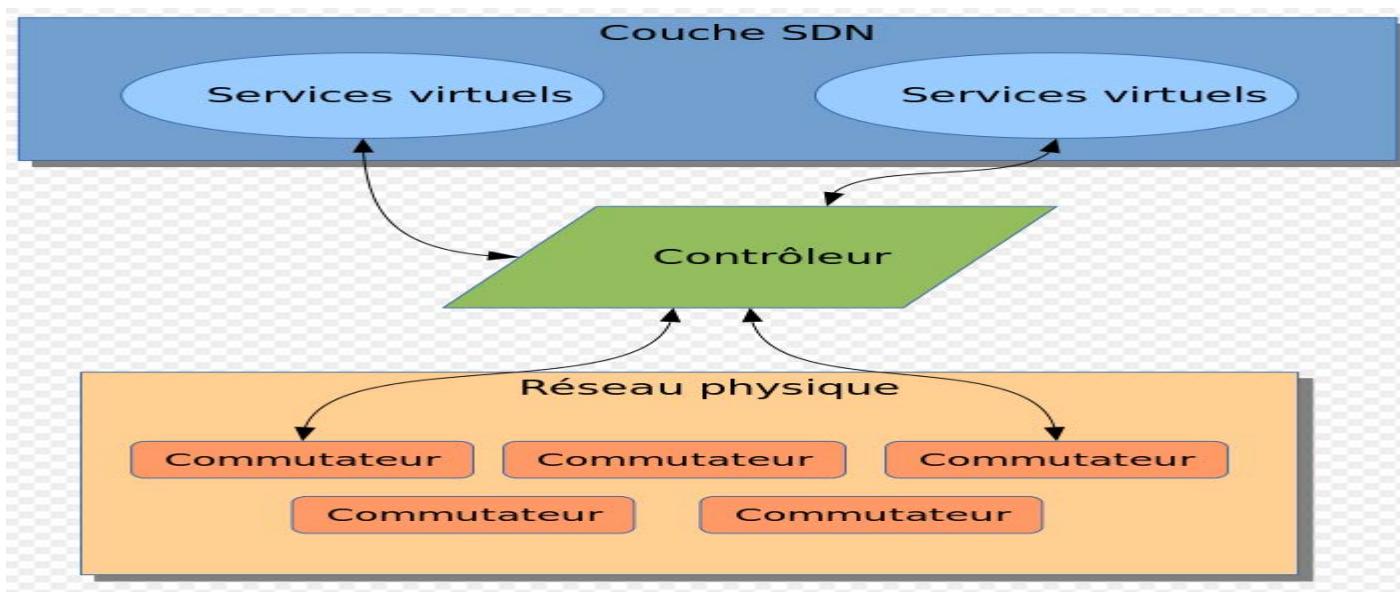
- ▶ Demain, l'intelligence du réseau sera centralisée dans des contrôleurs et distribuée à des « simples » commutateurs.



Réseaux de demain

Software Defined Network – SDN

- ▶ Objectifs :
 - ▶ Prise en compte des besoins applicatifs (Serveur) par le réseau
 - ▶ Le Datacenter devient le lieu privilégié pour tout contrôler
 - ▶ Standard : OpenFlow (Université de Stanford)



Réseaux de demain

Software Defined Network – SDN

- ▶ Guerre commercial entre les majors industriels
- ▶ Entrée de nouveaux acteurs sur la couche 3 venus du monde du logiciel :
 - ▶ IBM, HP...
- ▶ Réaction des industriels déjà en place : Cisco, Juniper, Nokia,...
 - ▶ Leur propre système SDN très évolué, qui prend en charge le parc existant, compatible avec les standards mais qui va plus loin avec des surcouches propriétaires.

Réseaux de demain

Software Defined Network – SDN

- ▶ Cas de Google :

<http://www.opennetsummit.org/archives/apr12/hoelzle-tue-openflow.pdf>

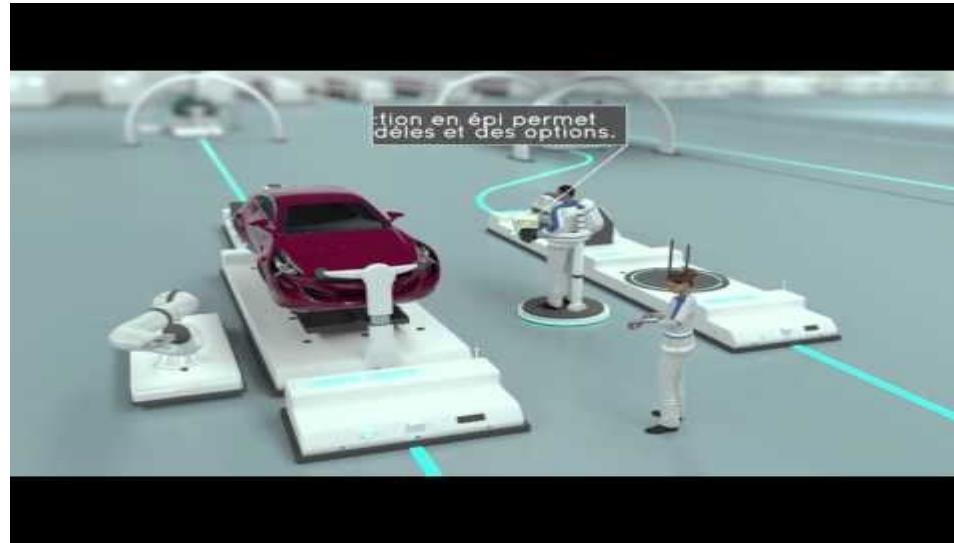


Et demain... Internet des Objets

- ▶ Tout objet peut être connecté :
 - ▶ Exemple : la montre connectée, la voiture connectée,...
- ▶ Tout objet contient aujourd’hui sa part d’électronique
- ▶ Là encore, une guerre commercial se livre entre les majors industriels
 - ▶ Convergence de plusieurs acteurs aux profils divers mais ayant déjà une brique de la solution cible :
 - ▶ Issus des couches applicatives : Dassault System, ...
 - ▶ Issus du monde de la robotique, automatisation : Bosch,
 - ▶ Issus de l’électronique : GE,...
 - ▶ Issus des opérateurs mobiles : Orange,...
 - ▶ Chacun considère que le premier installé dans ce marché aura un avantage décisif pour la suite

Et demain... Internet des Objets

- ▶ Exemple : Vidéo Usine Peugeot - Industrie 4.0



Les Réseaux

MERCI