

TR3

Réseaux étendus et réseaux d'opérateurs

IUT R&T Sophia-Antipolis 2012-2013

L. Sassatelli

sassatelli@i3s.unice.fr

Situation dans la formation DUT R&T

Répartition globale des modules

DUT Réseaux & Télécommunications

UE1 : Formation scientifique et humaine		
	Coefficient	horaire
Mathématiques	9	180
Physique	4	60
Culture - Communication	6	105
Anglais	6	120
PPP	3	45
Apprendre autrement	1	30
Connaissance de l'entreprise	1	30
Total Formation scientifique et humaine	30	570
UE2 : Informatique et électronique		
Informatique	15	240
Electronique	12	180
Apprendre autrement	1	30
Total Informatique et électronique	28	450
UE3 : Télécommunications et réseaux		
Télécommunications	10	150
Réseaux	10	150
Télécommunications - Réseaux	10	180
Total Télécommunications et réseaux	30	480
UE4 : Projets professionnels		
Projets tutorés	3	
Stages	9	
Total Projets professionnels	12	
Total 10 modules complémentaires	20	300
Total général	120	1800

Semestre 3

UE31 : Formation scientifique et humaine		
	Coefficient	horaire
Mathématiques	2	30
Physique	2	30
Culture-Communication	2	45
PPP	1	15
Anglais	2	30
Connaissance de l'entreprise	1	30
Total UE31 (cœur de compétences)	10	180
UE32 : Informatique et électronique		
Informatique	4	60
Electronique	4	60
Total UE32 (cœur de compétences)	8	120
UE33 : Télécommunications et réseaux		
Télécommunications – Réseaux	10	180
Total UE33 (cœur de compétences)	10	180
1 module complémentaire*	2	30
Total S3	30	510

Coefficients

- Coefficient de l'UE Télécommunications et Réseaux dans la moyenne générale: 10
- L'UE Télécommunications et Réseaux au semestre 3 est composée de:
 - TR1: Modulations numériques et notions de compression – Coeff 1.7
 - TR2: Technologies de l'Internet – Coeff 3.3
 - **TR3: Réseaux étendus et réseaux d'opérateurs** – Coeff 5.0
- TR3:
 - Note de Théorie: Coeff 4 – Composée de 2 DS de coeff 2 chacun (1 DS en sem 50 + 1 DS en sem 3)
 - Note de Pratique: Coeff 3 – Composée de 6TP coeff 1/8 + 1 DS coeff 6/8 + 1 exam TP coeff 1/8

Plan général du cours de TR3

I. Présentation des WAN

II. Les interfaces de la couche physique

III. Protocoles de niveau 2 dans les WAN

IV. MPLS : commutation par VC dans le monde IP

V. Qualité de service

VI. Technologies xDSL

Plan détaillé du cours de TR3

I. Présentation des WAN

I.1. Concepts généraux

I.2. Evolution de la commutation : commutation de circuit, de paquet avec et sans connexion

I.3. Options de connexion au WAN

I.3.a. Niveau 1, niveau 2 et niveau 3

I.3.b. Haut débit

I.3.c. Sans-fil

II. Les interfaces de la couche physique

II.1. Les différents types de multiplexage

II.2. La hiérarchie numérique synchrone PDH

II.3. La hiérarchie numérique synchrone SDH : réseaux de fibres optiques et redondance pour la fiabilité

III. Protocoles de niveau 2 dans les WAN

III.1. En mode point-à-point :

III.1.a. HDLC

III.1.b. PPP

III.2. En mode circuit virtuel de bout-en-bout :

III.2.a. Frame Relay

III.2.b. ATM

Plan détaillé du cours de TR3

IV. MPLS : commutation par VC dans le monde IP

IV.1. Fonctionnement de MPLS

IV.2. Ingénierie de trafic avec MPLS : MPLS-TE

IV.3. Offres de service MPLS : les VPN basés sur MPLS

IV.3.a. IP-VPN

IV.3.b. Ethernet-VPN : VPLS

V. Qualité de service

V.1. TCP et le contrôle de congestion dans le réseau

V.1.a. Rappels : transfert fiable et contrôle de flux

V.1.b. Principe du contrôle de congestion

V.1.c. Le contrôle de congestion par TCP

V.2. Classification des applications et besoin de QoS

V.2.a. Classification

V.2.b. Paramètres-clé de la QoS

V.2.c. Stratégies pour la QoS

V.3. Techniques de traitement de la QoS

V.3.a. Les outils

V.3.b. Traitements au niveau 2

V.3.c. Traitements au niveau 3

Plan détaillé du cours de TR3

VI. Technologies xDSL

VI.1. Principe : tirer le maximum de la paire de fils de cuivre

VI.2. Technique de TS pour xDSL : l'OFDM

VI.3. Fonctionnement protocolaire entre le FAI et l'abonné (cas dégroupé et non-dégroupé)

Références principales

- G. Pujolle, « *Les réseaux édition 2008* », ed. Eyrolles
- http://www.cisco.com/en/US/docs/internetworking/technology/handbook/ito_doc.html
- A. S. Tanenbaum, « *Computer Networks, Fourth edition* », ed. Prentice Hall
- J. F. Kurose and K. W. Ross, « *Computer Networking, a top-down approach, Fifth edition* », ed. Pearson education
- J. F. Kurose and K. W. Ross, slides of chapter 3, online
- Cours de J. Drouot (ESIL)
- AT&T website: <http://www.business.att.com/enterprise/business-solutions/>
- Cours de E. Bost (Freescale Semiconductors)
- C. Servin, “Réseaux et Télécoms”, 3e édition, ed. Dunod

Plan

I. Présentation des WAN

I.1. Concepts généraux

I.2. Evolution de la commutation : commutation de circuit, de paquet avec et sans connexion

I.3. Options de connexion au WAN

I.3.a. Niveau 1, niveau 2 et niveau 3

I.3.b. Haut débit

I.3.c. Sans-fil

II. Les interfaces de la couche physique

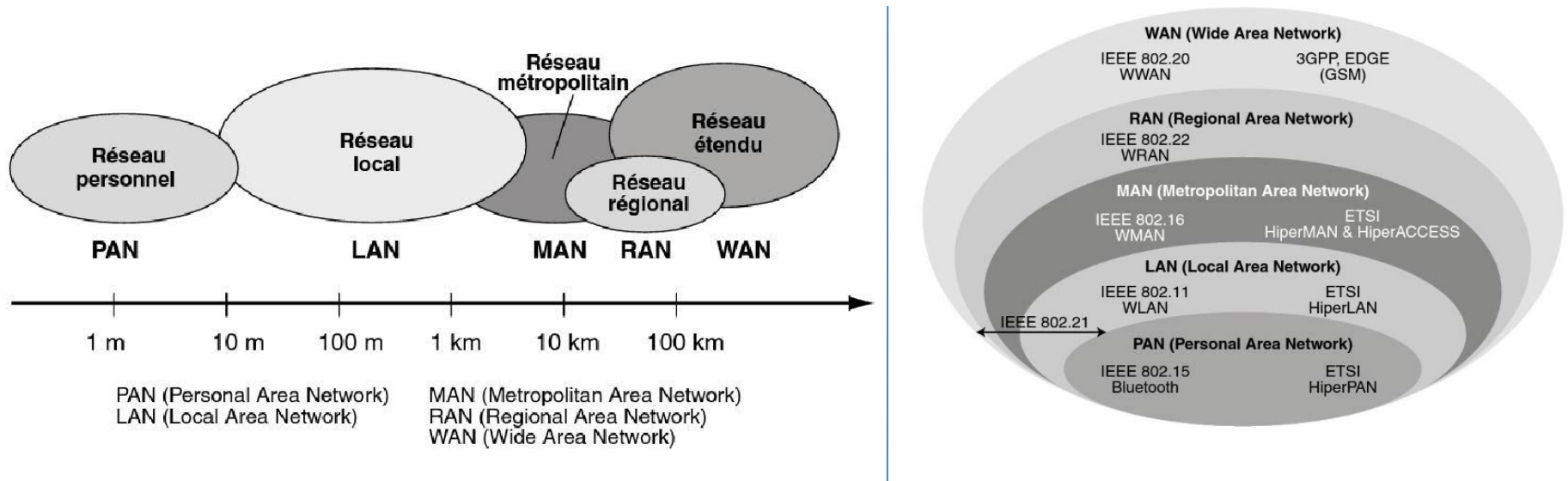
III. Protocoles de niveau 2 dans les WAN

IV. MPLS : commutation par VC dans le monde IP

V. Qualité de service

VI. Technologies xDSL

Les réseaux informatiques



- Personal Area Network: quelques mètres, pour équipements personnels
- Local Area Network: réseaux intra-entreprises, jusqu'à plusieurs Mbps
- Metropolitan Area Networks: interconnexion des entreprises sur un réseau spécialisé à haut débit
- Regional Area Network: 50km pour le sans-fil, beaucoup d'utilisateurs par antenne
- Wide Area Networks: pays ou plusieurs continents

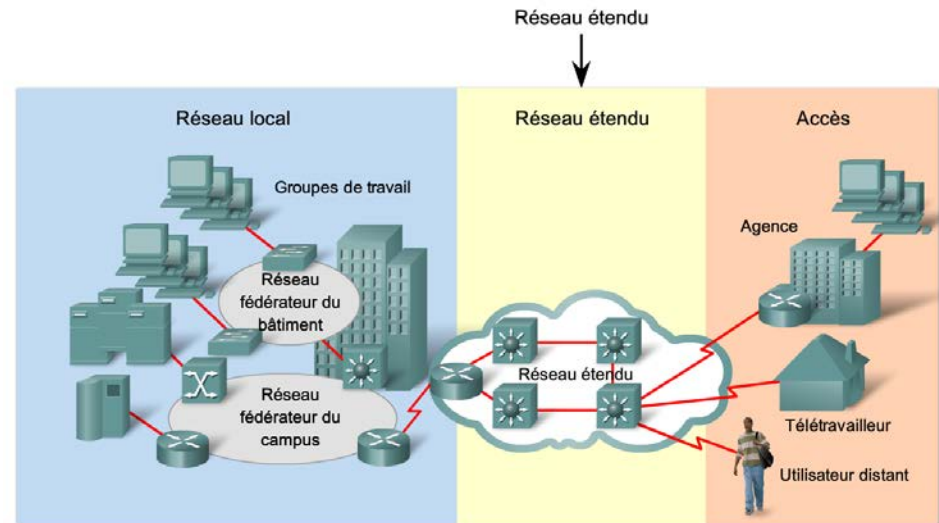
Réseaux étendus: présentation

Définition: Un réseau étendu est un réseau de communication de données qui fonctionne au-delà de la portée géographique d'un réseau local.

Principales caractéristiques:

- ils connectent généralement des périphériques séparés par une zone géographique plus étendue que ne peut couvrir un réseau local ;
- ils utilisent les services d'opérateurs, tels que des compagnies de téléphone ou de câble, des systèmes satellite et des fournisseurs de réseau ;
- ils utilisent divers types de connexions série pour permettre l'accès à la bande passante sur de vastes zones géographiques.

But: Les réseaux étendus, utilisés seuls ou conjointement avec Internet, apportent à des organisations ou des individus une réponse à leurs besoins de communication étendue.



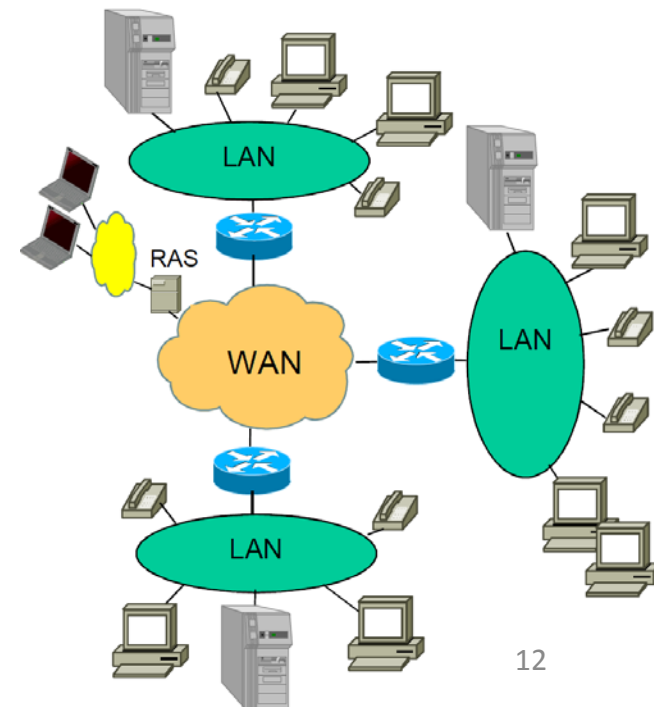
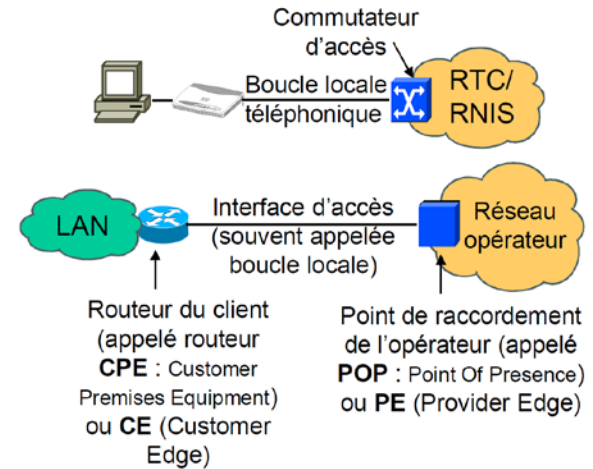
Réseaux étendus: présentation

- Caractéristiques de performance des WAN:

- Prix beaucoup plus élevés que ceux des LAN
 - Même si les prix baissent rapidement
- Délais de traversée du réseau plus élevés
 - Plusieurs dizaine ou centaine de ms

- Besoin croissant de convergence et de qualité de service:

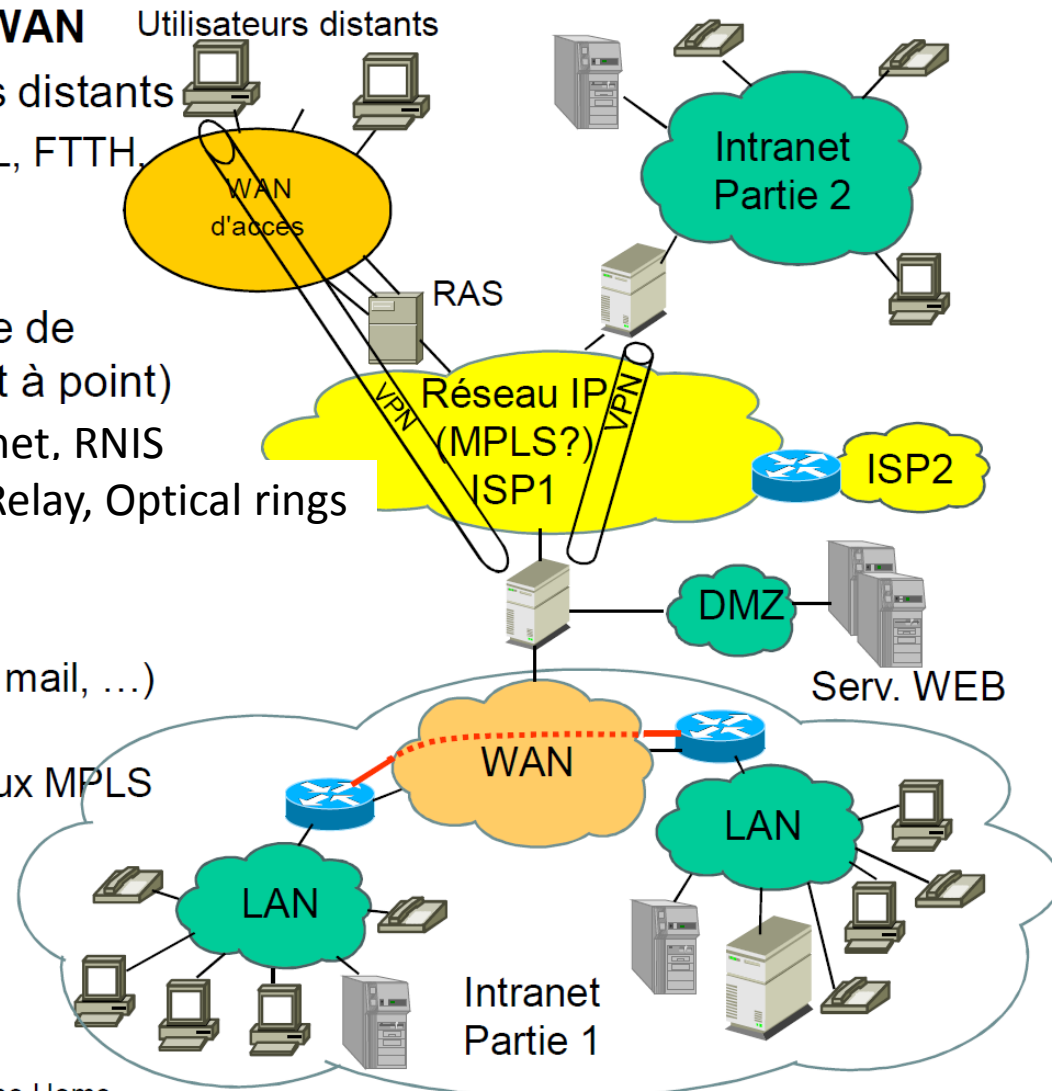
- Un seul réseau pour les trafics de données et les trafics télécoms
 - Au niveau LAN
 - Au niveau WAN
- Les trafics doivent être répartis selon des classes de service et traités en conséquence



Les différents aspects des WAN

- **Trois aspects des réseaux WAN**

- Raccorder des utilisateurs distants
 - RTC, RNIS, câble, ADSL, FTTH, UMTS, ...
- Raccorder les LAN d'une entreprise sous le contrôle de l'entreprise (services point à point)
 - Liaisons louées, Ethernet, RNIS
 - IP-VPN, VPLS, Frame Relay, Optical rings
- Réseaux WAN des ISP, interconnectés entre eux
 - Services Internet (WEB, mail, ...) sur réseau IP pur
 - Services VPN sur réseaux MPLS



RAS : Remote Access Server

DMZ : De-Militarized Zone

ISP : Internet Service Provider

VPN : Virtual Private Network FTTH : Fiber To The Home

Les offres de service

Personal Business About AT&T Enterprise Worldwide

at&t Enterprise Search Enterprise for... Go

PRODUCTS & SERVICES NETWORKING EXCHANGE NEWS & INSIGHTS SUPPORT

Application Services Content Delivery Hosting Services Mobility Services Network Security Network Services Unified Communications Voice Services [All]

Products & Services : Network Services

Ethernet

- Metro Ethernet
- Wide Area Ethernet

Frame Relay

Internet Connectivity

- Business DSL
- Managed Internet Service
- AT&T Wi-Fi Services, formerly Wayport, Inc.

IP VPN

- Remote Access VPN

Private Line

Ring Services

- SONET Ring
- WaveLength Ring

How to Address Your Top Tech Problems [PDF, 613KB]

Modernizing Your Approach to Network Management [PDF, 966KB]

Network Services: The Engines That Drive Your Business

Your network is much more than a physical structure. Today, you rely on your network to keep you connected - whether consulting with colleagues, video conferencing with suppliers or analyzing business intelligence.

AT&T is a network of intelligence that combines the world's best technology and expertise to unlock the greater potential of governments, businesses and individuals everywhere.

Emerging technologies and mobile applications are changing business processes and the way we communicate. Machines can now tell headquarters when they need refilling. Doctors can have immediate access to a patient's medical history even when away from home. Your network can become a living, breathing intelligent system that helps you rethink how you run your businesses.

AT&T applies our people, expertise and technology to bring our intelligent global network together with mobile access and devices, software and applications to create a world of new possibilities for companies. Our network services can help build a reliable foundation on which emerging applications can be built.

Portfolio of Network Services

- Ethernet
- Frame Relay
- Internet Connectivity
- IP VPN
- Private Line
- Ring Services

Build your ideal network solution

Rapidly changing technology and a tough economy make it difficult to effectively manage and maintain your network. You need to be mobile, nimble and work better, while increasing efficiency. The broad range of network services offered by AT&T can build a reliable, scalable network that supports your communications needs.

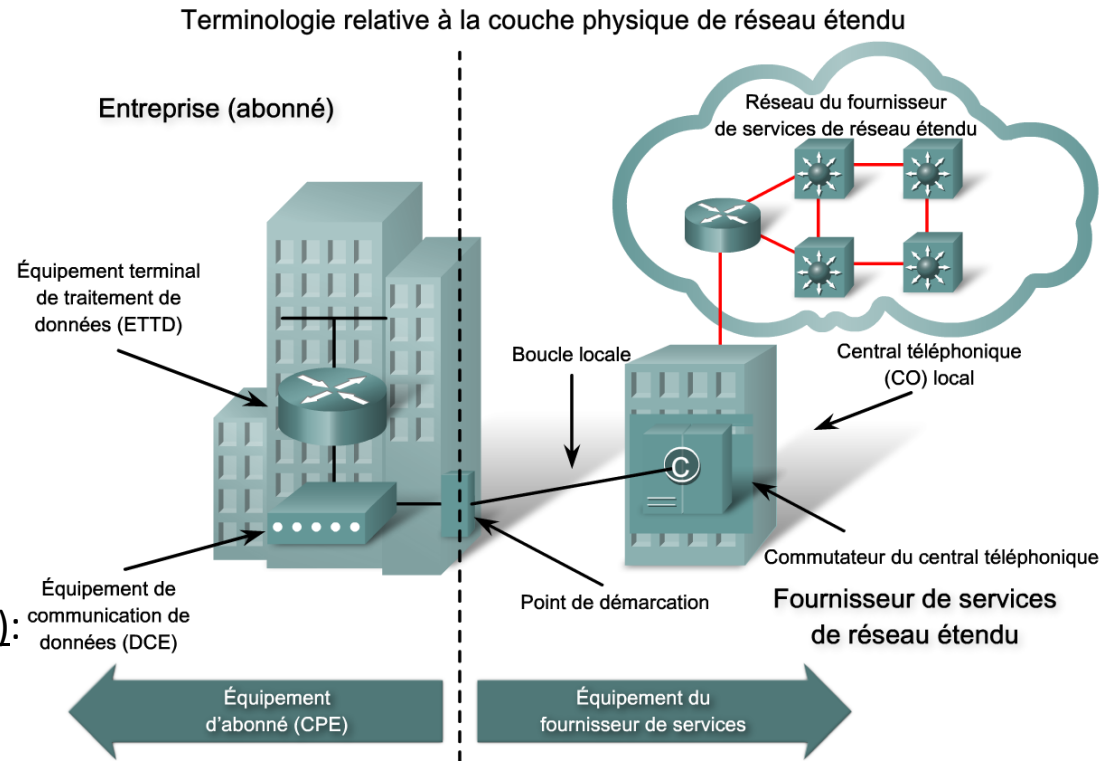
Concepts de la couche physique de réseaux étendus (1)

- CPE (Customer Premises Equipment): périphériques et câblage interne situés chez l'abonné et connectés via le canal de télécommunications d'un opérateur.

L'abonné est propriétaire de l'équipement ou le loue à son fournisseur de services.

- DCE (Data Circuit-terminating Equipment): périphériques qui placent des données sur la boucle locale.

- DTE (Data Terminal Equipment): périphériques de client qui transmettent des données depuis le réseau d'un client ou l'ordinateur hôte pour une transmission sur le réseau étendu.



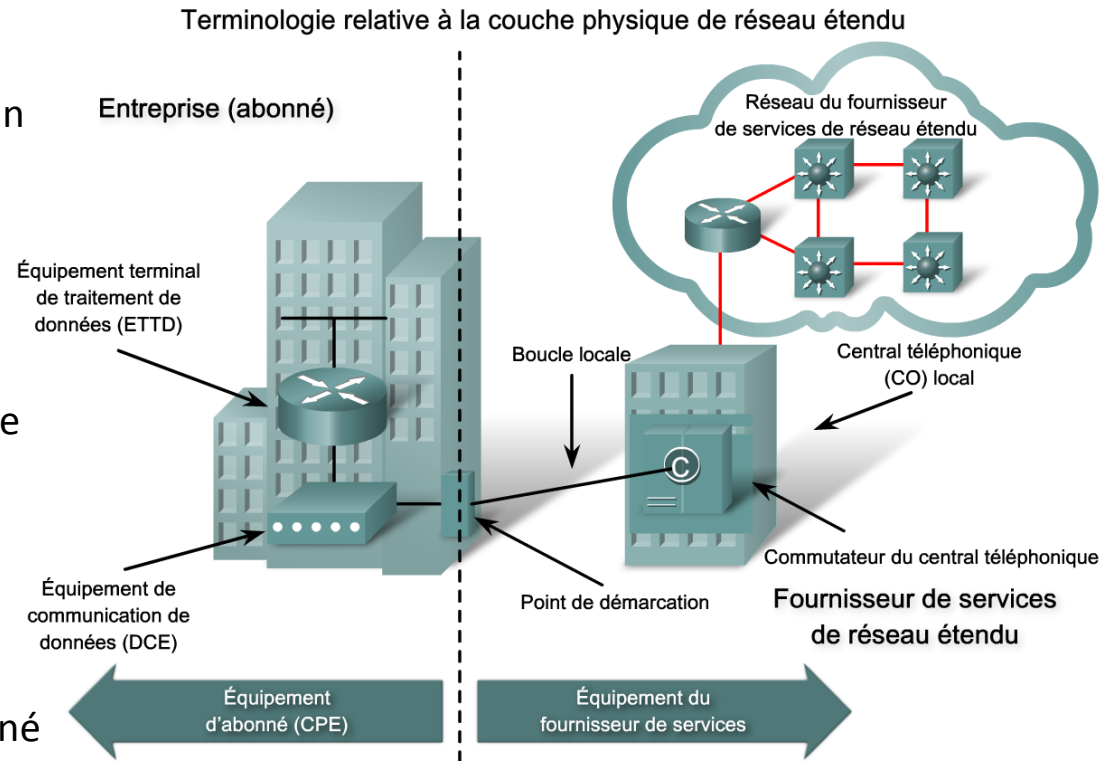
Concepts de la couche physique de réseaux étendus (2)

- Point de démarcation : point établi dans un bâtiment ou un complexe pour séparer l'équipement du client de celui du fournisseur de services.

➤ Physiquement: boîtier de raccordement de câblage, situé chez le client, qui connecte les câbles de l'équipement d'abonné à la boucle locale.

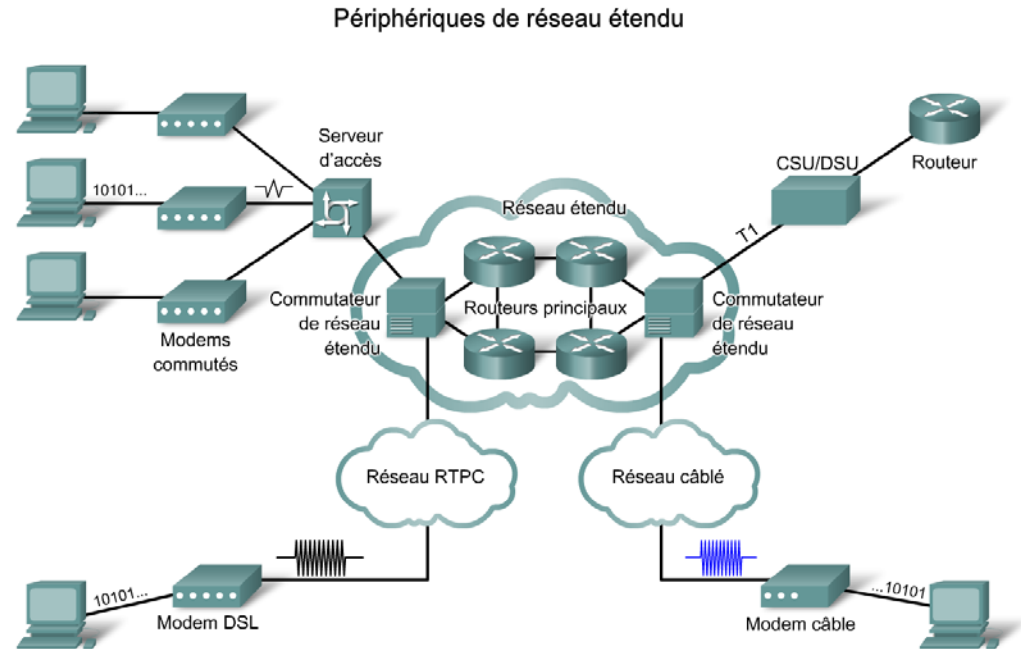
- Boucle locale : câble téléphonique de cuivre ou à fibre optique qui connecte l'équipement d'abonné sur le site de l'abonné au central téléphonique du fournisseur de services. « Last-mile network ».

- Central téléphonique (CO) : installation ou bâtiment de fournisseur de services local dans lequel des câbles téléphoniques locaux relient des lignes de communications grande distance, entièrement numériques et à fibre optique via un système de commutateurs et d'autres équipements.



Concepts de la couche physique de réseaux étendus (3)

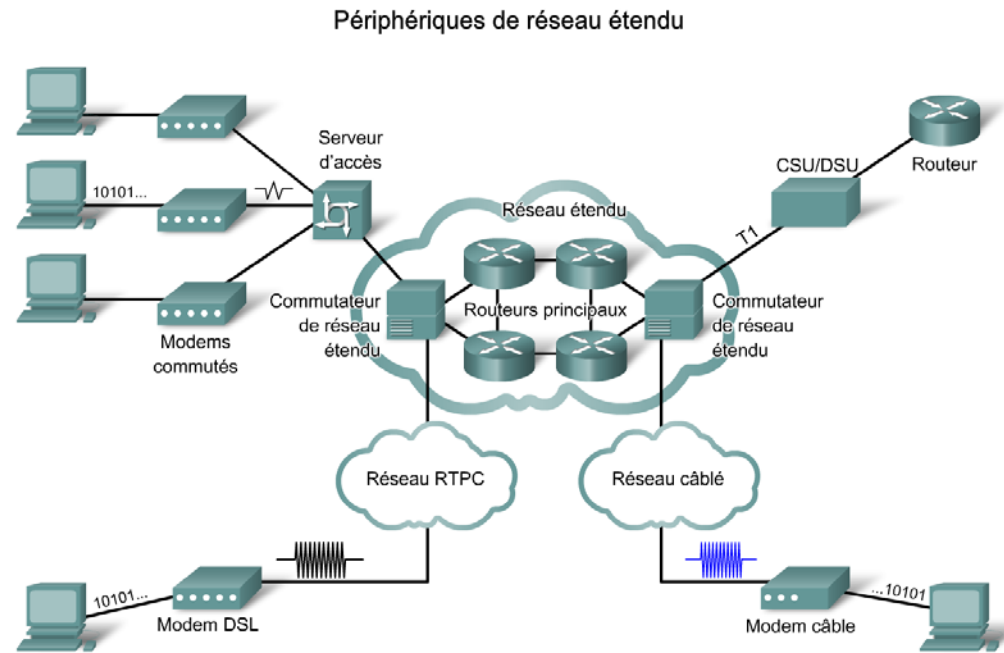
- CSU/DSU : les lignes numériques, telles que des lignes d'opérateur T1 ou T3 requièrent une unité Channel Service Unit (CSU) et une unité Data Service Unit (DSU) - CSU/DSU.
 - L'unité CSU fournit la terminaison pour le signal numérique et garantit l'intégrité de la connexion grâce à la correction des erreurs et la surveillance de ligne.
 - L'unité DSU convertit les trames de ligne de système multiplex T en trames pouvant être interprétées par le réseau local, et réciproquement.



- Serveur d'accès : concentre les communications utilisateur entrantes et sortantes.
 - Ils peuvent comporter un mélange d'interfaces analogiques et numériques, et prendre en charge des centaines d'utilisateurs simultanés.

Concepts de la couche physique de réseaux étendus (4)

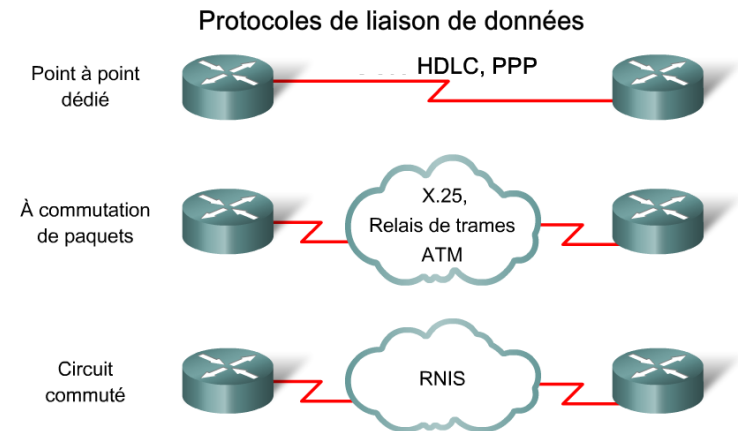
- Commutateur de réseau étendu : périphérique d'interconnexion multiport utilisé dans des réseaux d'opérateur.
 - FR, ATM ou MPLS, couche 2
 - commutateurs RTPC pour connexions à commutation de circuits telles RNIS ou pour une connexion commutée analogique



- Routeur de cœur de réseau : routeur qui réside au milieu ou sur le réseau fédérateur du réseau étendu plutôt qu'à sa périphérie.
 - doit pouvoir prendre en charge plusieurs interfaces de télécom parmi les plus rapides utilisées dans le cœur du réseau étendu, et transmettre des paquets IP à une vitesse optimale sur toutes ces interfaces.
 - doit également accepter les protocoles de routage utilisés dans le cœur de réseau.

Concepts de la couche liaison de réseaux étendus

- Protocoles de couche liaison de données pour établir la liaison sur la ligne de communication entre le périphérique d'envoi et de réception
- Différentes technologies: RNIS (ISDN), FR, ou ATM (Asynchronous Transfer Mode).
- Un certain nombre de ces protocoles utilisent le même mécanisme de tramage de base, HDLC, une norme ISO ou l'un de ses sous-ensembles ou variantes.
- Le mode ATM diffère des autres, car il utilise des petites cellules de taille fixe de 53 octets (48 octets pour les données), tandis que les autres technologies à commutation de paquets utilisent des paquets de taille variable.
- RNIS et X.25 plus anciens. Par ailleurs, X.25 est encore utilisé dans des PVD pour transactions par carte de crédit depuis des détaillants.



Protocole	Utilisation
LAPB (from HDLC)	RNIS canaux B, X.25
LAPD	RNIS canal D
LAPF	Frame Relay
PPP	Connexions commutées de réseau étendu série

Plan

I. Présentation des WAN

I.1. Concepts généraux

I.2. Evolution de la commutation : commutation de circuit, de paquet avec et sans connexion

I.3. Options de connexion au WAN

I.3.a. Niveau 1, niveau 2 et niveau 3

I.3.b. Haut débit

I.3.c. Sans-fil

II. Les interfaces de la couche physique

III. Protocoles de niveau 2 dans les WAN

IV. MPLS : commutation par VC dans le monde IP

V. Qualité de service

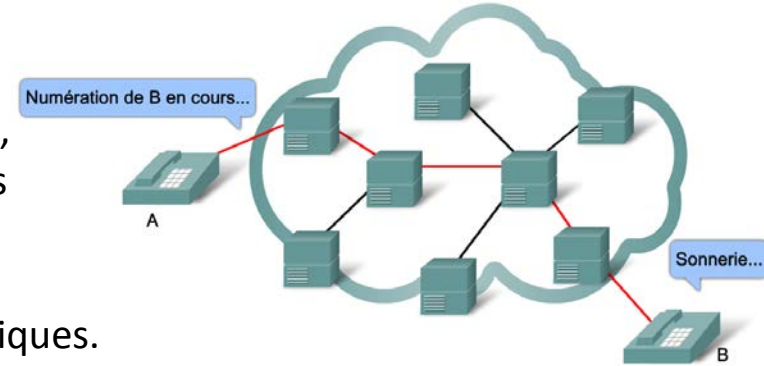
VI. Technologies xDSL

Concepts de commutation de réseaux étendus:

Commutation de circuits

Un réseau à commutation de circuits établit un circuit dédié entre des nœuds et des terminaux avant que les utilisateurs puissent communiquer.

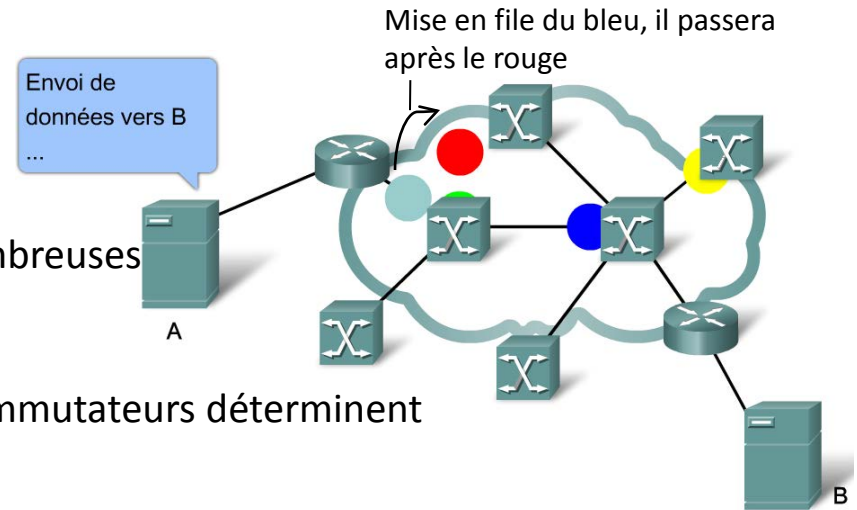
- Par exemple, lorsqu'un abonné passe un appel téléphonique, le numéro composé sert à définir des commutateurs dans les échanges effectués sur la route de l'appel
- Si les téléphones sont remplacés par des modems, le circuit commuté peut également transporter des données informatiques.
- Le chemin interne emprunté par le circuit entre les échanges est partagé par un certain nombre de conversations. Le **multiplexage temporel** (TDM) permet de partager la connexion à tour de rôle entre chaque conversation. Le multiplexage temporel assure qu'une connexion de capacité fixe soit mise à la disposition de l'abonné.
- Inefficacité dans le cas des **rafales** d'activité: cas des données informatiques
- Comme l'abonné a l'utilisation exclusive de son allocation de capacité fixe, les circuits commutés constituent généralement une méthode coûteuse de transport des données.
- **RTPC et RNIS** sont deux types de technologie à commutation de circuits qui peuvent être utilisés pour implémenter un réseau étendu dans une configuration d'entreprise.



Concepts de commutation de réseaux étendus:

Commutation de paquets (1)

- Contrairement à la commutation de circuits, la commutation de paquets fractionne les données de trafic en paquets acheminés sur un réseau partagé.
- Pas d'établissement (monopolisation) de circuit et nombreuses paires de nœuds communiquent sur le même canal.



➤ Informations d'adresse dans chaque paquet -> les commutateurs déterminent le lien vers lequel le paquet doit ensuite être envoyé.

- 2 approches à cette détermination des liaisons :

- **Systèmes sans connexion (IP)**: l'en-tête du paquet contient l'adresse de destination pour livraison autonome
- **Systèmes avec connexion**: route prédéterminée, seulement un identificateur sur le paquet pour déterminer le prochain saut

- FR: DLCI, ATM: VPi/VCi, MPLS: labels.

Le commutateur détermine la route à suivre en recherchant l'identificateur dans des tables en mémoire. Le jeu d'entrées des tables identifie un itinéraire ou circuit particulier sur le système.

- Si ce circuit n'existe physiquement, n'est occupé, que lorsqu'un paquet se déplace dessus : **circuit virtuel (VC)**.

Concepts de commutation de réseaux étendus:

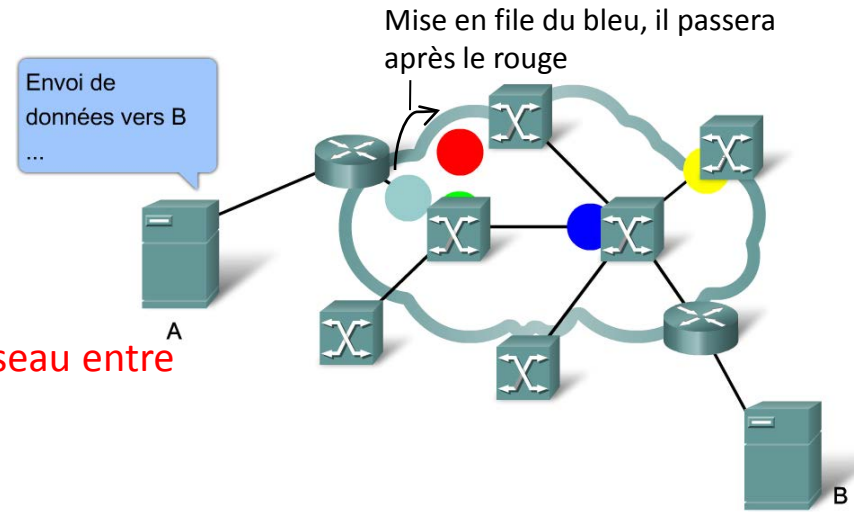
Commutation de paquets (2)

- Les réseaux à commutation de paquets établissent des routes via les commutateurs pour des connexions de bout en bout spécifiques. Ces routes sont appelées des circuits virtuels.

Circuit virtuel (VC): circuit logique établi au sein d'un réseau entre deux périphériques réseau.

Il existe deux types de circuits virtuels :

- Circuit virtuel permanent (PVC) : VC établi de façon permanente
 - Pour transmissions de données constantes entre les périphériques.
 - Consomment moins de bande passante lors de l'établissement et de la fermeture des circuits, mais ils augmentent les coûts en raison de leur continuité de service.
 - Généralement configurés par le fournisseur de services suite à une commande de service.



Concepts de commutation de réseaux étendus:

Commutation de paquets (3)

- Circuit virtuel commuté (SVC) : VC établi de façon dynamique sur demande et qui se ferme une fois la transmission terminée.
 - 3 phases pour la communication:
 1. établissement du circuit: création du VC entre les périph d'origine et de destination
 2. transfert des données: transmission des données entre les périphériques via le VC
 3. fermeture du circuit: démantèlement du VC

 - Utilisés pour des transmissions de données intermittentes entre les périph
 - > raisons financières: SVC relâchent le circuit une fois la transmission terminée
 - > réduction des frais de connexion p/r aux PVC

- Pour l'abonné: besoin d'une boucle locale jusqu'à l'emplacement le plus proche auquel le AP met le service à disposition= Point of Presence (POP) du service.

- Exemples de connexions à commutation de paquets ou de cellules: X.25, Frame Relay, ATM, MPLS

Commutation de circuits ou commutation de paquets ?

- **Avantages de la commutation de circuits**
 - Simple : pas de congestion et de priorités à gérer
 - Offre le meilleur niveau possible de QoS (Qualité de Service)
 - Réserve statique : bande passante garantie
 - Temps de traversée du réseau très court et presque fixe
 - Adapté de façon native aux trafics isochrones (téléphonie, vidéo)
- **Inconvénients de la commutation de circuits**
 - Mal adaptée aux trafics sporadiques et de débit variable
 - Ressources du réseau mal utilisées
 - Coûts supérieurs pour l'opérateur donc pour l'utilisateur
 - Les gâchis deviennent prohibitifs à haut débit (services large bande : ex. vidéo)
 - Le trafic de données est le plus souvent sporadique
 - Le trafic vocal devient à débit variable avec la compression des silences
 - Le trafic vidéo avec compression génère naturellement un débit variable
 - Problème d'évolutivité
 - Le débit des circuits n'est pas configurable dynamiquement

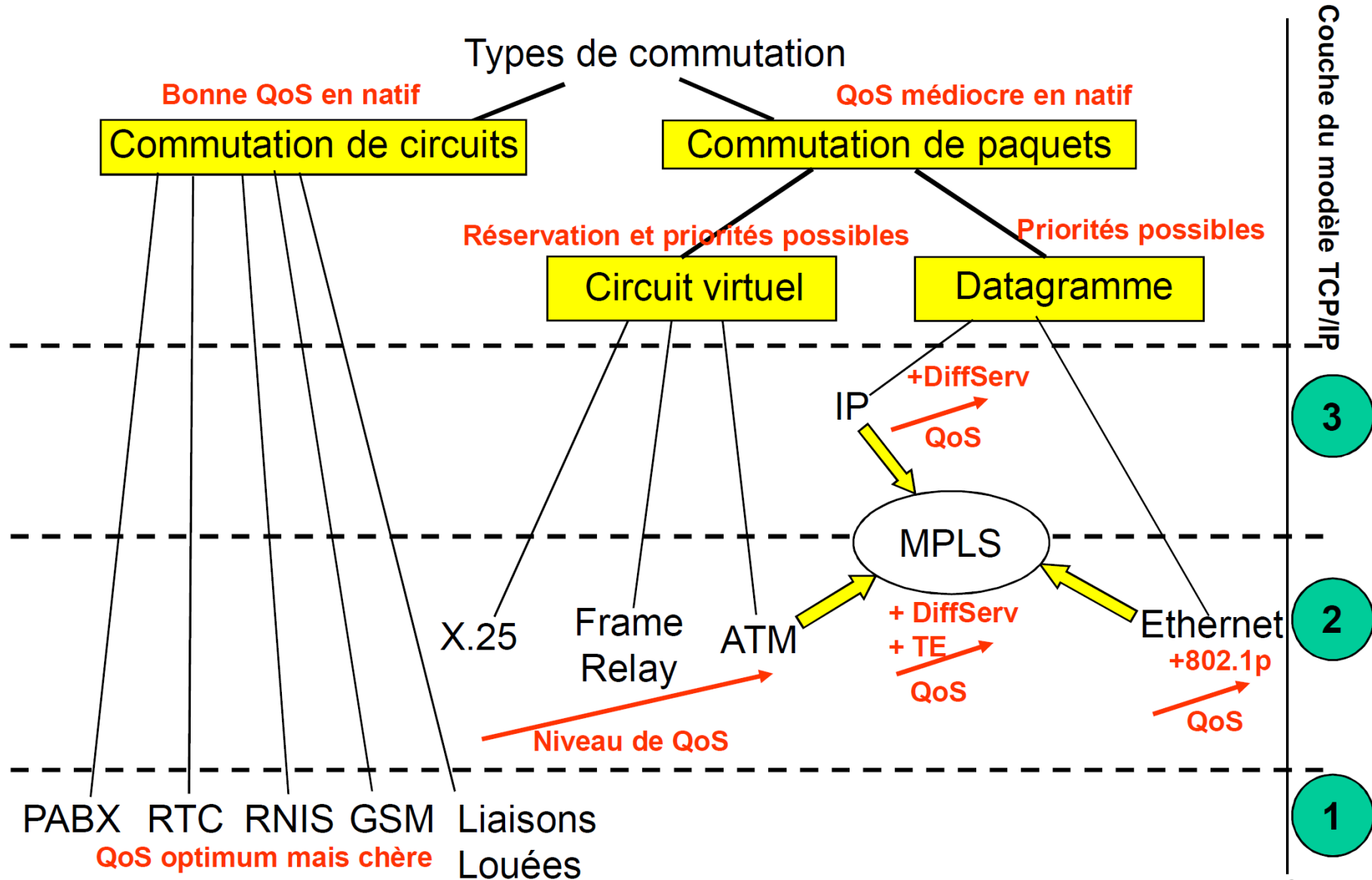
=> La commutation de circuits est progressivement abandonnée

Commutation de circuits ou commutation de paquets ?

- **Avantages de la commutation de paquets**
 - Les lignes sont partagées entre les différentes communications
 - Meilleure utilisation du réseau
 - Plus adapté aux trafics sporadiques et variables
- **Inconvénients de la commutation de paquets**
 - Les réseaux initiaux à commutation de paquets ne traitaient pas la QoS
 - Bande passante non garantie (fluctuante selon l'état de congestion)
 - Délais non garantis, plus longs et plus variables

- **Objectif : prendre le meilleur des 2 mondes de la commutation de circuits et de la commutation de paquets**
 - Partager les lignes entre plusieurs trafics
 - Grâce à des réseaux à commutation de paquets
 - Assurer des garanties de qualité de service variables selon les applications, réparties en classes de service
 - Garanties de débit
 - Temps de transit et gigue bornés ou au moins réduits

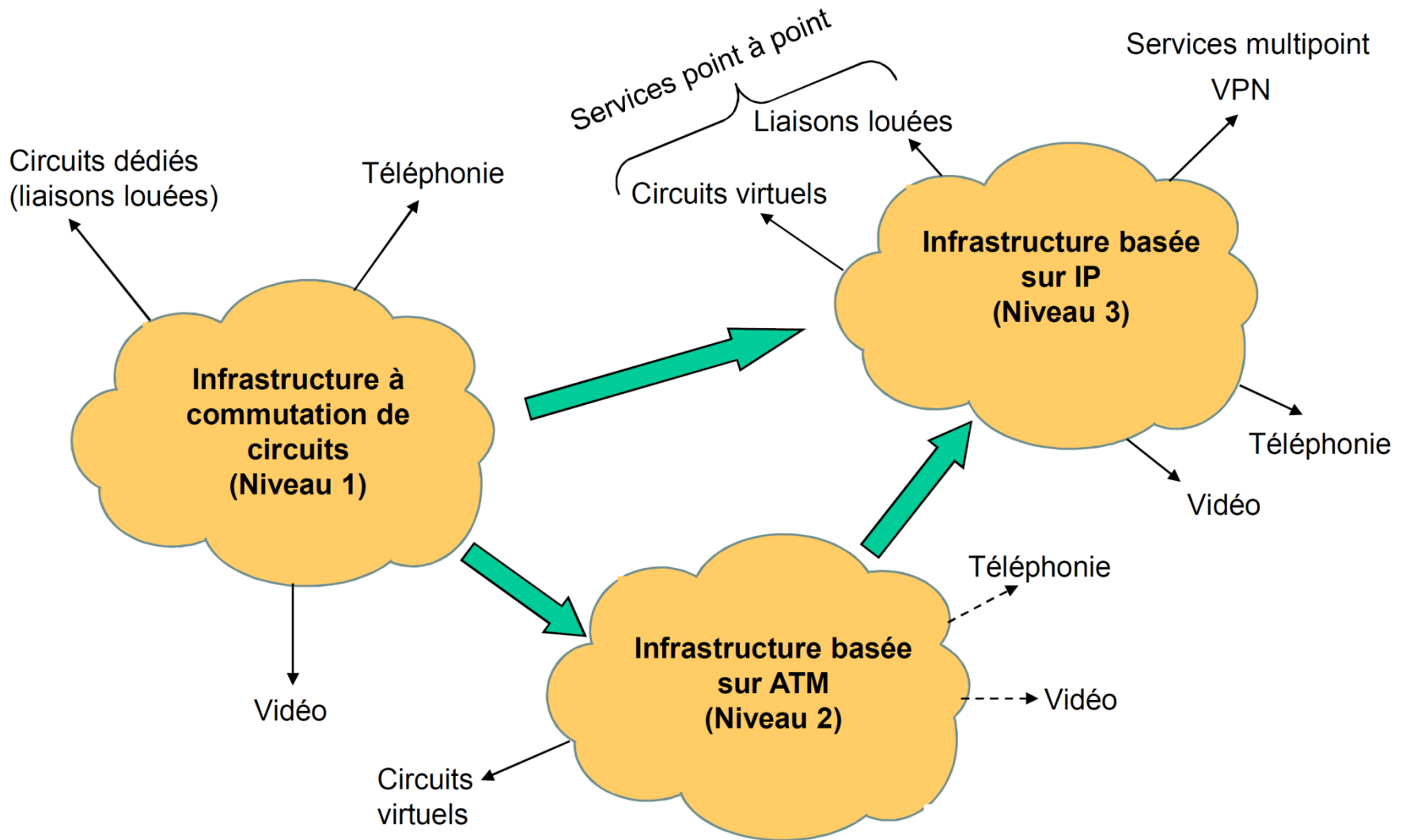
Evolution de la commutation et de la QoS



Les tendances de l'évolution des WAN

- **La technologie de commutation de circuits va peu à peu disparaître**
 - Mais l'héritage de la téléphonie explique un existant important
 - Qui impose une migration progressive de l'infrastructure
- **Le choix des opérateurs était de migrer vers un réseau basé sur la technologie ATM**
 - Réseau à commutation de paquets avec traitement de la qualité de service
 - ATM devait alors se généraliser aussi au niveau des entreprises
 - La migration a été très avancée chez les opérateurs historiques
- **Les succès de IP, Internet, et Ethernet ont changé cette orientation**
 - La migration se fait maintenant vers un réseau IP
 - En lui ajoutant des fonctionnalités de traitement de la qualité de service
- **Les trois types d'infrastructures cohabitent actuellement chez les opérateurs**

Les tendances de l'évolution des WAN



Les facteurs d'évolution

- **Les débits de la boucle locale explosent, les prix s'effondrent**
 - Depuis longtemps débit de base à 64 Kbps, haut débit à 2Mbps
 - 2Mbps devient un débit de base, accès possibles à 10 Gbps
- **Les fibres optiques du cœur de réseau ont des énormes possibilités**
 - DWDM : des dizaines de longueurs d'ondes avec 10, voire même 40 Gbps sur chacune
- **Ethernet devient aussi une technologie WAN**
 - A l'interface client – opérateur
 - Par liaison optique ou Ethernet sur xDSL
 - Dans le réseau de l'opérateur
 - Réseau de collecte ou cœur de réseau
- **Les trafics sont presque toujours IP**
 - Flux Intranet et flux Internet
 - Le réseau IP devient le réseau stratégique des opérateurs
- **La tendance des entreprises est à se recentrer sur leur métier**
 - Et à externaliser les tâches spécifiques réseau vers les opérateurs

Plan

I. Présentation des WAN

I.1. Concepts généraux

I.2. Evolution de la commutation : commutation de circuit, de paquet avec et sans connexion

I.3. Options de connexion au WAN

I.3.a. Niveau 1, niveau 2 et niveau 3

I.3.b. Haut débit

I.3.c. Sans-fil

II. Les interfaces de la couche physique

III. Protocoles de niveau 2 dans les WAN

IV. MPLS : commutation par VC dans le monde IP

V. Qualité de service

VI. Technologies xDSL

Identifier sa solution réseau idéale

- Solutions technologiques pour les contraintes de l'entreprise



- **IP**
- **Ethernet** metro, ou WAN (à plus grande échelle géographique)
- **Internet connectivity** : DSL et câble
- **Ring service** : anneaux optiques pour la fiabilité
- **Private line** : lignes louées

Options de connexions de réseaux étendus

- OPTIONS DE CONNEXION DE RÉSEAU ÉTENDU PRIVÉ:

- Liaison dédiée:

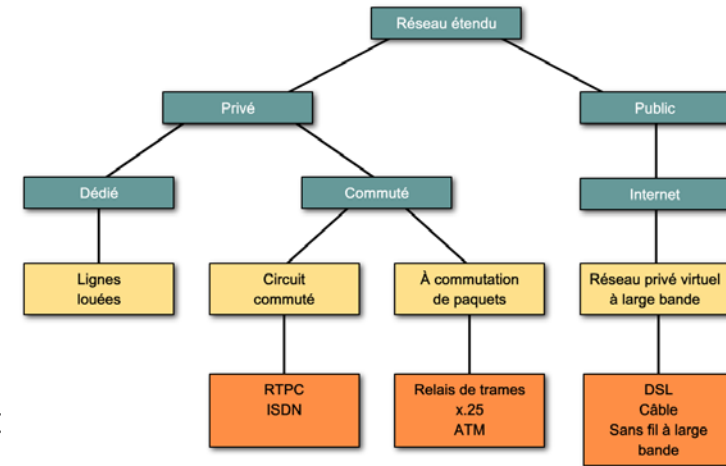
-Un circuit dédié et permanent entre 2 sites du client et une destination distante par l'intermédiaire du réseau du AP.

- Pour connexions dédiées permanentes: lignes point à point de capacités variées et limitées uniquement par les installations physiques sous-jacentes et la volonté des utilisateurs à payer.

Les lignes point à point sont généralement louées à un opérateur et prennent le nom de **lignes louées**.

- Liaison commutée :

- Liaisons à commutation de circuits: la commutation de circuits établit de façon dynamique une connexion dédiée pour la voix ou les données entre un expéditeur et un récepteur. Avant que la communication ne soit établie, il faut établir la connexion via le réseau du SP. ex: connexions commutées analogiques (RTPC) et les lignes RNIS
- Liaisons à commutation de paquets: données transmises dans des trames, des cellules ou des paquets libellés. Ex: FR, ATM, X.25 et Metro Ethernet + VPN basé réseau (sur MPLS)



Options de connexion de réseaux étendus

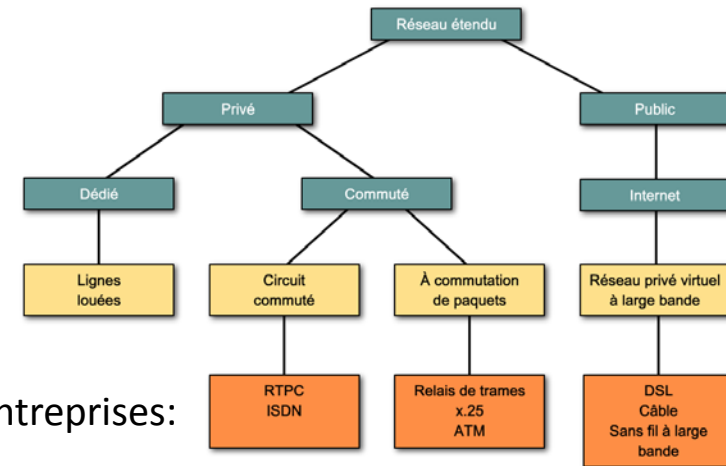
- OPTIONS DE CONNEXION DE RÉSEAU ÉTENDU PUBLIQUE:

- Utilisent l'infrastructure Internet globale.

- Encore récemment, Internet pas fiable pour de nombreuses entreprises: risques de sécurité et manque de garantie de performances

- Puis réseau privé virtuel (VPN): Internet est devenu une option peu coûteuse et sécurisée pour connecter des télétravailleurs et des bureaux distants pour lesquels les garanties en termes de performances ne sont pas essentielles.

- Liaisons de connexion WAN Internet: via des services à large bande tel que DSL, modem câble et connexions sans fil à large bande, et associées à la technologie de VPN pour garantir la confidentialité sur Internet.



Plan

I. Présentation des WAN

I.1. Concepts généraux

I.2. Evolution de la commutation : commutation de circuit, de paquet avec et sans connexion

I.3. Options de connexion au WAN

I.3.a. Niveau 1, niveau 2 et niveau 3

I.3.b. Haut débit

I.3.c. Sans-fil

II. Les interfaces de la couche physique

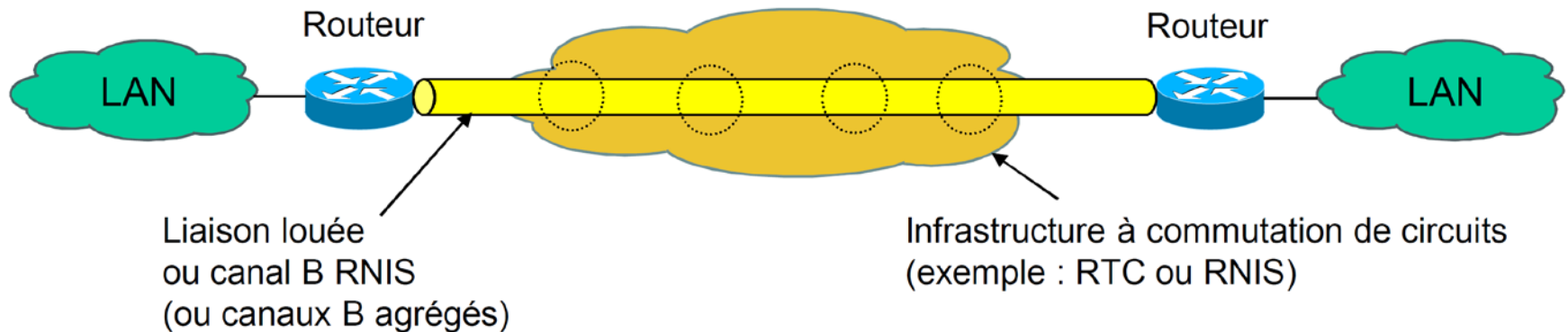
III. Protocoles de niveau 2 dans les WAN

IV. MPLS : commutation par VC dans le monde IP

V. Qualité de service

VI. Technologies xDSL

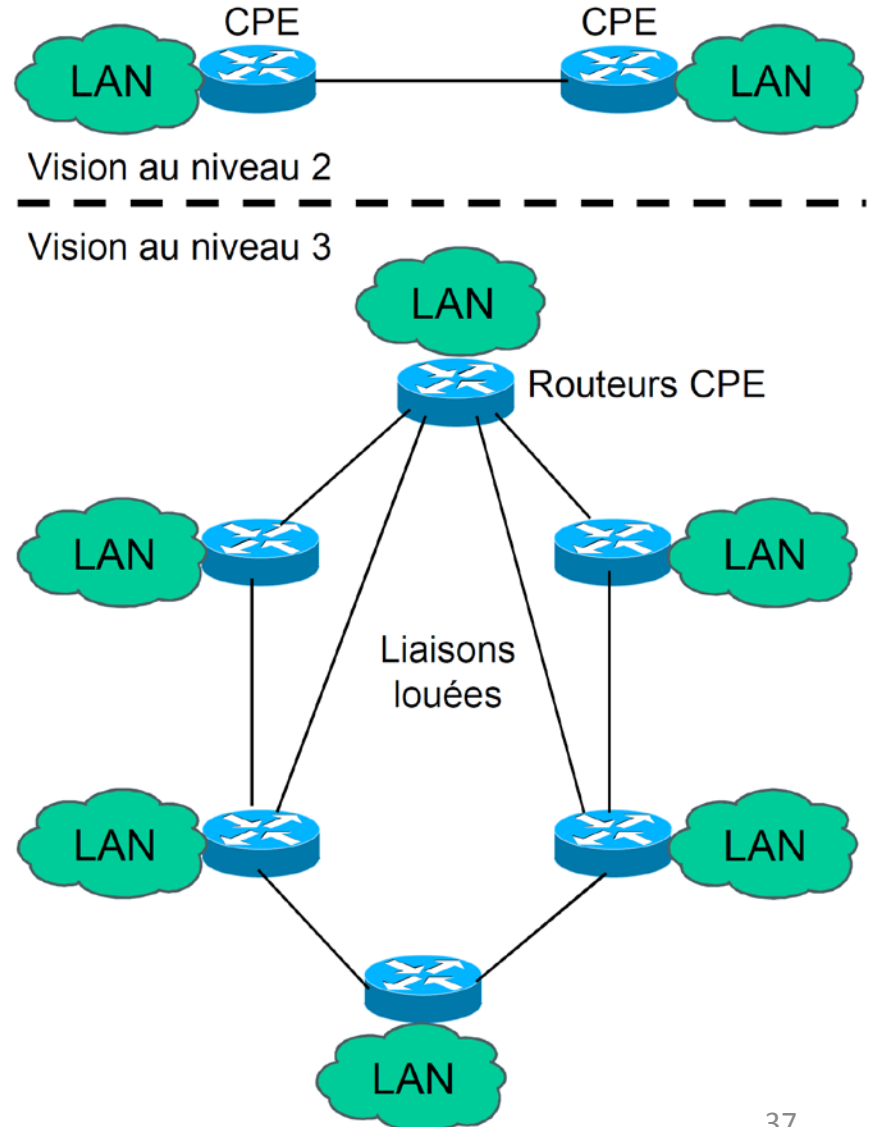
Services WAN de niveau 1



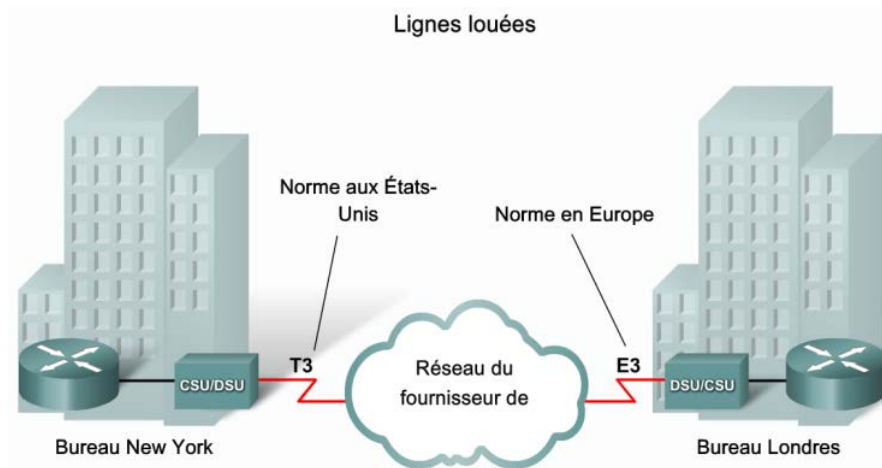
- **Le réseau WAN est basé sur la commutation de circuits**
 - L'opérateur fournit un « tuyau » : un circuit physique entre 2 routeurs
 - Les commutateurs de circuits sont transparents pour le protocole de niveau 2 (et protocoles de niveau supérieur)
- **Le protocole de niveau 2 entre les routeurs n'est pas imposé**
 - Protocole point à point quelconque
 - Le plus souvent PPP (Point to Point Protocol)
 - Sinon protocole propriétaire
- **Facturation selon la distance et le débit**
- **Solution chère, en général réservée aux très grosses entreprises**

Services WAN de niveau 1

- **Au niveau 2 les routeurs CPE se voient directement entre eux**
 - Par le protocole PPP par exemple
- **Au niveau 3 les routeurs CPE se voient directement entre eux**
 - Une liaison louée (ou un circuit) est vue comme un sous-réseau IP
 - Avec 2 adresses IP privées
 - Les routeurs CPE choisissent la route en fonction de leurs tables de routage
 - Tables statiques
 - Ou tables dynamiques alimentées par un protocole de routage (RIP, OSPF, ...)
- **Les équipements du réseau de l'opérateur (POP et commutateurs internes) ne sont pas concernés par les protocoles de niveau 2 et 3**



Options de connexion dédiée: lignes louées



- Lignes point à point généralement louées à un opérateur
-> « lignes louées »
- capacités variées, prix dépend de la BW requise et de la distance entre les deux points de connexion
- Plus coûteux que services partagés tels que le relais de trames
- Mais performances (latence, gigue) -> voix et video sur IP

Lignes louées: types de ligne et débits

Type de ligne	Débit binaire
56	56 Kbits/s
64	64 Kbits/s
T1	1,544 Mbits/s
E1	2,048 Mbits/s
J1	2,048 Mbits/s
E3	34,064 Mbits/s
T3	44,736 Mbits/s
OC-1	51,84 Mbits/s
OC-3	155,54 Mbits/s

Type de ligne	Débit binaire
OC-9	466,56 Mbits/s
OC-12	622,08 Mbits/s
OC-18	933,12 Mbits/s
OC-24	1 244,16 Mbits/s
OC-36	1 866,24 Mbits/s
OC-48	2 488,32 Mbits/s
OC-96	4 976,64 Mbits/s
OC-192	9 953,28 Mbits/s
OC-768	39 813,12 Mbits/s

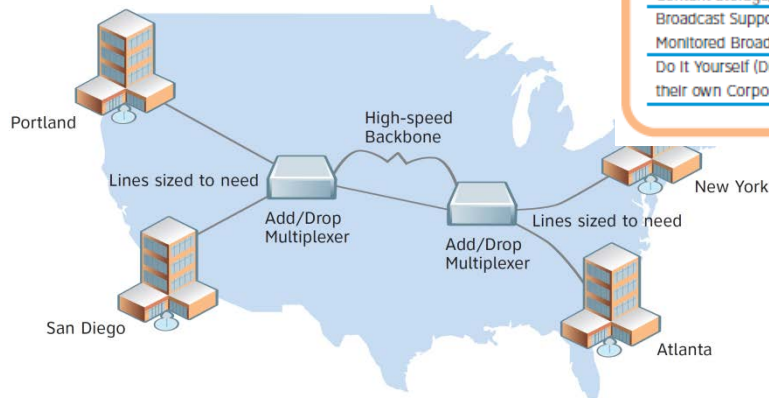
Private/Leased Lines

FEATURES

- Configures private lines over physically diverse POP to POP routes if required
- Uses self-healing SONET Network to route customer traffic
- SLAs that provide credits in the rare event of a service interruption
- Premium Services with Enhanced SLAs
- Multiple types of configurations – Point to Point, Multipoint and Add/Drop Multiplexer
- Cost-effective and scalable speeds up to 9.9 Gbps (OC192)

Business Need	Application	SC	T1	T3	Wavelength & SONET Service	Optical Mesh Service	
Supply-Chain Management: Lower costs by managing assets and resources	Inventory tracking	•		•	•	•	
	Order tracking	•			•	•	
	Point of sale	•	•		•	•	
	Shipment tracking	•			•	•	
	Electronic Data Interchange				•	•	
Information Sharing: Maintain a competitive edge by ensuring that employees have access to timely information and can work together to implement corporate goals	Hoot 'n' Hollers	•					
	Automatic Ring Down	•					
	Videoconferencing			•	•	•	
	CAD-CAM			•	•	•	
Connectivity: Increase productivity by enabling workgroup communication	CAD-CAM-CAE			•	•	•	
	Bulk File Transfer	•	•	•	•	•	
	Host-to-Host Connectivity		•	•	•	•	
	ISP Interconnectivity and Hosting		•	•	•	•	
	LAN Interconnection	•	•	•	•	•	
	High volume voice, video, data			•	•	•	
	Network Consolidation			•	•	•	
	Bulk voice, data and video to multiple locations				•	•	
	Imaging: Overcome the challenges of sharing large, graphic-intensive files	Imaging			•	•	•
		Teleradiology			•	•	•
Automatic Teller Machines		•			•	•	
Remote telemetry							
Automation: Increase efficiency by simplifying processes and automating tasks	Bulk file transfer & mirroring						
	Customer Info Systems				•	•	
Enhanced Customer Service: Retain customers by employing personalized customer service strategies							
Distance Learning: Overcome the challenges of a dispersed and/or mobile workforce	Distance Learning/ Remote Consultation		•	•	•	•	
Media Distribution: Deliver Broadcast Video/ Content Storage/Streaming Video	Distribution of various forms of media				•	•	
Broadcast Support: Deliver Managed/ Monitored Broadcast Video	Full-time or occasional use/ news/sports/special events			•	•	•	
Do It Yourself (DIY) Networking: Customers desire to build their own Corporate Utility Network	Customer looking to build their own backbone Infrastructure				•	•	

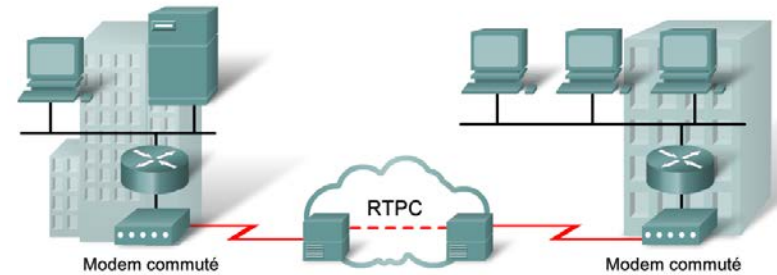
AT&T Private Line Service – Multiplexed



Options de connexion à commutation de circuits: accès commuté analogique

Historique :

- Transferts de données intermittents de faible volume: modems et lignes téléphoniques commutées analogiques pour connexions commutées de faible capacité et dédiées
- Téléphonie traditionnelle: câble de cuivre, appelé boucle locale, pour connecter le combiné téléphonique situé dans les locaux de l'abonné au central téléphonique (CO).
- Boucles locales traditionnelles: transport des données informatiques binaires par le réseau téléphonique vocal au moyen d'un modem.
- Les caractéristiques physiques de la boucle locale et sa connexion au RTPC limitent le débit de ce signal à moins de 56 Kbits/s.
 - Petites entreprises: pour l'échange de chiffres de vente, de prix, et de courriel.
 - Numérotation automatique la nuit ou le week-end -> tarifs heures creuses plus intéressants.
 - Tarifs fondés sur la distance entre les points d'extrémité, l'heure du jour et la durée de l'appel.
- Avantages du modem et des lignes analogiques: simplicité, disponibilité et faible coût d'implémentation.
- Inconvénients: faibles débits et temps de connexion relativement long.



Options de connexion à commutation de circuits: RNIS (ISDN)

- Boucle locale d'un RNIS: transport de signaux numériques
-> connexions commutées de plus haute capacité

- canaux Bearer à 64 Kbits/s (B): voix ou données
- canal delta de signalisation (D): configuration (et autres)

- 2 types d'interface RNIS:

➤ **Basic Rate Interface (BRI) :**

2 canaux B à 64 Kbits/s + 1 canal D à 16 Kbits/s

Pour utilisateurs individuels et petites entreprises

Canal D (contrôle) souvent sous-utilisé car seulement 2 canaux B à gérer.

-> Certains fournisseurs laissent le canal D transporter des données à bas débit (X.25 à 9,6 Kbps)

➤ **Primary Rate Interface (PRI) :**

USA: 23 canaux B à 64 Kbits/s + 1 canal D à 64 Kbits/s en, débit total jusqu'à 1,544 Mbits/s

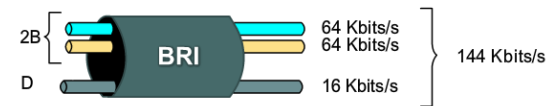
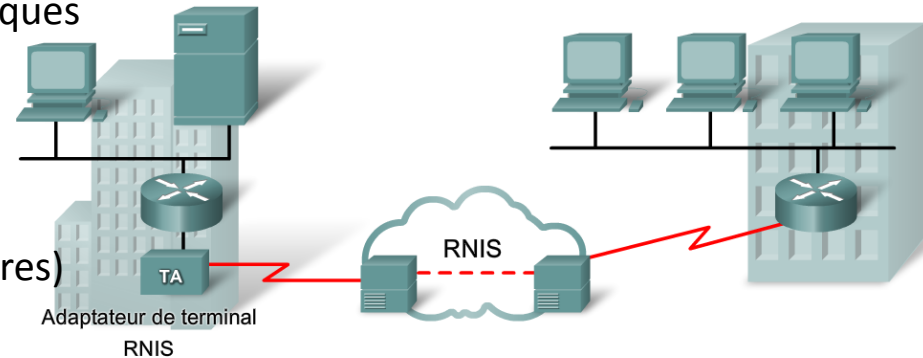
Pour des installations de plus grande taille.

Europe, Australie et autres régions: 30 canaux B +1 canal D, débit total jusqu'à 2,048 Mbits/s

Surcharge pour la synchronisation incluse

USA: connexion T1.

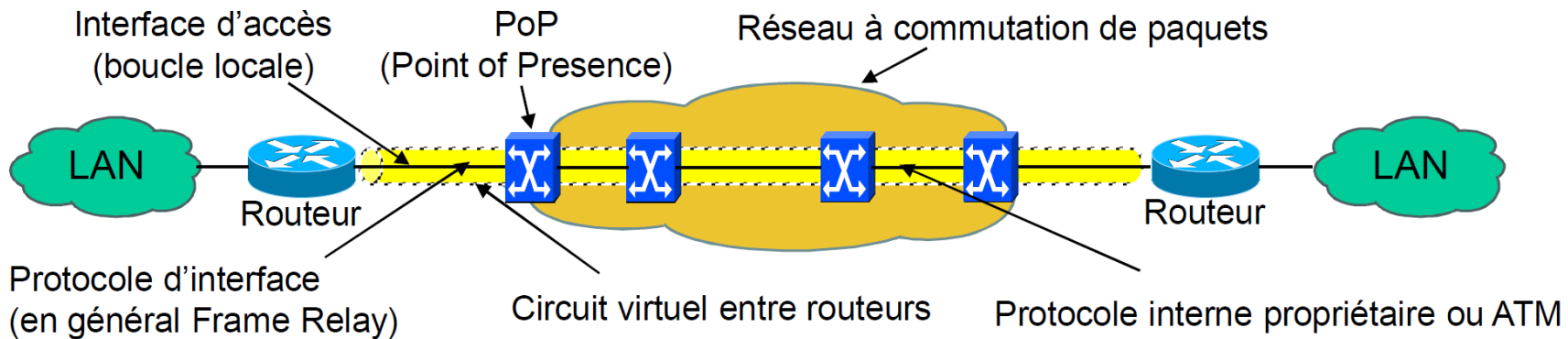
Le débit du PRI international correspond à une connexion E1 ou J1.



Options de connexion à commutation de circuits: RNIS (ISDN)

- RNIS BRI pour les petits réseaux étendus: durée d'établissement de la comm du BRI <1s
- Capacité du canal B de 64 Kbits/s > capa de liaison par modem analogique
- Si besoin de plus -> activation d'un 2^{ème} canal B -> total de 128 Kbits/s
- Autre application courante du RNIS: fournir des capacités suppl en fct des besoins à une connexion par ligne louée.
- Les tarifs RNIS sont calculés par canal B et sont similaires à ceux des connexions analogiques vocales.
- RNIS PRI: plusieurs canaux B peuvent être connectés entre deux points d'extrémité -> vidéoconférences et connexions de données à haut débit sans latence ni gigue

Services WAN de niveau 2 avec VC

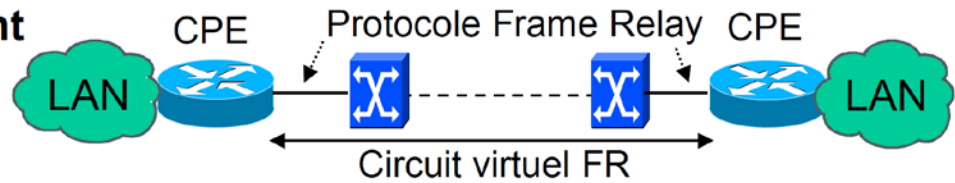


- **Le réseau WAN est basé sur la commutation de paquets**
 - Un circuit virtuel entre 2 routeurs CPE
 - Le routeur utilise un protocole d'interface avec le PoP pour créer et exploiter un circuit virtuel le reliant au routeur distant
 - Le protocole d'interface le plus courant à ce niveau était FR, est de plus en plus Ethernet
 - X25 est obsolète (adapté à des besoins périmés), ATM reste en général à l'intérieur du réseau
 - Le POP est un commutateur de paquets
- **Frame Relay encore courant car bien adapté au trafic de données**
 - Mais peu adaptée à la téléphonie sur IP
- **Mais en voie de déclin, car l'opérateur doit gérer plusieurs infrastructures réseau**
 - Une infrastructure pour la téléphonie (commutation de circuits)
 - Une infrastructure pour l'interconnexion des LAN
 - Une infrastructure pour Internet

Services WAN de niveau 2 avec VC

- **Au niveau 2 les routeurs CPE se voient indirectement entre eux**

- Un protocole d'interface (en général Frame Relay) permet d'établir et d'utiliser un circuit virtuel entre routeurs CPE

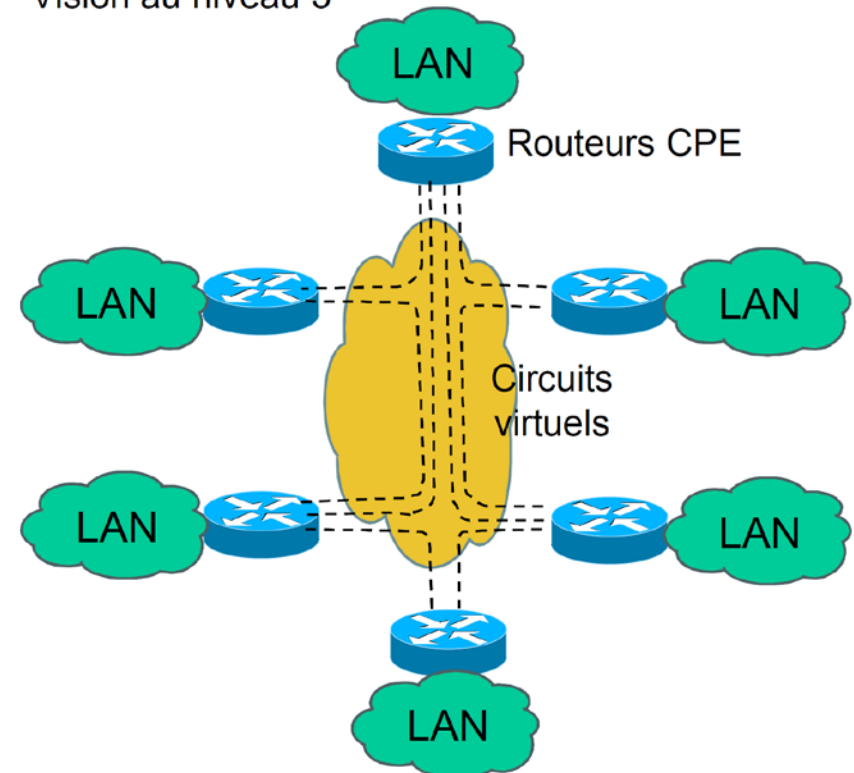


Vision au niveau 2

Vision au niveau 3

- **Au niveau 3 les routeurs CPE se voient directement entre eux**

- Un circuit virtuel est vu comme un sous-réseau IP
 - Avec 2 adresses IP privées
- Les routeurs CPE choisissent la route en fonction de leurs tables de routage
 - Tables statiques, ou tables dynamiques alimentées par un protocole de routage



- **Les équipements du réseau de l'opérateur (POP) sont concernés par le protocole de niveau 2 mais pas par le protocole de niveau 3**

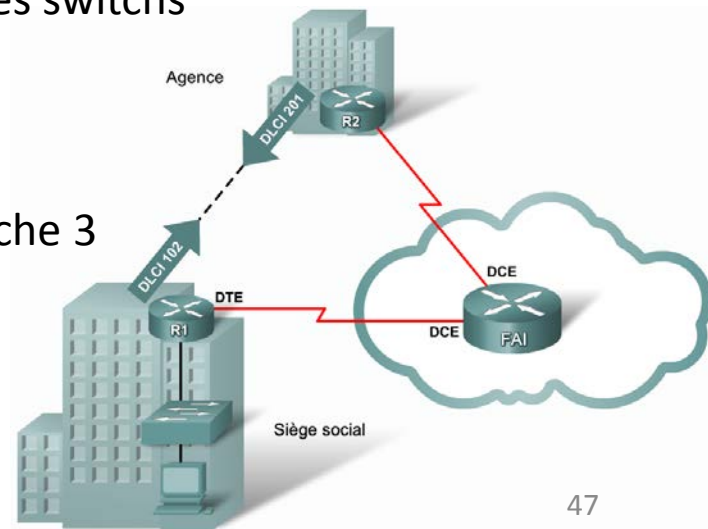
Options de connexion à commutation de paquets

Les plus utilisées aujourd'hui dans les réseaux étendus d'entreprise:

- Frame relay
- ATM
- Ethernet dans sa version Metro et WAN: layer-2 VPN

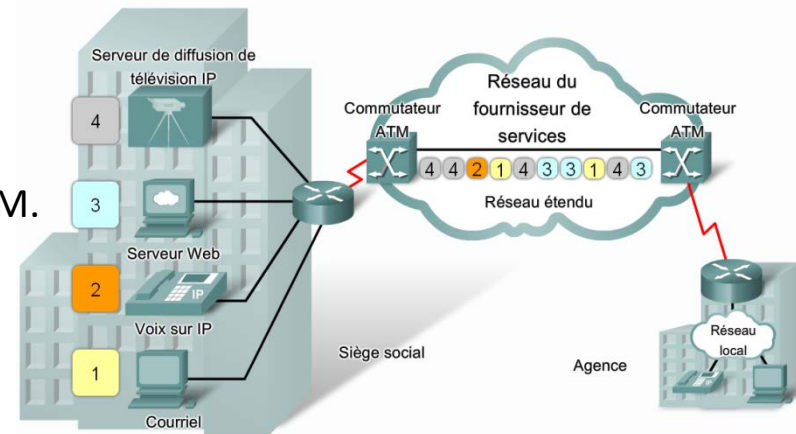
Options de connexion à commutation de paquets: Frame Relay

- **VC de FR identifiés de manière unique par un DLCI**, qui garantit une comm bidirectionnelle
- La plupart des connexions de relais de trames sont des PVC et non des SVC.
- Débit partagé moyen pouvant transporter du trafic vocal et de données.
- FR idéal pour connecter les réseaux locaux d'entreprise.
- Le routeur du réseau local ne nécessite qu'une interface, même avec plusieurs circuits virtuels.
- La courte ligne louée vers la périphérie du réseau de relais de trames autorise des **connexions économiques entre des réseaux locaux largement dispersés**.
- Mesures prises pour éviter l'accumulation des trames sur les switches intermédiaires -> phénomènes de gigue réduits
- Par rapport à X.25:
 - protocole plus simple, couche 2 au lieu de la couche 3
 - aucun contrôle d'erreur ou de flux
- > réduction de la latence
- Débits jusqu'à 4 Mbits/s, certains SP proposant même plus



Options de connexion à commutation de paquets: Asynchronous Transfer Mode

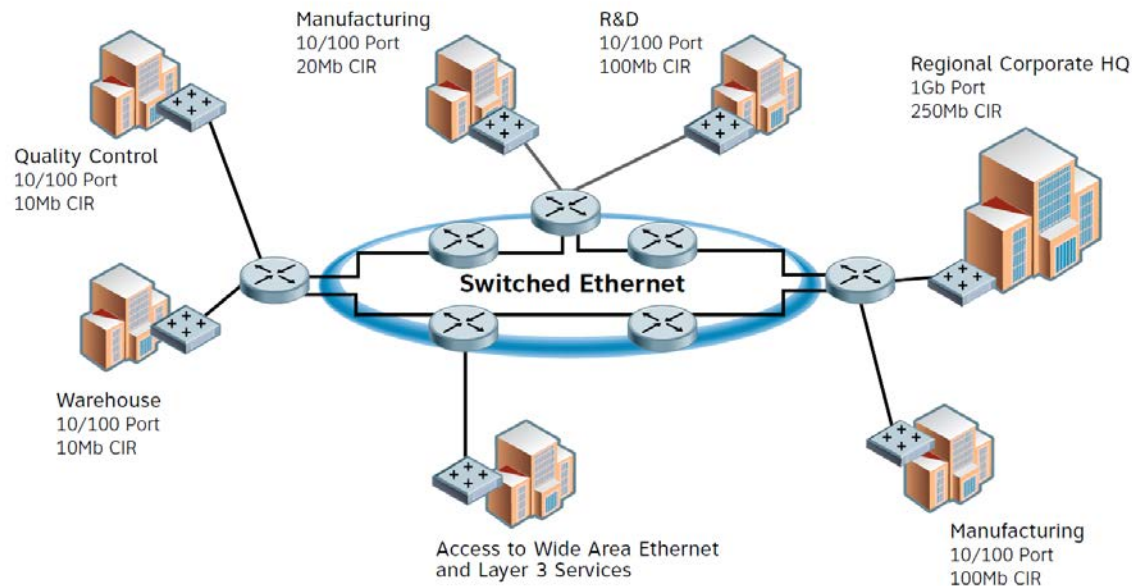
- Architecture à cellules, et non à trames.
- **Cellules ATM: toujours longueur fixe =53 octets**, contient: un en-tête ATM de 5 octets + 48 octets de données utiles ATM.
- > **trafic vocal et vidéo, car ce trafic ne tolère pas les délais.**
- En effet, le trafic vidéo et vocal n'a pas à attendre la fin de transmission d'un paquet de données de plus grande taille.



- But: QoS et performance (traitement hardware)
- Cellule ATM de petite taille fixe moins efficace que les trames et paquets de plus grande taille de FR et X.25
5 octets de surcharge pour chaque ensemble de données utiles de 48 octets
-> surcharge plus importante (perte de rendement) quand la cellule transporte des paquets de couche réseau segmentés
+ le commutateur ATM doit regrouper les paquets au niveau de la destination.
-> Une ligne ATM typique nécessite un débit presque 20 % > FR pour transporter au même débit *utile* des données de couche réseau.
- PVC plus courants avec les réseaux étendus.
- Comme les autres technologies partagées, ATM accepte plusieurs VC sur une seule connexion par ligne louée vers la périphérie du réseau.

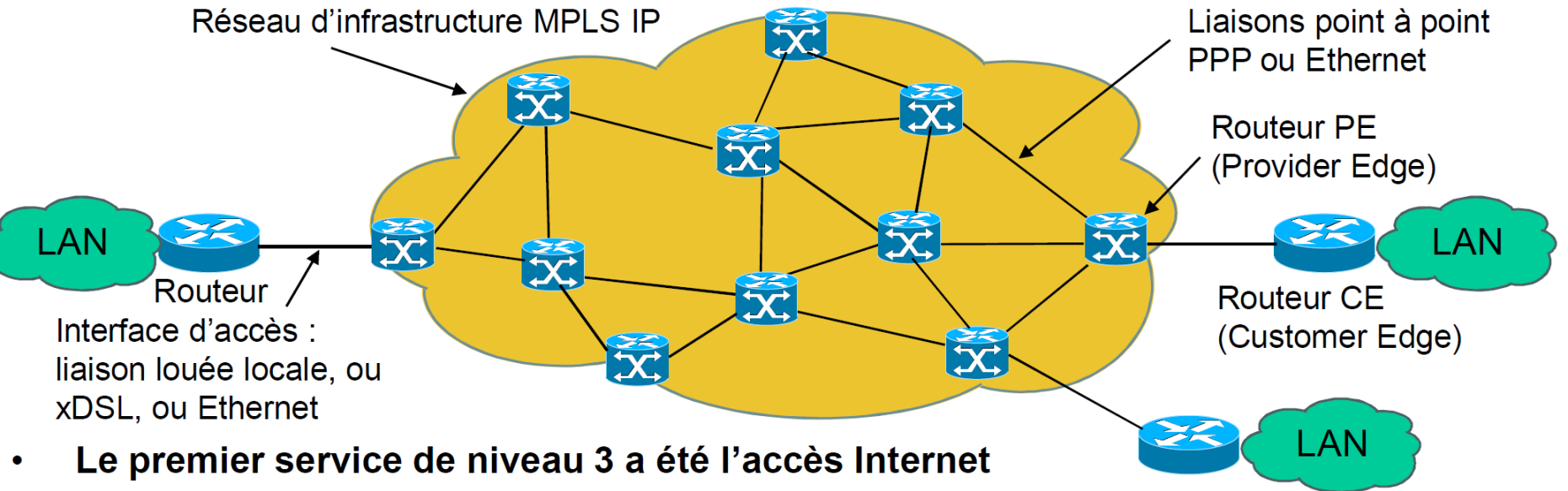
Switched Ethernet & Virtual Private LAN Service (VPLS or layer-2 VPN)

Ethernet switché peut étendre le LAN tout en connectant des sites distants à l'échelle de la ville ou plus.



You can use Ethernet Virtual Private Line (EVPL) in your Metro or across a Wide Area Network, nationwide or globally and potentially save since unlike other private line services, you only pay based on the ports or connections to the network and not mileage.

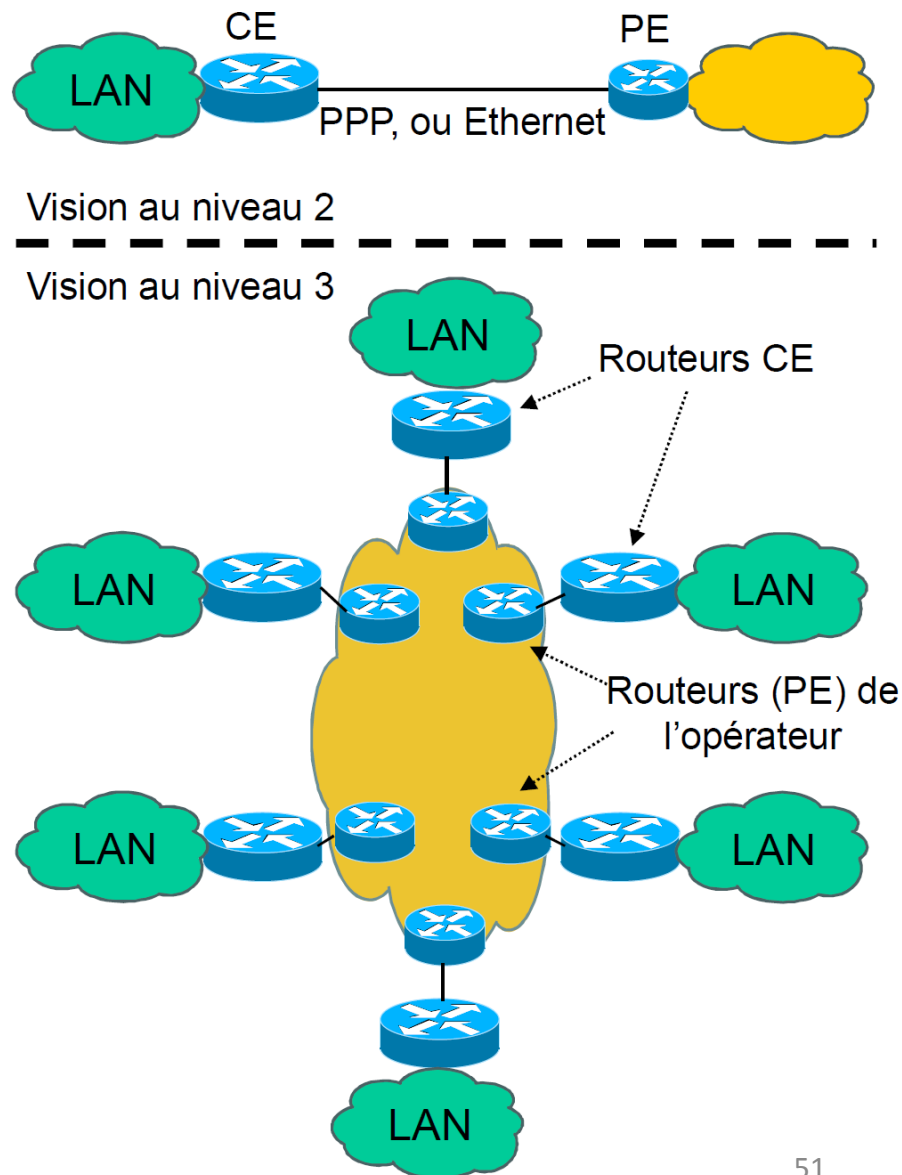
Services WAN de niveau 3



- **Le premier service de niveau 3 a été l'accès Internet**
 - Basé sur une infrastructure en IP pur
- **Puis les opérateurs ont fourni des services VPN IP multipoint**
 - L'opérateur se charge de relier en IP les routeurs CE de l'entreprise
 - L'opérateur se charge de l'étanchéité des trafics entre ses clients
 - Grâce à la technologie MPLS (Multi Protocol Label Switching)
 - Qui permet une forme de circuits virtuels sur un réseau IP
- **Cette solution permettra à terme la convergence des infrastructures réseau**
 - Une infrastructure commune IP pour la téléphonie, l'interconnexion des LAN et Internet
- **Solution de plus en plus souvent proposée par les opérateurs**
 - Cette solution devient dominante avec le développement de MPLS et des solutions de QoS/IP

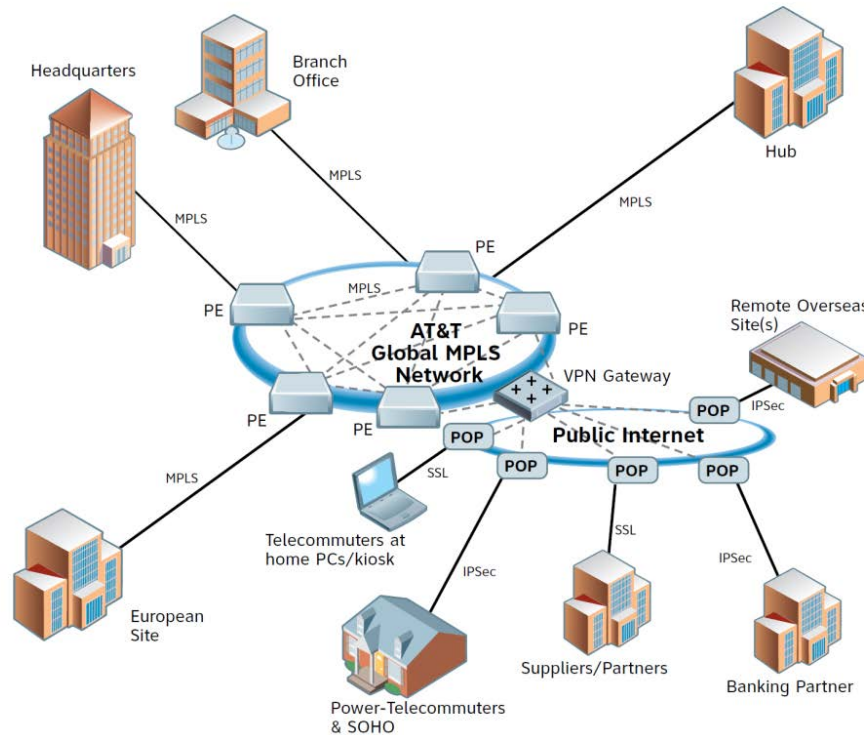
Services WAN de niveau 3

- **Au niveau 2 les routeurs CE ne se voient pas**
 - Le routeur CE voit le routeur PE
 - Le protocole de niveau 2 peut être quelconque
 - PPP, Ethernet, etc...
- **Au niveau 3 les routeurs CE ne se voient pas directement**
 - Le routeur CE voit le routeur PE
 - Les routeurs CE envoient tout le trafic externe ver le routeur PE
 - Par une table statique (la route par défaut)
- **Les équipements du réseau de l'opérateur (PE) sont concernés par le protocole de niveau 3 IP**
 - Le client a externalisé son routage : c'est l'opérateur qui s'en charge
 - Solution appelée VPRN (Virtual Private Routed Network)



IP (layer-3)- VPN

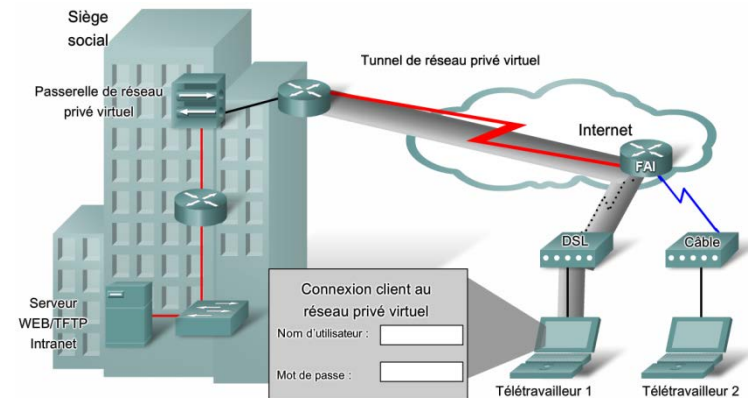
- **VPN basés réseau** : basés sur la techno MPLS (qui réalise la convergence entre commutation avec connexion et monde IP, et supporte la QoS).
- **VPN basés client** : tunnels VPN depuis les locaux du client , protection de la confidentialité et de l'intégrité des données à travers le réseau grâce à des tunnels encryptés : IP Security (IPSec) et Secure Sockets Layer (SSL).



Options de connexion Internet: Technologie de VPN (1)

- Utilisation par un télétravailleur ou un bureau distant de services à large bande pour accéder au réseau étendu d'une entreprise -> risques en termes de sécurité.
- > Les services à large bande offrent la possibilité d'utiliser des connexions de réseau privé virtuel (VPN) vers un serveur de réseau privé virtuel (généralement situé dans les locaux de l'entreprise).
- Réseau privé virtuel (VPN): connexion chiffrée entre des réseaux privés sur un réseau public (Internet).
- Au lieu d'utiliser une connexion de couche 2 dédiée telle qu'une ligne louée, un VPN utilise des connexions virtuelles appelées tunnels de réseau privé virtuel, qui sont acheminées via Internet depuis le réseau privé de l'entreprise vers le site distant ou l'hôte de l'employé.

→ « VPN à accès à distance » ou « Premises-Based VPNs »
(cf. slide 48)



Options de connexion Internet: Technologie de VPN (2)

Avantages du VPN:

- **Économique** : les VPN permettent aux organisations d'utiliser le réseau Internet global pour connecter des bureaux et des utilisateurs distants aux locaux principaux d'une entreprise, éliminant ainsi le besoin de liaisons de réseau étendu dédiées et de banques de modems.
- **Sécurité** : tunneling et/ou protocoles avancés de chiffrement et d'authentification qui protègent les données contre des accès non autorisés.
- **Extensibilité** : utilisent l'infrastructure Internet au sein des périphériques et des FAI - > il est très facile d'ajouter des nouveaux utilisateurs. Les grandes entreprises peuvent ajouter des volumes importants de capacité sans ajouter d'infrastructure.
- **Compatibilité** avec la technologie à large bande : VPN pris en charge par AP de services à large bande tels que DSL et câble pour travailleurs mobiles.

Plan

I. Présentation des WAN

I.1. Concepts généraux

I.2. Evolution de la commutation : commutation de circuit, de paquet avec et sans connexion

I.3. Options de connexion au WAN

I.3.a. Niveau 1, niveau 2 et niveau 3

I.3.b. Haut débit

I.3.c. Sans-fil

II. Les interfaces de la couche physique

III. Protocoles de niveau 2 dans les WAN

IV. MPLS : commutation par VC dans le monde IP

V. Qualité de service

VI. Technologies xDSL

Options de connexion Internet: Services à large bande

- Les options de connexion à large bande sont généralement utilisées pour connecter via Internet des télétravailleurs au site de l'entreprise.
- Les options disponibles sont les suivantes :
 - DSL
 - câble
 - sans fil
 - optique

Options de connexion Internet:

Services à large bande: DSL

- DSL: technologie de connexion permanente qui utilise les lignes téléphoniques à paires torsadées existantes pour transporter des données à haut débit et fournir des services IP aux abonnés.

- Modem DSL: signal Ethernet de périph d'utilisateur vers signal DSL, transmis au central téléphonique.

- Plusieurs lignes d'abonnés DSL multiplexées en une liaison unique à haute capacité au moyen d'un multiplexeur d'accès DSL (DSLAM) dans les locaux AP.

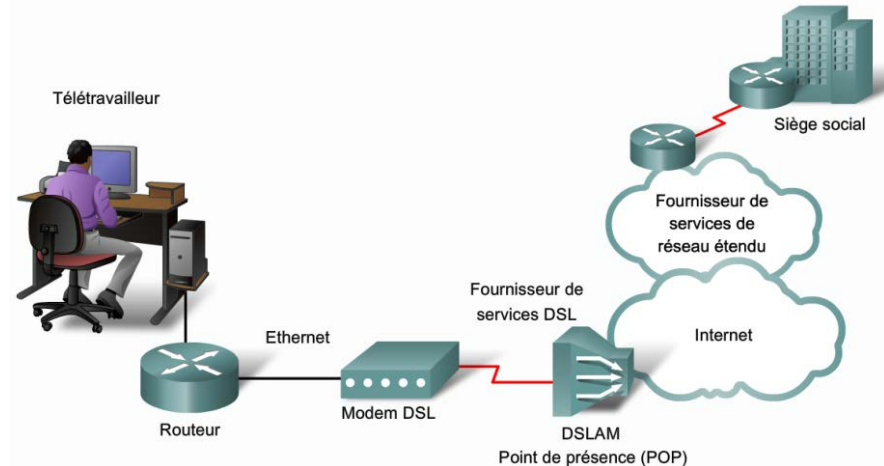
- DSLAM: TDM pour agréger lignes d'abonnés vers fibre ou T3/DS3.

- Codage et modulation sophistiqués -> débits pouvant atteindre 20 Mbps.

- Grande diversité de types, normes et normes émergentes DSL.

- Choix populaire pour les services informatiques d'entreprise desservant des télétravailleurs.

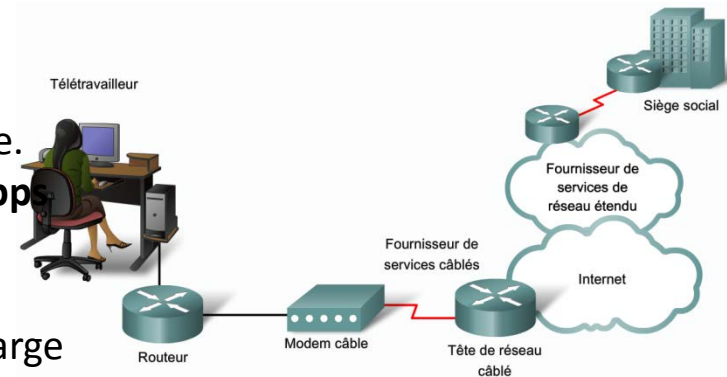
- Les risques encourus en termes de sécurité lors de ce processus peuvent être tempérés par des mesures de sécurité.



Options de connexion Internet:

Services à large bande: Câble

- **Câble coaxial**: répandu dans les zones urbaines pour distribuer des signaux de télévision.
- Accès réseau disponible sur certains réseaux de télévision câblée. BW > boucle locale téléphonique conventionnelle -> **30 à 100Mbps**
- Connexion permanente et facile à installer.
- Modem câble: traduit les signaux numériques en fréquences à large bande utilisées pour la transmission sur un réseau de télévision câblée.
- Le bureau local de télévision câblée, appelé **tête de réseau câblé**, comprend le système informatique et les bases de données requises pour fournir l'accès Internet.
- Le composant le plus important situé au niveau de la tête de réseau est le système de terminaison du modem câble (CMTS): envoie et reçoit des signaux numériques du modem câble sur un réseau câblé et est requis pour fournir des services Internet aux abonnés du câble.
- Les abonnés au modem câble doivent utiliser le FAI associé au fournisseur d'accès TV.
- Tous les abonnés locaux partagent la même bande passante.
- > À mesure que des utilisateurs rejoignent le service, le débit dispo peut être inférieur au débit attendu.



Options de connexion Internet: Metro Ethernet

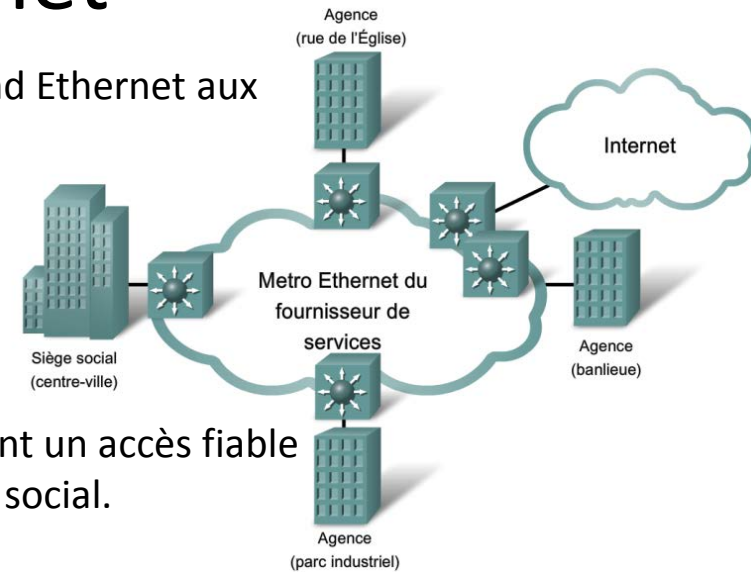
- Metro Ethernet: Techno de réseau en rapide évolution qui étend Ethernet aux réseaux publics gérés par des sociétés de télécommunications.

- Permet à des SP d'offrir aux entreprises des services convergés de voix, données et vidéo: ToIP, stockage de données.

- Ethernet étendu à la zone métropolitaine -> bureaux distants ont un accès fiable aux applications et données situées sur le réseau local du siège social.

- Avantages:

- Réduction des dépenses d'administration: réseau commuté à large BW de couche 2 capable de gérer données, signaux vocaux et vidéo sur une seule infrastructure
-> BW augmente et élimination des conversions coûteuses vers ATM et le FR
Connexions des sites d'entr entre eux et à Internet au sein d'une zone métropolitaine, à faible coût.
- Intégration simplifiée avec les réseaux existants: connexion facile aux LAN Ethernet existants
-> réduction des coûts et de la durée d'installation.

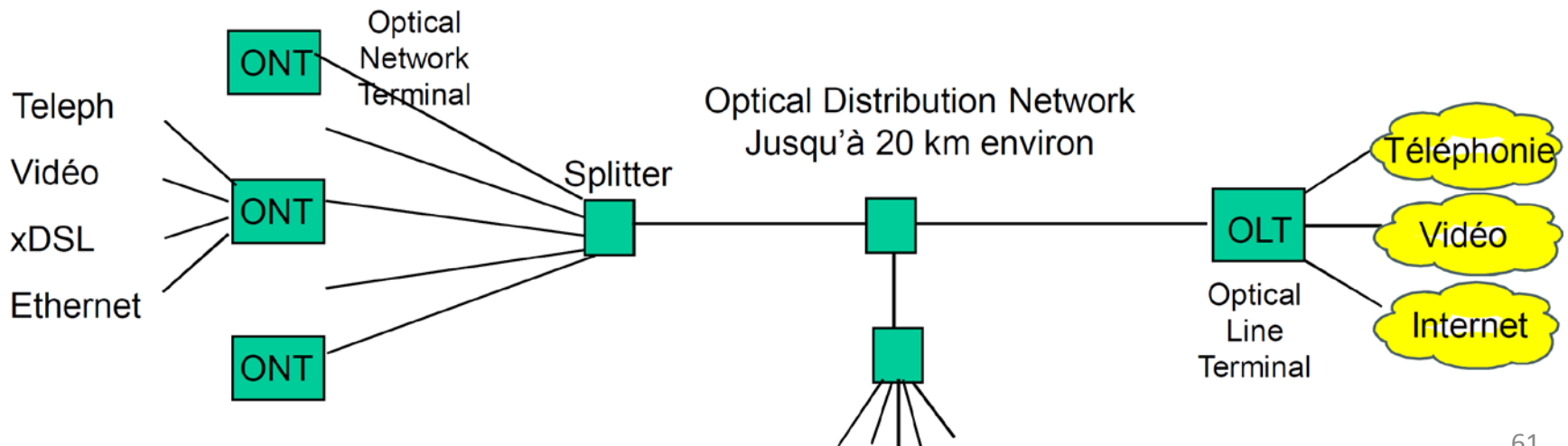


EFM (Ethernet in the First Mile) physiquement

- **Les entreprises ont de plus en plus besoin de débits symétriques**
 - Centralisation des serveurs sur un site, ToIP, vidéoconférence, etc.
 - Décroissance de ADSL au profit de SDSL
- **EFM comble le vide entre les lignes SDSL agrégées (8Mbps) et la fibre optique (50 Mbps et plus)**
- **EFM est normalisé par l'IEEE (802.3ah)**
 - 2 Base-TL : débit max symétrique de 15 à 40 Mbps selon la distance (3 à 1 km) par agrégation de 8 paires de cuivre SDSL (5,7 Mbps par paire)
 - Couche physique : variante améliorée de SDSL
 - Appelé E-SDSL (Enhanced SDSL) par l'ETSI, et G.SHDSL par l'IUT
 - Modulation à 32 niveaux (PAM32) au lieu de 16 niveaux (PAM16)
 - Couche 2 : Ethernet en natif
 - 802.3ah spécifie aussi des versions EFM sur fibre optique
 - 100 Base-LX10 (100Mbps sur 10km), 1000 Base-LX10 (1Gbps sur 10km), 1000 Base-PX10 (1Gbps sur 10km sur fibre FTTH passive)
- **La version cuivre intéresse surtout les opérateurs alternatifs**
 - Qui n'ont pas de réseau dense de fibres optiques

Boucle locale fibre optique

- **Les accès fibre optique doivent succéder aux accès xDSL**
 - FTTC (FTT-Curb), FTTB (FTT-Building), FTTH (Fiber-To-The-Home)
 - C'est surtout FTTH qui se déploie en France
 - Option d'architecture point à point
 - Ethernet actif : chaque client est relié à l'équipement actif par une fibre qui lui est dédiée
 - Plus adapté aux infrastructures nouvellement créées et aux services aux entreprises
 - Option Point à Multipoint ou Passive Optical Network (PON)
 - Le signal optique est divisé en plusieurs branches (jusqu'à 64) dans un splitter
 - La bande passante est partagée



Plan

I. Présentation des WAN

I.1. Concepts généraux

I.2. Evolution de la commutation : commutation de circuit, de paquet avec et sans connexion

I.3. Options de connexion au WAN

I.3.a. Niveau 1, niveau 2 et niveau 3

I.3.b. Haut débit

I.3.c. Sans-fil

II. Les interfaces de la couche physique

III. Protocoles de niveau 2 dans les WAN

IV. MPLS : commutation par VC dans le monde IP

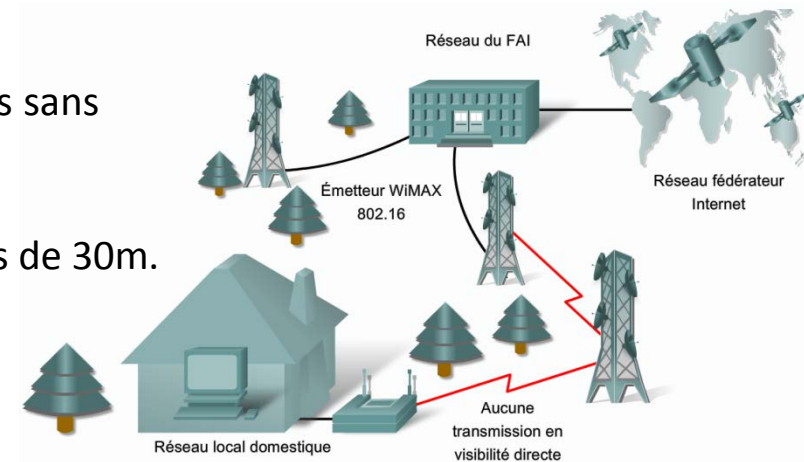
V. Qualité de service

VI. Technologies xDSL

Options de connexion Internet:

Services à large bande: Sans-fil (1)

- La technologie sans fil utilise le spectre des radiofréquences sans licence pour envoyer et recevoir des données.
- Jusqu'à une période récente: obligation de portée de moins de 30m.
- Récentes améliorations de la techno sans fil à large bande:



- **WiFi municipal** : réseaux sans fil au niveau des municipalités. Accès Internet à haut débit, gratuit ou moins cher qu'autres services à large bande.
Pour se connecter: modem sans fil avec antenne de radio et directionnelle plus puissante que les adaptateurs sans fil traditionnels.
- **WiMAX** : la nouvelle technologie d'interopérabilité mondiale pour l'accès micro-ondes. Norme IEEE 802.16. Haut débit, accès sans fil, couverture similaire au réseau de tel portable. Similaire à WiFi, mais vitesses, distance et nb utilisateurs plus élevés.
Tours WiMAX similaires aux tours de téléphones portables.
Pour accéder: s'abonner auprès d'un FAI via une tour WiMAX située dans un rayon de 15 km de leur emplacement + ordinateur compatible WiMAX + un code de chiffrement spécifique.

Options de connexion Internet: Services à large bande: Sans-fil (2)

➤ Internet par satellite:

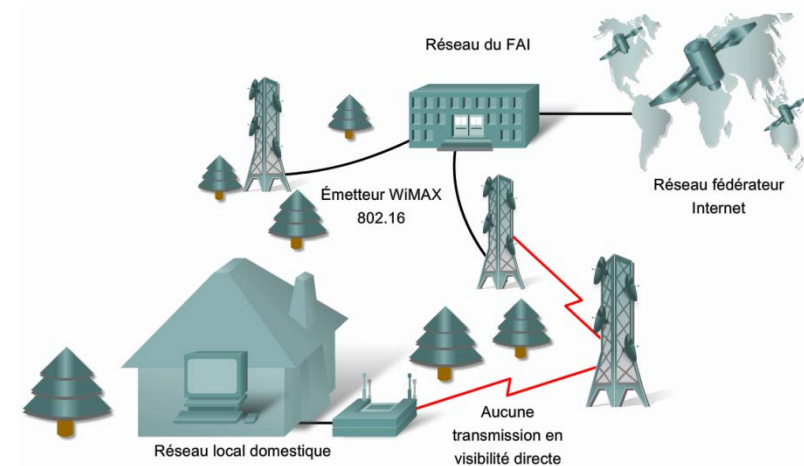
pour zones rurales où les connexions câblées ou DSL ne sont pas disponibles.

Antenne parabolique pour communications de données bidirectionnelles.

La vitesse uplink représente environ 1/10^e de la vitesse downlink qui est de 500 Kbits/s.

Les connexions câble et DSL présentent des vitesses de chargement plus élevées, mais les systèmes par satellite sont dix fois plus rapides qu'un modem analogique.

Pour accéder: antenne parabolique, deux modems (liaison montante et liaison descendante), et des câbles coaxiaux reliant l'antenne au modem.



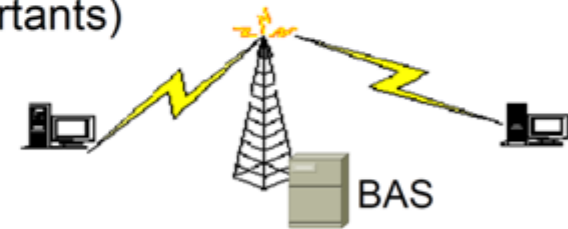
Autres boucles locales

- **Accès par câble**
 - Utilisable pour l'accès Internet
 - Utilisation plutôt personnelle que professionnelle
- **Accès par la téléphonie cellulaire**
 - GSM avec GPRS (2,5G) : débit <56kbps
 - Edge : débit 100 à 200 Kbps
 - UMTS (3G) : débit 384 kbps
 - 3G+ HSDPA : débit 1,8Mbps puis 3,6 Mbps à terme 7,2 Mbps
 - 3G+ HSUPA : débit montant de 1,4 Mbps
- **Accès par des hotspots 802.11 (Wi-Fi)**
 - Dans les gares, aéroports, cafés, hôtels, immeubles, etc...

Autres boucles locales

- **Boucle locale radio (BLR)**

- Accès sans fil point à multipoint en milieu urbain
- Débuts difficiles
- Renaissance avec le groupement **WiMAX** : Worldwide Interoperability for Microwave Access
- Standard 802.16 : bande de 10 à 66Mhz
 - Débit potentiels supérieurs à 100 Mbps, distance 5 km en ligne de vue
- Amendement 802.16a : extension dans la bande de 2 à 11Ghz
 - Bande 3,5 Ghz ouverte en France pour la BLR
 - Débits moins grands (ex. 75 Mbps), distances supérieures (50km)
 - Pas forcément en ligne de vue
 - Projets en cours de déploiement (mais retards importants)
 - Possibilités de communication point à point
 - Extension vers les mobiles : 802.16e et 802.20
- Cibles : couverture des zones blanches xDSL



- **Courants porteurs en ligne**

- Problème de régulation du marché
- 1ere génération limitée à 2 Mbps par abonné
- 2e génération en cours de développement
 - Jusqu'à 25 Mbps par abonné

Sélection d'une liaison de réseau étendu

Option	Description	Avantages	Inconvénients	Exemples de protocoles utilisés
Ligne louée	Connexion point à point entre deux ordinateurs ou réseaux locaux.	Sécurité optimale	Coûteuse	PPP, HDLC, SDLC, HNAS
Commutation de circuits	Un chemin de circuit dédié est créé entre des points d'extrémité. Les connexions commutées sont un exemple efficace de commutation de circuits.	Moins coûteuse	Établissement de la communication, faible débit	PPP, RNIS
Commutation de paquets	Les périphériques transmettent des paquets via une liaison partagée unique point à point ou point-à-multipoint sur un interréseau d'opérateur. Des paquets de longueur variable sont transmis sur des circuits virtuels permanents (PVC) ou des circuits virtuels commutés (SVC).	Moins cher, optimisation de l'utilisation des ressources des lignes	Support partagé sur une liaison	X.25, Relais de trames
Relais de cellules	Similaire à la commutation de paquets, mais utilise des cellules de longueur	Idéale pour l'utilisation de voix et de données	Les surcharges peuvent être	ATM

Rappel sur la notion de trafic

Trafic et occupation de ligne

- Le trafic est une notion liée à l'utilisation d'une voie de transmission.
 - Le trafic permet de connaître le degré d'utilisation d'une voie et donc de choisir une voie adaptée à l'utilisation que l'on veut en faire (posséder des lignes de transmission surdimensionnées ne sert pas, sauf à perdre de l'argent en abonnements).
- > L'intensité du trafic mesure la proportion d'utilisation de la voie par unité de temps (durée d'occupation pendant période d'observation/période d'observation).

La notion de trafic : définition

- Nous appellerons « machine » tout ce qui présente la propriété d'être soit libre, soit occupé. Pour nous, une ligne de téléphone est une machine: soit elle est libre (raccrochée), soit elle est occupée (décrochée).
- **Définition** : le **trafic** « a » d'une machine est la proportion du temps pendant laquelle elle est occupée.

$$a = \frac{t}{T}$$

t : temps d'occupation
pendant l'observation
 T : temps d'observation

- L'unité de trafic est l'occupation permanente que les téléphonistes appellent « **Erlang** », en honneur de l'ingénieur Danois Agner Krarup Erlang (1878-1929), qui a été le pionnier de l'application du calcul des probabilités au téléphone.
- Si une machine est occupée 10 % du temps, son trafic est de 0,1 Erlang.
- On parlera indifféremment de « **trafic** » ou « **intensité de trafic** ».

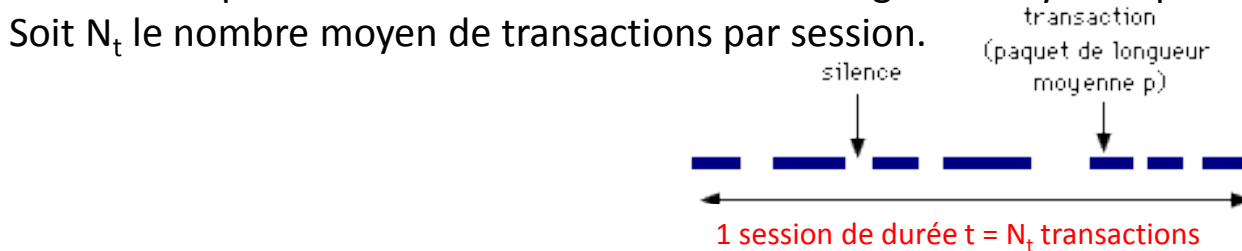
La notion de trafic : précisions

- Dans le cas d'une seule machine, son trafic exprimé en Erlang est aussi sa probabilité d'occupation.
- Le trafic d'*1* machine ne peut pas être supérieur à *1 Erlang*.
- Le trafic **A** d'un groupe de *N* machines ne peut pas être supérieur à *N Erlang*.

$$A = \frac{\sum_{i=1}^N t_i}{T} = \frac{N \cdot t}{T}$$

Débit effectif et débit nominal

- Problème de la mesure du temps d'utilisation effectif:
 - on peut considérer la durée d'une session, MAIS
 - session comporte un certain nombre de "silences", notamment dans les applications conversationnelles. On peut distinguer les deux cas extrêmes suivants concernant les types de sessions :
 - sessions où t est pleinement utilisé (rare)
 - sessions où t comprend des "silences "
- Dans ce dernier cas, l'intensité du trafic ne donne pas l'occupation réelle du canal.
- > On décompose la session en transactions de longueur moyenne p en bits, entrecoupées par des silences.



- D_n étant le **débit nominal** de la voie, le **débit effectif (ou utile)** de la voie (pour cette utilisation)

est: $D_u = N_t p / t$

et le **taux d'occupation du canal** est défini par le rapport : $\theta = D_u / D_n$

- *exemple* : calcul scientifique à distance : l'utilisateur dialogue avec un ordinateur central ;

$p = 900$ bits, $N_t = 200$, $t = 2700$ s, $N_c = 0.8$ sessions/h, $D_n = 1200$ b/s

d'où $E = N_c * t / T = 0.6$ Erlangs et $D_u = N_t * p / t = 66.6$ b/s donc $\theta = 0.05$

(voie utilisée théoriquement à 60% et effectivement à 5%).

Plan

I. Présentation des WAN

II. Les interfaces de la couche physique

II.1. Les différents types de multiplexage

II.2. La hiérarchie numérique synchrone PDH

II.3. La hiérarchie numérique synchrone SDH : réseaux de fibres optiques et redondance pour la fiabilité

III. Protocoles de niveau 2 dans les WAN

IV. MPLS : commutation par VC dans le monde IP

V. Qualité de service

VI. Technologies xDSL

Techniques de multiplexage

- Réseau de téléphone : même coût financier pour installer et entretenir une section de câble à large bande passante (haute capacité) qu'une section de câble de faible BP (les coûts correspondent à creuser la tranchée majoritairement).

-> Les compagnies de téléphone ont donc développé des schémas élaborés pour multiplexer plusieurs conversations sur un seul câble physique.

- 2 catégories de base : **FDM (Frequency Division Multiplexing)** et **TDM (Time Division Multiplexing)**

- FDM: le spectre de fréquence est divisé en bandes de fréquence, chaque utilisateur ayant l'usage exclusif d'une bande

exemple: radio AM – Le spectre alloué est de 1 MHz, entre 500 et 1500 KHz

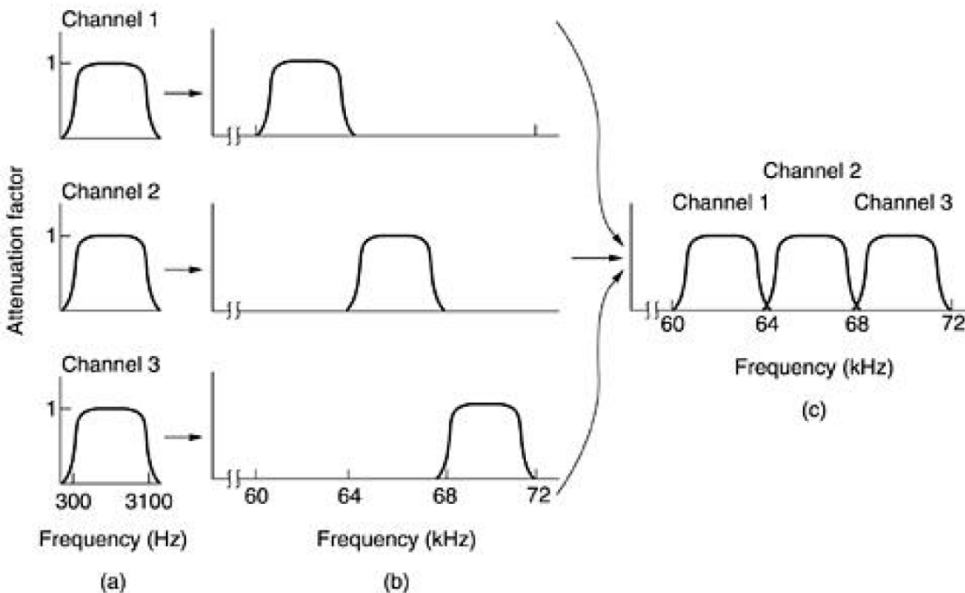
- TDM: les utilisateurs utilisent le câble à tour de rôle (façon *round-robin*), chacun obtenant périodiquement la totalité de la BP pour une courte durée.

- 1. FDM
- 2. FDM appliqué aux fibres optiques (*wavelength division multiplexing*).
- 3. TDM
- 4. TDM avancé pour les fibres optiques (SONET)

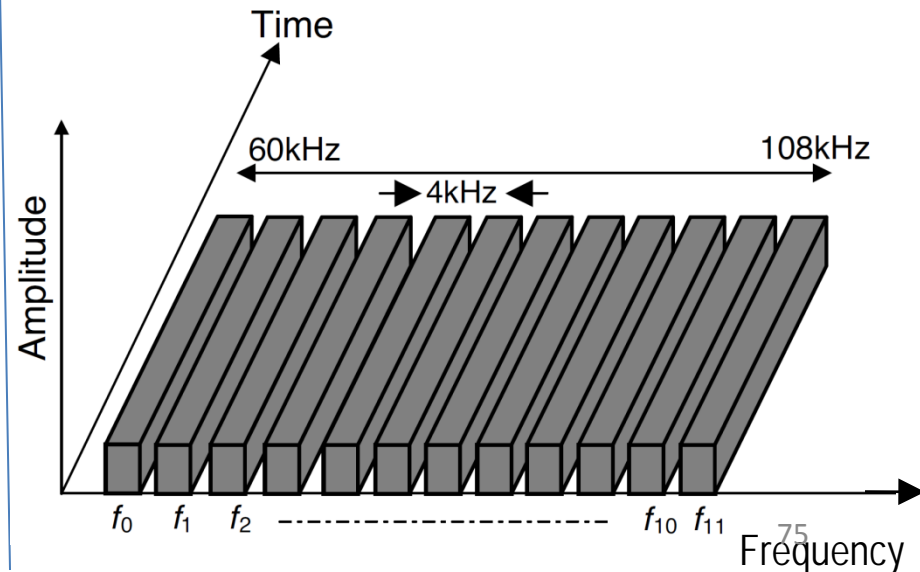
Frequency Division Multiplexing (FDM)

- Figure de gauche: comment 3 canaux téléphoniques sont multiplexés avec FDM
- Le filtres limitent la BP utilisable à 3100 Hz par canal de voix
- 4000 Hz sont alloués à chaque canal pour les garder bien séparés
- Noter que malgré les *guard bands* entre les canaux, il y a du recouvrement entre les canaux adjacents à cause des imperfections des filtres

- (a) Spectre initial
- (b) Spectre translaté en fréquence
- (c) Canaux multiplexés en fréquence

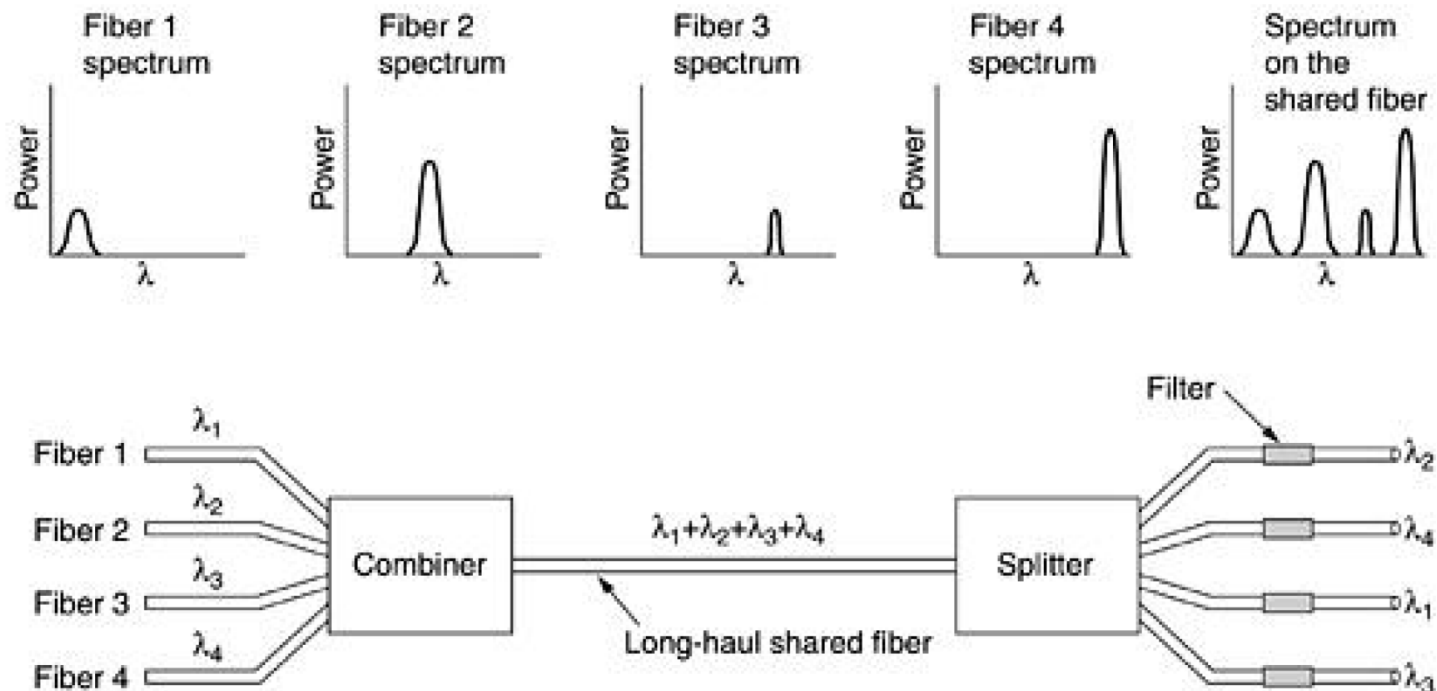


FDM est utilisé en multiplexant 12 abonnés chacun avec 4 KHz de BP dans les fréquences entre 60 et 108 KHz.



Wavelength Division Multiplexing (WDM)

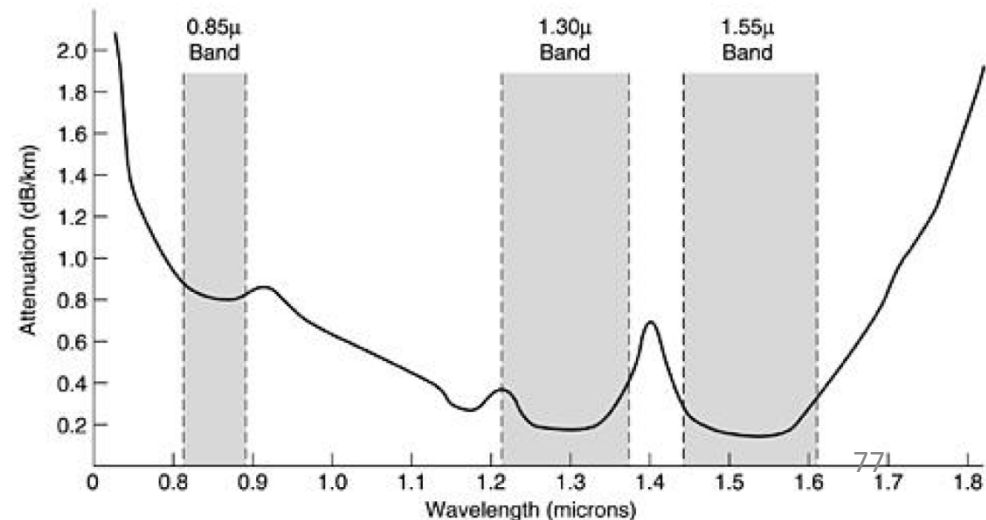
- Pour les fibres optiques, une variante de FDM est utilisée : **WDM (Wavelength Division Multiplexing)**
- Figure: 4 fibres dans un *combiner* optique (chacune avec une longueur d'onde différente) Les 4 sont combinées dans une seule fibre partagée pour transmission. A la sortie, le signal est séparé sur plusieurs fibres comme à l'entrée (avec un filtre sur les longueurs d'onde).
- La seule différence avec FDM électrique est que dans un système optique le traitement est passif et fiable.



Wavelength Division Multiplexing (WDM)

- WDM inventé dans les années 1990. Fibres mono-mode et multi-mode.
- En 2000, fibres avec 96 canaux de 10 Gbps, soit 960 Gbps au total.
- Quand le nombre de canaux est très grand et les longueurs d'onde très proches (ex : 0.1 nm), c'est du **DWDM (Dense WDM)**.
- Depuis que la BP d'une seule fibre est de 25000 GHz (voir figure), il y a théoriquement la place pour 2500 canaux de 10 Gbps à 1 bit/Hz (et des plus hauts débit sont aussi possibles).
- Une autre avancée réside dans les amplificateurs optiques :
 - Avant, tous les 100 km il était nécessaire de séparer les canaux et de convertir chacun en signal électrique, l'amplifier séparément, le reconvertir en optiques et recombinaison.
 - Maintenant, **tous les amplificateurs optiques peuvent régénérer le signal combiné qu'une fois tous les 1000 km sans conversions optiques/électriques.**

- **Switches optiques** basés sur:
Interféromètres de Fabry-Perot
ou Mach-Zehnder.



Time Division Multiplexing (TDM)

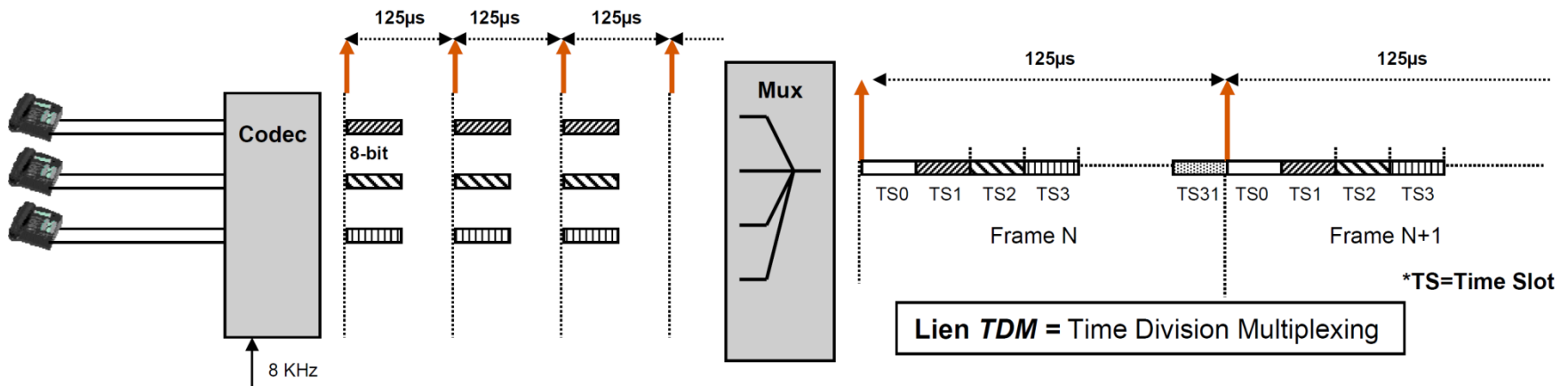
- FDM: toujours utilisé sur fils de cuivre ou canaux micro-ondes, mais nécessite circuit analogiques et n'est pas adaptés au traitement par les équipement filaires numériques.
- TDM: géré entièrement par de l'électronique numérique, donc plus répandu de loin.
- Cependant, les boucles locales produisent des signaux analogiques -> conversion A/N nécessaire au CO où toutes les lignes d'abonnés sont combinées sur des câbles haute capacité en sortie du CO
- Comment les multiples signaux analogiques de voix sont numérisés et combinés ?:
- Signaux analogiques numérisés au CO en utilisant **PCM (Pulse Code Modulation)** :
 - 1 échantillon toutes les $125\mu\text{s}$ <--> 8000 échantillons par seconde
 - 8 bits par échantillon (loi A ou loi μ pour la quantification)
 - > Canal de voix à 64Kbits/s
- Le théorème de Shannon-Nyquist dit qu'un échantillonnage à 8000Hz est suffisant pour capturer toute l'information d'un canal téléphonique de BP 4KHz. A un taux d'échantillonnage plus petit, de l'info serait perdue; à un taux plus grand, pas d'info supplémentaire serait acquise.
- En conséquence :

all time intervals within the telephone system are multiples of 125 μsec .

Principe du réseau numérique synchrone

Tous les principes du réseau numérique synchrone trouvent leur fondement dans les besoins d'acheminement de la voix (*c'est le service attendu du réseau des opérateurs initialement !*)

A l'établissement d'une communication, un circuit synchrone à 64 Kbit/s est établi de bout en bout dans le réseau.



- Chaque circuit se voit allouer une partie fixe de la ressource du réseau pendant toute la durée de la communication.
- L'information est insérée de manière brute dans le circuit physique (échantillons de voix).
- > Réseau extrêmement simple dans son principe, pas de "couches" à proprement parler

--> Comment on a utilisé et on utilise ce TDM dans les réseaux de communication de données à haut débit ?

Plan

I. Présentation des WAN

II. Les interfaces de la couche physique

II.1. Les différents types de multiplexage

II.2. La hiérarchie numérique synchrone PDH

II.3. La hiérarchie numérique synchrone SDH : réseaux de fibres optiques et redondance pour la fiabilité

III. Protocoles de niveau 2 dans les WAN

IV. MPLS : commutation par VC dans le monde IP

V. Qualité de service

VI. Technologies xDSL

PDH – Plesiochronous Digital Hierarchy

- Technologie de transport développée dans les 60's pour déployer les réseaux téléphoniques numériques nationaux et internationaux basés sur le multiplexage et la commutation de circuits synchrones (TDM).
- Plesiochronous: plesio = presque ... presque synchrone, les différents équipements sont synchronisés sur des horloges différentes mais de fréquence et stabilité identiques
- Initialement réservée au transport de la voix, puis dans les 70's s'ouvre au transport de data (RNIS, X.25)
- **1^{er} débit standard T1 adopté par les US: 24 voies a 64 Kbps multiplexées sur un support à 1544 Kbps**
- **suivi par le E1 en Europe: 30 canaux multiplexés sur un support à 2048 Kbps**
- Définit une **hiérarchie standard de débit : chaque niveau de la hiérarchie constituant un multiplex des niveaux inférieurs.**
- **Le principe d'une trame de base de 125µs (8KHz) reste le point commun à tous les niveaux de la hiérarchie.**
- Pour des raisons historiques liées aux infrastructure existantes, la hiérarchie diffère entre Europe, US et Japon.

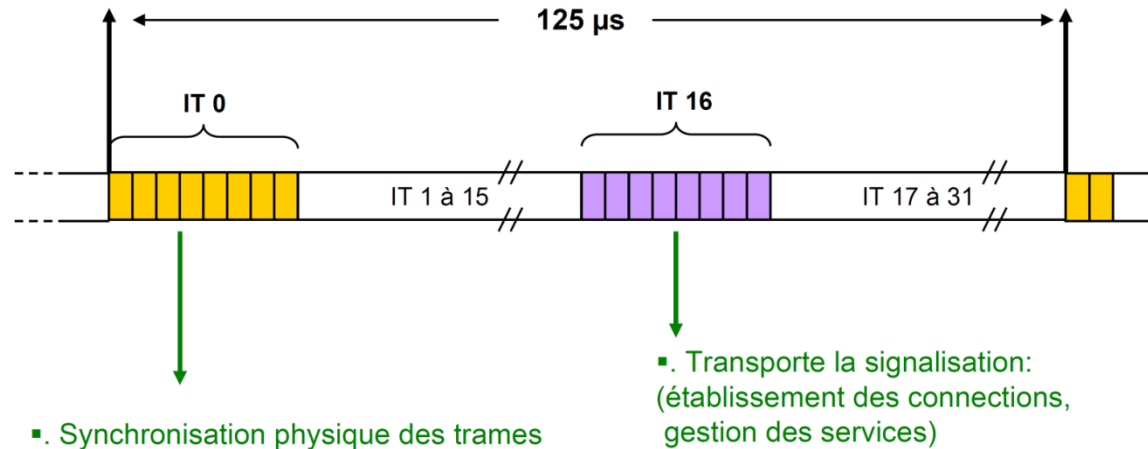
Trame de base E1

- CCITT -> multiplex E1 à 2048 Kbps : 32 échantillons de 8 bits combinés dans la trame de base durant 125 μ sec.

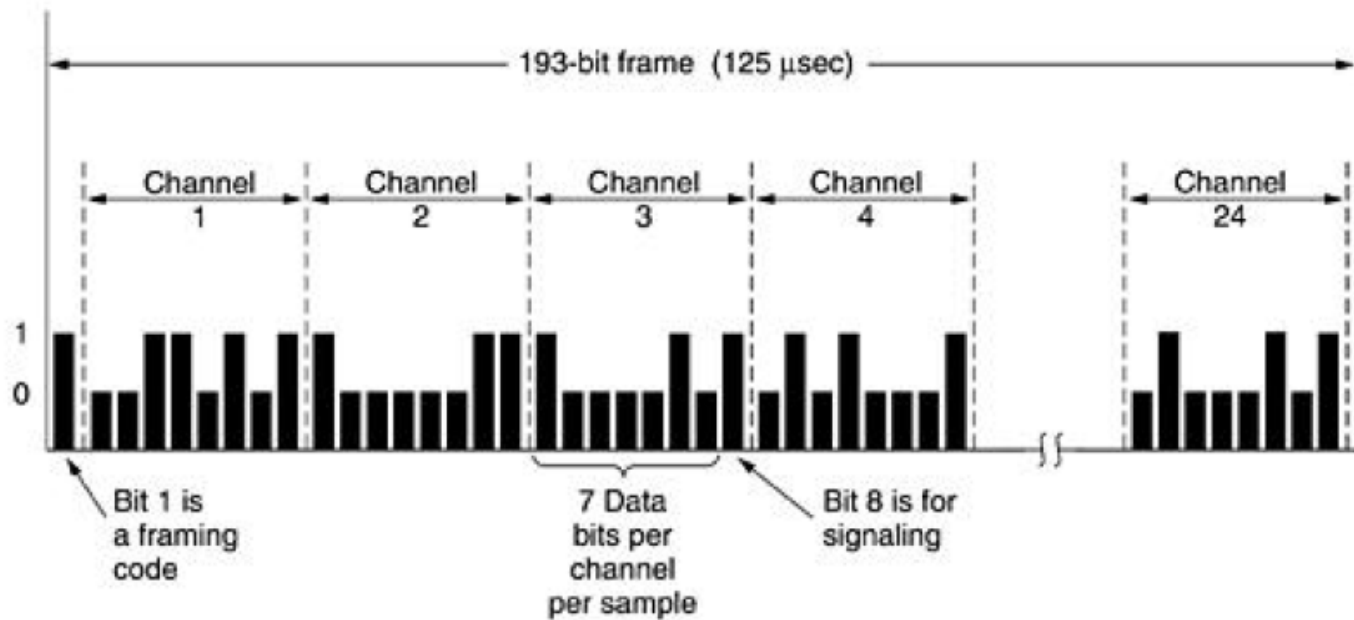
- 30 des canaux sont utilisés pour porter de l'information et 2 pour la signalisation:

- 1 canal pour la signalisation des canaux
- 1 canal pour la synchronisation de trame

Standard ITU-T G.704

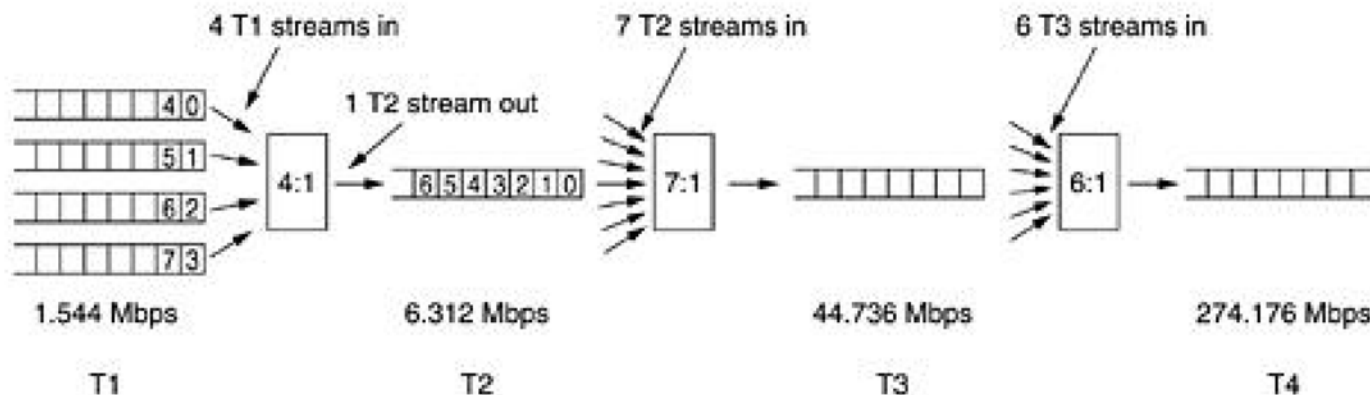


Frame T1



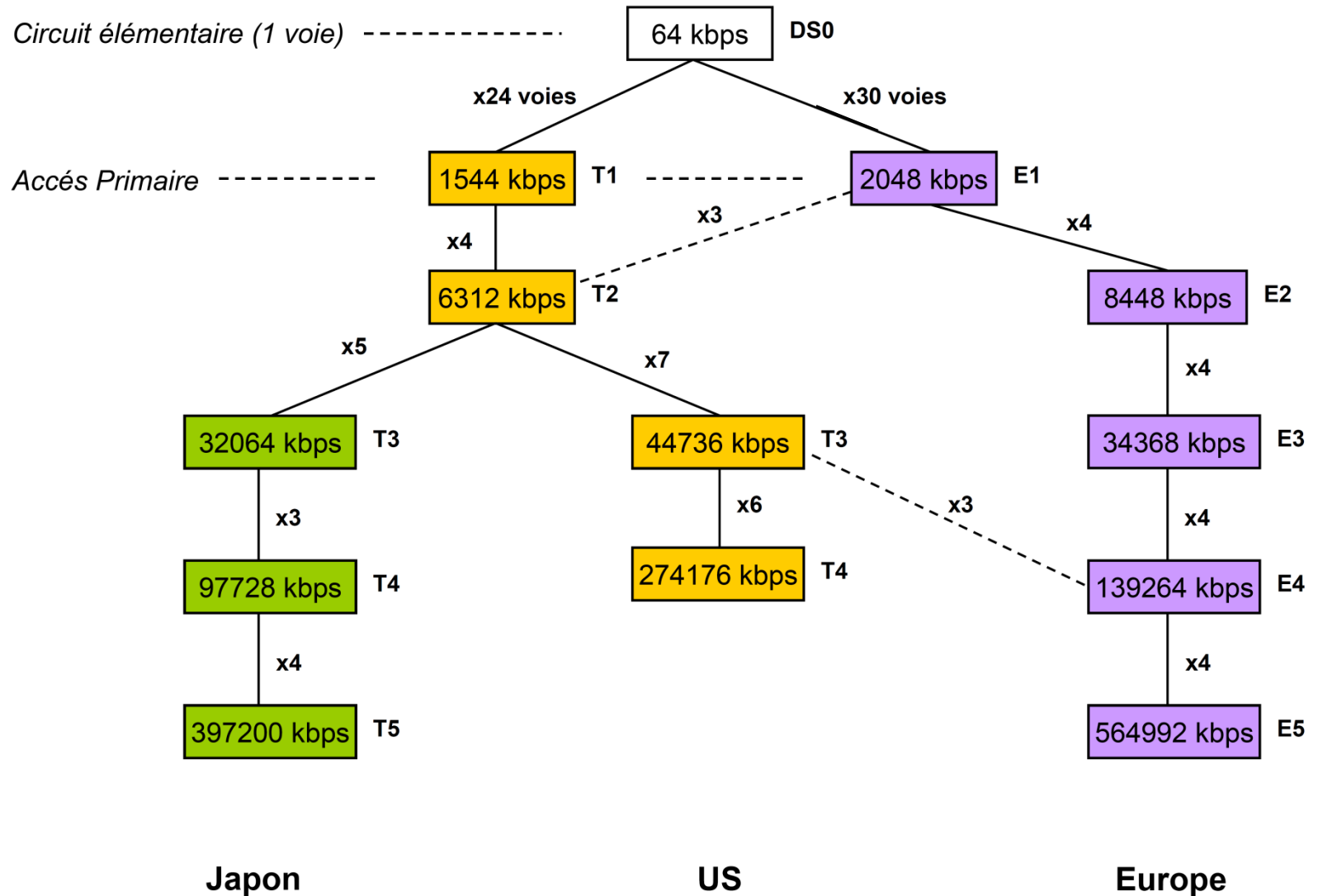
PDH – Multiplexage de flux T1 dans de multiplexes d'ordres élevés

- TDM permet d'avoir plusieurs flux T1 dans des multiplexes d'ordres supérieurs.
- T1 et T3 sont largement utilisés par les clients, tandis que T2 et T4 sont utilisés seulement dans le coeur du réseau.
- A chaque étape de multiplexage, un petit *overhead* (surcharge) est ajouté pour décrire la structure du multiplex, et la récupération en case de perte de synchro entre l'émetteur et le récepteur.



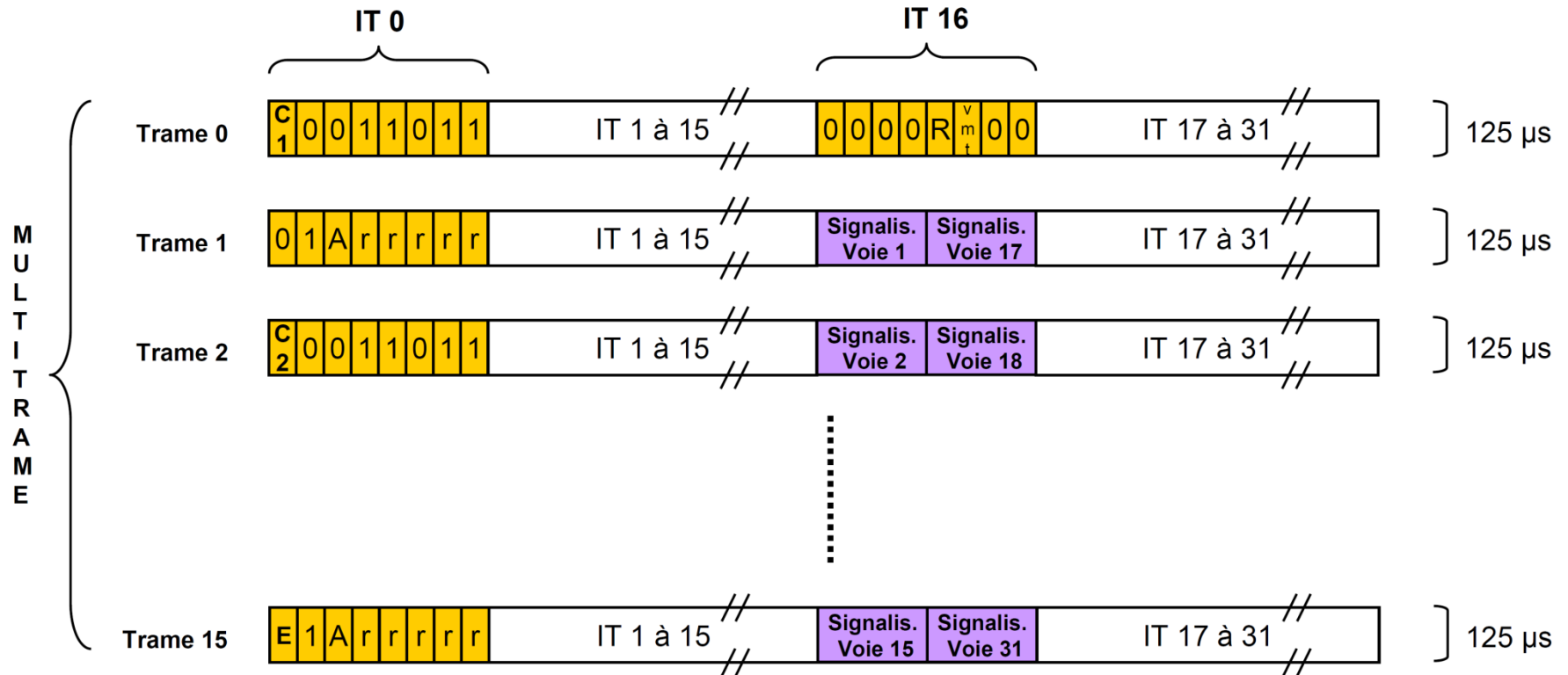
$\geq 4 \times 1.544 \text{ Mbps}$
Bits suppl. pour récup. de synchro

PDH – la hiérarchie



PDH – trame et multi-trame E1

Pour référence

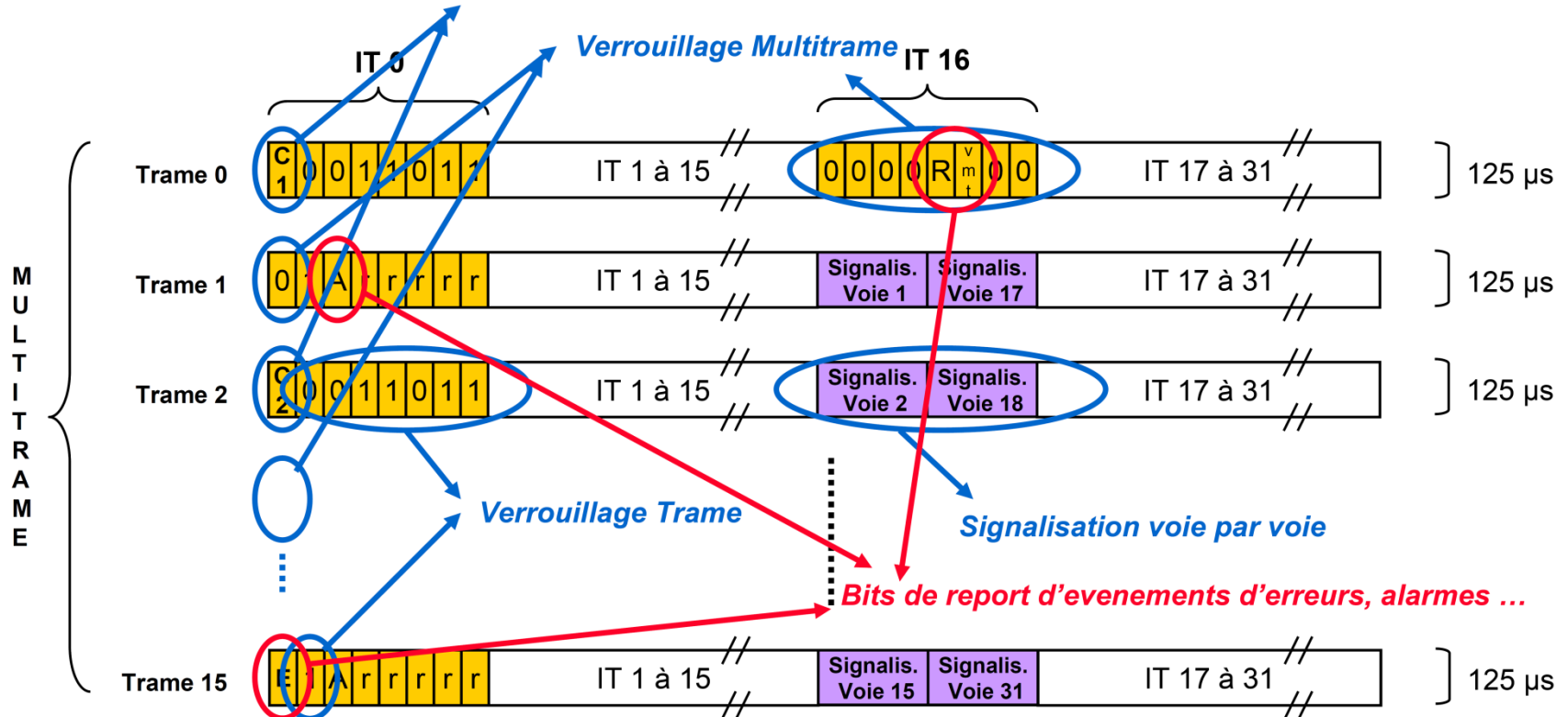


- Des mécanismes de synchronisation résident à plusieurs niveaux: notion de **Trame**, de **Double-Trame** et de **Multi-Trame**.
- L' IT 0 transporte une synchronisation Trame (bit 1), Double-Trame (bits 1 à 7) & Multi-Trame (bit 0 trames impaires) ainsi qu'un contrôle d'erreur par CRC (bit 0 trames paires)
- L' IT 16 de la trame 0 transporte une synchronisation Multi-Trame supplémentaire
- L' IT 16 transporte la signalisation voie par voie (4 bits par voie, 2 voies par trame)

PDH – format de la trame de base E1

Standard ITU-T G.704

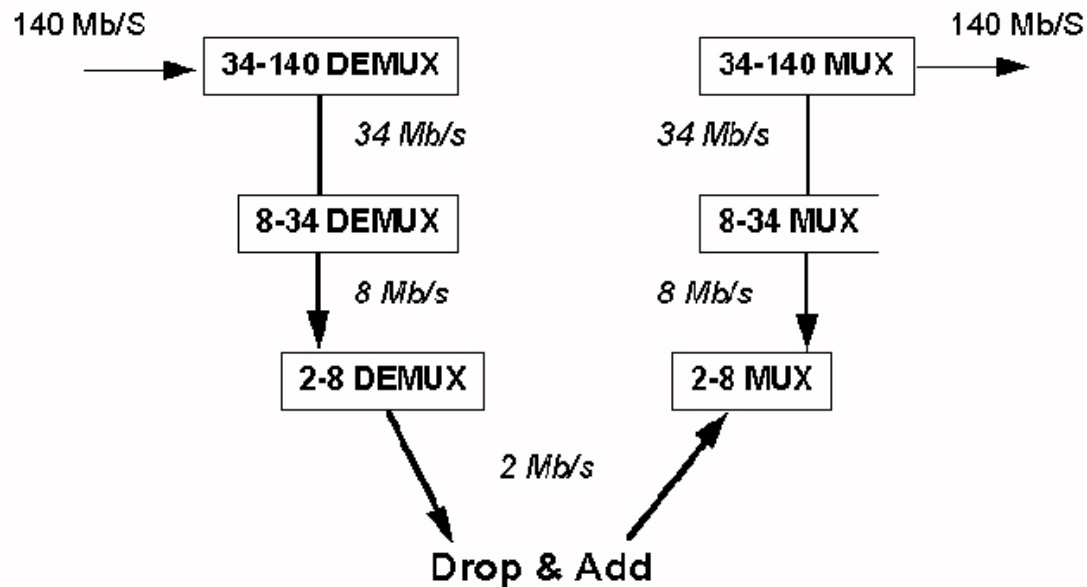
CRC calculé sur des demi Multitrames (C1, C2, C3, C4) toutes les 8 trames



- Des mécanismes de synchronisation résident à plusieurs niveaux: notion de **Trame**, de **Double-Frame** et de **Multi-Frame**.
- L' IT 0 transporte une synchronisation Trame (bit 1), Double-Frame (bits 1 à 7) & Multi-Frame (bit 0 trames impaires) ainsi qu'un contrôle d'erreur par CRC (bit 0 trames paires)
- L' IT 16 de la trame 0 transporte une synchronisation Multi-Frame supplémentaire
- L' IT 16 transporte la signalisation voie par voie (4 bits par voie, 2 voies par trame)

Plesiochronous Digital Hierarchy (PDH)

- Traditionnellement, le multiplexage des signaux est **plésiochrone** (fait **presque** au même rythme car basé sur des horloges très proches).
- De plus, des hiérarchies différentes dans le monde -> problèmes de compatibilité au niveau international
- Pour récupérer un canal à 64 kbit/s d'un signal PDH à 140 Mbit/s, il faut entièrement démultiplexer jusqu'au E1 à 2 Mbit/s avant d'identifier l'emplacement du canal voulu à 64 kbit/s channel.



PDH multiplexing by steps

Limitations des réseaux PDH

- Incapacité à identifier les canaux individuels dans des multiplexes d'ordres élevés (=flux haut débit) : seulement les topologies point-to-point sont possibles
- Pas assez de possibilité de contrôle et gestion du réseau
- Pas de définition des débits au delà de 565 Mbit/s dans PDH
- Pas les mêmes systèmes au niveau international : besoin d'équipement d'interface

Plan

I. Présentation des WAN

II. Les interfaces de la couche physique

II.1. Les différents types de multiplexage

II.2. La hiérarchie numérique synchrone PDH

II.3. La hiérarchie numérique synchrone SDH : réseaux de fibres optiques et redondance pour la fiabilité

III. Protocoles de niveau 2 dans les WAN

IV. MPLS : commutation par VC dans le monde IP

V. Qualité de service

VI. Technologies xDSL

SDH – Synchronous Digital Hierarchy

- SDH, standardisée par l'ITU est une technologie de transport synchrone qui **prolonge les principes de PDH**, conservant notamment la trame de base à 125 μ s, avec les avantages et **améliorations** suivants:
 - débits plus élevés, jusqu'à 10Gbit/s sur fibres optiques exclusivement
 - inclut des mécanismes de maintenance et de tolérance aux fautes (SDH réserve plus d'overhead que PDH pour ces fonctions)
 - beaucoup mieux architecturée pour supporter dans les équipements les opérations d'insertion/extraction (Add/Drop) entre les différents débits et affluents
 - peut multiplexer et transporter aussi bien des circuits élémentaires 64Kbit/s, des cellules ATM, des trames/paquets
- la technologie équivalente aux US est **SONET** (Synchronous Optical Network) développée par l'ANSI.
- SDH et SONET sont inter-opérables.
- aujourd'hui SDH & SONET sont très utilisées comme technologies de transport dans les coeurs de réseau (Core networks, Backbones)

Plan de la partie SDH

1. SDH Integration of TDM Signals
2. SDH Layers
3. SDH Multiplexing
4. SDH Framing
5. SDH Transport Overhead
6. SDH Topologies
7. SDH Protection Architectures
8. SDH Ring Architectures

SDH Integration of TDM Signals

- Le format SDH permet différents types de format de signaux sur fibres
- La communication entre différents réseaux est complexe à cause des différences dans les hiérarchies numériques, les techniques d'encodage et de multiplexage.
- Pour résoudre ce pb de conversion de signal, SDH standardise les débits, formats de trames, signalisation, et terminaison entre équipements SDH.



Un multiplexeur SDH accepte différents formats de signaux TDM et multiplexe (*adds*) ces signaux sans conversion. Ces signaux peuvent être démultiplexés (*dropped*) n'importe où.

SDH Integration of TDM Signals

- **Horloge:** Au début des réseaux, on travaillait avec des horloges locales
 -> pas bien synchronisées, large variations dans la fréquence d'horloge, affectant le débit binaire des signaux.
 -> synchroniser tout ça avec une seule horloge
- Signaux optiques et électriques SDH:
 - Le terme *Synchronous Transport Module-N (STM-N)* correspond à un lien de transmission de niveau N.
 - SONET utilise le terme **OC-N** pour porteuse optique et **STS-N** pour le niveau de signal élec.
 - L'unité basique de transmission en SDH est 155.52 Mbps (STM-1).

SDH Level	Line Rate (Mbps)	Payload Rate (Mbps)	Overhead Rate (Mbps)	SONET Equivalent
STM-0	51.840	50.112	1.728	STS-1
STM-1	155.520	150.336	5.184	STS-3
STM-3	466.560	451.008	15.552	STS-9
STM-4	622.080	601.344	20.736	STS-12
STM-6	933.120	902.016	31.104	STS-18
STM-8	1244.160	1202.688	41.472	STS-24
STM-13	1866.240	1804.032	62.208	STS-36
STM-16	2488.320	2405.376	82.944	STS-48
STM-32	4976.640	4810.752	165.888	STS-96
STM-64	9953.280	9621.504	331.776	STS-192
STM-256	39813.120	38486.016	1327.104	STS-768

STM-n line rates

SDH – la hiérarchie

SONET (US)

Bit rates

SDH

STS-1 OC-1

51.84 Mbps

STM-0

STS-3 OC-3

155.52 Mbps

STM-1

STS-12 OC-12

622.08 Mbps

STM-4

STS-48 OC-48

2488.32 Mbps

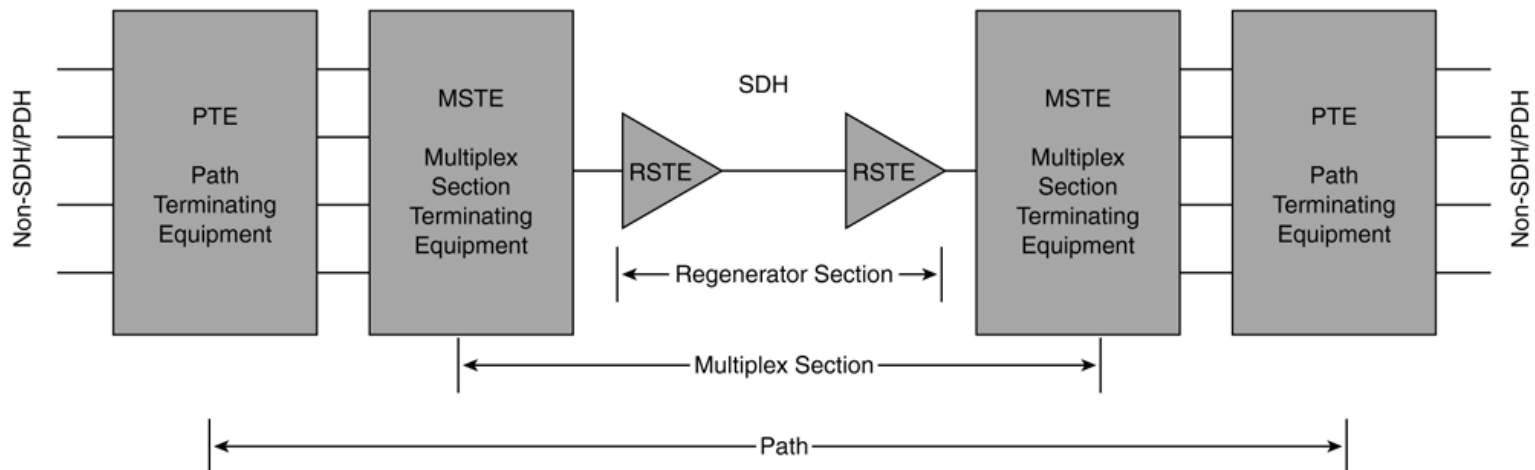
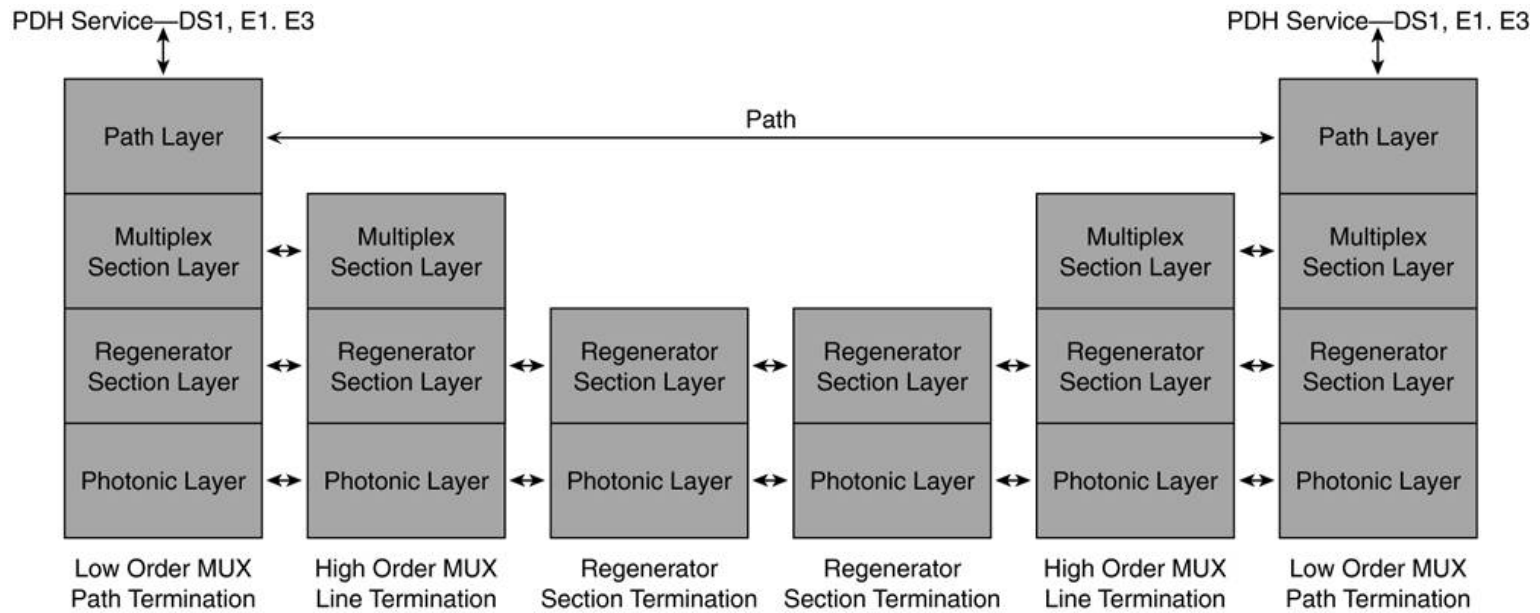
STM-16

STS-192 OC-192

9953.28 Mbps

STM-64

SDH layers

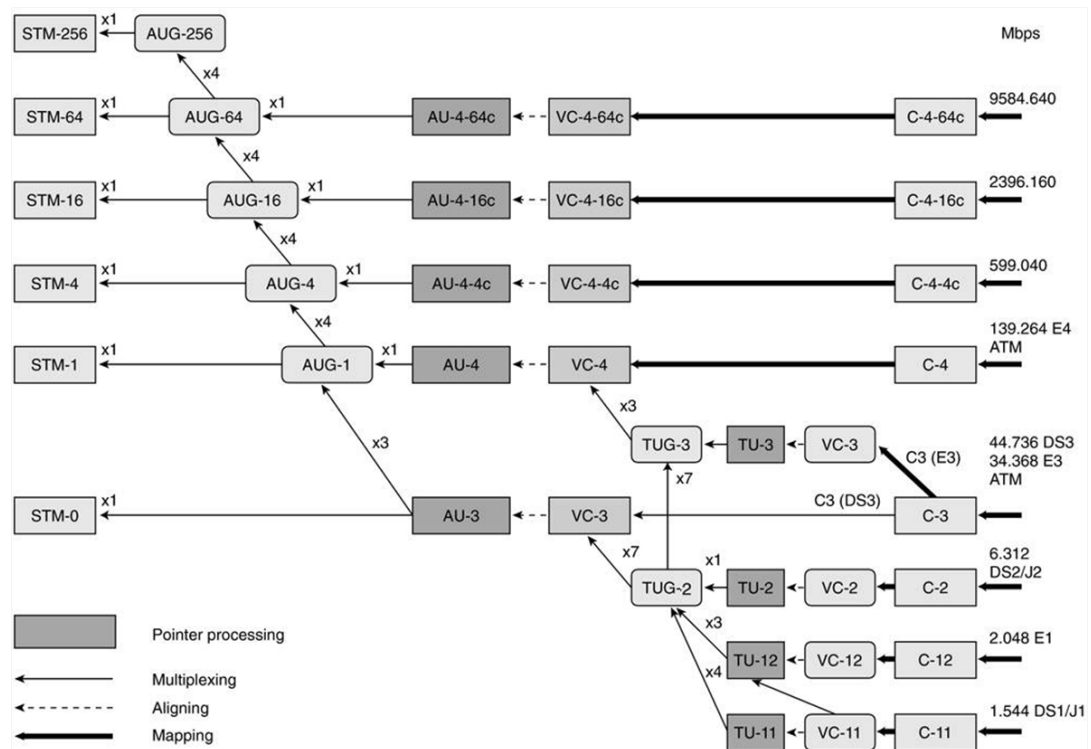


SDH layers

- ***Path layer***: point auquel le format de trame SDH standard à un débit donné est assemblé.
 - Le *path overhead* (POH) y est ajouté et enlevé, et les infos d'erreur et alarmes sur l'état de bout-en-bout sont gérées à cette couche.
 - PTE: équipt qui multiplexe ou démultiplexe le payload du VC-N.
- ***Multiplex section layer***: Le MSOH pour communication, synchronisation et surveillance des erreurs.
- ***Regenerator section layer***: ajoute le RSOH.

SDH multiplexing

- 4 termes à comprendre pour le principe du multiplexage SDH:
 - **Mapping**— Quand les affluents sont adaptés dans les VCs par ajout de bits de *justification* et info POH.
 - **Alignement**— Quand un pointeur est inclus dans une TU ou une AU, pour localiser le 1er octet du VC.
 - **Multiplexage**— Quand plusieurs signaux de la lower-order path layer sont adaptés dans un signal de higher-order path.
 - **Stuffing**— Quand les affluents sont multiplexés et alignés, de la capacité de secours est prévue dans les trames SDH pour donner assez d'espace aux divers débits d'affluents. Donc à certains moments de la hiérarchie, cette capacité en plus est remplie avec des bits de bourrage ne portant pas d'info.



- Les signaux PDH bas niveau (*low-order*) sont mappés dans une entité SDH appelée **containeur (C)**.
- C est **mappé** avec **octets POH** = lower-order **virtual container (VC)**.
- **But: Créer un payload VC uniforme en utilisant des bits de bourrage pour ramener tous les flux d'entrée à un débit binaire commun pour multiplexage synchrone.**
- Lower-order VCs sont **alignés** avec **pointeurs tributary unit (TU) = tributary units (TUs)**.
- Les TUs sont **multiplexés** en **tributary unit groups (TUGs)**.
- Les TUGs sont encore multiplexés pour former des **higher-order VCs**.
- Ces higher-order VCs sont alignés avec **byte-stuffing** et administration units (AU) = **administration units (AUs)**.
- Les AUs sont encore multiplexés en **administrative unit groups (AUGs)**.
- Les AUGs sont finalement multiplexés avec les **octets RSOH and MSOH** = **STM-N signal**.

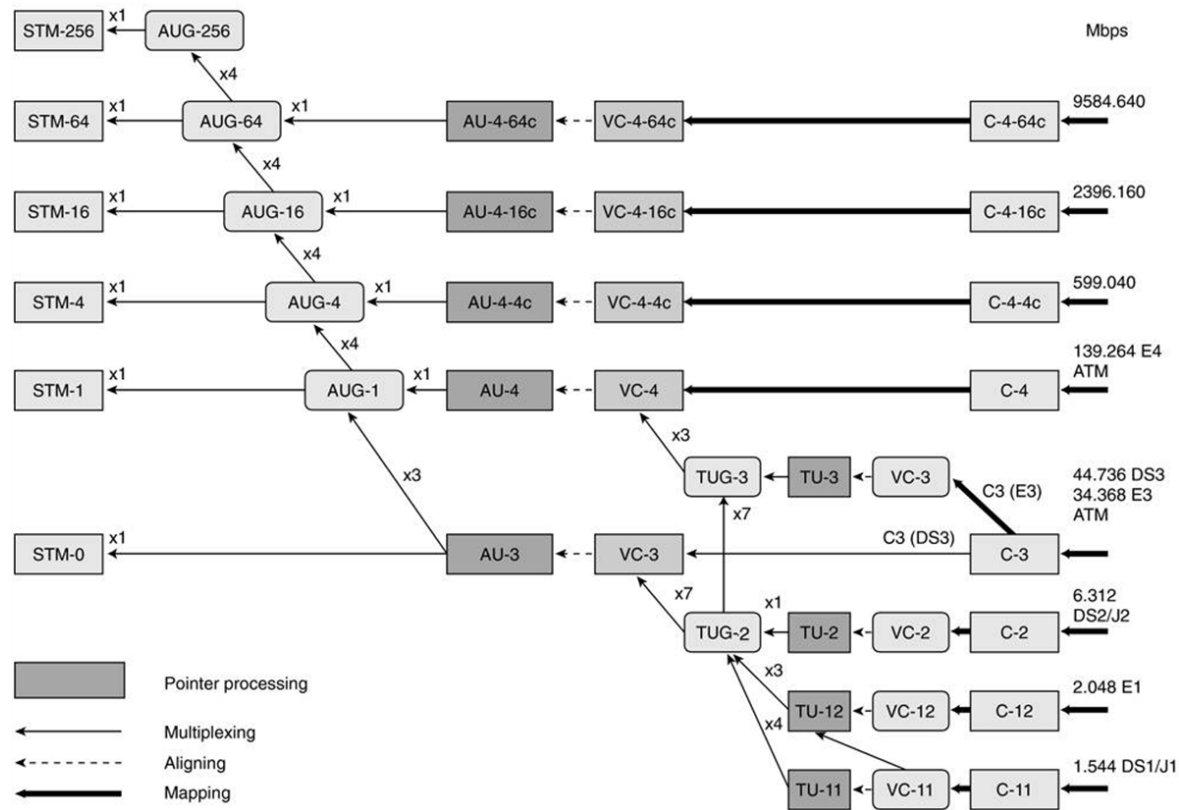
SDH multiplexing

Low-Order VC Level	VC Bit Rate (Mbps)	PDH Level
VC-11	1.728	DS1/J1/ISDN H11
VC-12	2.304	E1/ISDN H12
VC-2	6.912	DS2/J2
High-Order VC Level		PD Level
VC-3	48.960	E3/J3/ISDN H31
VC-3	48.960	DS3/ISDN H32
VC-4	150.336	E4/ISDN H4

- Grâce aux pointeurs et aux valeurs d'offset, les VCs peuvent être portés dans le payload SDH comme des ensembles de donnée indépendants.
- Les VCs sont utilisés pour le transport des affluents bas débit.
- Les VCs peuvent commencer n'importe où dans la trame STM-1.
- L'endroit de départ est indiqué dans le pointeur TU ou AU.

Path	SDH Overhead
C-N to VC-N	$C-N + VC-N \text{ POH} = VC-N$ (N = 11, 12, 2, 3, or 4)
VC-N to TU-N	$VC-N + TU-N \text{ pointers} = TU-N$ (N = 11, 12, 2, or 3)
VC-N to AU-N	$VC-N + AU-N \text{ pointers} = AU-N$ (N = 3 or 4)
AUG-N to STM-N	$AUG-N + RSOH + MSOH = STM-N$

SDH multiplexing of E1-signals



Les signaux E1 (2.048-Mbps) bas niveau sont mappés vers le container C-12.

Le container C-12 est mappé avec des bytes POH de VC-12 dans un container virtuel VC-12 de bas niveau.

Le VC-12 avec des pointeurs TU-12 est aligné dans une unité d'affluent TU-12 (*tributary unit*).

Le TU-12 est multiplexé (x3) dans un TUG-2.

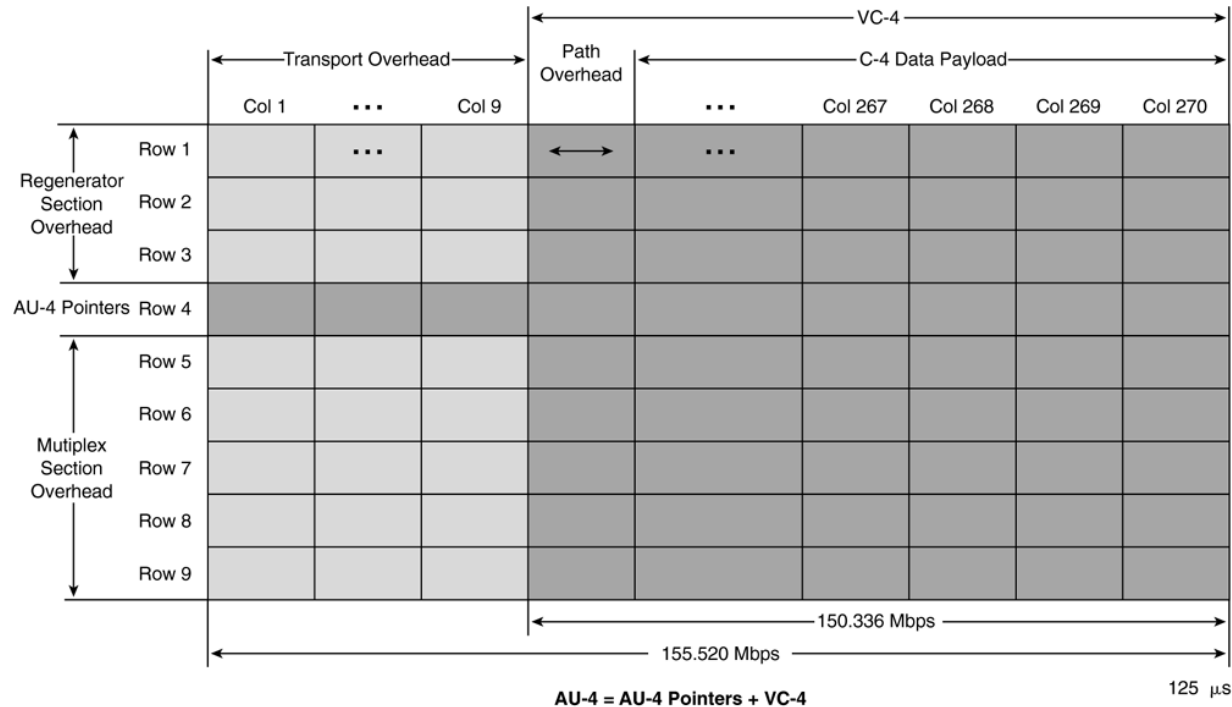
Le TUG-2 est multiplexé (x7) dans un VC-3 de haut niveau.

Le VC-3 est aligné avec des pointeurs AU-3 pour former un AU-3.

Le AU-3 peut directement former un signal STM-0 ou être multiplexé (x3) pour former un AUG-1.

Le AUG-1 est multiplexé (x1) avec des octets MSOH et des octets RSOH pour former un STM-1.

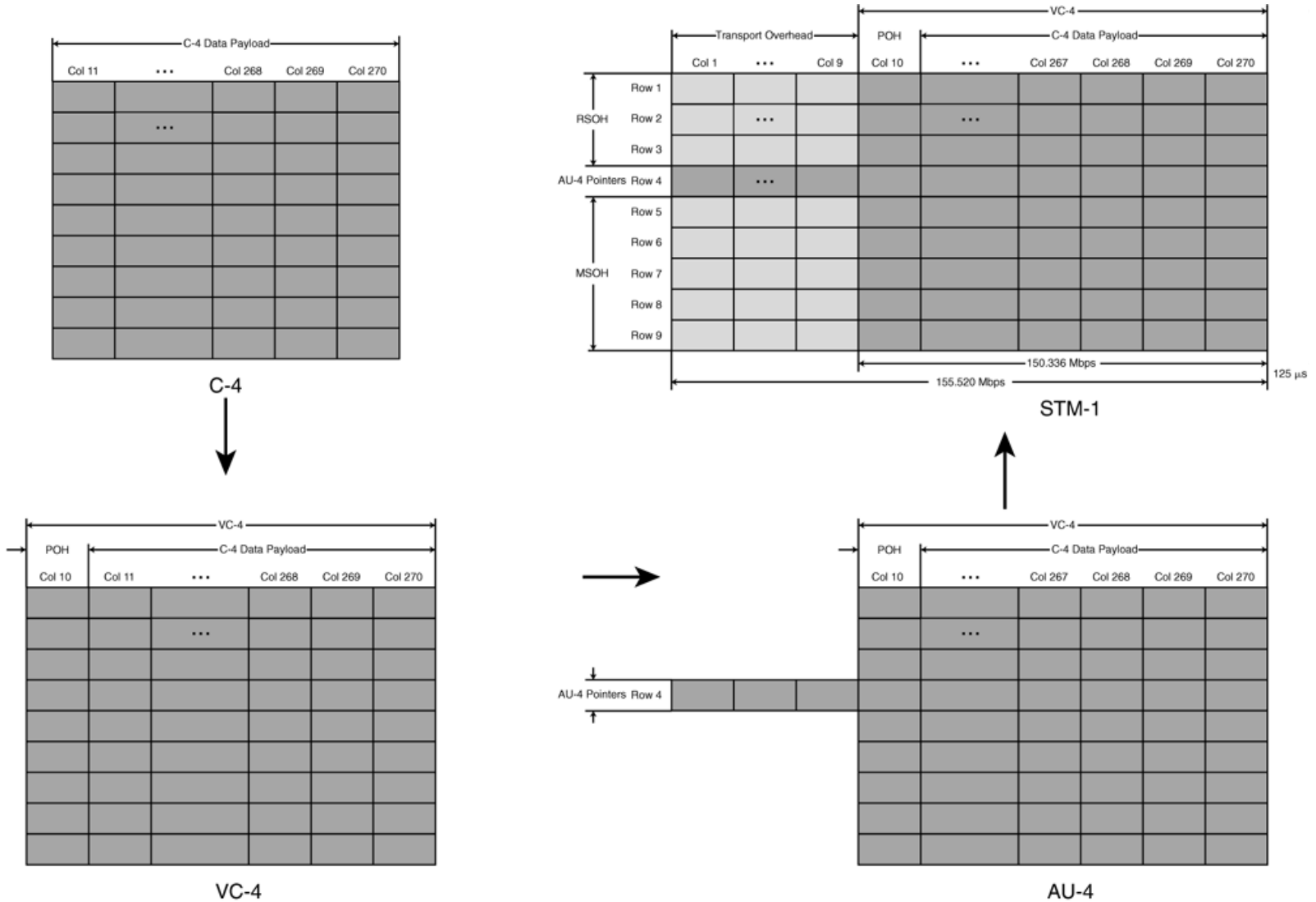
SDH framing



SDH adopte une cadence de 8000 trames par seconde.

- Une trame STM-1 = 9 lignes et 270 colonnes d'octets -> total de $9 \times 270 = 2430$ bytes -> 155.520 Mbps
- Une trame STM-1 = un *transport overhead* + un VC-4
- Les 9 premières colonnes = le *transport overhead*, et les autres 261 colonnes = le VC-4
- Le VC-4 + les 9 bytes de pointeurs ($H1 \times 3$, $H2 \times 3$, $H3 \times 3$) ligne 4 = la AU-4
- Les premières colonnes du VC-4 sont le POH.
- Le VC-4 flotte dans la trame STM-1 et peut occuper n'importe quelle colonne de 10 à 270.
- Les octets du pointeur d'AU-N indiquent la position du POH de VC-4 dans la trame STM-1.
- Dans le transport overhead, les 3 1ères lignes pour le RSOH, les 5 autres pour le MSOH.

STM-1 frame creation



SDH pointers

- SDH fournit des pointeurs sur payload pour autoriser les différences en phase et en fréquence des VCs (VC-N) par rapport à la trame STM-N.
- Dans chaque trame STM-N, un pointeur indique où commence le VC:
 - **les octets H1 et H2 sont la valeur du pointeur = offset en octets du pointeur au premier octet du VC**
- Exemple: si le pointeur de payload de VC-4 est 0, le VC-4 commence à l'octet adjacent à l'octet H3 du TOH.
- **Outil: byte stuffing, ou justification** – permet l'alignement dynamique du VC au cas où il glisserait dans le temps.
 - Quand le début du VC n'est pas au tac d'horloge du début de STM-1, des octets non-informatifs sont rajoutés (*stuffed*) juste derrière l'octet H3 = **positive stuffing or positive pointer justification**.
 - Quand le débit du VC est rapide p/r au débit de STM-1, les données sont écrites dans l'octet H3 = **negative stuffing or negative pointer justification**.

SDH Transport Overhead

- Le transport overhead SDH a 2 couches incluant le RSOH et le MSOH.
- Le RSOH est utilisé pour la communication entre régénérateurs.
- Le MSOH est utilisé pour la signalisation entre les multiplexeurs STM-N.
- --> la compréhension de ces octets d'overhead est capitale dans les réseaux optiques

		STM-1 Transport Overhead								
		Col 1	Col 2	Col 3	Col 4	Col 5	Col 6	Col 7	Col 8	Col 9
RSOH	Row 1	Framing A1	Framing A1	Framing A1	Framing A2	Framing A2	Framing A2	Trace J0	Reserved for National Use	Reserved for National Use
	Row 2	BIP-8 B1	Media Dependent	Media Dependent	Orderwire E1	Media Dependent	Reserved	User F1	Reserved for National Use	Reserved for National Use
	Row 3	Data Com D1	Media Dependent	Media Dependent	Data Com D2	Media Dependent	Reserved	Data Com D3	Reserved	Reserved
AU-4 Pointers		Pointer H1	Pointer H1	Pointer H1	Pointer H2	Pointer H2	Pointer H2	Pointer Action H3	Pointer Action H3	Pointer Action H3
MSOH	Row 5	BIP-8 B2	BIP-8 B2	BIP-8 B2	APS K1	Reserved	Reserved	APS K2	Reserved	Reserved
	Row 6	Data Com D4	Reserved	Reserved	Data Com D5	Reserved	Reserved	Data Com D6	Reserved	Reserved
	Row 7	Data Com D7	Reserved	Reserved	Data Com D8	Reserved	Reserved	Data Com D9	Reserved	Reserved
	Row 8	Data Com D10	Reserved	Reserved	Data Com D11	Reserved	Reserved	Data Com D12	Reserved	Reserved
	Row 9	Sync S1	Reserved	Reserved	Reserved	Reserved	Reserved	REI-L M1	Orderwire E2	Reserved for National Use

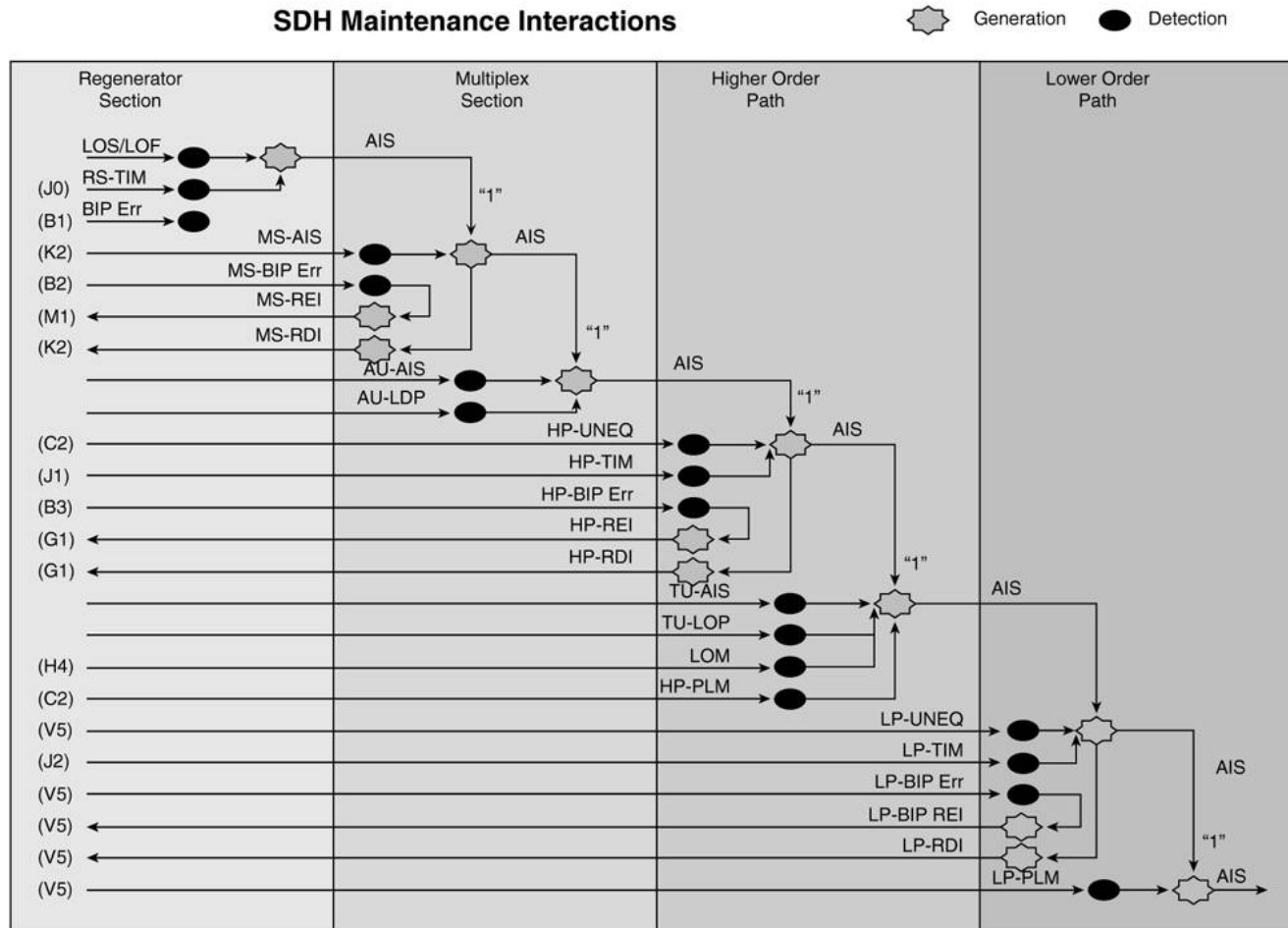
SDH Transport Overhead

- SDH Regenerator Section Overhead:
 - Le RSOH contient uniquement les infos pour les équipements de terminaison de section de régénération : les régénérateurs.
 - Regenerator Section Trace Byte (J0): L'octet J0 est utilisé pour qu'un récepteur de section puisse vérifier la continuité de la connexion vers l'autre bout.
- SDH Multiplex Section Overhead:
 - Le MSOH contient les infos pour les équipements de terminaison de section de multiplex.
 - **Automatic Protection Switching** Bytes (K1, K2): utilisés pour la signalisation pour *multiplex section protection* (MSP) pour APS, pour *alarm indication signal* (AIS), et *remote defect indication* (RDI).
- SDH High-Order Path Overhead:
 - Le POH est lié au VC du moment de la création du VC par un *path-terminating equipment* (PTE) jusqu'au démultiplexage.
 - Path Status Byte (G1): utilisé pour rapporter le statut du PTE et les performances au PTE origine. Les 2 sens du chemin peuvent être surveillés entièrement.

SDH alarms

- L'overhead SDH fournit un nombre d'infos de management et autres fonctions, comme surveillance d'erreur, info de pointeurs, statuts de chemins et sections, problèmes distants, indications de défaillance, messages de synchronisation.
- Les alarmes SDH se définissent en anomalies, défauts et défaillances:
 - **Anomalie (*anomaly*)**: plus petite différence pouvant être observée entre le fonctionnement désiré et effectif. Une seule anomalie ne constitue pas une interruption de la fonction en question.
 - **Défaut (*defect*)**: Si la densité d'anomalie atteint un niveau tel que la fonction est interrompue. Les défauts sont utilisés comme input pour performance monitoring, contrôle des mesures prises et détermination de la cause du défaut.
 - **Défaillance (*failure*)**: Incapacité d'une fonction à effectuer l'action requise au delà d'une durée max.
- La surveillance d'erreur est basée sur *bit-interleaved-parity* (BIP) calculés trame à trame. **Ces vérifications BIP sont insérées dans RSOH, MSOH, and POH.**
- HO PTE et LO PTE produisent des *remote error indications* (REIs) basées sur des erreurs détectées dans les BIP de HO path et LO path respectivement.

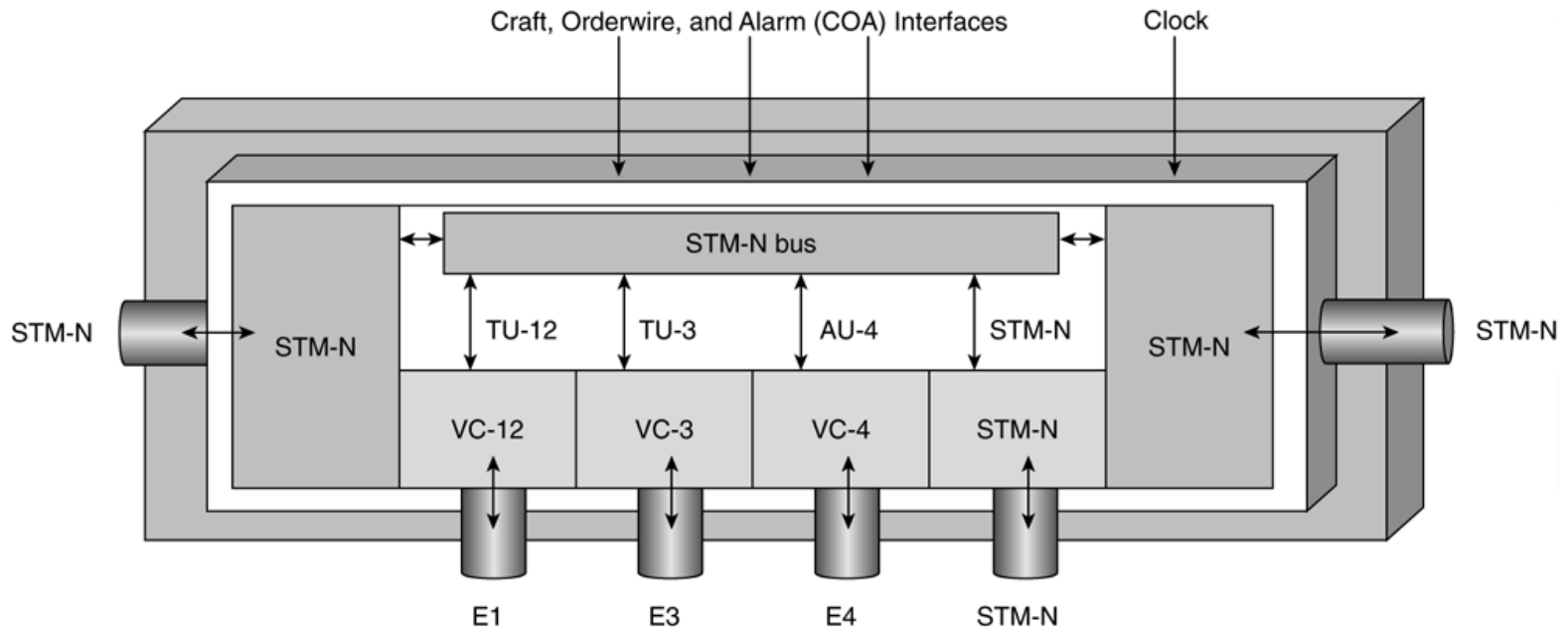
SDH alarms



The various SDH maintenance interactions, alarms and the overhead bytes used to carry the alarms and maintenance information.

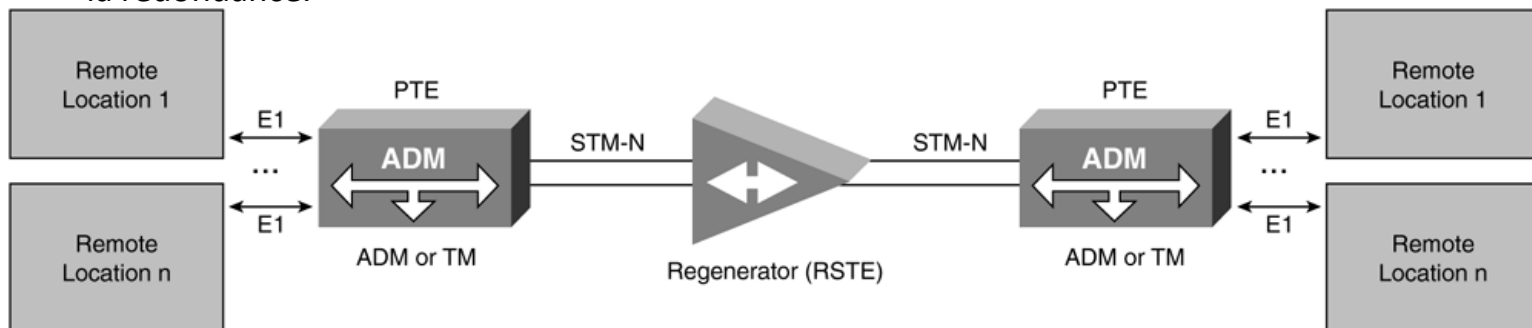
SDH network element

- Equipements effectuant transmission SDH définis some NEs.
- Incluent *regenerator section*, *multiplex section*, et *path-terminating equipment*.
- **Add/Drop multiplexer:**



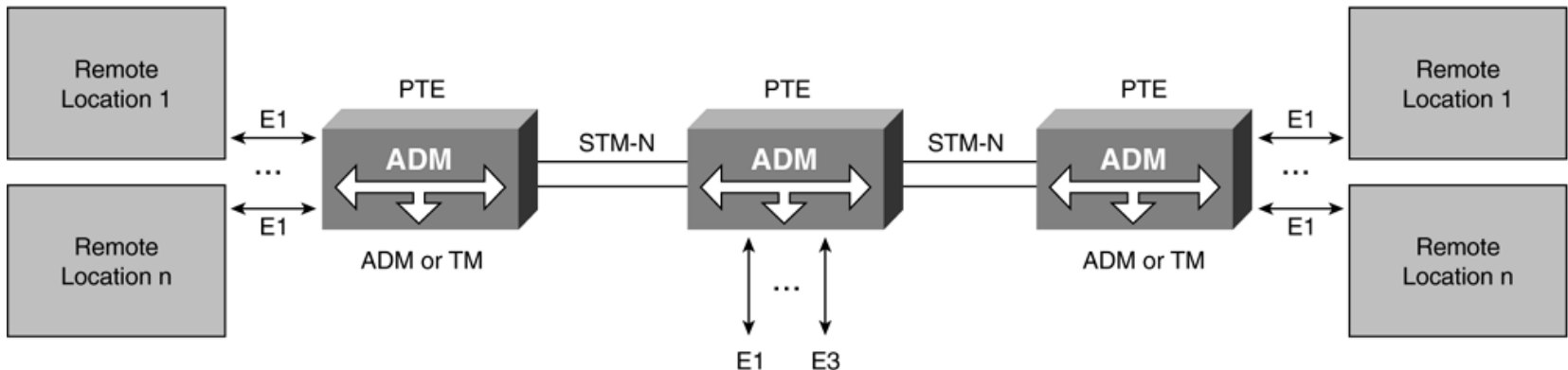
SDH topologies

- Les topologies SDH sont centrées autour de la survivabilité du réseau avec 50 ms ou moins de restauration.
- Différentes topologies peuvent être configurées avec soit des ADMs (*add/drop multiplexers*) soit des DCSs (*digital cross-connect systems*).
- Les topologies SONET ring sont fréquentes aux US, alors qu'en Europe, Asie, et Amérique Latine, c'est plutôt SDH-ring et mesh.
- Protection switching is mainly performed by the intelligent ADMs or DCSs.
- SDH Point-to-Point:
 - très populaires pour interconnecter des datacenters (SAN).
 - utilise des mécanismes de protection 1:N où un lien de protection en réserve (*standby*) pour protéger les N liens actifs (*working*). Protection max avec ratio 1:1
 - Si défaillance, le chemin de protection est utilisé avec un temps de switchover <50 ms
 - Idéalement, le chemin de protection ou fibre doit emprunter un autre chemin physique pour assurer la redondance.



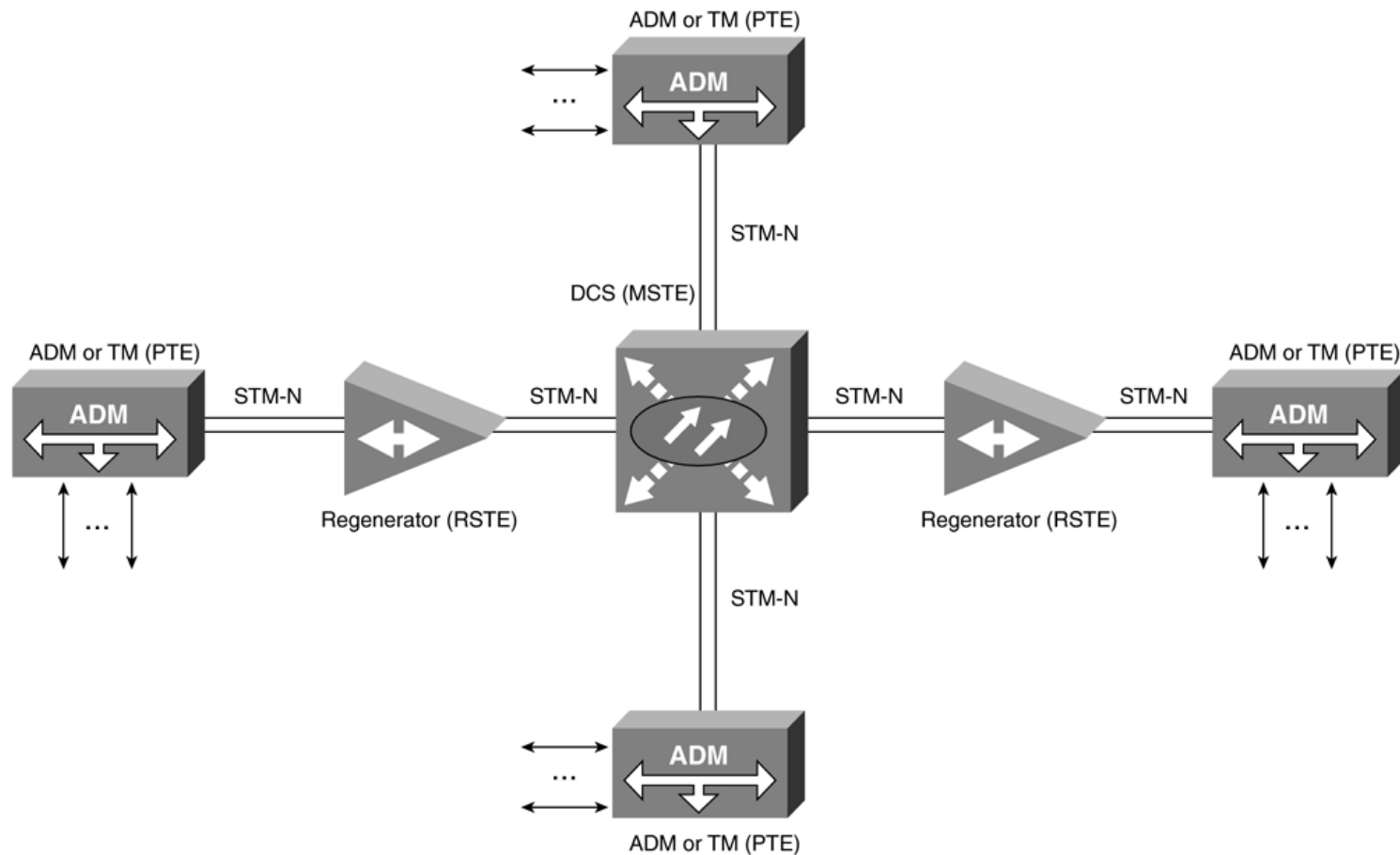
SDH topologies

- Topologie SDH Point-to-Multipoint:
 - implémente l'ajout (*adding*) et l'abandon (*dropping*) de circuits sur le chemin.
 - Topologie implémentée pour architectures SDH linéaires moyenne et longue distance, peut avoir à ajouter ou retirer des circuits.



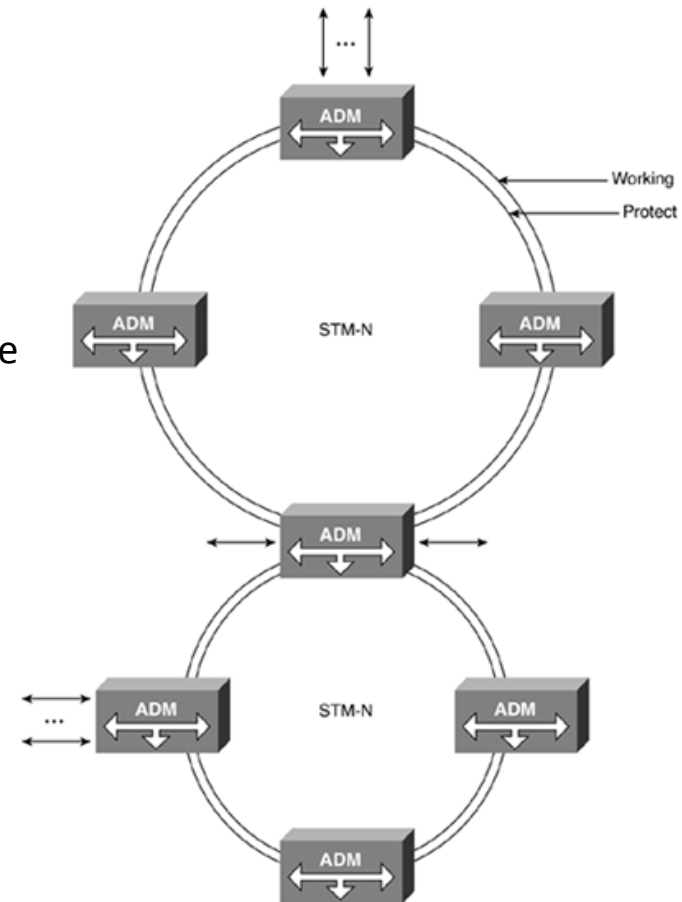
SDH topologies

- SDH Hub Topology:



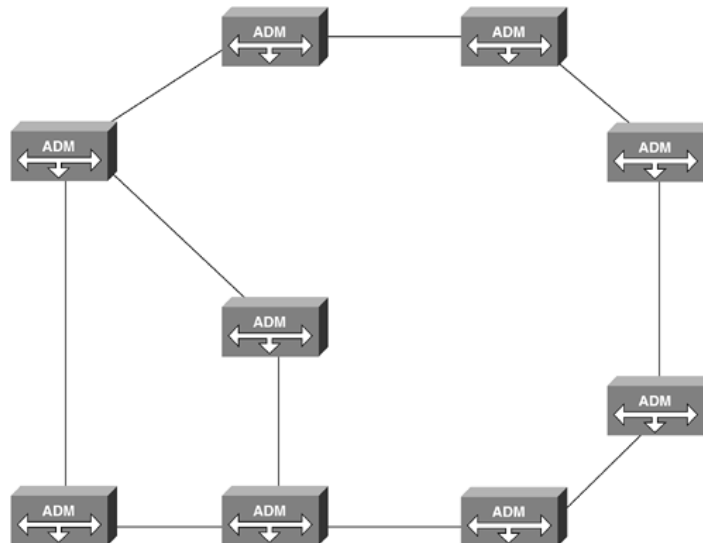
SDH topologies

- Topologie SDH Ring: principal avantage est sa survivabilité et rapide réparation.
 - temps de restauration <50ms
 - robust protection mechanisms.
 - Le bloc de base est ADM.
 - Si une fibre est coupée, les ADMs ont l'intelligence de rerouter les services affectés sur un autre chemin sur l'anneau sans interruption.
 - La demande pour des services résistants, la diversité de routage et la flexibilité à ré-arranger des services vers d'autres noeuds
 - > Les anneaux sont l'architecture la plus populaire pour le coeur SDH et les accès metro.
 - Mécanismes de protection avancés, tels que APS, SubNetwork Connection Protection (SNCP) two-fiber, MS-SPRing two-fiber, and MS-SPRing four-fiber.



SDH topologies

- Topologie SDH Mesh : ensemble de sites arbitrairement connectés avec au moins une boucle.
 - Redondance maximum avec options de re-routage multiples.
 - MSPPs de nlle génération profitent de protocoles de protection, tels que *Path Protected Mesh Networking* (PPMN), avec procédures basées Dijkstra pour re-routage --> tables de routage construites au démarrage et chgt d'état des liens
 - En qql minutes, chaque noeud a une vision complète de la topologie et de l'état des liens.
 - Créer des circuits TDM ou Ethernet au dessus est alors facile en spécifiant les noeuds source et destination.



SDH Protection Architectures

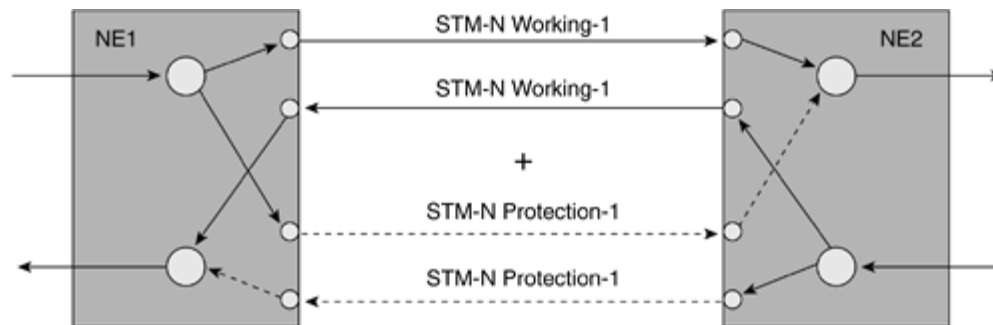
- APS, linéaires et anneaux
- La spécification stipule 60 ms pour découverte du pb et restauration.
- En général encore plus rapide. (Sur cable, temps de switchover plus grands: 250ms.)
- *SDH protection switching* est invoqué s'il y a LOS, LOF, ou dégradation de signal (BER>limit).
 - peut aussi être déclenché manuellement, pour maintenance.
- Protection implique qu'une ressource de secours est prévue pour le rétablissement si la ressource primaire défaille, et restauration implique un rétablissement du chemin de bout-en-bout sur les ressources disponibles après défaillance.
- Non-revertive and revertive protection mechanisms.
- With nonrevertive protection, after the original working line has been restored to its proper operating condition, the system will not revert to use the original line as the working path. Instead, it continues to use what was originally the protection line as the working line.
- With revertive protection, the system reverts to the original line after restoration. Revertive protection is most common with 1:N protection schemes.

SDH Protection Architectures

- **Automatic Protection Switching (APS)**: pour restauration dans le cas d'une défaillance.
 - 2 ensembles de fibres: 1 (*transmit and receive*) pour le trafic actif (*working traffic*), et l'autre (*transmit and receive pair*) pour **protection**
 - Les fibres active et de protection doivent emprunter des **chemins physiques différents** pour être efficaces. Les fibres utilisées pour protection peuvent éventuellement porter une copie du trafic (cas 1+1).
 - APS pour topologies linéaires et ring.
 - Seule la *multiplex section* est protégée par APS. Géré par les octets K1 et K2 du MSOH.
 - Path protection gérées par des fonctions réseau de management de plus haut niveau.

SDH protection architectures

- Automatic Protection Switching:
 - **Protection 1+1**: recopie des signaux STM-n sur les 2 fibres (actif et de protection).
 - ne peut pas transporter de trafic supplémentaire non-protégé
 - signaux constamment et indépendamment surveillés pour failles
 - les équipts sélectionnent entre les 2 selon règles locale
 - commute entre les 2 si faille, en moins de 50 ms
 - pour une vraie efficacité, l'installation de fibre doit avoir de la diversité physique

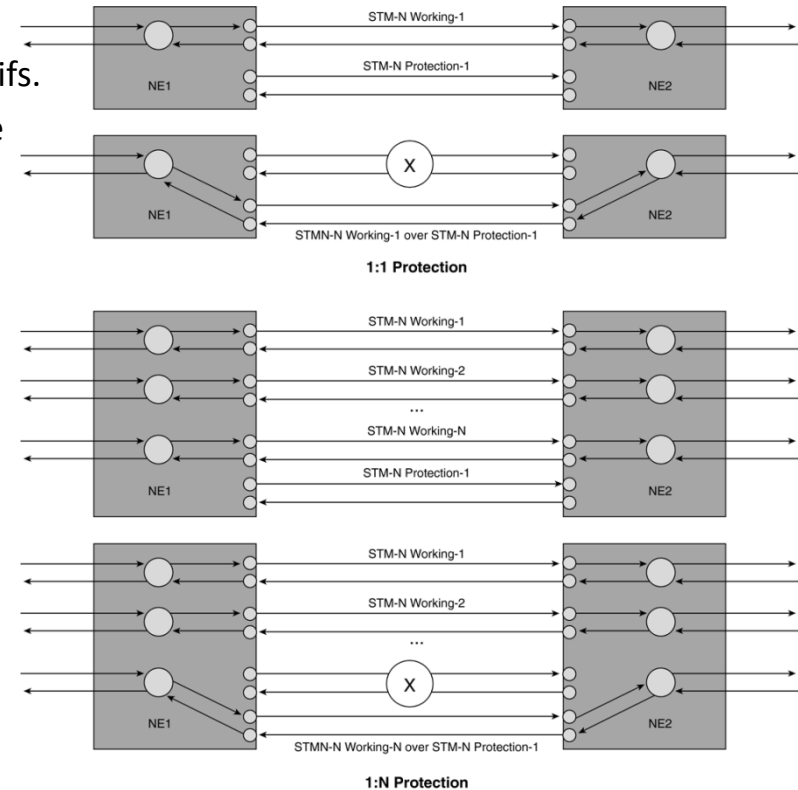


SDH protection architectures

- Automatic Protection Switching:

- **1:1 and 1:N Protection:** trafic sur la ligne active jusqu'à ce qu'une faille arrive.

- Ligne de protection utilisée si faille sur l'active.
- 1:N: 1 chemin de protection pour N chemins actifs.
- N'importe lequel, mais un seul chemin peut être protégé à la fois. Si faille sur plus d'un chemin à la fois, besoin de priorités.
- Comme la ligne de protection ne porte pas de trafic en temps normal, possible de porter d'autre trafic non-prioritaire appelé extra trafic, abandonné si la ligne de protection est invoquée.



SDH Ring Architectures

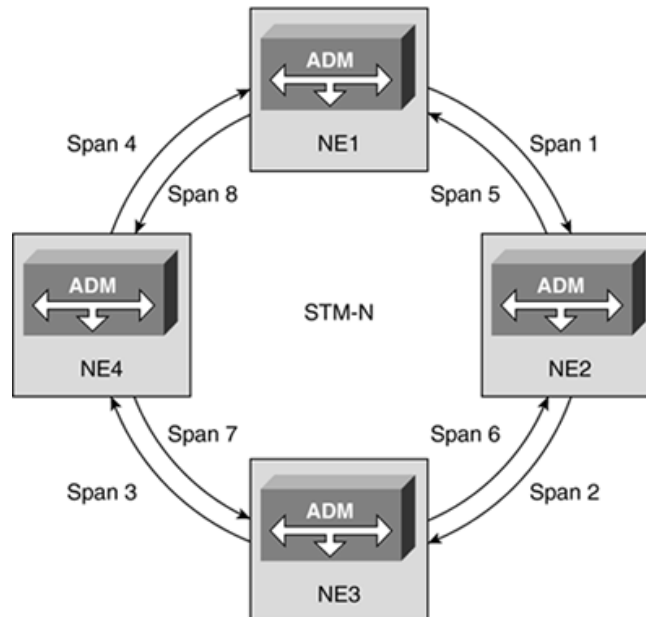
SDH Attribute	Value
Fibers per link	2-fiber 4-fiber
Signal direction	Unidirectional Bidirectional
Protection switching	Multiplex section switching Path switching

- Différentes config d'anneau SDH avec caractéristiques précises.
- 3 types majoritaires:
 - Two-fiber subnetwork connection protection ring (**two-fiber SNCP**)
 - Two-fiber multiplex section-shared protection ring (**two-fiber MS-SPRing**)
 - Four-fiber multiplex section-shared protection ring (**four-fiber MS-SPRing**)

SDH Ring Architectures

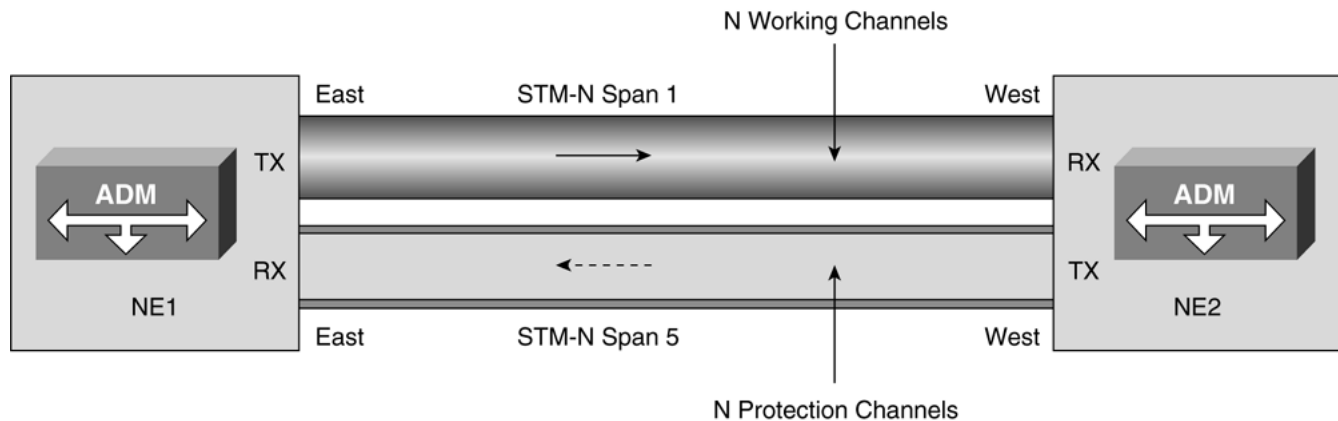
- **Unidirectional Versus Bidirectional Rings:**

- Unidirectional ring: trafic actif routé dans le sens des aiguilles d'une montre, de protection dans sens trigo.
- Bidirectional ring: chemin le plus court quelque soit le sens. Si un lien défaille, le trafic est routé dans le sens inverse.



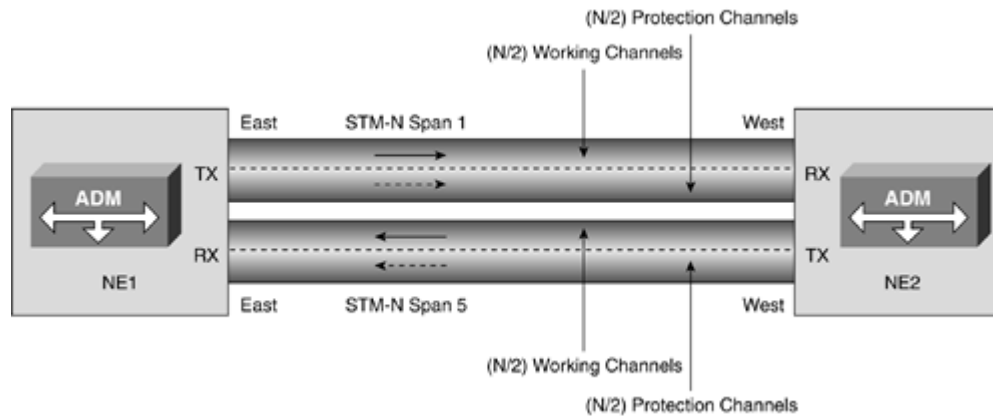
SDH Ring Architectures

- **Two-Fiber Versus Four-Fiber Rings:**
 - Pour systèmes unidirectionnels et bidirectionnels
 - Systèmes unidirectionnels commercialisés, tel que SNCP, sont de type two-fiber, les bidirectionnels, tel que MS-SPRing, sont des 2 types.
 - Un système STM-N unidirectionnel two-fiber avec 2 noeuds:
 - Fibre 1 porte N canaux actifs vers NE2, et fibre 5 N canaux de protection vers NE1.
 - (For example, an STM-16 system would carry 16 working VC-4s eastbound from NE1 to NE2, while carrying 16 separate protection VC-4s westbound from NE2 to NE1.)



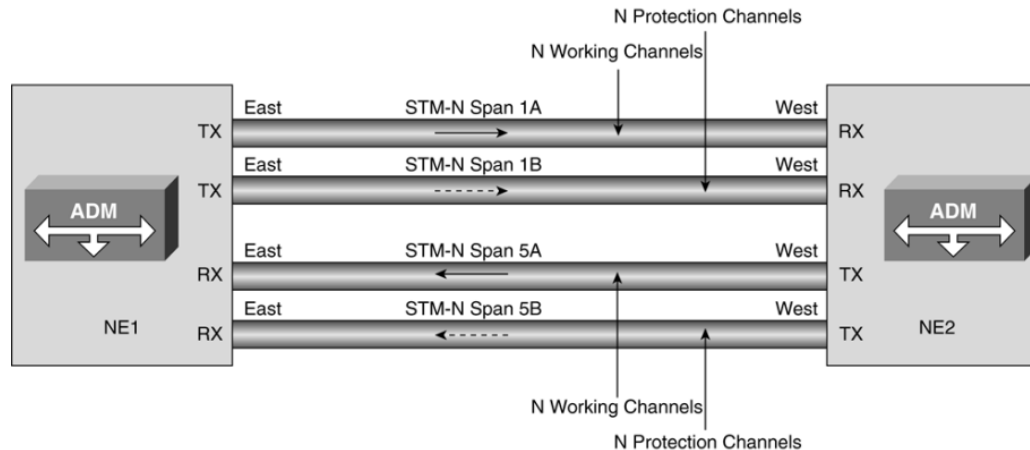
SDH Ring Architectures

- Un système STM-N bidirectionnel two-fiber avec 2 noeuds:
 - Sur chaque fibre, un maximum de la moitié des canaux est défini comme canaux actifs, l'autre moitié comme canaux de protection.
 - Fiber span 1 carries $(N/2)$ working channels and $(N/2)$ protection channels eastbound, and fiber span 5 carries $(N/2)$ working channels and $(N/2)$ protection channels westbound.



SDH Ring Architectures

- Un système STM-N bidirectionnel four-fiber avec 2 noeuds:

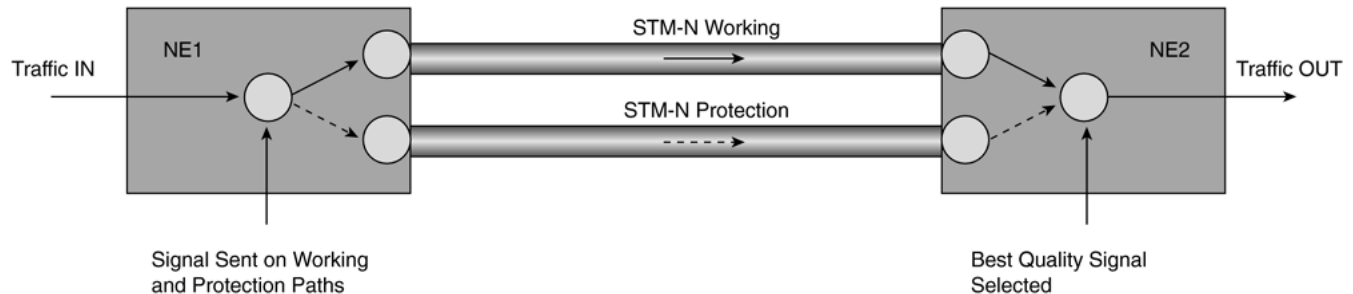


- > Two-fiber SNCP fournit N canaux actifs dans une direction, tandis qu'un two-fiber MS-SPRing fournit $(N/2)$ canaux actifs dans chaque direction.
- > Four-fiber MS-SPRing fournit N canaux dans chaque direction.
- > 1 défaillance sur chaque segment cause une défaillance réseau sur un two-fiber ring de chaque type.
- > Un four-fiber avec diversité de routage peut supporter de multiples failles.
- > Les four-fiber sont très utilisés pour les anneaux sur de grandes distances ou au trafic critique.

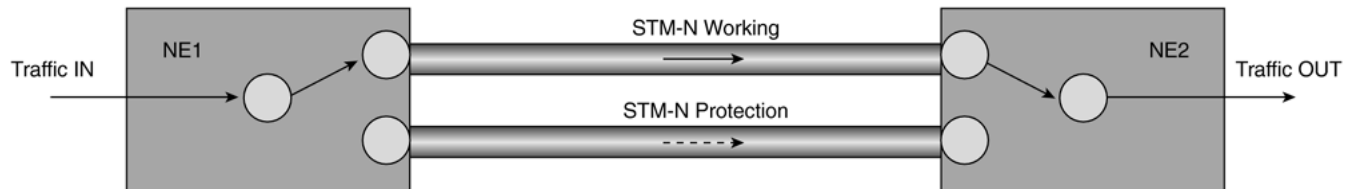
SDH Ring Architectures

- **Path and Multiplex Section Switching:**

- Path switching: une copie du trafic protégé est aussi transmise sur la fibre de protection. Path switching avec two-fiber SNCP rings.



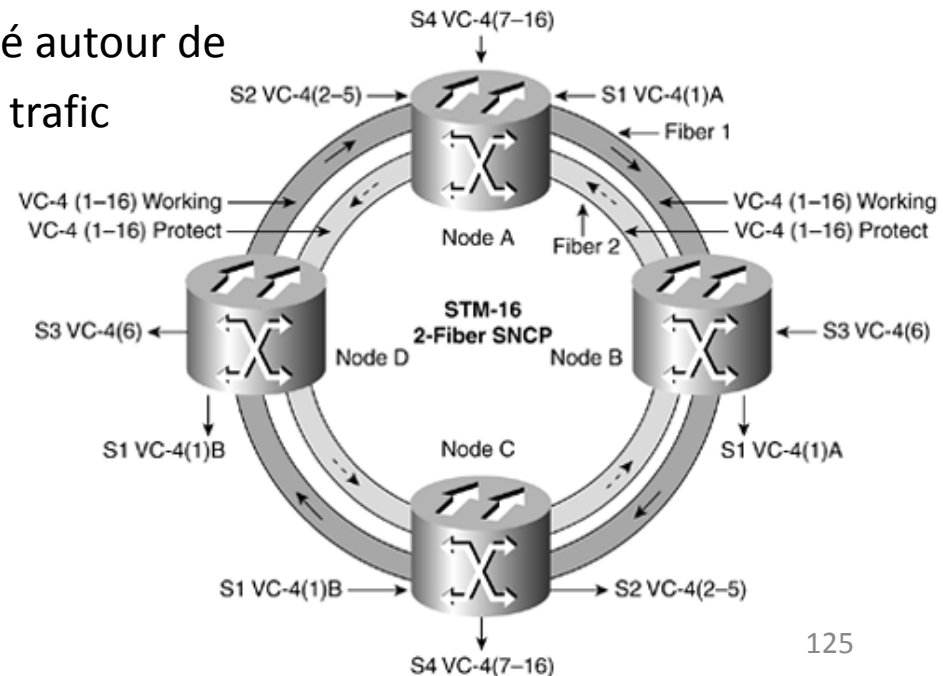
- MS switching: Si défaillance de fibre ou de noeud, le trafic protégé est switché sur canal de protection, tout trafic présent sur ce canal est abandonné.



SDH Ring Architectures

- **Subnetwork Connection Protection Rings (SNCP):**

- Un anneau SNCP est une architecture de transport résiliente, en boucle fermée, qui protège contre les coupures de fibre en fournissant des chemins dupliqués divers géographiqht pour chaque circuit.
- SNCP fournit un chemin double de fibres sur l’anneau.
- Trafic actif dans un sens, protection dans l’autre (recopie).
- Comme chaque trafic est transporté autour de l’anneau, SNCPs plutôt pour cas où trafic vient de 2 noeuds uniquement.
- Cas d’une faille: figure.

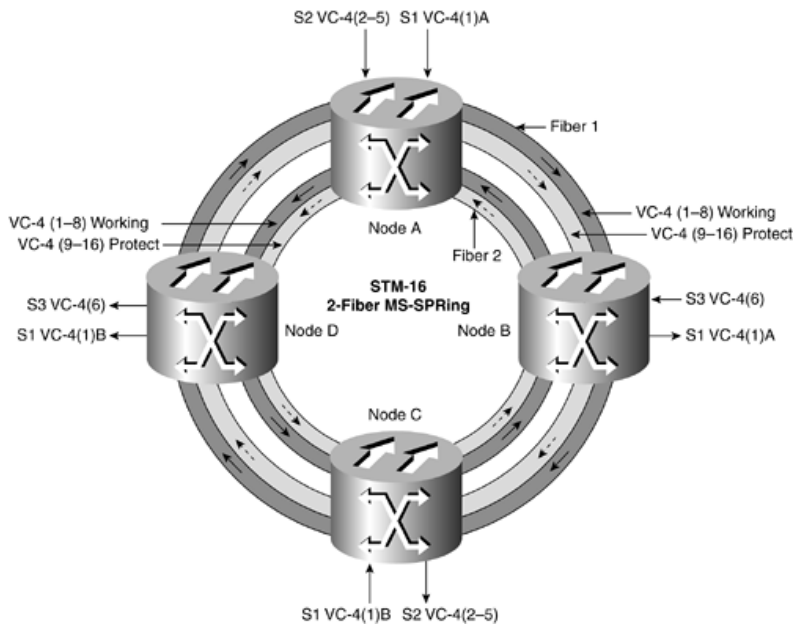


SDH Ring Architectures

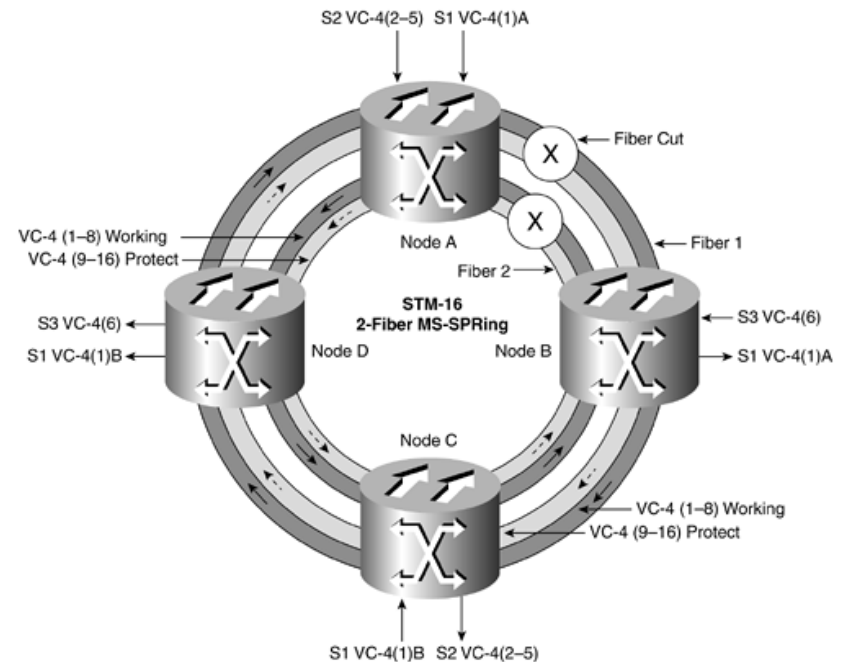
- **Multiplex Section-Shared Protection Rings:**
 - MS-SPRing avec multiplex section bidirectionnelle – système two-fiber ou four-fiber.
 - Adapté aux trafic distribués, tel que réseau d'interconnexion entre sites.
 - Permet ré-utilisation de BW autour de l'anneau.
 - supports non-revertive and revertive protection mechanisms.

SDH Ring Architectures

- **Two-Fiber MS-SPRing:** 1 fiber per direction, working and protection traffic in each.
 - With careful bandwidth-capacity planning, MS-SPRing could be quite efficient.



Two-Fiber MS-SPRing

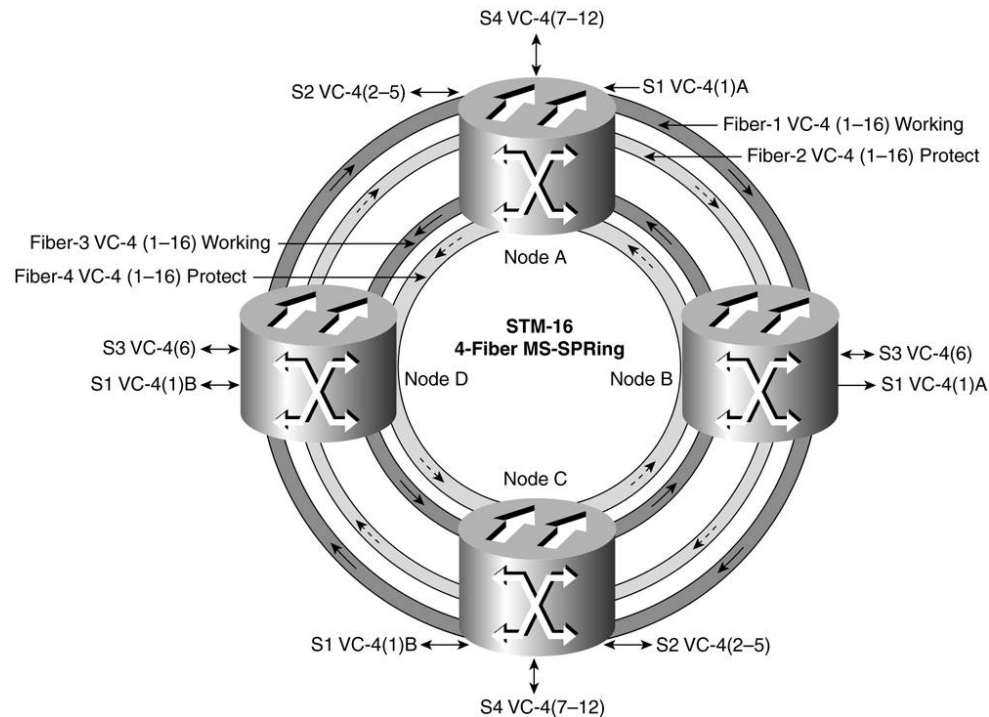


Two-Fiber MS-SPRing Protection

SDH Ring Architectures

— Four-Fiber MS-SPRing:

- double the bandwidth of two-fiber MS-SPRings
- two fibers are allocated for working traffic and two fibers are allocated for protection



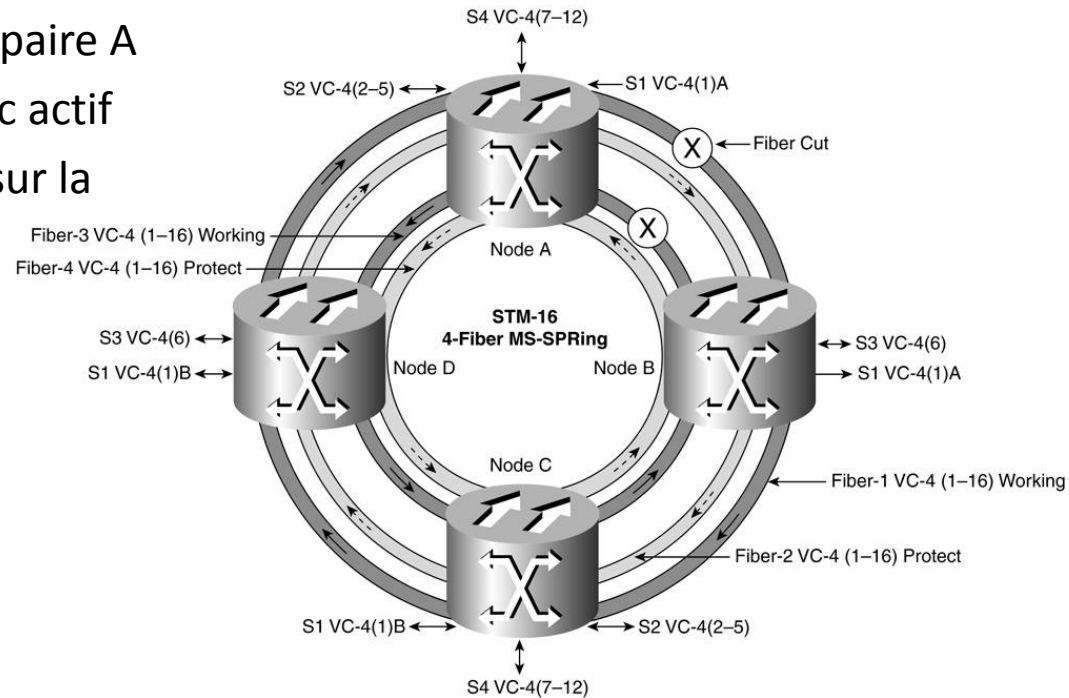
SDH Ring Architectures

- Four-fiber MS-SPRing permet Path Switching et MS Switching
--> plus de flexibilité et fiabilité pour trafic protégé.

- Quand une fibre active défailit, le trafic switché vers les fibres de protection entre les noeuds, puis retourne vers les fibres actives.

- Si la fibre active entre la paire A et B défailit, tout le trafic actif entre ces noeuds passe sur la fibre de protection.

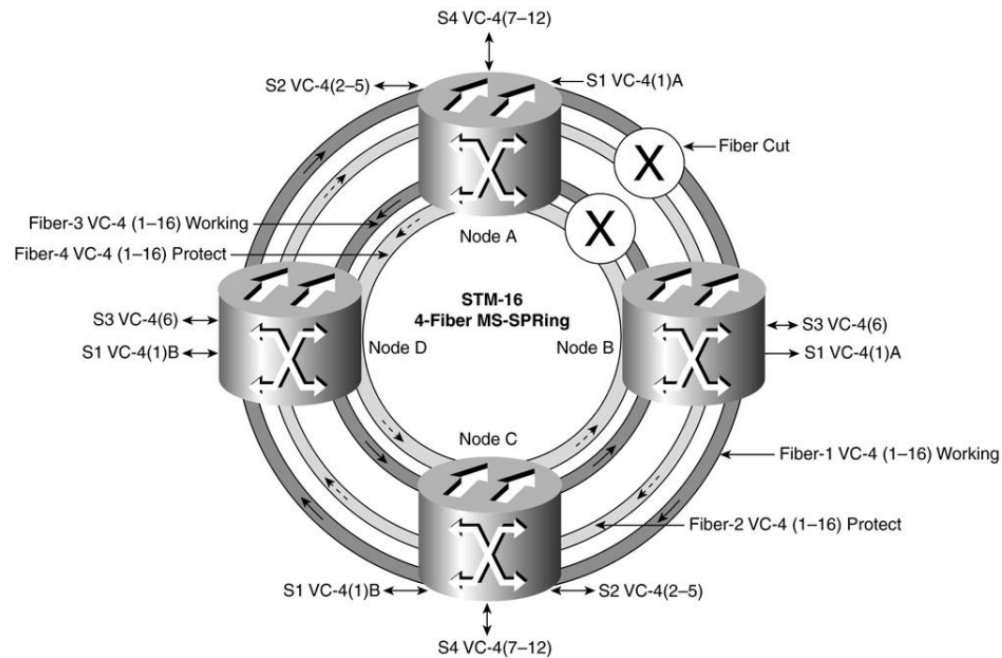
Tout trafic non-protégé entre 2 autres noeuds n'est pas affecté.



Four-Fiber MS-SPRing Span Switch

SDH Ring Architectures

- Four-fiber MS-SPRing ring:
 - Si les 2 paires de fibres entre A et B défailissent, tout le trafic actif entre ces noeuds est passé sur les paires de protection.
 - Tout trafic non protégé entre d'autres noeuds peut être droppé.



Four-Fiber MS-SPRing Ring Switch

Plan

I. Présentation des WAN

II. Les interfaces de la couche physique

III. Protocoles de niveau 2 dans les WAN

III.1. En mode point-à-point :

III.1.a. HDLC

III.1.b. PPP

III.2. En mode circuit virtuel de bout-en-bout :

III.2.a. Frame Relay

III.2.b. ATM

IV. MPLS : commutation par VC dans le monde IP

V. Qualité de service

VI. Technologies xDSL

HDLC

- HDLC (**High-level Data Link Control**) est né en 1976 pour faire communiquer un terminal avec une machine distante, tout en évitant un trop grand nombre d'erreurs lors de la transmission.
- HDLC est un protocole de couche 2 du modèle OSI
- Son but est de définir un mécanisme pour délimiter des trames de différents types, en ajoutant un contrôle d'erreur.
- L'unité de transfert est la trame.
- **Avant HDLC: protocoles (SDLC) beaucoup plus simples avec attente de ACK avant émission de la trame suivante.**
- **Avec la génération HDLC: l'attente de l'ACK n'empêche pas la transmission des trames suivantes.**
- Pour liaisons entre nœuds de transfert des réseaux des opérateurs, l'ITU-T a développé un sous-ensemble de la norme HDLC, appelé LAP-B (*Link Access Protocol-Balanced*).
- **Le protocole HDLC LAP-B utilise deux modes de fonctionnement :**
 - **mode normal: numérotation des trames sur 3 bits, modulo 8**
 - **mode étendu: numérotation des trames sur 7 bits, modulo 128**

Encapsulation HDLC

Format de trame HDLC standard et Cisco



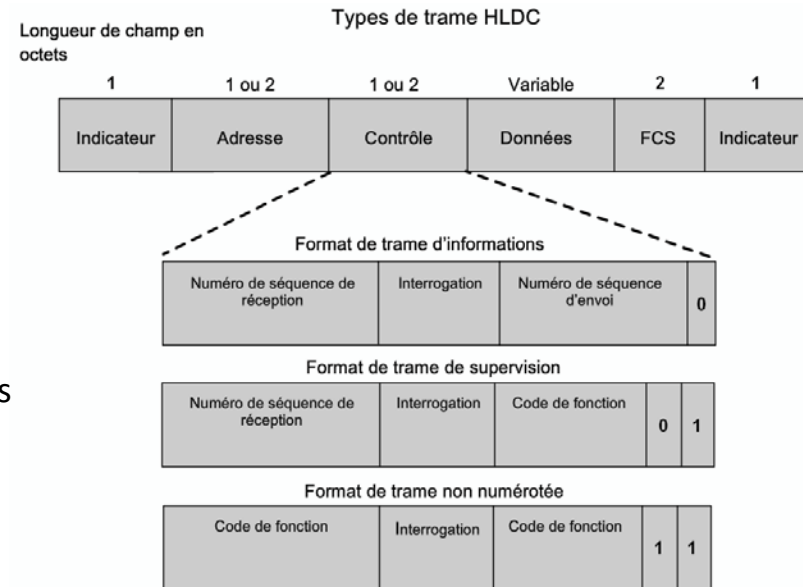
- ISO 13239, synchrone, services avec et sans connexion, vient de SDLC
- transmission série synchrone pour communications sans erreurs entre deux points
- contrôle de flux et des erreurs par accusés de réception
- Même format pour trames de données et de contrôle
- Indicateur:
 - pour marquer le début et la fin de chaque trame
 - 01111110 (=0x7E) pour démarrer et terminer la trame
 - > bit stuffing: un '0' inséré après chaque série de 5 '1' du champ données
- Adresse: HDLC de la station secondaire (uni-,multi- ou broadcast)

Encapsulation HDLC: le champ contrôle

Contrôle: 3 formats selon le type de trame HDLC:

- **Trame d'information (I)**: infos de couches sup et de contrôle
 - Numéro N(S) de la trame, numéro N(R) de la prochaine trame attendue par l'émetteur
 - Élément binaire P/F de commande (interrogation).
 - La valeur N(R) joue le rôle d'ACK positif en indiquant que toutes les trames ayant un numéro $<$ à N(R) ont bien été reçues.

- **Trame de supervision (S)**: informations de contrôle, 2 fonctions:
 - soit remplacer les trames I, quand pas de données à transmettre et que le récepteur veut envoyer un ACK positif,
 - soit réaliser les fonctions de commande de supervision de la liaison, comme la demande de retransmission ou la demande de suspension temporaire de transmission.
 - 3 types de trames S pour le transport des commandes:
 - La trame RR (*Receive Ready*) porte les ACK qui ne sont pas émis dans une trame I.
 - La trame RNR (*Receive Not Ready*) donne un contrôle de flux de niveau trame, en demandant à l'émetteur de stopper les envois jusqu'à la réception d'une nouvelle trame RR spécifiant le N(R).
 - La trame REJ (*Reject*) correspond à la reprise sur erreur en cas de détection d'anomalies.
 - Une 4e possibilité existe dans la norme HDLC de base, la trame SREJ (*Selective Reject*), qui ne demande la retransmission que de la seule trame en erreur.



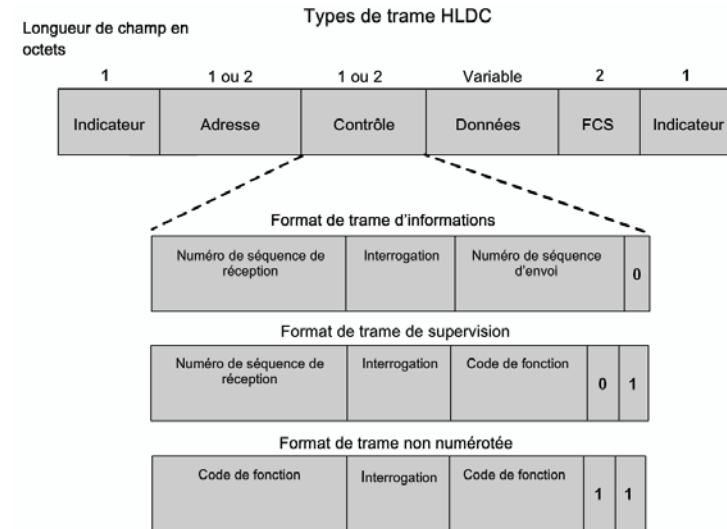
- **Trame non-numérotée (U)**: gèrent la liaison, aucun compteur (initialisation des stations pour la connexion).

Encapsulation HDLC: le champ contrôle

- **Interrogation: The P/F bit** - Poll/Final est un seul bit avec 2 noms:
 - Poll quand configuré par émetteur pour obtenir une réponse du récepteur,
 - Final quand configuré par récepteur pour indiquer une réponse ou une fin de transmission. Dans tous les autres cas, le bit est à 0.

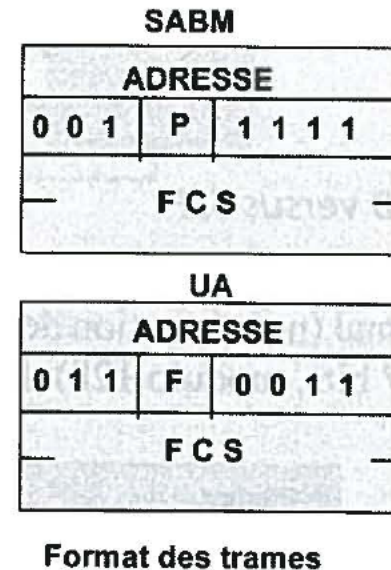
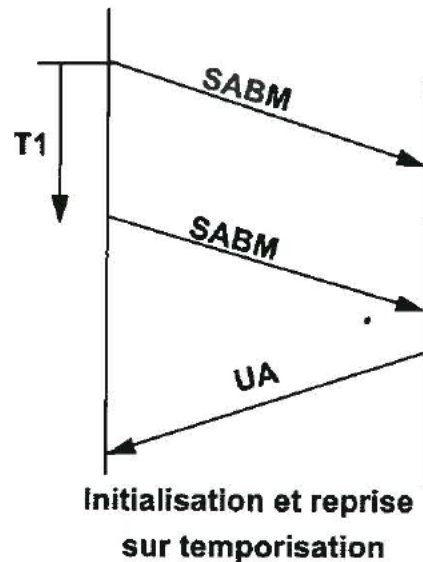
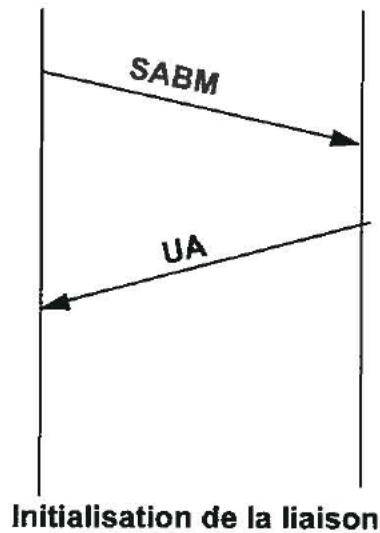
The bit is used as a token that is passed back and forth between the stations. Only one token should exist at a time. The secondary only sends a Final when it has received a Poll from the primary.

The primary only sends a Poll when it has received a Final back from the secondary, or after a timeout indicating that the bit has been lost.



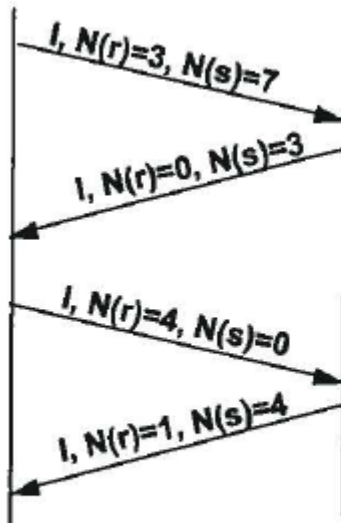
Ouverture de connexion

- Pour ouvrir une connexion, le DCE appelant émet une trame U SABM (ouverture en mode normal) ou SABME (ouverture en mode étendu).
- L'appelé l'acquiesce avec la trame U UA.
- Sans réponse de l'appelé, l'appelant à échéance d'un timer (T1) renouvelle sa demande.
- Il abandonne la demande d'établissement après N2 tentatives infructueuses, en principe le compteur N2 est initialisé à 10, il est décrémenté de 1 à chaque tentative.



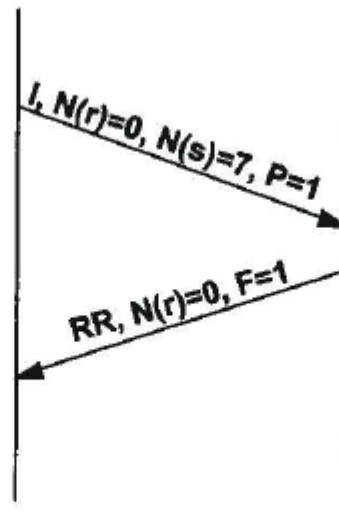
Transfert de données

- Lorsque la connexion est acceptée, l'appelant et l'appelé peuvent procéder à l'échange d'information (trames I), cet échange est contrôlé par des trames de supervision (trames S).
- Les trames I sont numérotées modulo 8 (mode de base) ou modulo 128 (mode étendu).
- L'ACK peut être explicite, il est alors réalisé par une trame RR, ou implicite, ce sont alors les trames I du correspondant distant (échange *full duplex*) qui effectuent l'acquittement (champ N(R)).

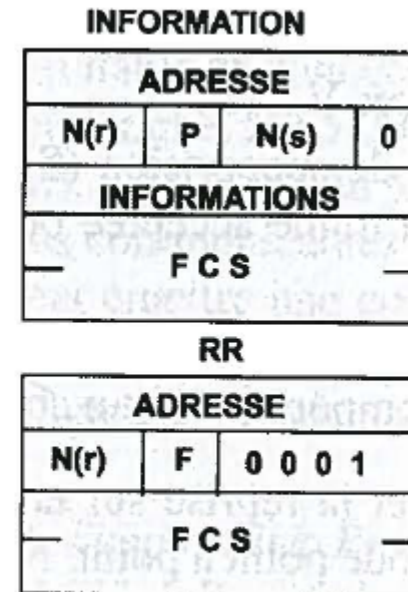


Acquittement implicite

Je t'envoie 7 j'attends 3,
 Je t'envoie 3, j'attends 0,
 Je t'envoie 0, j'attends 4, ...



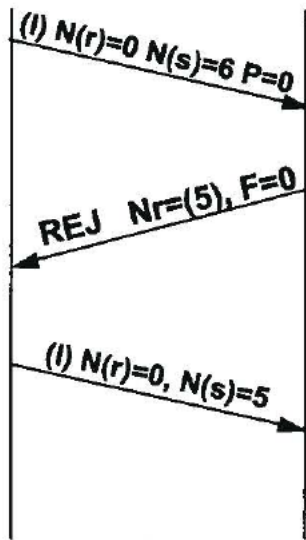
Acquittement explicite



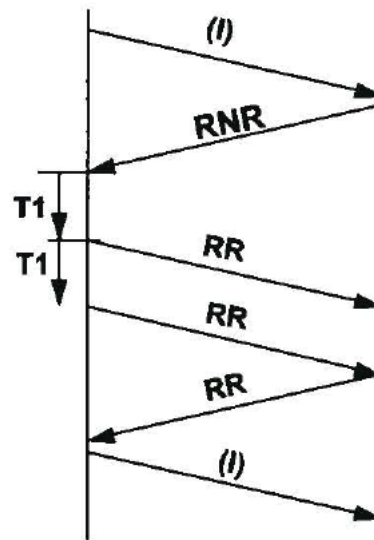
Format des trames

Reprise sur erreurs et contrôle de flux

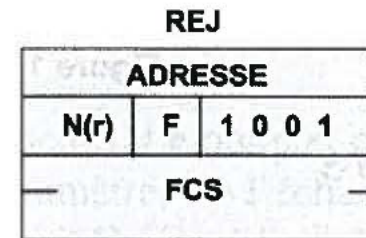
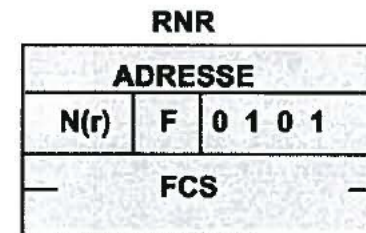
- Les trames S, RR, REJ et RNR supervisent l'échange.
- La trame RR sert à l'acquittement
- La trame REJ indique la trame rejetée (trame erronée ou numéro de séquence invalide) et demande de reprendre la transmission depuis la trame erronée (compteur N(R)).
- La trame SREJ (rejet sélectif) ne demande la retransmission que de la trame rejetée.
- La trame RNR acquitte la trame N(R)-1 et demande à l'émetteur d'arrêter provisoirement son émission, c'est le mécanisme du contrôle de flux (état bloqué ou occupé), les émissions ne reprendront qu'à réception d'une trame RR ou REJ.



Reprise sur erreur



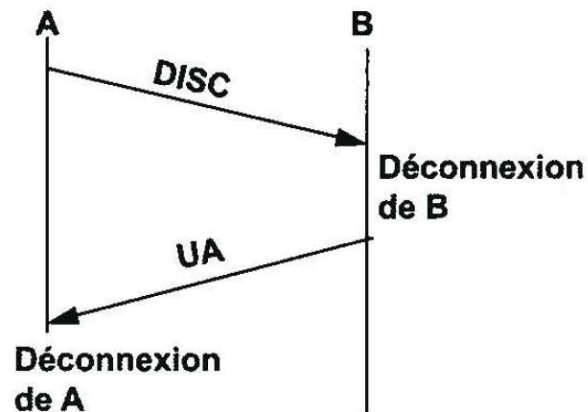
Contrôle de flux



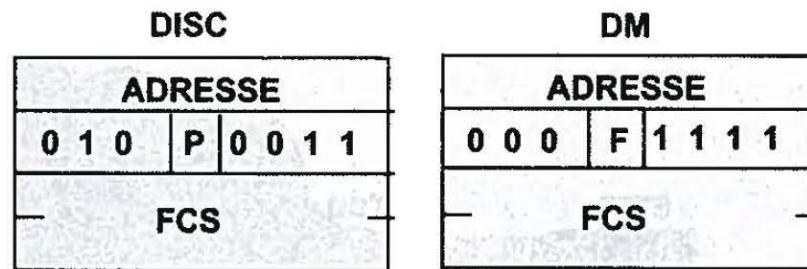
Format des trames

Rupture de liaison

- La déconnexion est demandée par le DCE.
- A réception d'une demande de déconnexion (trame DISC), le destinataire l'acquiesce (trame UA) et se déconnecte.
- Côté émetteur la déconnexion n'est effective qu'après avoir reçu l'ACK de sa demande.
- Le réseau (DCE) peut signaler un incident de ligne (modem coupé par ex) par l'émission de trames DM.
- Après N2 retransmissions, il passe à l'état déconnecté.



Procédure de déconnexion



Format des trames

Plan

I. Présentation des WAN

II. Les interfaces de la couche physique

III. Protocoles de niveau 2 dans les WAN

III.1. En mode point-à-point :

III.1.a. HDLC

III.1.b. PPP

III.2. En mode circuit virtuel de bout-en-bout :

III.2.a. Frame Relay

III.2.b. ATM

IV. MPLS : commutation par VC dans le monde IP

V. Qualité de service

VI. Technologies xDSL

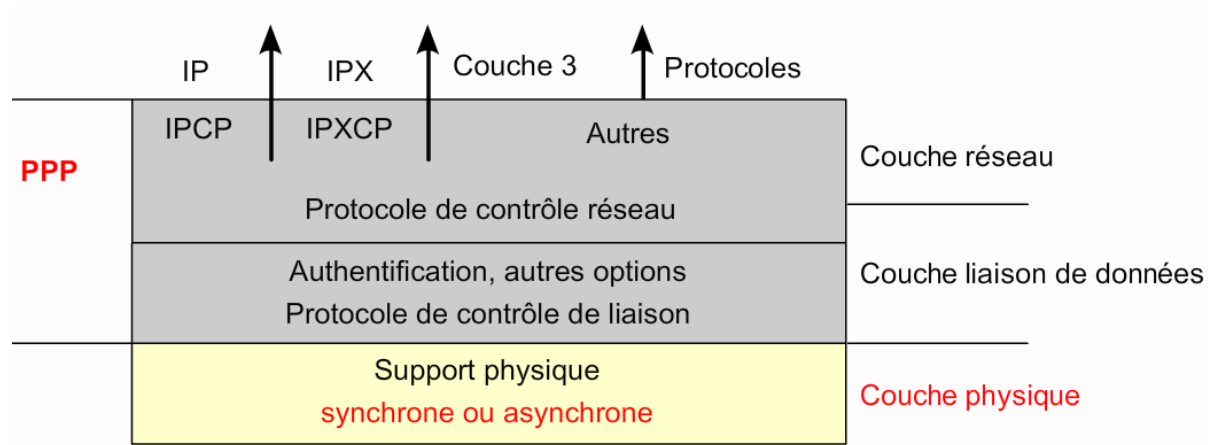
PPP: Concepts

- Établit connexion directe par câbles série, de lignes tel, tel portable, liaisons radio spécialisées ou fibre
- > utilisé dans les accès DSL avec collecte IP (en non-dégroupé) sous les formes PPPoE, PPPoA et PPPoEOA (cf. dernières slides du chapitre et chapitre 8)
- Nombreuses fonctionnalités absentes dans HDLC:
 - Gestion de qualité de la liaison: liaison désactivée si trop d'erreurs
 - Authentification PAP et CHAP

PPP a 3 composants principaux:

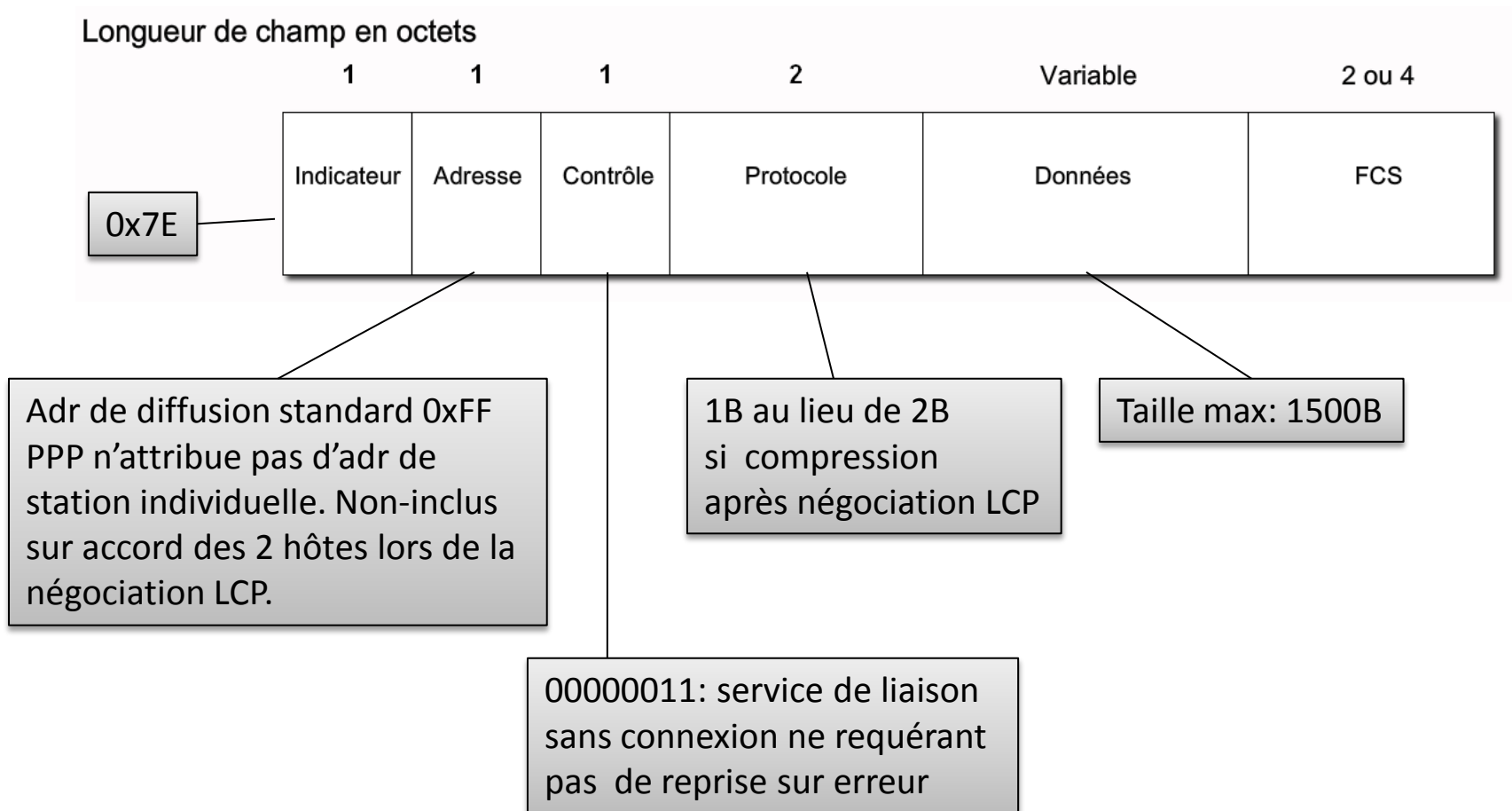
- Le protocole **HDLC** pour l'encapsulation de datagrammes sur des liaisons point à point.
- Le protocole de contrôle de liaison extensible (**LCP**, Link Control Protocol) pour établir, configurer et tester la connexion des liaisons de données.
- Une famille de protocoles de contrôle réseau (**NCP**, Network Control Protocol) pour établir et configurer différents protocoles de couche réseau.
PPP permet l'utilisation simultanée de plusieurs protocoles de couche réseau:
protocoles NCP les plus courants pour TCP/IP, Appletalk, IPX (Novell IPX Control Protocol)

Architecture en couche PPP: couche PHY



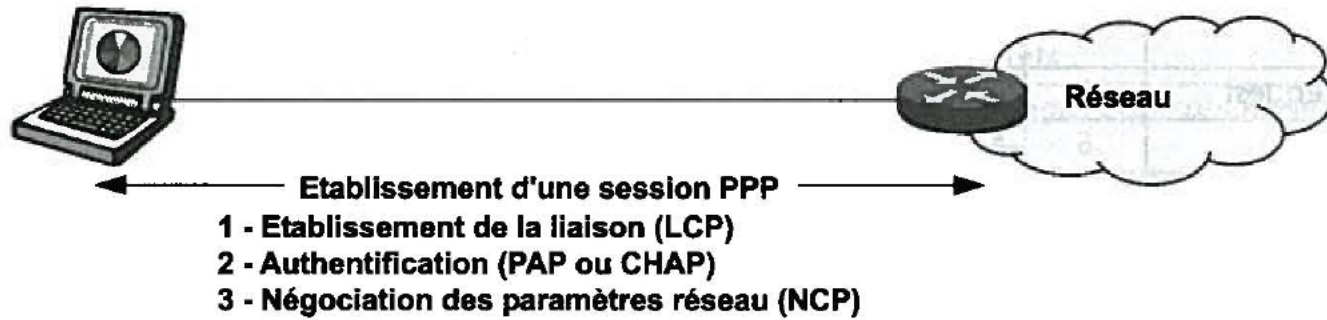
- PPP et OSI: même couche PHY mais fonctions LCP et NCP réparties différemment
- Couche PHY: configuration de PPP pour diverses interfaces: série synchrone, série asynchrone, HSSI, RNIS
- PPP fonctionne sur toutes les interfaces DTE/DCE (RS-232-C, RS-422, RS-423 ou V.35).
- PPP impose: circuit bidirectionnel, dédié ou commuté, fonctionnant en mode série de bit asynchrone ou synchrone, et qui est transparent pour les trames de la couche PPP
- PPP: niveaux 2 et 3 par LCP et NCP – LCP configure la connexion PPP, NCP gère des configurations de protocole de couche plus élevé, LCP met fin à la connexion

Structure de trame PPP

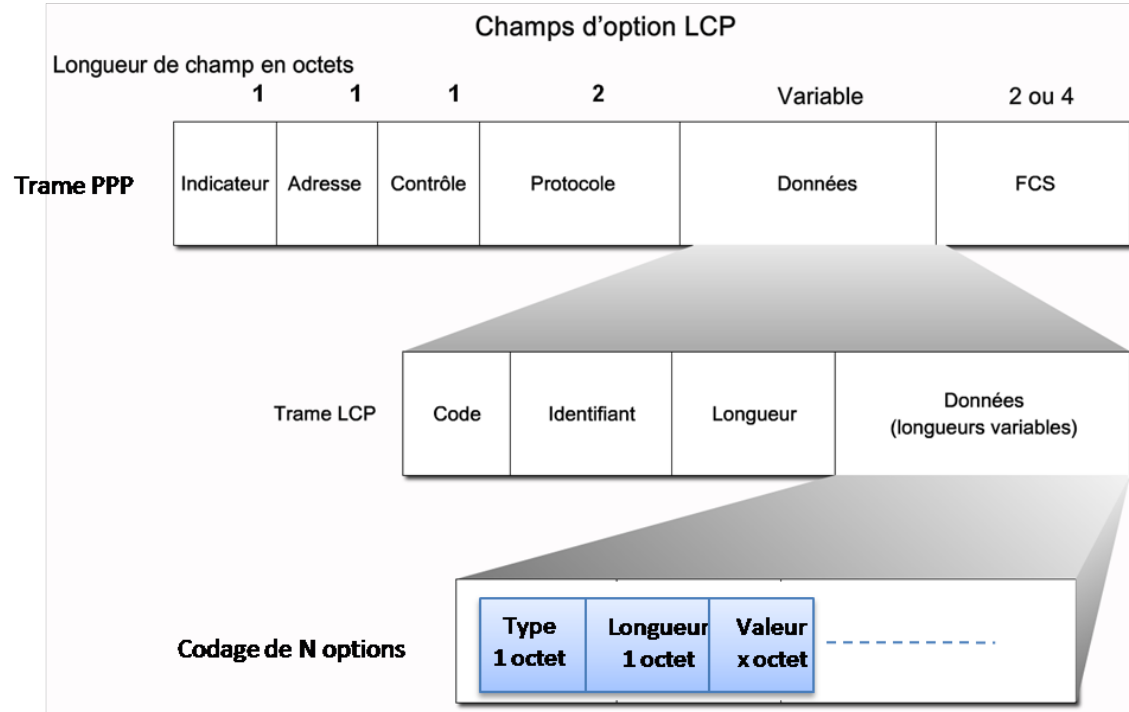


Le champ Contrôle qui a la même signification qu'en HDLC. Si la liaison est fiable, aucun contrôle de séquençement n'est utile (fenêtrage), PPP utilise une trame HDLC «UI» (Trame d'information non numérotée), le champ Contrôle vaut alors 0x03.

Etablissement d'une session PPP



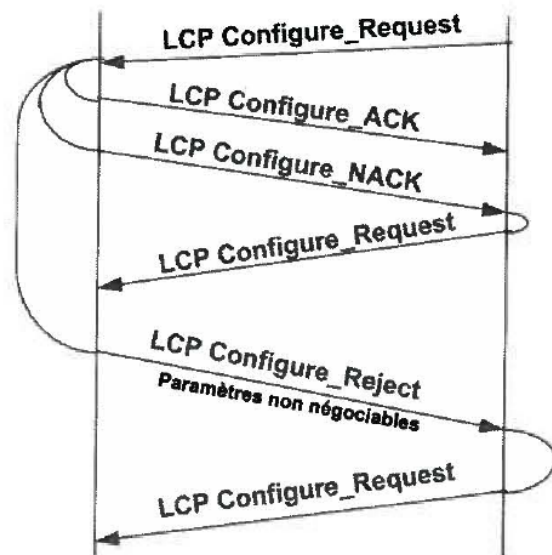
Structure de trame LCP



- Le protocole LCP est identifié dans la trame PPP par le code Protocole_ID = « OxCO21 »
- Le champ Code précise le type de trame
- Le champ Identification permet d'associer une requête à une réponse
- Le champ Longueur permet de distinguer les données utiles d'éventuelles données de bourrage.
- Les options LCP sont codées: type d'option, longueur du champ valeur et valeur des données de l'option

Phases d'initialisation de PPP

- Voici les différentes phases d'un échange.
- Dès que la liaison est établie, chaque entité négocie à son tour ses propres options, la liaison n'est pas nécessairement symétrique.
- L'échange débute par la trame `Configure_Request`
- Le champ données contient les modifications à apporter aux valeurs par défaut (négociation des options).
- Si ces valeurs sont acceptées par le récepteur, celui-ci répond par la trame `Configure_Ack`.
- Si les valeurs ne conviennent pas au récepteur, celui-ci peut demander à la source de lui proposer d'autres valeurs (`Configure_Nack`) ou lui indiquer que les valeurs ne sont pas négociables (`Configure_Reject`).



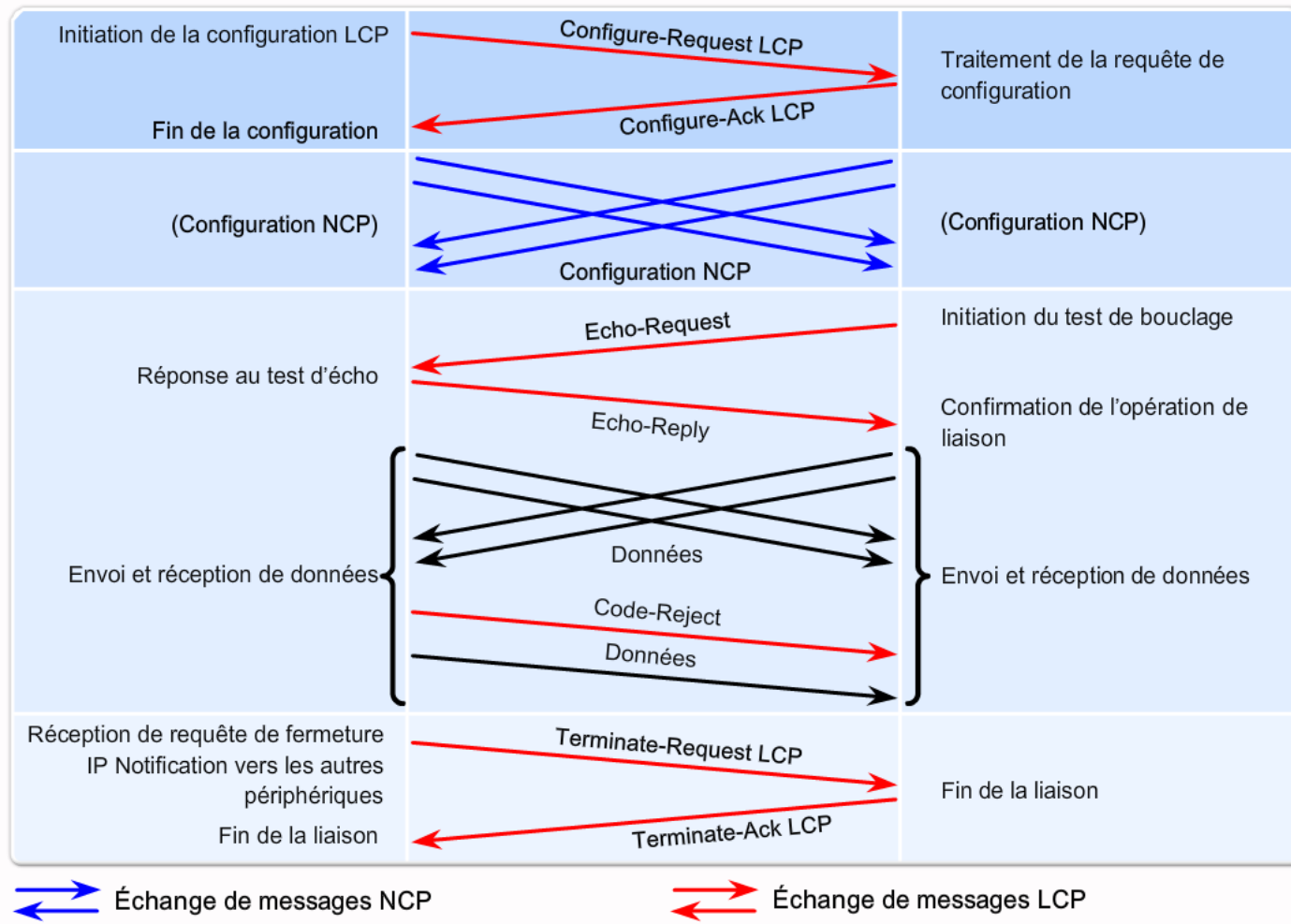
Exemples d'options LCP

- Voici quelques options négociables par LCP.
- Le champ données de la trame LCP contient autant de triplets « Type option, longueur du champ Valeur, Valeur proposée » que d'options négociées.
- La longueur totale du champ données est fournie par le champ longueur de la trame LCP.

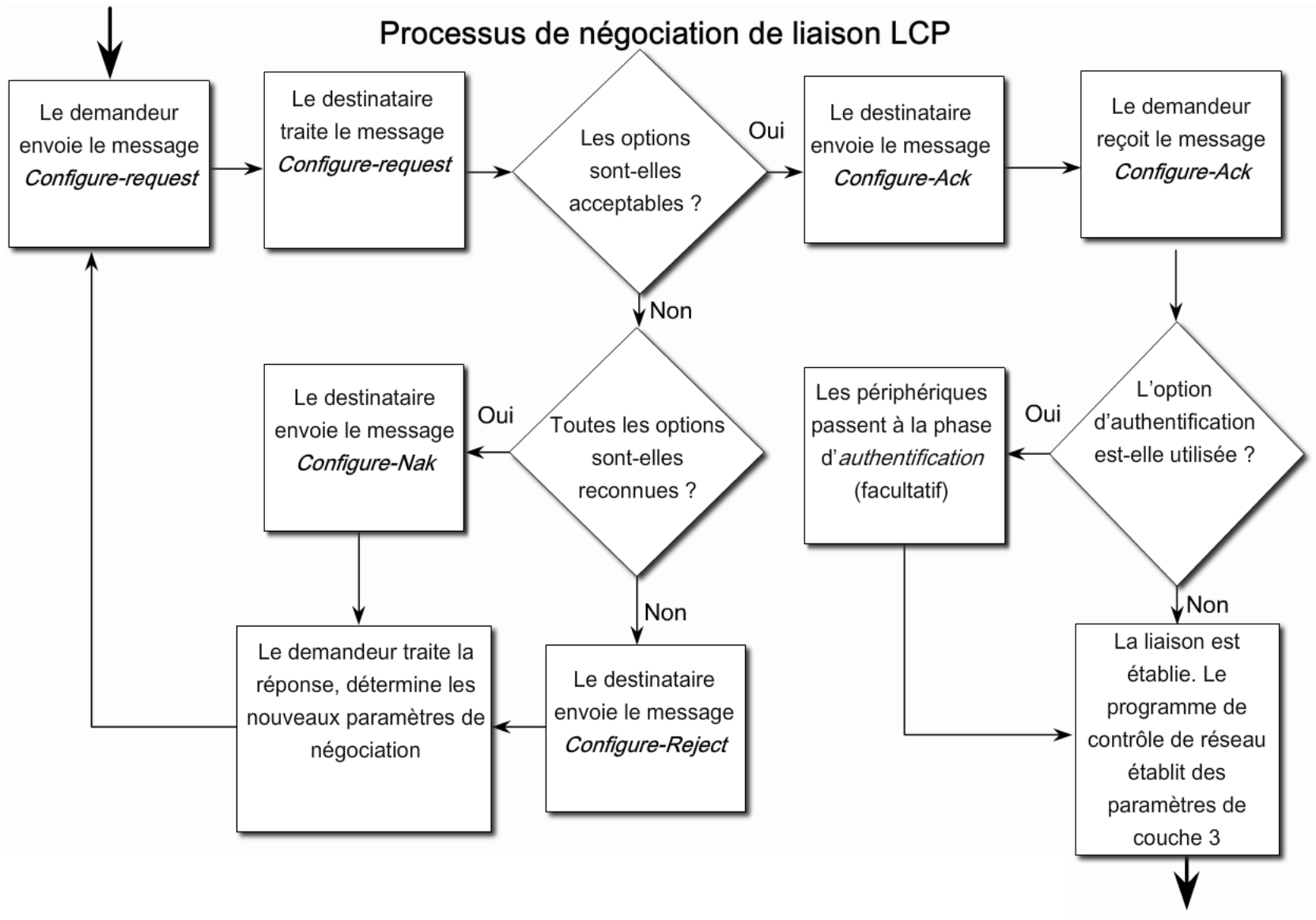
- PPP peut être configuré pour :
 - authentification à l'aide de PAP ou CHAP
 - compression à l'aide de Stacker ou Predictor
 - multi-liaison qui associe un ou plusieurs canaux en vue d'augmenter la BW de réseau étendu.

Code Option	Fonction	Longueur	Signification
1	MRU	4	MRU, <i>Maximum Receipt Unit</i> ; valeur par défaut 1 500 octets.
2	ACCM	6	ACCM, <i>Asynchronous Control Character Map</i> ; table de 4 octets ;
3	Authentification	6	Indique sur 2 octets le protocole de sécurisation utilisé (valeur du champ protocole de PPP) soit 0xC023 pour PAP et 0xC223 pour CHAP.
5	Nombre magique Magic Number	6	Déterminée aléatoirement par chaque extrémité, cette valeur sur 4 octets permet d'identifier l'origine du message et de détecter les boucles (réception par une entité de ce qu'elle a émis).
7	Compression Stacker, Predictor	2	Codage du champ Protocole de PPP sur un octet.
8	Compression	2	Suppression des champs Adresse et Commande de la trame PPP.
13	Rappel automatique	≥ 3	Option de sécurité, cette option non seulement permet l'identification de l'appelant par son rappel mais aussi la prise en compte du coût des communications par le serveur appelé initialement.

Établissement d'une liaison avec LCP



Processus de négociation de liaison LCP



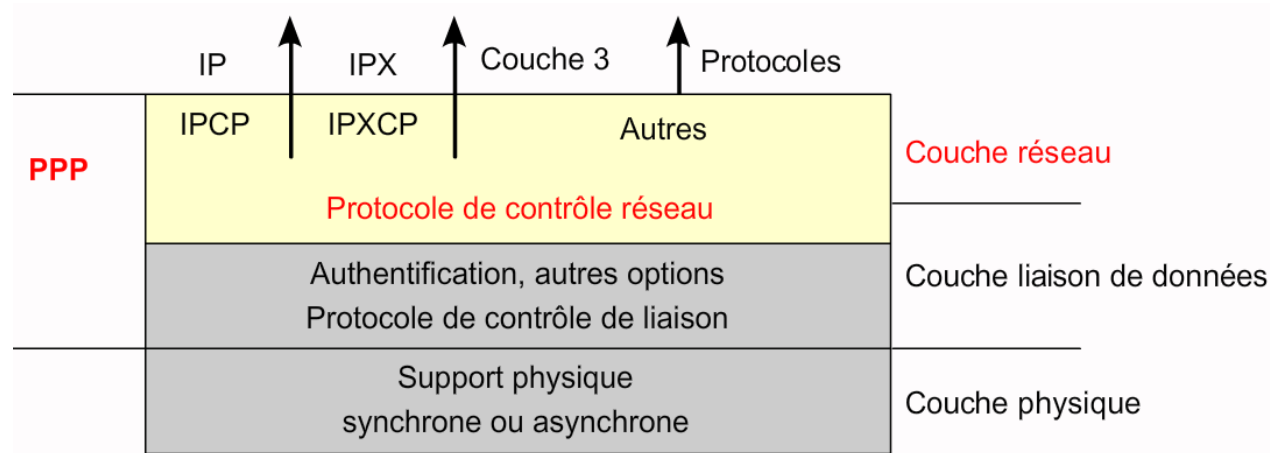
Établissement d'une liaison avec LCP

Code LCP	Type de paquet LCP	Description
1	Configure-Request	Envoyé pour ouvrir ou réinitialiser une connexion PPP. Le message Configure-Request comprend une liste des options LCP avec les changements apportés aux valeurs d'option par défaut.
2	Configure-Ack	Envoyé lorsque toutes les valeurs de toutes les options LCP du dernier message Configure-Request reçu sont reconnues et acceptables. Une fois que les deux homologues PPP envoient et reçoivent des messages Configure-Ack, la négociation LCP est terminée.
3	Configure-Nack	Envoyé lorsque toutes les options LCP sont reconnues, mais que les valeurs de certaines options ne sont pas acceptables. Le message Configure-Nack inclut les options problématiques et leurs valeurs acceptables.
4	Configure-Reject	Envoyé lorsque des options LCP ne sont pas reconnues ou ne sont pas acceptables pour la négociation. Le message Configure-Reject inclut les options non reconnues ou non négociables.
5	Terminate-Request	Envoyé éventuellement pour fermer la connexion PPP.
6	Terminate-Ack	Envoyé en réponse au message Terminate-Request.
7	Code-Reject	Envoyé lorsque le code LCP est inconnu. Le message Code-Reject inclut le paquet LCP problématique.

Établissement d'une liaison avec LCP

Code LCP	Type de paquet LCP	Description
8	Protocol-Reject	Envoyé lorsque la trame PPP comprend un ID de protocole inconnu. Le message Protocol-Reject inclut le paquet LCP problématique. Le message Protocol-Reject est généralement envoyé par un homologue PPP en réponse à un protocole de contrôle de réseau PPP pour un protocole de réseau local non activé sur l'homologue PPP.
9	Echo-Request	Envoyé éventuellement pour tester la connexion PPP.
10	Echo-Reply	Envoyé en réponse au message Echo-Request. Les messages Echo-Request et Echo-Reply du protocole PPP ne sont pas liés aux messages Echo Request et Echo Reply du protocole ICMP.
11	Discard-Request	Envoyé éventuellement pour tester la liaison en sortie.

Architecture en couche PPP: couche NCP



- Liaisons point à point à commutation de circuits et xDSL

-> difficultés dans l'attribution et la gestion d'adresses IP

-> PPP permet de résoudre ces problèmes, grâce aux couches NCP.

- Avec PPP, plusieurs protocoles de couche réseau peuvent fonctionner sur la même liaison: diff couches NCP

Ex: IP utilise IPCP, IPX (Novell) utilise IPXCP

⇒ Avec ses fonctions de haut niveau, le protocole PPP transporte des paquets de plusieurs protocoles de couche réseau grâce aux protocoles NCP. Il s'agit de champs fonctionnels qui contiennent des codes standard pour indiquer le type de protocole de couche réseau qu'encapsule le protocole PPP.

Valeur (hex)	Nom du protocole
8021	Protocole de contrôle de protocole Internet
8023	Protocole de contrôle de couche réseau OSI
8029	Protocole de contrôle Appletalk
802b	Protocole de contrôle IPX de Novell
c021	Protocole de contrôle de liaison
c023	Protocole d'authentification du mot de passe
c223	Protocole d'authentification à échanges confirmés

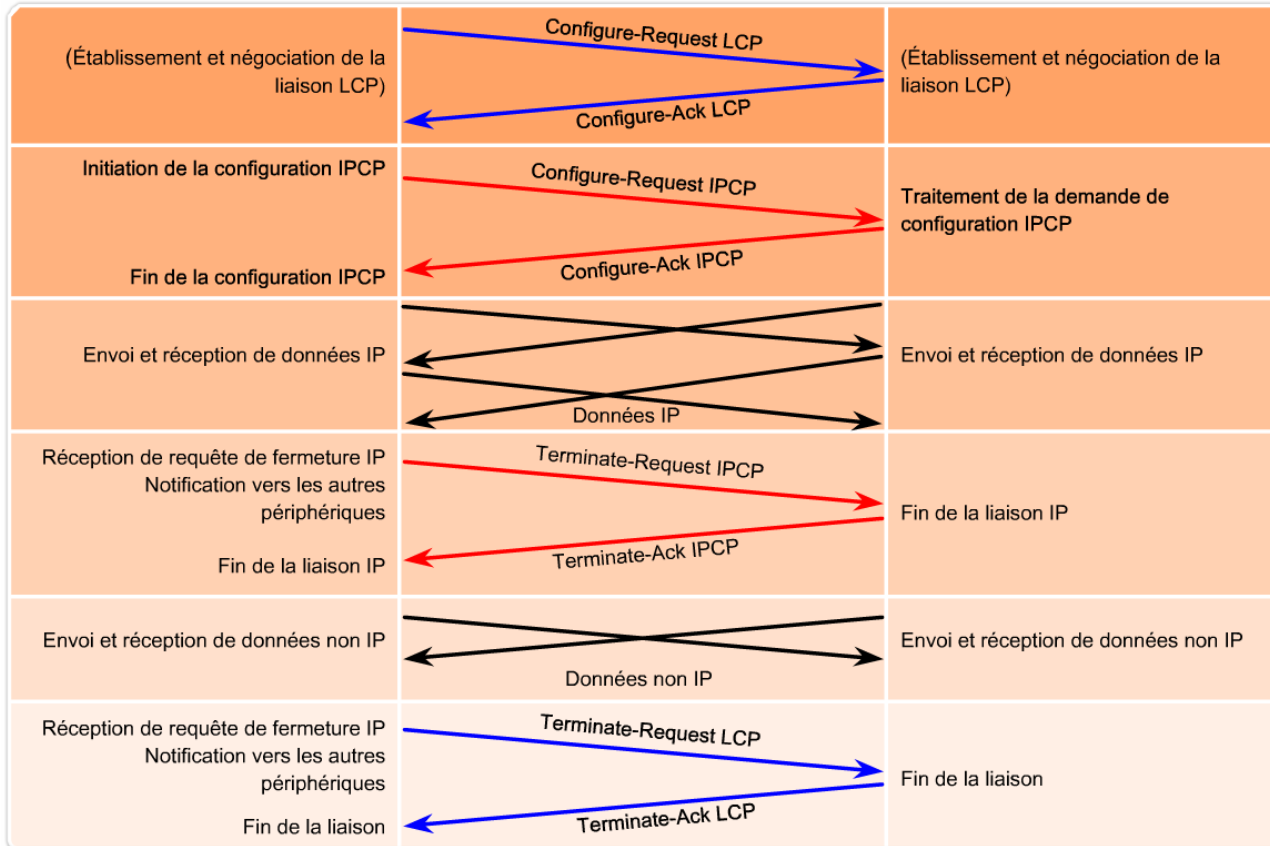
Présentation de NCP


- Une fois que le LCP a configuré et authentifié la liaison de base,
- le protocole NCP est utilisé pour définir les paramètres du niveau réseau.


- Il utilise le même format de trames que celui de LCP.

- Le codage du champ Option dépend de l'option invoquée :
 - Le protocole de compression:
 - en-têtes IP et TCP occupent une part non négligeable des données émises (40 octets hors option)
-> peut être intéressant, lors de l'envoi de petits paquets, de réduire en-têtes:
compression Van Jacobson: codage des différences
 - La négociation d'adresse IP de l'équipement terminal:
 - option pour négocier une adresse IP: le lien local peut demander une adresse IP à l'hôte distant, ou
 - l'informer de l'ad IP qu'il veut utiliser, le distant accepte ou refuse en fournissant une adresse IP valide.

Place de NCP dans la session PPP

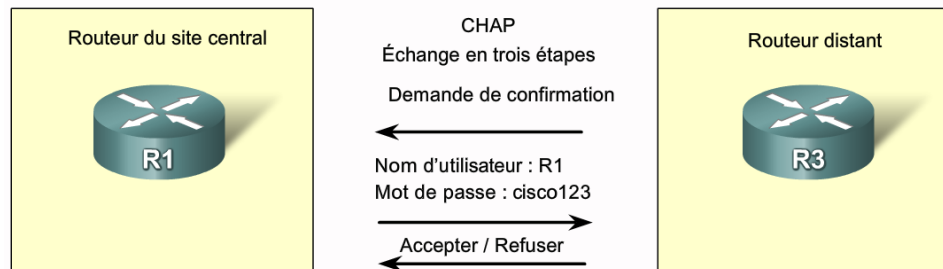
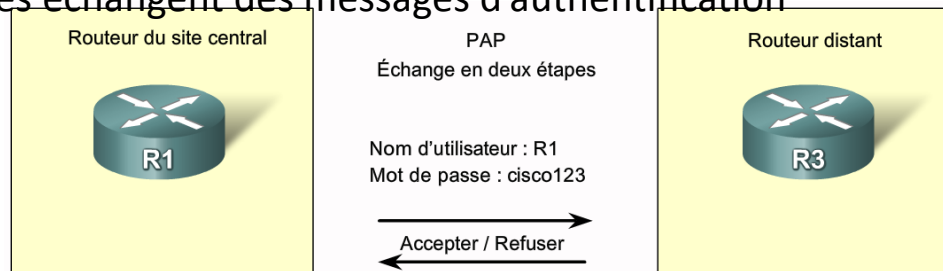


 Échange de messages LCP

 Échange de messages NCP

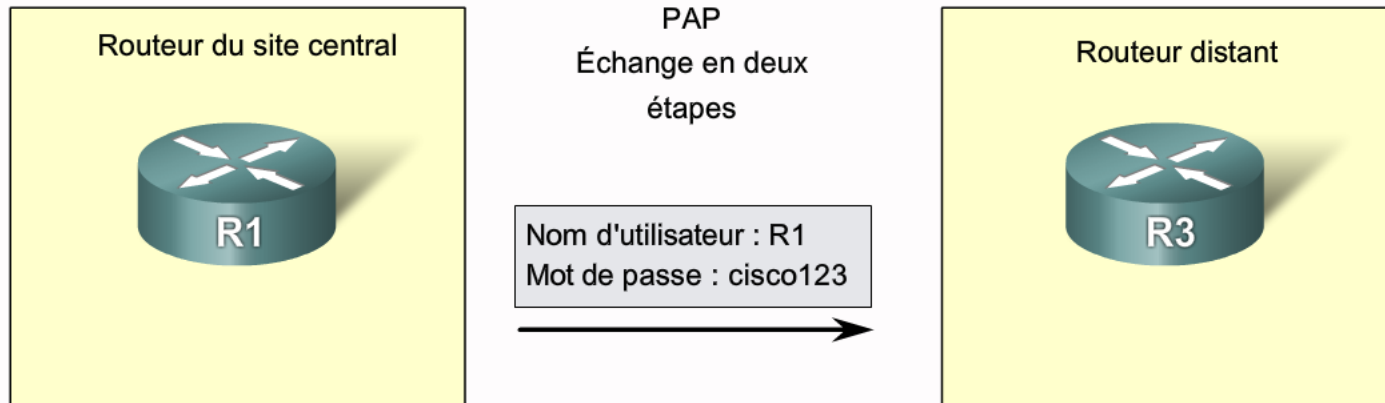
Protocoles d'authentification PPP: PAP

- LCP extensible: négociation d'un protocole d'authentification avant d'autoriser la transmission par des protocoles de couche réseau sur la liaison – RFC 1334
- **PAP (Password Authentication Protocol): processus bidirectionnel sans chiffrement**
- **CHAP (Challenge-Handshake Authentication Protocol): échange en 3 étapes d'un secret partagé (plus sécurisé)**
- Authentification facultative, après l'établissement de liaison par LCP et avant la config de la couche 3
- Le côté appelant de la liaison doit saisir des infos d'authentification.
- Les routeurs homologues échangent des messages d'authentification



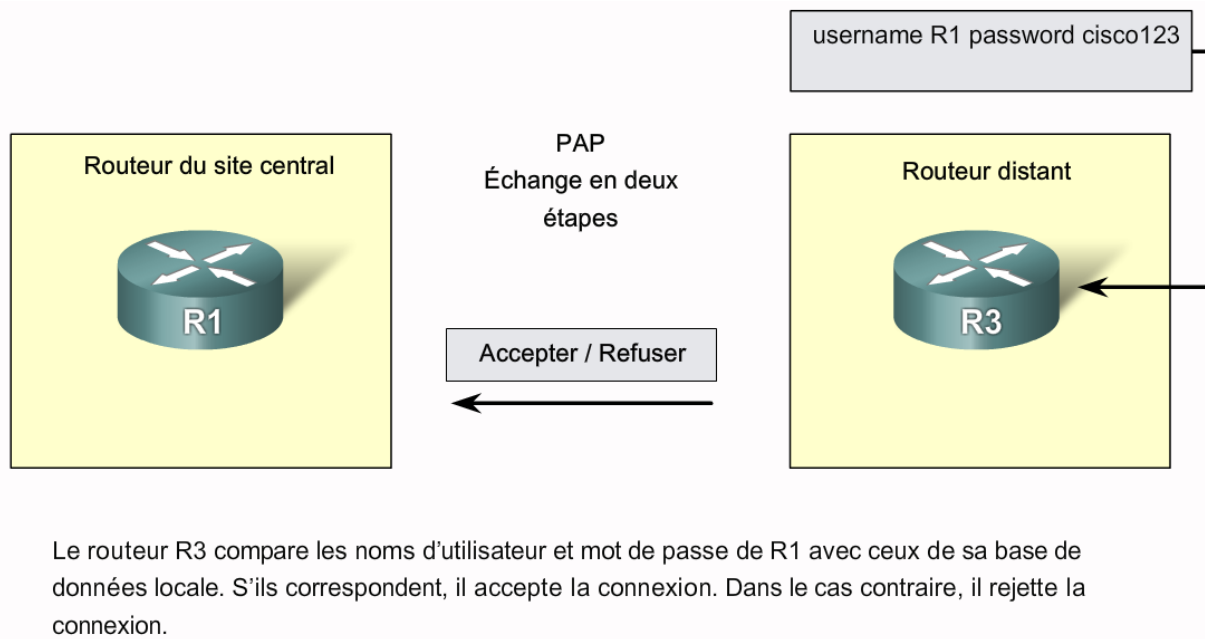
Initialisation de PAP

- PAP n'est pas interactif
- Commande *ppp authentication pap* -> login et pwd envoyés en tant que données LCP
-> pas d'invite de connexion de la part du serveur
- Une fois liaison établie par PPP, le nœud distant envoie de façon répétitive une paire login-pwd sur la liaison jusqu'à ce que le nœud expéditeur en accuse réception ou mette fin à la connexion



Le routeur R1 envoie ses nom d'utilisateur et mot de passe PAP au routeur R3.

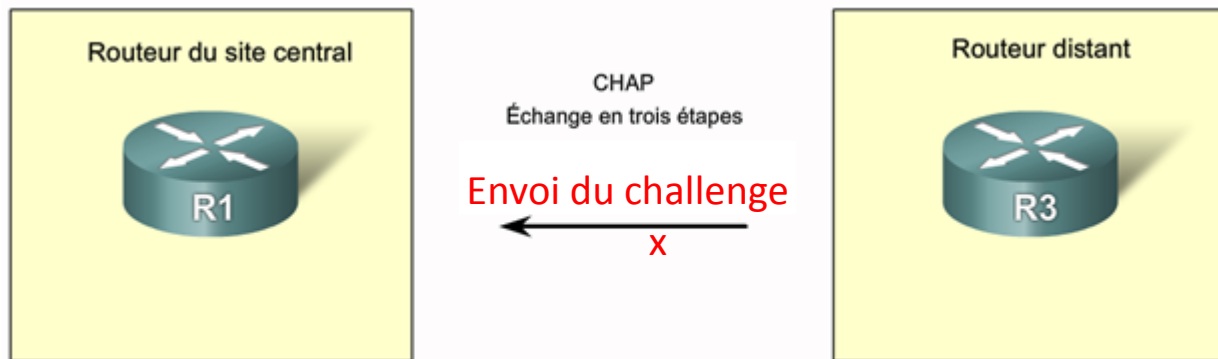
Finalisation de PAP



- PAP n'est pas un protocole d'authentification très fort: login et pwd en clair, pas de protection contre lecture répétée ou attaques par essais-erreurs
- Malgré ses lacunes, PAP peut être utilisé dans les environnements suivants :
 - une base étendue d'applications client qui ne prennent pas en charge CHAP
 - lorsque des implémentations de CHAP par des fournisseurs multiples sont incompatibles

Protocole d'authentification à échanges confirmés : CHAP

- PAP: une fois l'authentification établie, le protocole cesse de fonctionner -> réseau exposé à attaques
 - CHAP: vérifications régulières pour s'assurer que le nœud distant peut toujours répondre au challenge, dont la valeur change de façon imprévisible pendant l'existence de la liaison.
1. Initialisation CHAP: Une fois l'établissement de la liaison PPP terminée, le routeur local envoie un message challenge au nœud distant.



After the completion of the link establishment phase, the authenticator sends a "challenge" message to the peer.

Protocole d'authentification à échanges confirmés : CHAP

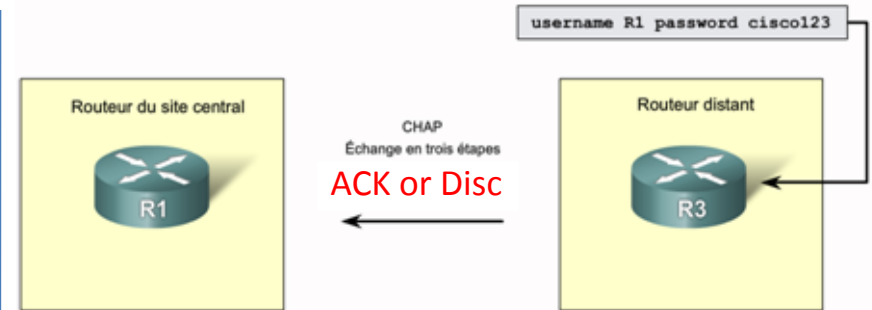
2. Réponse CHAP:

Le nœud distant répond par une valeur fonction du pwd et du challenge.

(calculée au moyen d'une fonction de hachage unidirectionnelle, généralement l'algorithme Message Digest 5 (MD5))



The peer responds with a value calculated using a one-way hash function on the challenge and the secret combined.



The authenticator checks the response against its own calculation of the expected hash value.

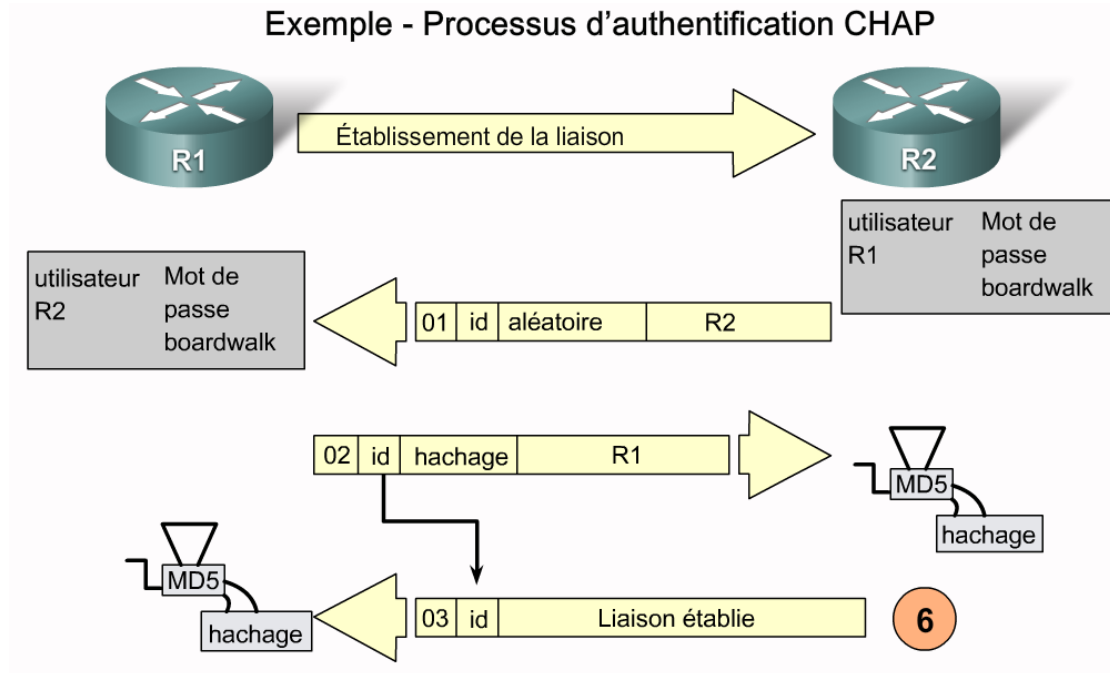
3. Finalisation CHAP:

Le routeur local compare la réponse à son propre calcul de la valeur de hash attendue.

- > soit le nœud demandeur ack l'auth
- > soit il met immédiatement fin à la connexion

At random intervals the authenticator sends a new challenge to the peer and repeats steps 1 through 3.

Processus d'encapsulation et d'authentification PPP



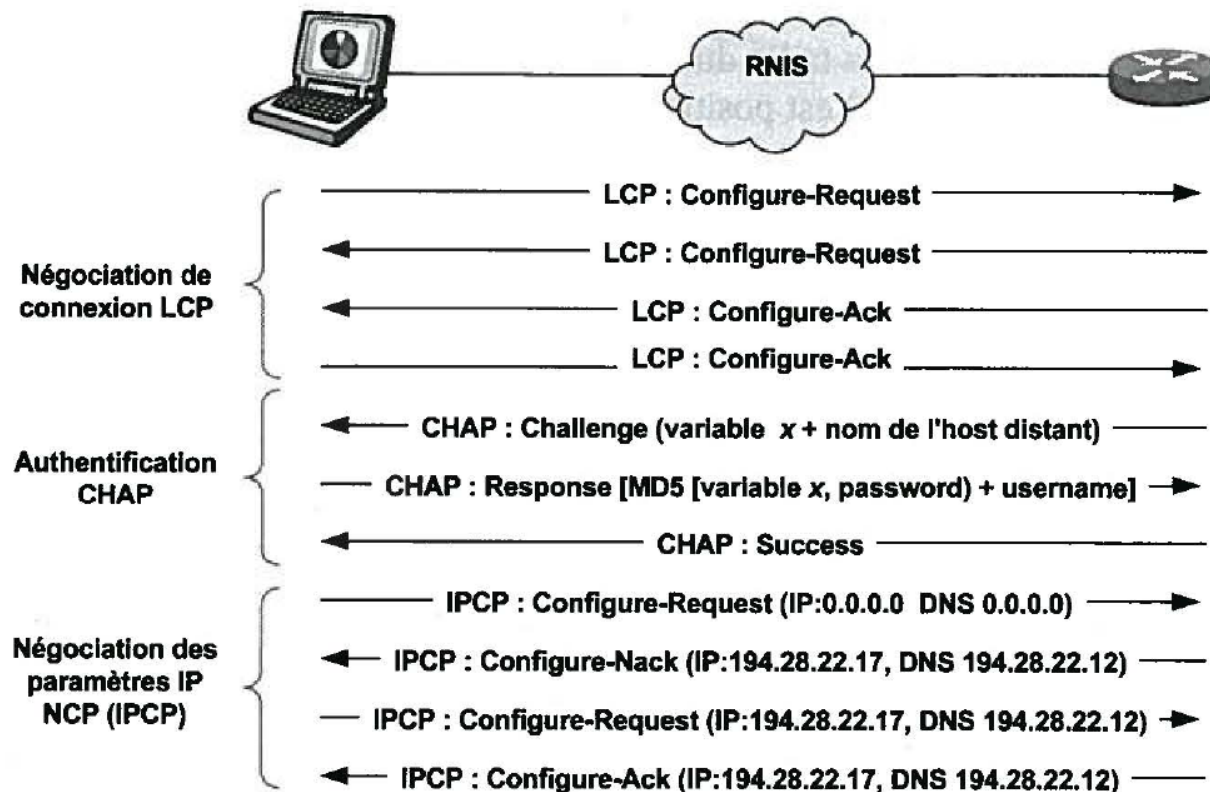
Résumé: Etablissement d'une connexion PPP

- PPP est donc un standard pour transporter du TCP/IP sur des lignes série, et ainsi assurer l'établissement d'une connexion à un ISP sur une ligne série (une connexion par modem) au lieu d'une connexion par carte réseau.
- > PPP répond aux problèmes d'authentification et d'attribution dynamique d'adresse IP :

1- Une fois la liaison modem établie, votre ISP veut s'assurer que vous avez un compte utilisateur chez lui.

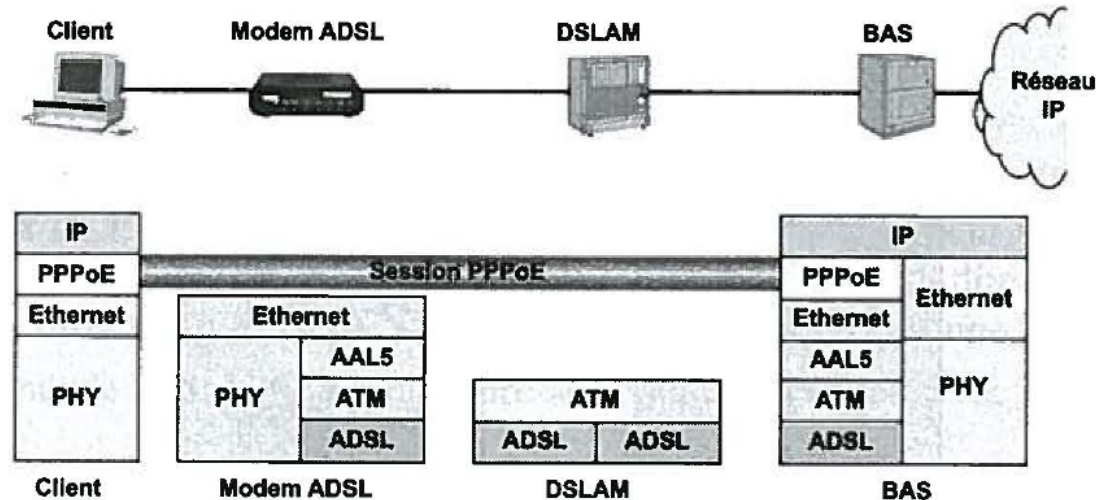
2- Pour utiliser TCP/IP, il va falloir configurer la connexion avec tous les paramètres réseau sur votre machine : ad. IP, masque de sous-réseau, servers DNS, etc

-> PPP s'occupe de l'authentification et de la configuration IP de votre machine auprès de l'ISP



Les tunnels PPP

- Initialement conçu pour être utilisé sur des liens point-à-point, PPP est rapidement devenu le protocole d'accès à un réseau et notamment à Internet en DSL non-dégroupé.
- Avec l'arrivée des connexions à haut débit (xDSL), les AP ont dû s'équiper de BAS pour gérer les connexions.
- La connexion entre l'utilisateur et le point d'accès au réseau de l'opérateur est réalisée, selon le type d'accès, par une adaptation du protocole PPP.
- L'accès peut alors être réalisé via un circuit virtuel ATM entre l'abonné et le BAS: **PPPoA**.



- Données IP encapsulées dans une trame PPP, (encapsulée dans une trame Ethernet,) puis dans des cell ATM

Plan

I. Présentation des WAN

II. Les interfaces de la couche physique

III. Protocoles de niveau 2 dans les WAN

III.1. En mode point-à-point :

III.1.a. HDLC

III.1.b. PPP

III.2. En mode circuit virtuel de bout-en-bout :

III.2.a. Frame Relay

III.2.b. ATM

IV. MPLS : commutation par VC dans le monde IP

V. Qualité de service

VI. Technologies xDSL

Frame Relay: présentation

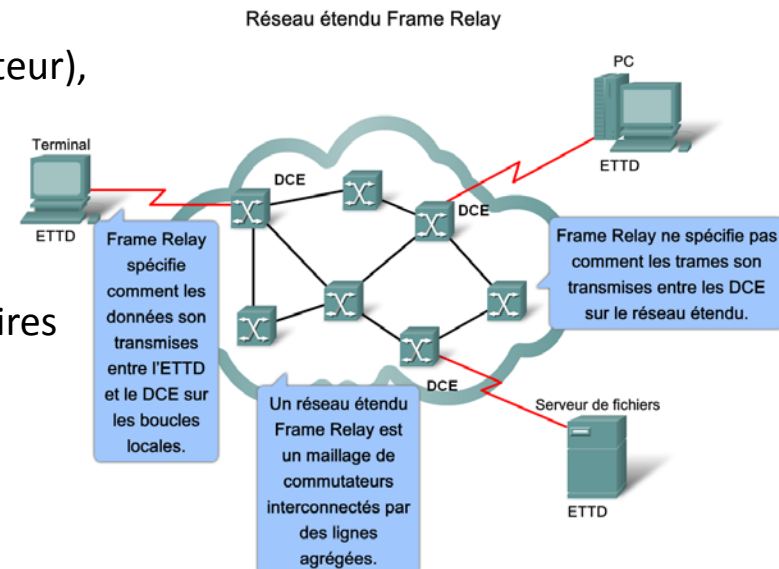
- **Objectif:** un service de telecommunication pour transmissions à faible coût du trafic intermittent entre LANs et entre end-points de WAN
- Correction d'erreur à la charge des end-points -> Accélération de la transmission
- En général, le réseau fournit un PVC: le client voit une connexion continue, sans payer pour une ligne louée permanente
- Le SP décide quelle route pour chaque trame jusqu'à sa destination et peut facturer selon l'usage.
- Une entreprise peut choisir un niveau de QoS – le niveau de priorité des frames est variable.
- FR peut fonctionner sur du T1 (fractionné ou complet)
- FR complémente et fournit un service entre le basic rate ISDN (128 Kbps) et ATM
- ATM opère de façon similaire mais de 155.520 Mbps à 622.080 Mbps.

Frame Relay: présentation

- FR a été un des protocoles WAN les plus utilisés en raison de:
 - son faible coût (p/r à lignes louées)
 - la simplicité de configuration des équipements utilisateurs
- La structure de frame FR est similaire à celle de LAP-D (juste absence de champ de contrôle).

Interconnexion de réseaux

- Les switches FR créent des VC pour connecter des LANs distants au travers d'un WAN.
- Le réseau FR existe entre un équipement LAN de bordure (ex routeur), et le switch de l'opérateur:
 - Différentes technologies sont utilisées par l'opérateur pour transporter les données entre les switches:
 - ex: frames FR transportées par un réseaux intermédiaires ATM



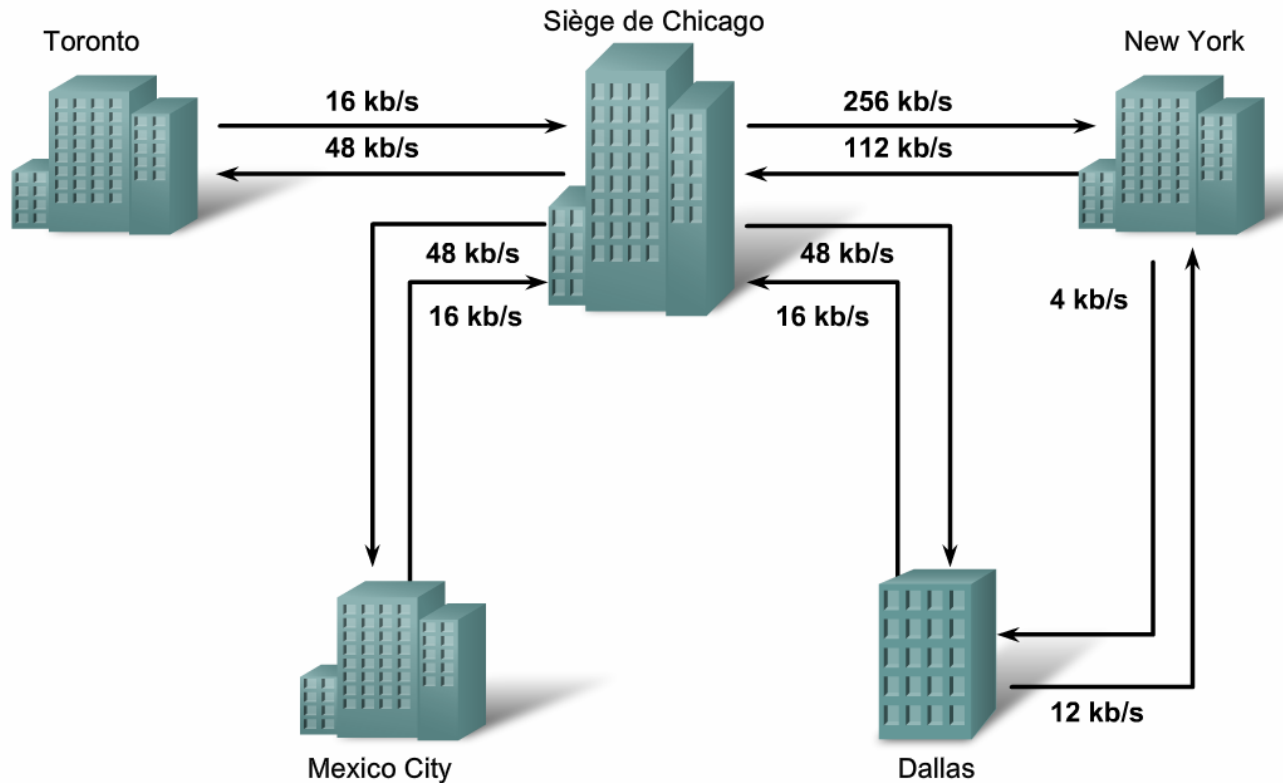
Frame Relay: présentation

Positionnement du marché

- FR vise à rendre efficace l'utilisation des ressources physiques, qui permettent aux telcos de sous-provisionner (*underprovisioning*) les services pour les clients, car il est peu probable que les clients utilisent les ressources 100% du temps, ou tous simultanément.
- FR a pu entraîner une mauvaise réputation à cause d'un overbooking excessif de BW par les telcos.
- Parmi les 1ers telcos à vendre FR: StrataCom (ensuite acquis par Cisco Systems) et Cascade Communications (Lucent Technologies).
- En juin 2007, AT&T était le plus gros fournisseur FR aux USA

Frame Relay: exemple

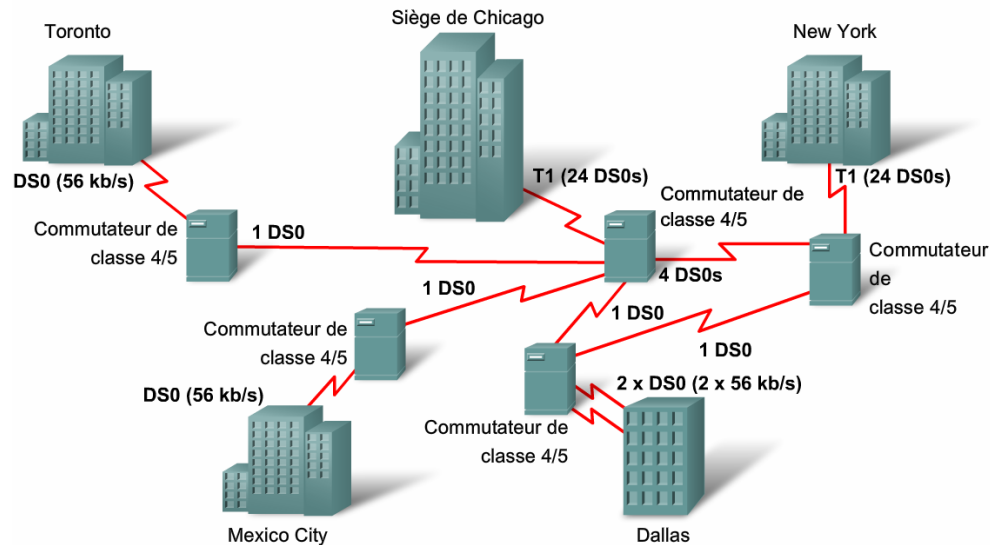
Exigences en matière de bande passante pour l'entreprise



1^{ère} caractéristique à prendre en compte: le besoin en bande passante de chaque site

Frame Relay: exemple

Exigences en matière de réseau étendu de la liaison spécialisée



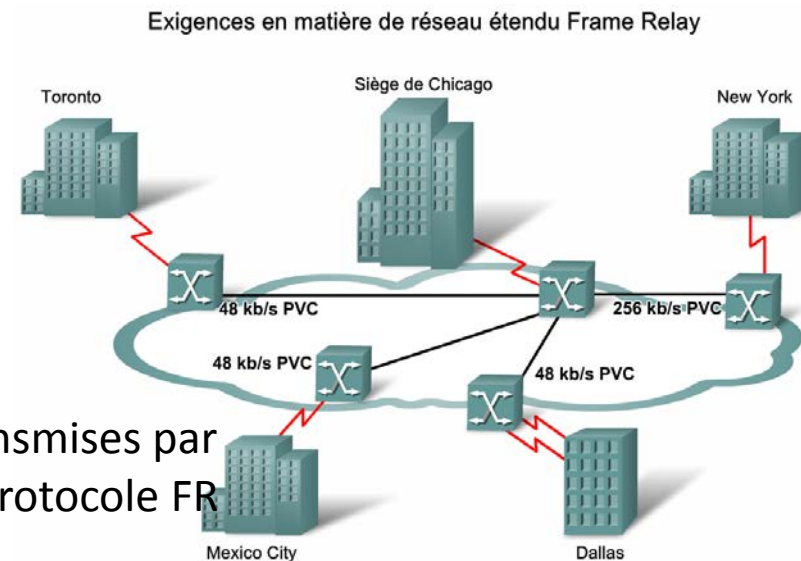
- Le NP fournit canaux DS0 entre centraux téléphoniques: aucun partage et la société paie pour l'ensemble du circuit de bout en bout quelle que soit la bande passante utilisée
- Lignes dédiées: peu de possibilités pour liaison un à plusieurs
- Manque d'efficacité:
 - le site de Chicago n'utilise que: 7 des 24 canaux DS0 disponibles de la liaison T1
 - NYC : 5/24
 - Dallas : 2 lignes pour relier les centraux tel pour NYC et Chicago

⇒ Liaisons dédiées limitent la flexibilité: nouveaux sites -> nouvelles installations -> long délai
Pour fiabilité du réseau: ajout de circuits redondants -> coût et complexité

Frame Relay: exemple

- Le réseau de la société utilise à présent Frame Relay avec des PVC.
- Solution FR économique:
 - clients ne paient que l'utilisation de la LL et la BW achetée au NP (vs. dédiées: LL+liaison réseau)
 - la distance source-dest n'a plus d'importance
 - lignes fournies par incréments de 64Kbits/s vs. FR: finesse dans l'offre VC (incr de 4Kbits/s)
 - partage de BW avec plus de clients - vs.- dédiées
 - moins d'éqt et moins de maintenance
 - => économies pour le NP

- Solution FR flexible grâce à VC:
 - filières connectées au nuage FR par LL
 - FR: extrémité de chaque liaison id par DLCI, pour tous les DLCI configurés, données transmises par le même port du routeur configuré selon protocole FR



Frame Relay: exemple

Coûts Frame Relay

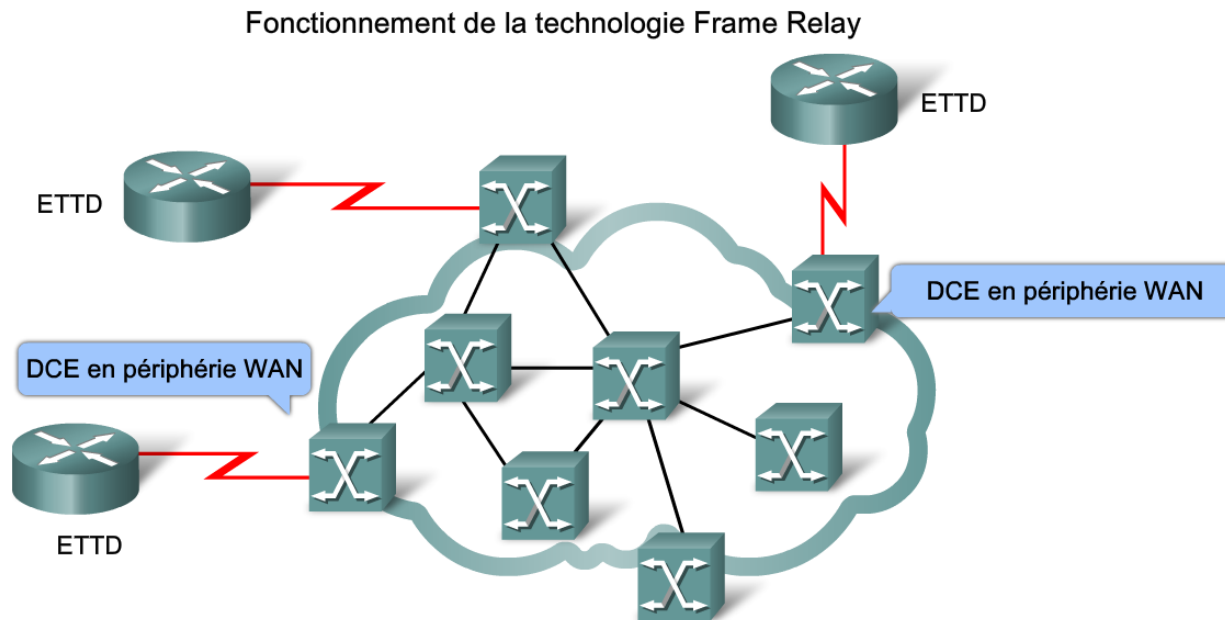
	RNIS 64 Kbits/s	Frame Relay 56 Kbits/s
Frais mensuels de boucle locale	\$185	\$85
Configuration FAI	\$380	\$750
Équipement	\$700	\$1600
Frais mensuels de FAI	\$195	\$195
Frais fixes	\$1080	\$2660
Frais mensuels	\$380	\$280

Équipement : Routeur RNIS 700 dollars*
Router Cisco 1600 dollars*

*dollars US

Frame Relay: fonctionnement

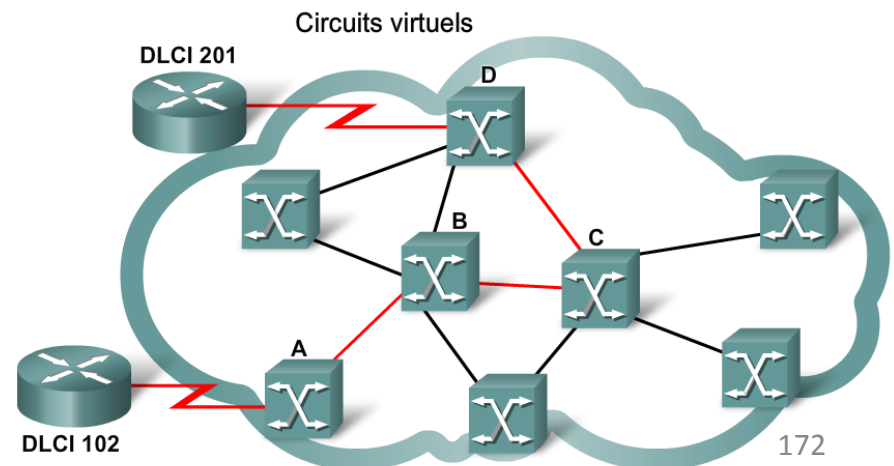
- Si FR interconnecte LAN, DTE est routeur.
- Connexion série (ligne louée T1/E1) connecte le routeur à un switch FR au POP le + proche du NP
- le NP interconnecte les switchs FR



- L'ETTD envoie des trames au commutateur DCE en périphérie du réseau étendu.
- Les trames se déplacent d'un commutateur à l'autre dans le réseau à destination du commutateur DCE situé en périphérie.
- Le DCE de destination livre les trames à l'ETTD de destination.

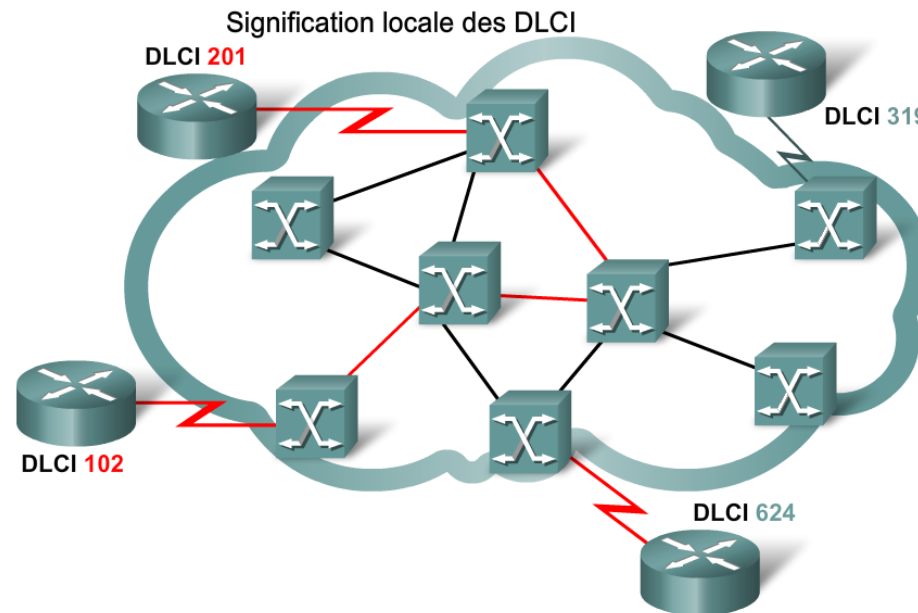
Frame Relay: circuits virtuels

- VC : connexion de 2 DTE par un réseau FR
- « virtuel » car ... -> connexion « logique »
- > partage de la BW entre les utilisateurs -> plus besoin de lignes physique dédiées
- Circuits virtuels commutés (SVC): établis de façon dynamique par l'envoi de messages de signalisation au réseau (CALL SETUP, DATA TRANSFER, IDLE, CALL TERMINATION)
- Circuits virtuels permanents (PVC): préconfigurés par l'opérateur et, une fois configurés, fonctionnent uniquement dans les modes DATA TRANSFER et IDLE.
- FR crée un VC en établissant la correspondance entre ports d'entrée et ports de sortie dans la mémoire de chaque commutateur
- > comment sont identifiés les différents nœuds et commutateurs ?



Frame Relay: signification locale des DLCI

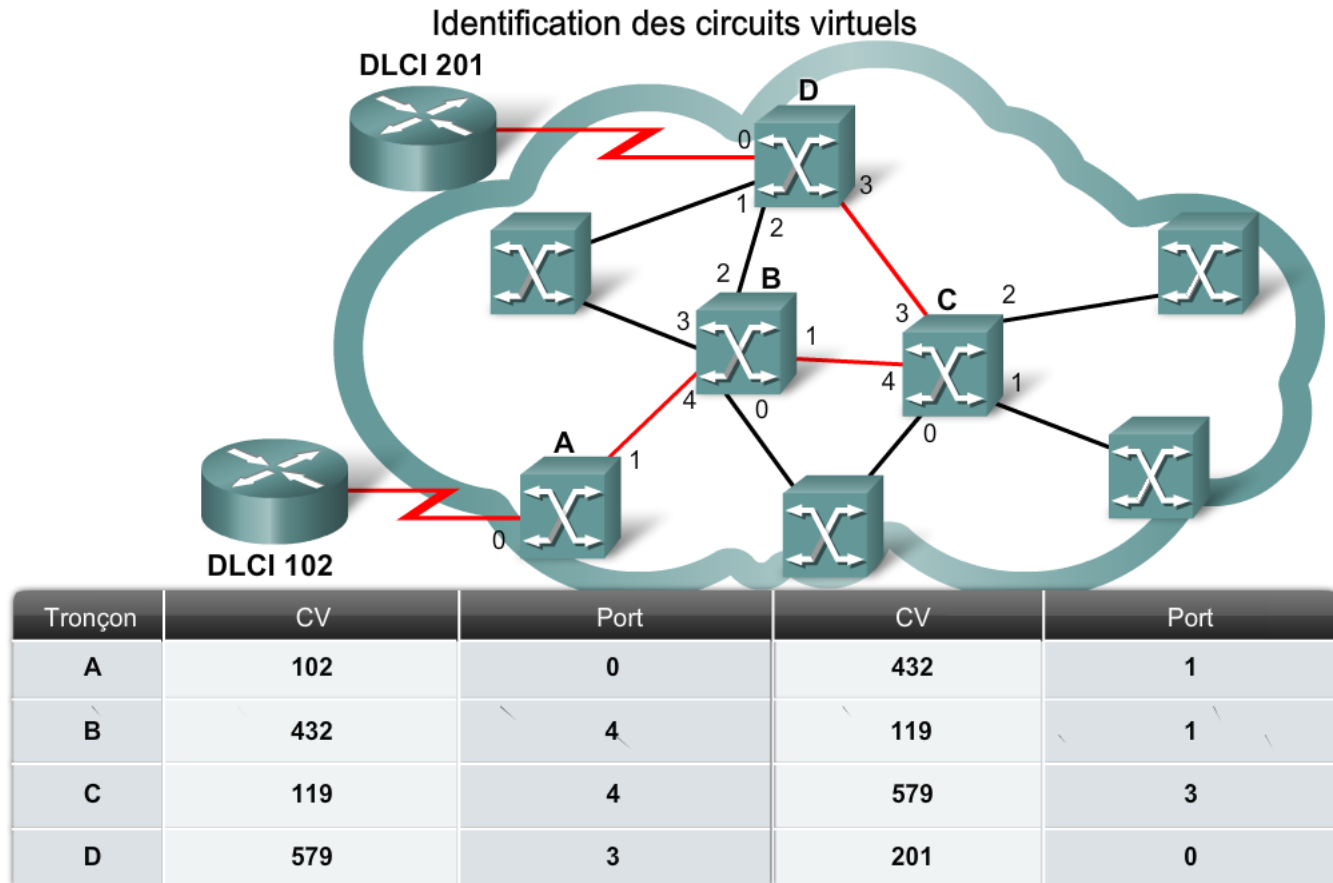
- DLCI identifient les VC
- DLCI généralement attribués par le SP FR (ex telco)
- les DLCI FR ont une signification locale: les valeurs ne sont pas uniques dans le WAN FR
- un DLCI identifie un VC sur un équipement situé à une extrémité
- Au-delà de la liaison, ce DLCI n'a aucune signification
- > 2 équipements reliés par un VC peuvent utiliser un DLCI différent pour désigner la même connexion



Les identificateurs DLCI ont une signification locale, ce qui signifie qu'ils sont spécifiques au canal physique sur lequel ils résident. Les équipements situés à l'autre extrémité d'une connexion peuvent donc utiliser les mêmes identificateurs DLCI pour identifier des circuits virtuels différents.

Frame Relay: identification des VC

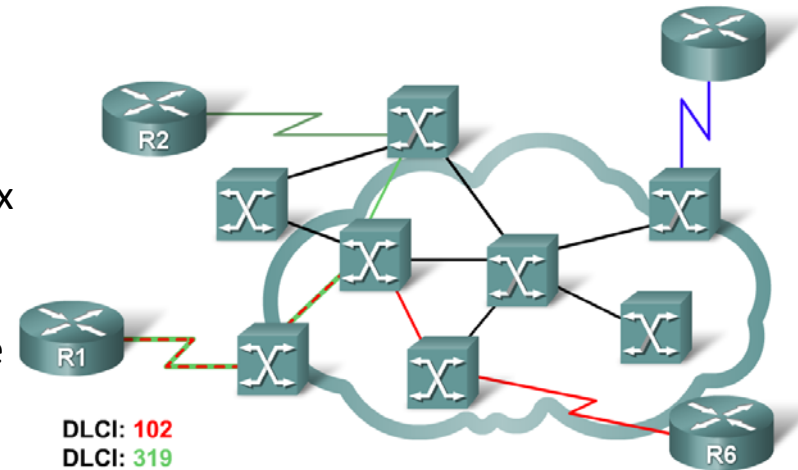
- FR identifie chaque VC par un DLCI
- le DLCI est stocké dans le champ adresse de chaque trame
- le SP FR attribue les DLCI entre 16 et 1007 (plages 0-15 et 1008-1023 réservées)



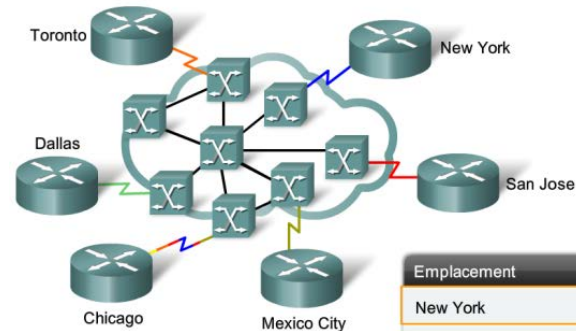
Frame Relay: circuits virtuels multiples

- Le réseau Frame Relay est statistiquement multiplexé:
1 trame à la fois, mais nombreuses connexions logiques possibles sur une même ligne physique
- un DTE peut être connecté à plusieurs périphériques finaux par différents circuits virtuels
 - > réduction de la complexité et du réseau
 - > solution économique pour remplacer réseaux à maillage (mesh networks) des lignes d'accès
- seulement une ligne d'accès et une interface pour chaque point d'extrémité
- avec FR, les clients ne paient que la BW qu'ils utilisent:
ils paient au nombre de ports utilisés
augmenter nb de ports -> payer pour plus grande BW
MAIS pas besoin de plus d'équipement, car les ports sont virtuels
vs. RNIS

Plusieurs circuits virtuels sur une seule ligne d'accès

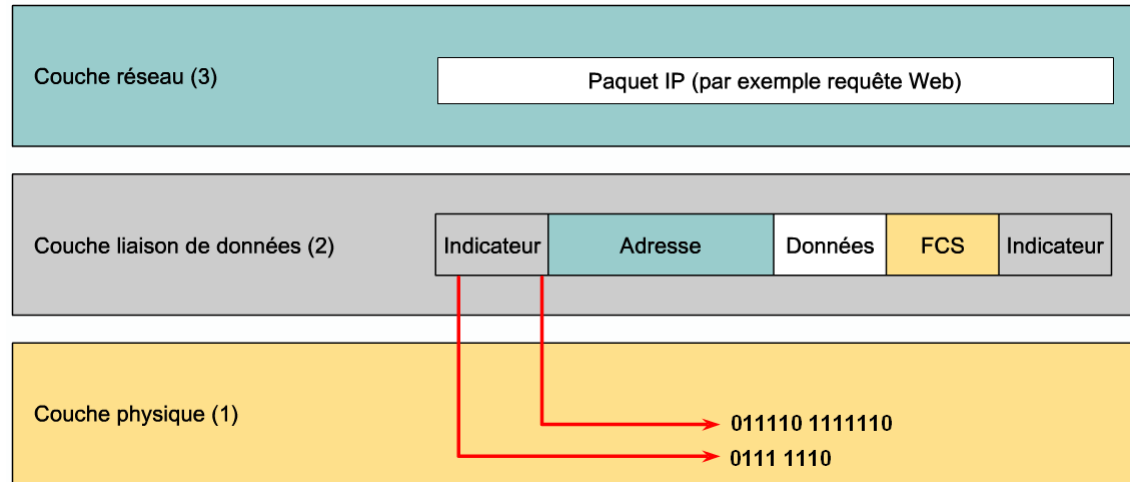


L'identificateur DLCI permet de distinguer plusieurs circuits virtuels sur une même ligne d'accès.



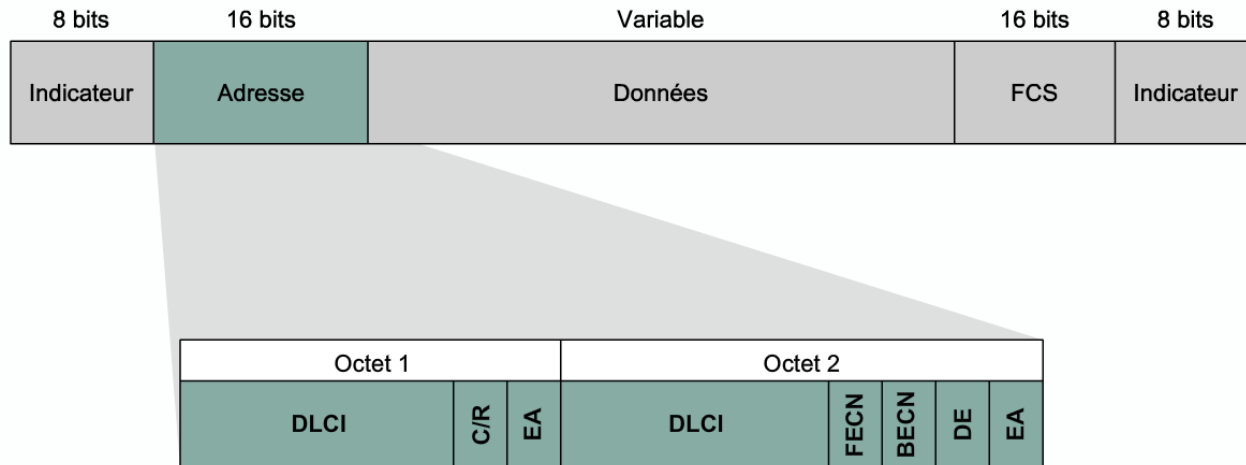
Emplacement	DLCI
New York	17
Toronto	18
Dallas	19
Mexico City	20
San Jose	175 21

Frame Relay: encapsulation



1. FR reçoit un paquet d'un protocole de couche 3
2. FR l'enveloppe avec un champ d'adresse contenant l'identificateur DLCI et une somme de contrôle
Des champs d'indicateurs de début et fin de la trame sont ajoutés - LAPF
3. Passage de la trame à la couche 1 pour le transport

Frame Relay: format de trame



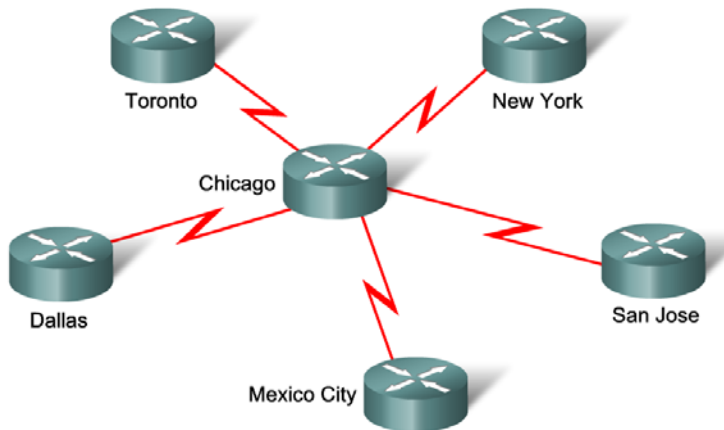
- le routeur CPE rajoute header et trailer FR au paquet de couche 3 -> envoi dans VC
- header et trailer définis par la norme ITU, intitulée Link Access Procedure for Frame Relay, LAPF
- header FR (champ d'adresse) contient :
 - DLCI : 10 bits. Extended address (EA): =1 pour DLCI sur 2B
 - C/R: non défini
 - Contrôle de congestion: 3 bits pour *congestion notification*
- pas d'avertissement envoyé à la source si abandon de trame (charge des couches plus hautes)

Frame Relay: topologies

- les réseaux FR rentables relient des 10nes voire des 100nes de sites
- tout réseau ou segment de réseau peut être vu comme:
topologie en étoile, à maillage global ou à maillage partiel

- Site central = concentrateur

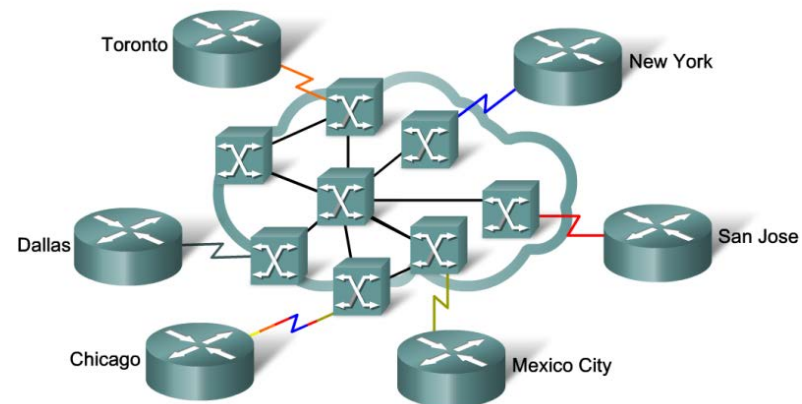
Topologie en étoile (Hub and Spoke)



Topologie en étoile : concentrateur avec 5 liaisons physiques (rayons)

- Le concentrateur de Chicago a une liaison d'accès avec plusieurs VC, un pour chaque site distant
- lignes sortant du nuage: connexions du SP FR vers locaux des clients. En général: 56 Kbits/s à E-1 (2,048 Mbits/s) et plus.
- le concentrateur ne doit pas oblig être au centre

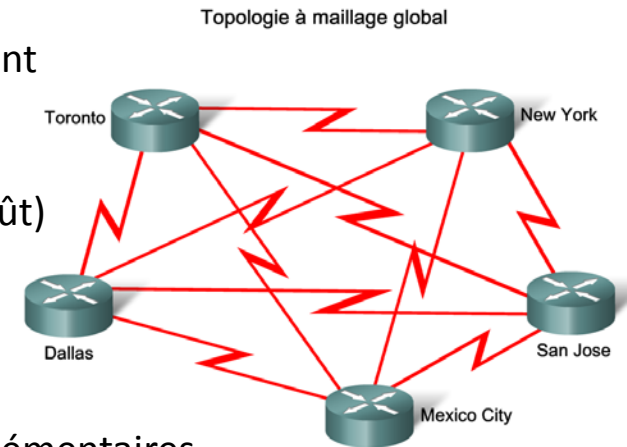
Topologie en étoile Frame Relay



Topologie en étoile Frame Relay : concentrateur avec une liaison physique comportant 5 circuits virtuels

Frame Relay: topologies

- topologie à maillage global avec lignes dédiées
- quand l'accès aux services doit être très fiable et que ces services sont dispersés géographiquement
- connecte un site à chacun des autres sites
 - > lignes louées pour les interconnexions (int série+lignes suppl->coût)

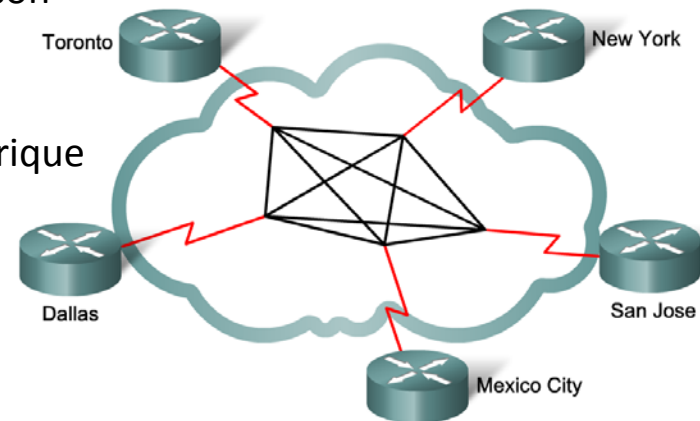


- Avec FR: plusieurs connexions possibles en configurant des VC supplémentaires sur chaque liaison existante
- mise à niveau logicielle -> évolution de la topologie en étoile en une topologie à maillage global, sans supplément de coût en matériel ou lignes dédiées
- VC utilisent le multiplexage statistique -> plusieurs VC sur une liaison d'accès

Maillage Frame Relay

- full mesh rarement réalisable pour grands réseaux car limite théorique du nb de VC par liaison est 1000

- > maillage partiel pour les grands réseaux:
plus d'interconnexions qu'en étoile mais moins qu'en full mesh



Frame Relay: mapping d'adresses

- Pour qu'un routeur puisse transmettre des données par le protocole FR, la correspondance entre le DLCI local et l'adresse de couche 3 de destination doit être connue.
- Ce mapping entre adresse et DLCI peut être réalisé de manière statique ou dynamique.
- ARP inverse (IARP):
 - obtient adresse couche 3 à partir de adresse couche 2, comme le DLCI dans réseaux FR
 - utilisé dans FR et ATM
 - adresses couche 3 nécessaires pour utiliser VC
- Mapping dynamique:
 - utilise IARP pour résoudre l'adresse de protocole réseau du saut suivant en une valeur DLCI locale
 - le routeur FR envoie demandes IARP sur son PVC pour détecter l'adr de niv 3 du périph distant
 - le routeur utilise les réponses obtenues pour compléter une table de mapping d'adresse en DLCI sur le routeur FR ou le serveur d'accès

Frame Relay: mapping d'adresses

- Mapping statique:

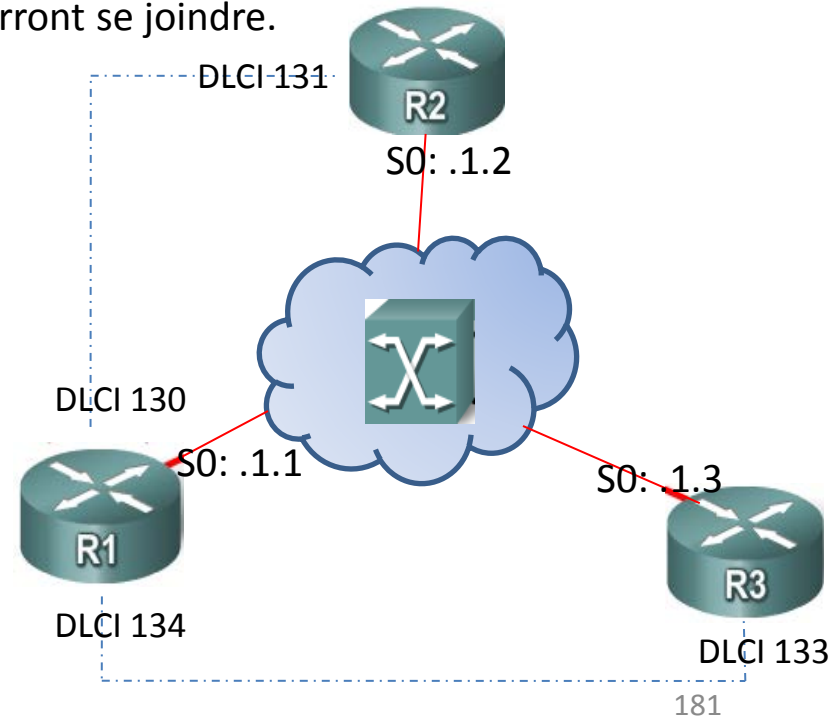
- mapping manuel statique entre l'adresse réseau du saut suivant et un DLCI local
- utile si un routeur n'intègre pas la résolution dyn inverse pour un protocole réseau spécifique
- ou pour une topo en étoile, pour routeurs situés sur les rayons (car pas de connexion pt à pt):

- Exemple du dernier cas:

- pas de VC défini de R2 à R3 -> R2 et R3 ne peuvent pas se joindre par interfaces séries
- > R2 et R3 ne peuvent pas se joindre car IARP ne peut connaître que l'adresse de R1.
- En établissant un mapping manuel de R2 à R3, ils pourront se joindre.

RA2
interface Serial0 ip address 192.168.1.2 255.255.255.0 encapsulation frame-relay frame-relay map ip 192.168.1.3 131
RA3
interface Serial0 ip address 192.168.1.3 255.255.255.0 encapsulation frame-relay frame-relay map ip 192.168.1.2 133

```
RA2#show frame-relay map
Serial0 (up): ip 192.168.1.1 dlci 131(0x83,0x2030), dynamic,
broadcast,, status defined, active
Serial0 (up): ip 192.168.1.3 dlci 131(0x83,0x2030), static,
CISCO, status defined, active
```

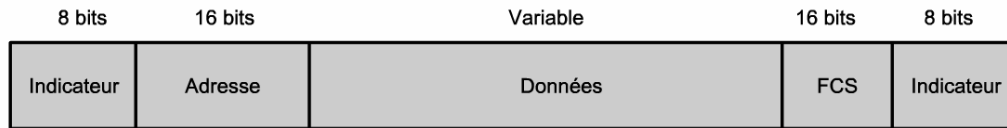


Frame Relay: Local Management Interface (LMI)

- Concept FR: transmettre données à commutation de paquets avec un retard min de bout-en-bout
- Quand FR est devenu technologie séparée (et plus seulement composant de RNIS), il fallait que les DTE puissent acquérir dynamiquement informations sur l'état du réseau
- > ensemble de ces extensions = LMI
- Le DTE et le DCE s'échangent des messages LMI à l'aide d'identificateurs DLCI réservés
- Plusieurs interfaces LMI mutuellement incompatibles
- > Type LMI configuré sur routeur doit être le même que celui du SP
- 3 types:
 - Cisco: extension LMI d'origine
 - Ansi: correspondant à la norme ANSI T1.617 annexe D
 - q933a: correspondant à la norme ITU Q.933 annexe A

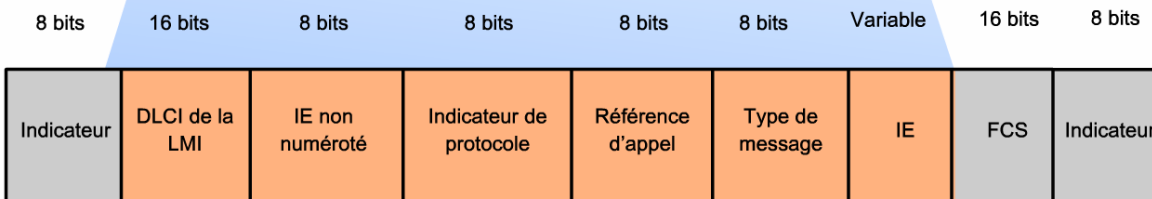
Frame Relay: format de trame LMI

- Les messages LMI sont contenus dans une variante des trames LAPF.
 - Le champ d'adresse contient l'un des identificateurs DLCI réservés.
 - Il est suivi des champs de contrôle, d'indicateur de protocole et de référence d'appel, restant inchangés.
 - Le quatrième champ indique le type de message LMI.
-
- Les messages d'état facilitent la vérification de l'intégrité des liaisons logiques et physiques.
 - Ces informations sont vitales au sein d'un environnement de routage, car les protocoles de routage fondent leurs décisions sur l'intégrité des liaisons.



La trame Frame Relay standard constitue la base d'une trame LMI

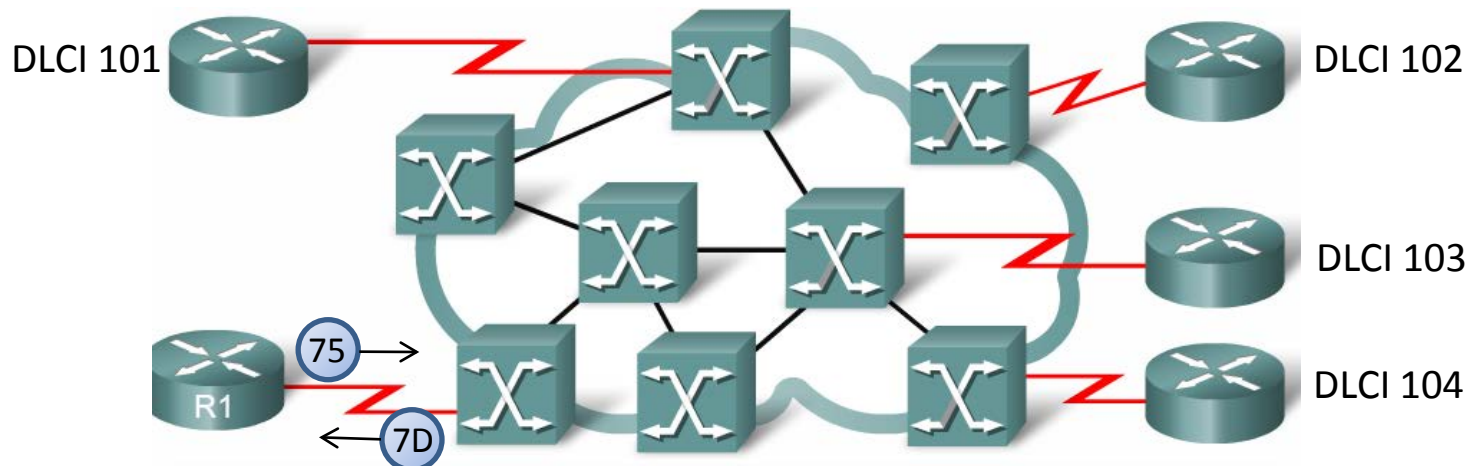
Identificateurs de circuit virtuel	Types de circuits virtuels
0	LMI (ANSI, ITU)
1..15	Réservé pour une utilisation ultérieure
992..1007	CLLM
1008..1022	Réservé pour une utilisation ultérieure (ANSI, ITU)
1019..1020	Multidiffusion (Cisco)
1023	LMI (Cisco)



Frame Relay: LMI et InARP pour mapping d'adresses

- Les messages d'état LMI associés aux messages d'ARP inverse permettent à un routeur d'établir la correspondance entre les adresses de couche réseau et de couche liaison de données.

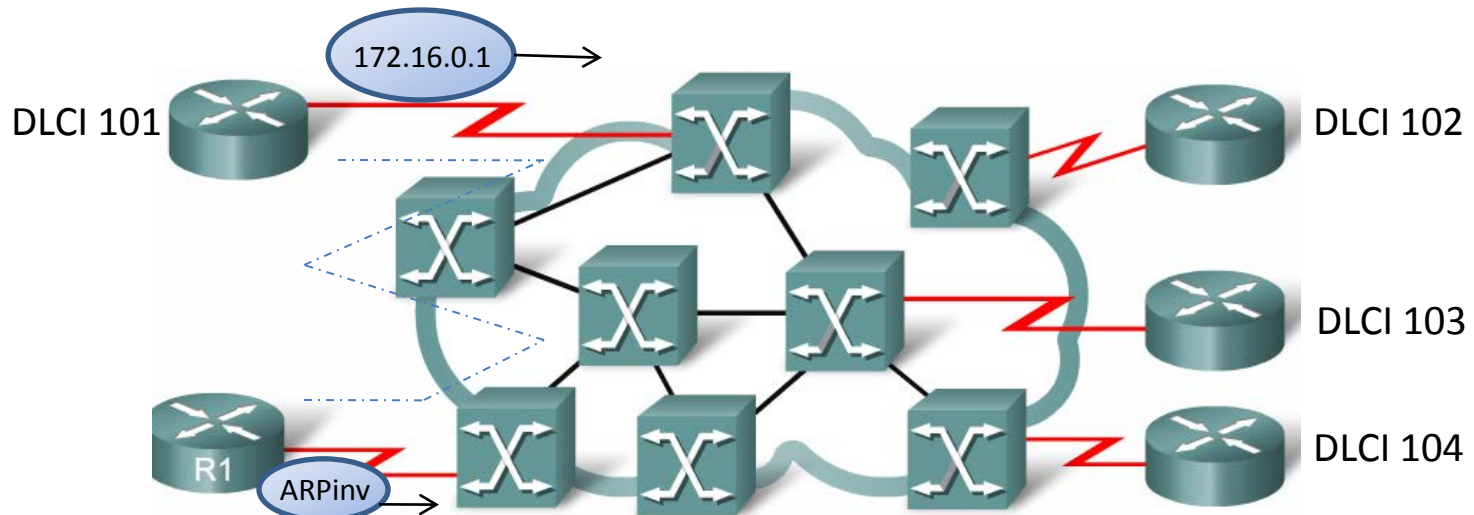
- 1 L'ETTD envoie un message d'interrogation d'état (75) au DCE
- 2 Le DCE répond par un message d'état (7D) qui comprend des identificateurs DLCI configurés
- 3 **L'ETTD est informé des circuits virtuels dont il dispose**



DLCI	État
101	Actif
102	Actif
103	Actif
104	Actif

Frame Relay: LMI et InARP pour mapping d'adresses

- 1 L'ETTD envoie une résolution d'adresse inverse à un circuit virtuel pour le mapper à une adresse réseau
- 2 L'ETTD distant répond en transmettant l'adresse de couche 3
- 3 L'ETTD effectue le mappage de couche 2 à couche 3
- 4 Le processus est répété pour chaque circuit virtuel et chaque protocole de couche 3



DLCI	État
101	Actif
102	Actif
103	Actif
104	Actif

Frame Relay: Résolution des problèmes d'accessibilité

- Les réseaux Frame Relay, ATM et X.25 sont des **réseaux NBMA** (*non-broadcast multiple access*)
 - > ne permettent le transfert de données que d'un ordinateur à l'autre sur un VC ou au travers d'un périphérique de commutation
 - > pas de prise en charge du trafic de type diffusion ou multidiffusion: un paquet ne peut donc pas atteindre toutes les destinations
 - > duplication manuelle des paquets pour obtenir la diffusion
- **mot-clé *broadcast*** à rajouter dans la configuration d'un VC pour le **transfert des mise à jour de routage**:

```
R1(config-if)#frame-relay map ip 192.168.1.2 102 broadcast
```
- Les nuages NBMA présentent généralement une topologie en étoile appelée également *Hub and Spoke*
- **Découpage d'horizon**: technique de prévention de boucles de routage pour réseaux avec protocole DV:
 - une mise à jour du routage reçue sur une interface physique n'est pas retransmise par la même interface

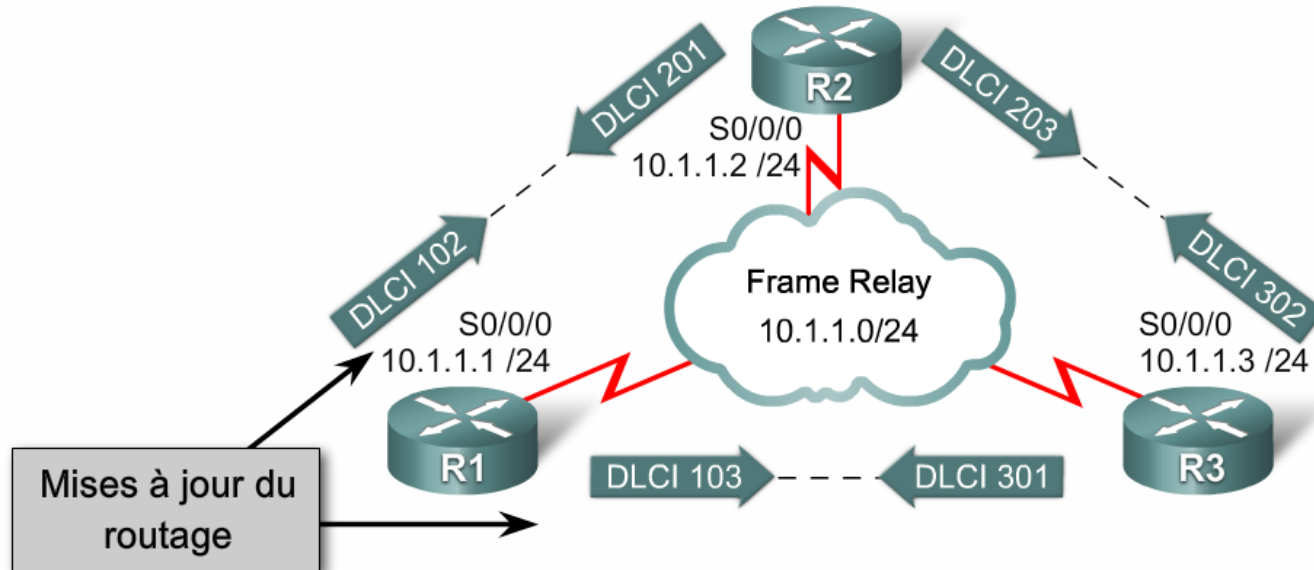
Frame Relay: Résolution des problèmes d'accessibilité

Problèmes:

- La mise à jour reçue par une interface physique n'est pas retransmise par cette même interface
- Le trafic de diffusion doit être dupliqué pour chaque connexion active

Solutions:

- désactivation du mécanisme de découpage d'horizon
mais: que IP le permet ET risque de boucles de routage dans le réseau
- utiliser une topologie *full mesh*
mais: coûteuse car requiert un plus grand nombre de PVC
- la meilleure solution: les sous-interfaces



Frame Relay: Résolution des problèmes d'accessibilité

- FR peut **partitionner une interface physique en plusieurs interfaces virtuelles: les sous-interfaces**
- une sous-interface = une interface logique, correspondant à un VC, associée à une interface physique
- configuration de sous-interfaces sur les routeurs
- Chaque sous-réseau point à point peut recevoir une adresse réseau unique.
- Les paquets reçus sur une interface physique peuvent alors être réacheminés sur cette même interface
- Sous-interfaces FR point-à-point:
 - 1 PVC par sous-interface
 - Chaque paire de routeurs point à point réside sur son propre sous-réseau et chaque sous-interface point à point ne dispose que d'un identificateur DLCI.
 - Chaque VC correspond à un sous-réseau séparé
 - > le trafic des mises à jour du routage n'est pas soumis à la règle du découpage d'horizon.

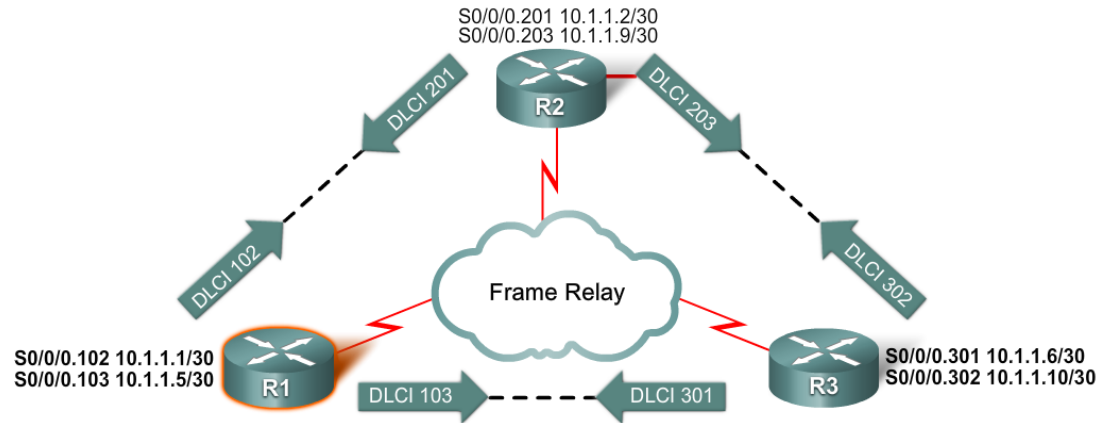
Frame Relay: Résolution des problèmes d'accessibilité

Configuration de sous-interfaces point-à-point

```
interface s0/0/0
  no ip address
  encapsulation frame-relay
  no shut
exit
```

```
interface s0/0/0.102 point-to-point
  ip address 10.1.1.1 255.255.255.252
  frame-relay interface-dlci 102
exit
```

```
interface s0/0/0.103 point-to-point
  ip address 10.1.1.5 255.255.255.252
  frame-relay interface-dlci 103
exit
```



Frame Relay: Paiement

- le client ne fait qu'acheter des services FR au SP et ne voit pas le fonctionnement interne du réseau (technologies à haut débit comme T1, T3, ATM, SDH)

- Débit d'accès ou vitesse du port : pour le client, le SP fournit une connexion série, ou liaison d'accès, au réseau FR sur une ligne louée. La vitesse de la ligne est assujettie au débit d'accès ou à la vitesse du port.

débit d'accès= débit auquel les circuits accèdent au réseau Frame Relay

Ces débits sont généralement de 56 Kbits/s, de 1,536 Mbits/s (T1) ou d'un multiple de 56 Kbits/s ou 64 Kbits/s (T1 fractionnée). Les vitesses des ports sont cadencées sur le commutateur Frame Relay.

Il n'est pas possible d'envoyer des données à une vitesse supérieure à celle du port.

- Débit de données garanti (CIR ou *Committed Information Rate*) : les clients négocient ce débit avec leurs SP pour chaque PVC.

CIR = débit de données que le réseau doit garantir au client

Le fournisseur de services garantit que le client peut envoyer des données au débit garanti. Toutes les trames reçues à un débit égal ou inférieur au CIR sont acceptées.

- Avantage de FR: les clients se partagent la BW inutilisée du réseau, en général gratuitement
-> les clients peuvent ainsi bénéficier de rafales (*burst*) supérieures à leur CIR

Frame Relay: Paiement

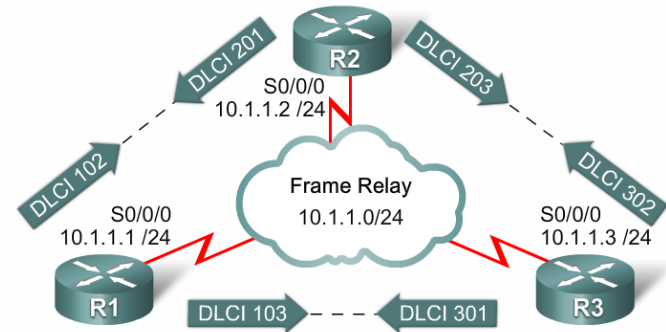
- Le client paie:

- Débit d'accès (vitesse du port): coût de la liaison d'accès du DTE au DCE
- PVC: Quand un VC est établi, le supplément de coût pour augmenter le débit de données garanti est en général faible (par petits incréments de 4 Kbits/s)
- CIR: les clients choisissent en général un CIR inférieur au débit d'accès, pour bénéficier des rafales de données

-Exemple:

- une ligne d'accès à 64 Kbits/s entre son DTE et le DCE du SP par un port série S0/0/0
- 2 ports virtuels à 32 Kbits/s et 16 Kbits/s
- un CIR de 48 Kbits/s sur l'ensemble du réseau FR
- Surréservation (*overbooking*): les SP vendent plus de BW qu'ils n'en disposent
-> congestion et abandon de trafic (frame dropping)

Frais de Frame Relay – Exemple



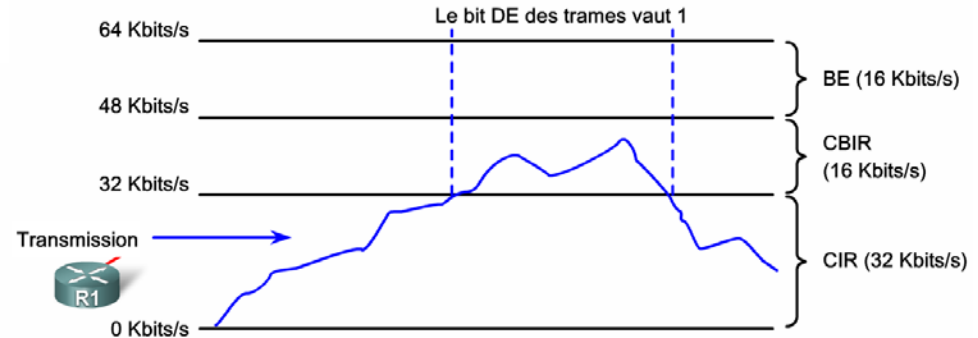
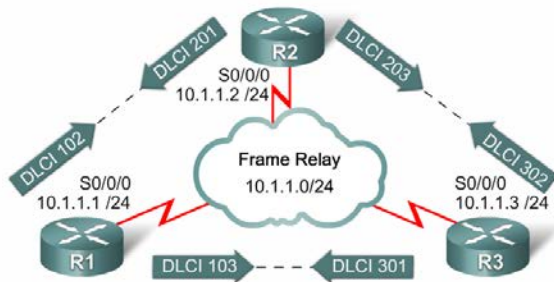
Trois éléments facturables	
Boucle locale	64 Kbits/s
Deux ports	DLCI 102 DLCI 103
Débit de données garanti (CIR)	48 Kbits/s

CIR de chaque circuit virtuel permanent	
DLCI du circuit virtuel permanent	Débit de données garanti (CIR)
DLCI 102	32 Kbits/s
DLCI 103	16 Kbits/s
Débit de données total garanti	48 Kbits/s

Frame Relay: data burst

- gros avantage de FR: partager entre les clients toute la BW inutilisée du réseau
 - > envoi gratuit de *data bursts* supérieurs à leur CIR
 - la rafale doit durer moins de 3 à 4s
 - on parle de **CBIR (Committed Burst Information Rate)** et de débit garanti en excès (*Burst Excess*):
 - le CBIR est un débit négocié en plus du CIR que le client peut utiliser pour de courtes rafales
 - BE: BW disponible au-dessus du CBIR jusqu'au débit d'accès de la liaison.
- Contrairement au CBIR, ce surplus de débit n'est pas négocié: trames transmises à ce débit, mais particulièrement susceptibles d'être abandonnées

- ex: DLCI 102 a un CIR de 32 Kbits/s avec un supplément de CBIR de 16 Kbits/s pour un total de 48 Kbits/s. Au-delà de 3-4s, les trames transmises à ce débit ont leur bit d'éligibilité à la suppression (Discard Eligible) mis à 1.

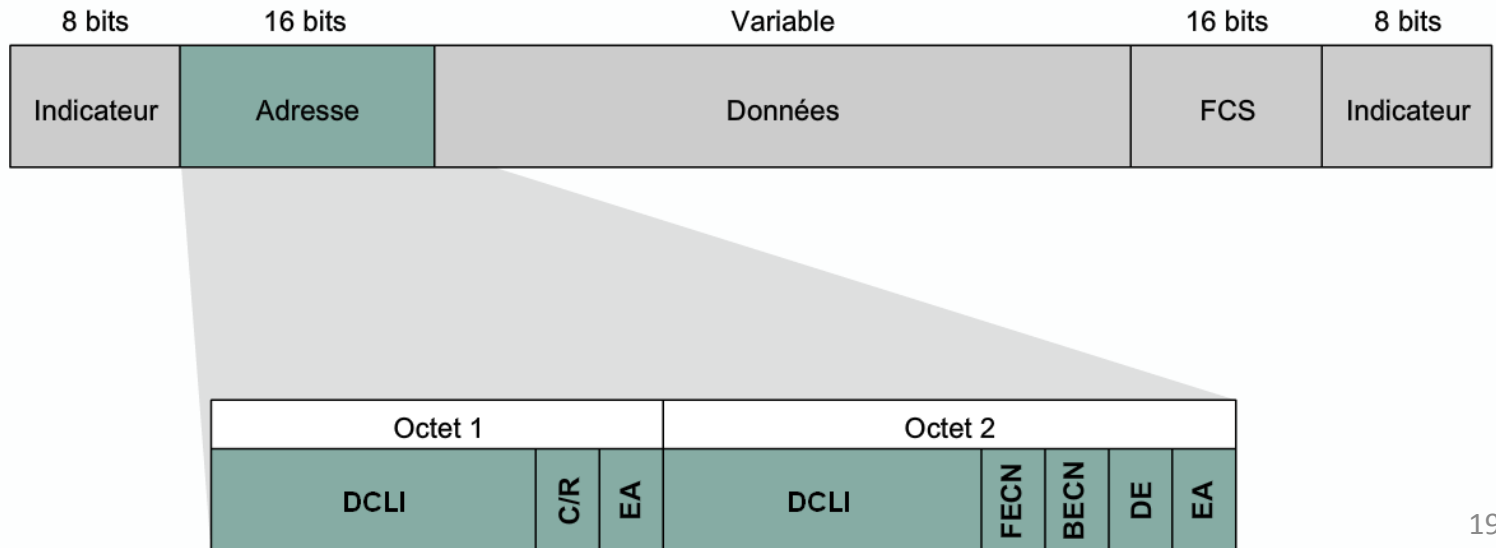


DLCI du circuit virtuel permanent	Débit de données garanti (CIR) normal	Exemple de débit garanti en rafale (CBIR)	BE
DLCI 102	32 Kbits/s	48 Kbits/s	16 Kbits/s
DLCI 103	16 Kbits/s	0 Kbits/s	48 Kbits/s
	Toutes les trames sont acheminées	Les trames sont acheminées, mais marquées par le bit DE	Les trames seront très probablement abandonnées

Frame Relay: Contrôle de congestion

- FR réduit la charge de contrôle du réseau par la mise en œuvre de mécanismes de notification de congestion simples plutôt qu'un contrôle de flux explicite par circuit virtuel:
Forward Explicit Congestion Notification (FECN) et *Backward Explicit Congestion Notification (BECN)*
- Mécanismes contrôlés par un seul bit dans l'en-tête de trame
- le switch détecte la congestion -> peut prendre les mesures nécessaires
- bit d'éligibilité à la suppression (DE) (1 si trame moins importante)

Trame Frame Relay standard

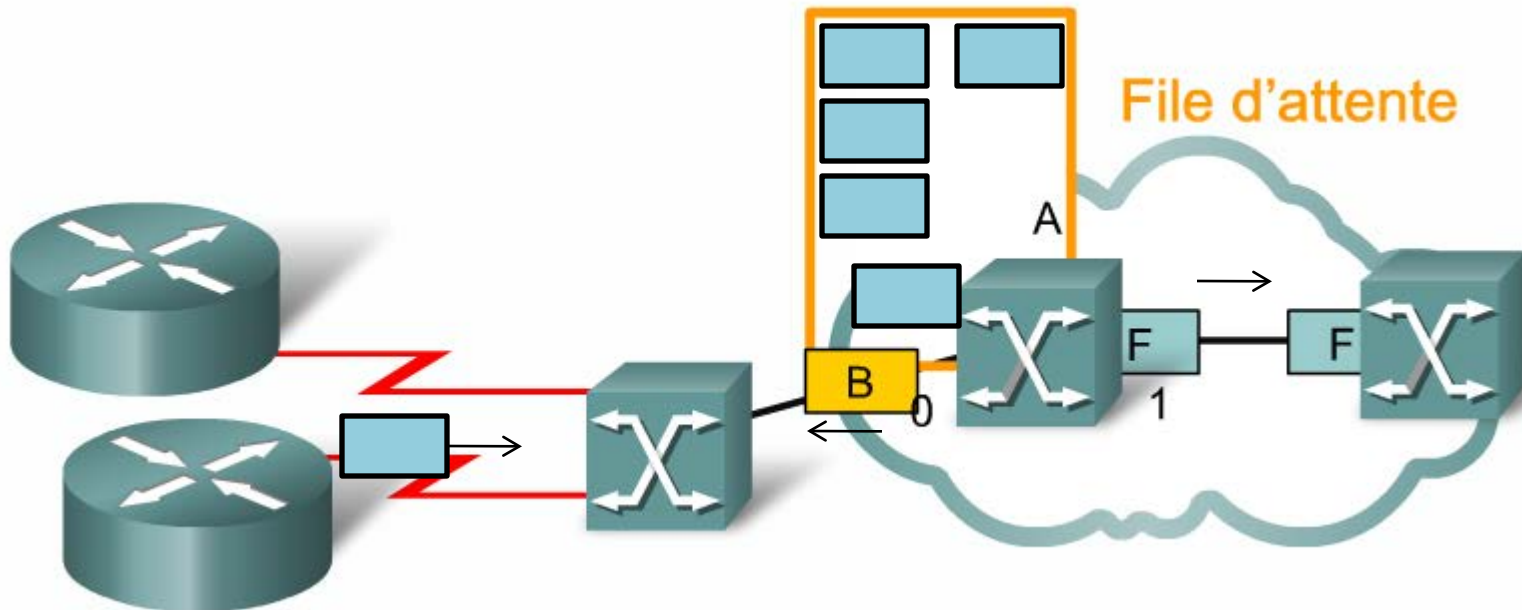


Frame Relay: Contrôle de congestion

- trames arrivant au switch mises en file d'attente (en tampon) avant d'être transférées
- > accumulation excessive possible -> retards -> retransmissions inutiles -> et même effondrement du débit (congestion collapse)
- => Pour éviter ce problème, Frame Relay intègre une fonction de contrôle de congestion.

Contrôle de la bande passante FR : mise en file d'attente

- 1 Tandis que le commutateur A place une trame de grande taille sur l'interface 1, les autres trames destinées à cette interface sont mises en file d'attente.
- 2 Les équipements en aval sont informés de la file d'attente en configurant le bit FECN.
- 3 Les équipements en amont sont informés de la file d'attente en configurant le bit BECN, même s'ils n'ont pas contribué à l'encombrement.



Plan

I. Présentation des WAN

II. Les interfaces de la couche physique

III. Protocoles de niveau 2 dans les WAN

III.1. En mode point-à-point :

III.1.a. HDLC

III.1.b. PPP

III.2. En mode circuit virtuel de bout-en-bout :

III.2.a. Frame Relay

III.2.b. ATM

IV. MPLS : commutation par VC dans le monde IP

V. Qualité de service

VI. Technologies xDSL

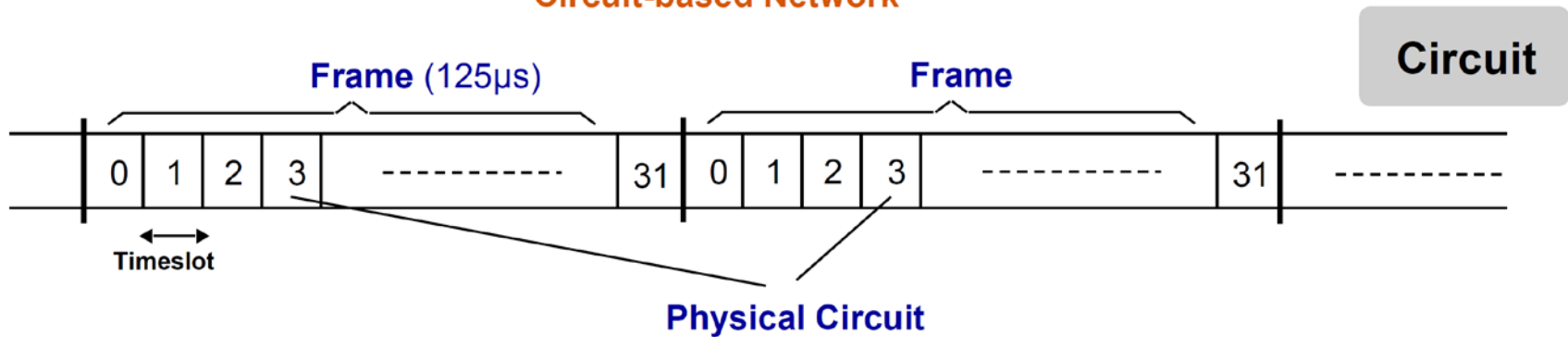
ATM: Introduction

- 2 techniques différentes: routage de paquets et commutation de paquets/trames
- Routage: souple car chaque paquet transporte l'adresse du dest-> paquet pas égaré MAIS QoS difficile
- Commutation de paquets avec connexion: QoS facilement assurée MAIS pb de la mise en place du chemin (VC)
- Chemin ouvert par une procédure de *signalisation*: on signale l'ouverture d'un chemin à « marquer »
-> la signalisation exige ressources importantes -> réseaux à commutation de paquets plus chers que routage

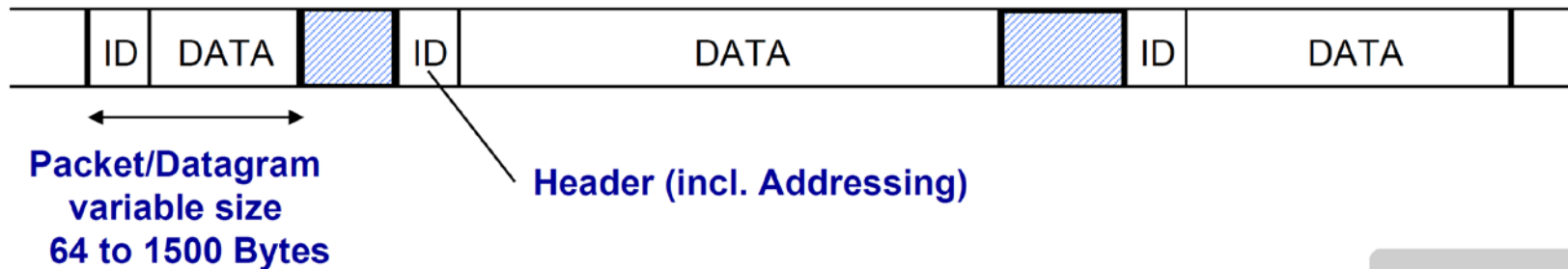
- Ces 2 catégories se sont développées en parallèle: au départ peu de concurrence
- Avec le temps, routage -> Internet -> étendues au transport d'applis synchrones (téléphonie et video)
- Aujourd'hui, tous 2 en concurrence, puis convergence, pour applis multimédia

Circuits / Paquets / Cellules

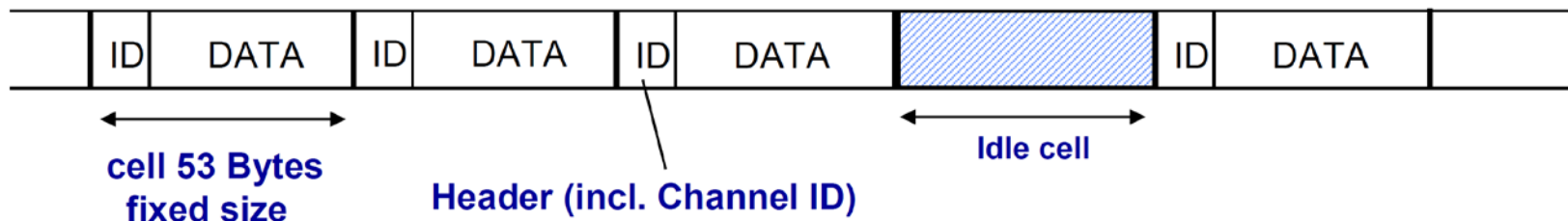
Circuit-based Network



Packet-based Network (ex: Ethernet, x25, IP)



ATM-based Network



ATM: Objectifs de départ

1 - Pouvoir transporter de manière efficace (?) tout type de flux

2 - Repondre aux exigences des services synchrones, donc maitriser débits / délais / gigue

Ex: Lien a 2Mbps, Packet 1500 bytes (12000 bits), delai=6ms

3 - Optimiser la bande passante

DONC ceci a abouti aux caractéristiques suivantes:

→ Réseau asynchrone (mode circuits mais circuits virtuels)

→ Cellules de taille fixe

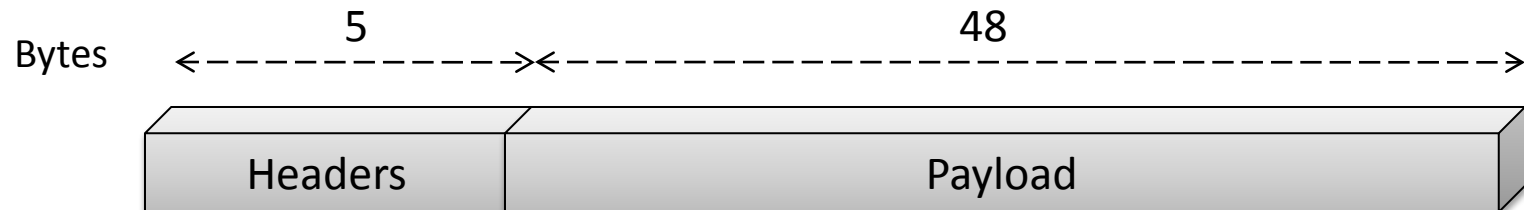
→ Traffic Management (QoS)

ATM: Principes

- ▶ ATM est **Asynchrone** en référence à la commutation de circuits
- ▶ Le format fixe des cellules permet un **multiplexage temporel très précis** de la bande passante entre les applications et une **gestion déterministe des délais**.
→ avantage par rapport à commutation/routage de paquets (de taille variable)
- ▶ Contrairement aux circuits synchrones, lorsqu'une source de trafic n'émet pas, elle ne consomme pas de bande passante
- ▶ ATM a dès le départ pris en compte tous les aspects de l'Intégration de Services (Notion de RNIS Large Bande) --> différenciation des service, **Traffic Management (TM)**
- ▶ ATM est aujourd'hui essentiellement utilisé dans les **réseaux d'accès des technologies multi-services** (Wireless-3G, ADSL), là où les limitations et le coût de la bande passante imposent une allocation fine des ressources du réseau en fonction des applications.

ATM : Principes

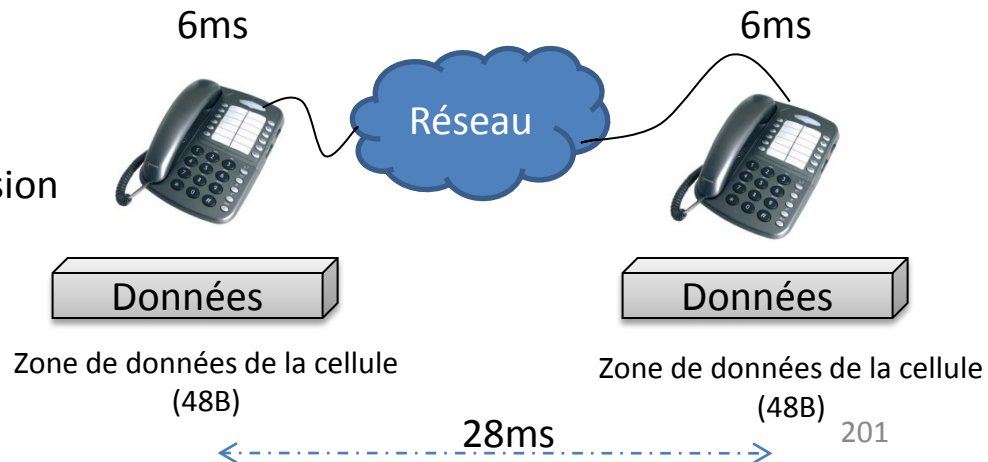
- Le flux d'info multiplexé est structuré en petits blocs, ou cellules.
- Assignées à la demande, selon l'activité de la source et les ressources possibles.
- La commutation de cellules est une commutation de trames assez particulière: de petite taille constante.
- 53B, avec 5 d'entête et 43B de données.



ATM : Principes

- Très faible longueur de la cellule explicable
- **Exemple avec parole téléphonique requérant 64Kbits/s :**
 - Application isochrone avec 2 contraintes:
 - synchronisation très forte des données: émission 1B/125 μ s, doivent arriver toutes les 125 μ s
 - délai de propagation <28ms pour éviter les problèmes liés à la transmission sur grande distance (suppression des échos, adaptation, etc...)
- Le temps de transit des B pour la parole sortant d'un combiné téléphonique se décompose en:
 - un tps de remplissage de la cellule par les octets qui sortent du combiné tel toutes les 125 μ s
 - > 6ms pour remplir 48B
 - un tps de transport de la cell dans le réseau
- > reste seulement 22ms de délai de propagation sur le réseau lui-même

- Signal transmis sur câble électrique à $2 \cdot 10^8$ m/s
 - > 4400km au max
- Distance augmentée avec équipement de suppression de l'écho, adaptation, ...



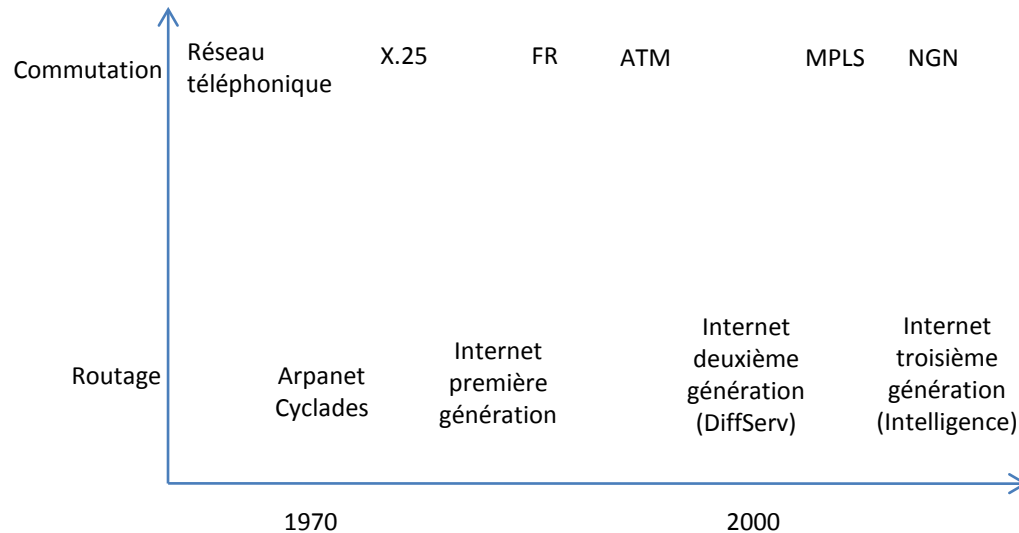
X.25 puis Frame Relay puis ATM

- Conçu fin 1980, lancé début 90s avec gros battage: devait résoudre tous les pbs réseaux-télécoms en intégrant voix, données, TV câblée, etc...
- Ca n'a pas été le cas car: pbs de mauvais timing, technologie, implémentation et politique
- Répondait au pb de la QoS sur Internet
- ATM a eu plus gros succès que OSI, et est maintenant largement utilisé en téléphonie, svt pour paquets IP

- Parallèlement à la standardisation ATM, grosses compagnies mondiales ont investi en R&D
 - > il y a dans les réseaux énormément d'équipement ATM haute-perf (ATM switchs à xTbits/s)
- Les réseaux dorsaux Internet doivent distribuer le trafic à très haut débit -> plusieurs dorsales d'ISP utilisent beaucoup ATM
- Principalement utilisé pour transport interne des flux, les utilisateurs n'en ont souvent pas conscience, mais ATM est là est encore bien vivant.

ATM: Evolution

- Les techniques de routage n'ont que peu changé, mais la commutation a bcp évolué:
 - 1^{ère} grande norme: X.25 dans les années 1980
 - Puis révolution en 1988 avec adoption du mode de transfert asynchrone: ATM



ATM: Evolution

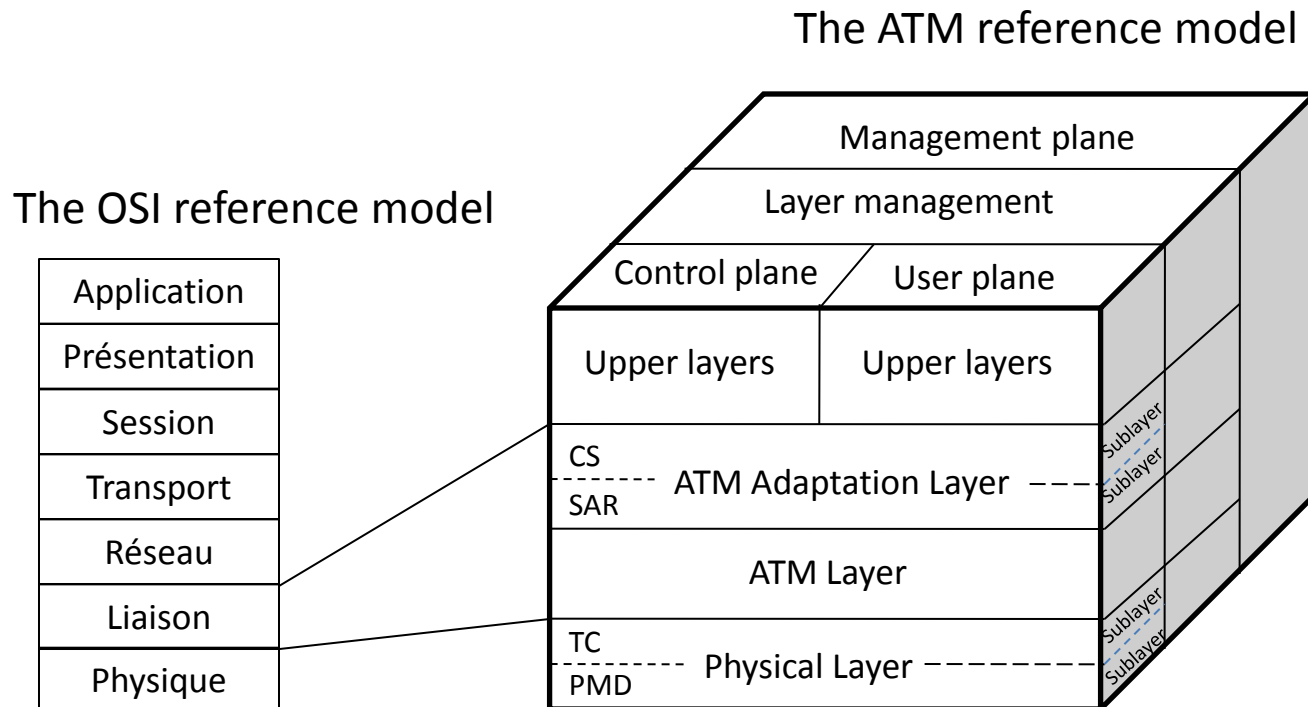
- Le monde des télécoms admet, depuis le début des années 2000, que les réseaux doivent posséder des interfaces IP
 - > Débat: quelle façon de transporter les paquets IP ?
 - Le monde des télécoms propose d'encapsuler le paquet IP dans une trame, transporter et décapsuler à l'arrivée.
 - Le cas de l'encapsulation dans un réseau ATM demande une étape supplémentaire, consistant à découper le paquet IP
 - > performance bottleneck: **SAR** le plus rapide à 10Gbit/s et possibilités en traffic shaping limitées.
 - MPLS a pris beaucoup de points techniques faisant la force d'ATM.**
- ⇒ Les réseaux de télécoms sont passés d'une techno circuit à une techno paquet. Malgré le succès du transfert ATM, optimisé pour le multimédia, l'utilisation du paquet IP est devenue incontournable. La divergence avec le monde informatique provient de la façon de transporter le paquet IP pour assurer une QoS.

ATM: Caractéristiques

- Mode avec connexion: cellule transmise qu'une fois que VC ouvert
- La référence d'un circuit virtuel comporte 2 parties:
 - le numéro VCI (*Virtual Circuit Identifier*): identificateur de circuit virtuel
 - le numéro VPI (*Virtual Path Identifier*): identificateur de chemin virtuel
- ATM étant en mode connexion, avant toute émission de cell, une connexion doit être mise en place:
 - une association entre les références d'entrée et de sortie du réseau doit être définie.
- Routage de la cell de supervision -> met en place le VC, est effectué par des tables de routage
- Cette cell détermine pour chaque nœud l'association entre le ports d'entrée et le port de sortie.
- Ces associations sont regroupées dans la table de commutation.

Le modèle de référence ATM

- **Cette architecture comporte 3 plans: plan utilisateur, plan de contrôle et plan de gestion.**
- Un plan est un réseau. Les 3 réseaux sont multiplexés sur un même réseau physique pour économie, le multiplexage indiquant la simultanéité d'utilisation d'un même composant logiciel ou matériel.
- **Plan utilisateur:** transport de l'information, contrôle de flux, d'erreur, et autres fonctions
- **Plan de contrôle:** signalisation (management de connexion)
- **Plan de management et de couche:** gestion de ressource et coordination entre couches
- Couches PHY et AAL divisés en 2 sous-couches: celle du bas faisant le travail, et au dessus la convergence qui procure une interface à la couche du dessus.



Le modèle de référence ATM

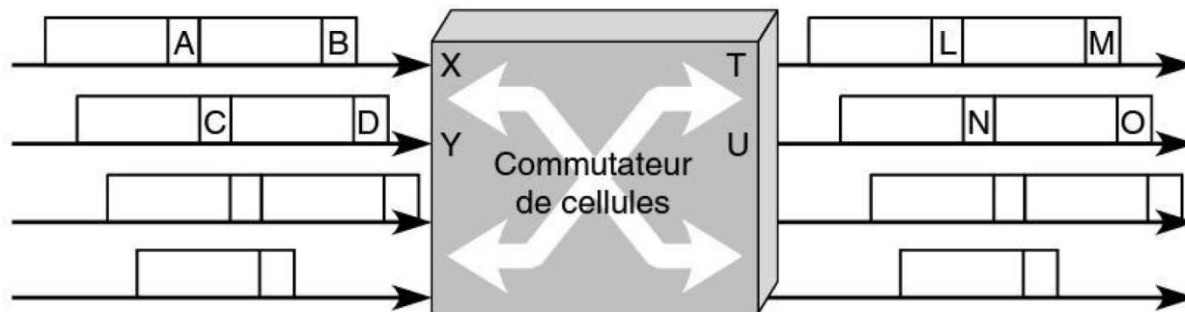
OSI layer	ATM Layer	ATM sublayer	Functionality
	AAL	CS	Providing the standard interface (convergence)
		SAR	Segmentation and Reassembly
2/3	ATM		Flow control Cell header generation/extraction Virtual circuit/path management Cell multiplexing/demultiplexing
2	Physical	TC	Cell rate decoupling Header checksum generation and verification Cell generation Packing/unpacking cells from the enclosing envelope Frame generation
1		PMD	Bit timing Physical network access

ATM connections: Virtual Circuits

- Marche avec VC comme FR
- Une partie du header est l'id de connexion -> source, dest et noeuds interm savent à quelle connexion appartient chaque cell -> chaque noeud interm (switch) sait comment commuter la cell
- Commutation de cell en hardware à haute vitesse: plus facile de construire en hardware des switchs pour manipuler des cell courtes de taille fixe = principal argument pour cellules de taille fixe
- Les paquets IP de taille variable doivent être routés en software: process plus long
- Autre plus de l'ATM: hardware peut être configuré pour multiplier les cell en sortie (multi ou broadcast)
- De petites cell ne bloquent pas une ligne pendant longtemps -> QoS plus facile à garantir
- Réseaux ATM organisés comme traditionnels WAN, avec lignes et switch
- La vitesse la plus commune pour des réseaux ATM est 155 Mbps et 622 Mbps
- 155.52 Mbps pour compatibilité avec sys de trans AT&T's SONET
- 622 Mbps = 4 channels of 155.52 Mbps

ATM connections: Virtual Circuits

- Association effectuée entre (référence, port d'entrée) et (référence, port de sortie) dans un switch
- Exemple: si une cell se présente à la porte X avec la ref A, elle est transmise à la sortie T avec la ref L.
La 2^e ligne du tableau de commutation constitue un autre ex: une cell qui entre sur la ligne X avec la ref B est envoyée vers la sortie U, accompagnée de la ref N de sortie

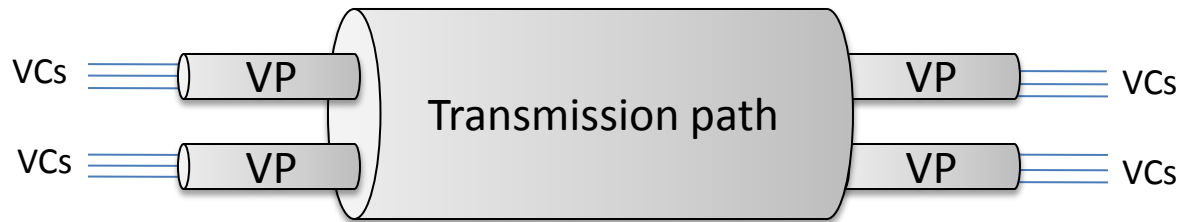


Les trames arrivant sur la porte d'entrée X avec la référence A sont dirigées sur la sortie T avec la référence L.

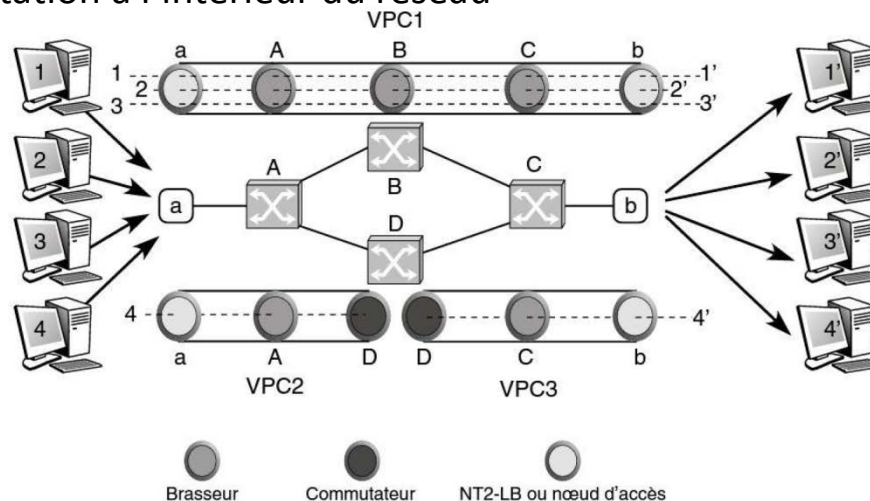
Ligne d'entrée	Référence d'entrée	Ligne de sortie	Référence de sortie
X	A	T	L
X	B	U	N
Y	C	T	M
Y	D	U	O
.			

ATM connections: Virtual Circuits

- Réseaux ATM orienté connexion => un *virtual channel* doit être établi avant tout transfert de données (*virtual circuit* est *virtual channel* en ATM -> noté VC)
- 2 types de connexion: *virtual path* (VP) identifié par VPI, et *virtual channel* (VC) identifié par VPI+VCI
- Un VP est un faisceau de VC, dont tous sont commutés de façon transparente par réseau basé sur VPI
- VPI et VCI ont signification seulement locale (à chaque switch)
- un *transmission path* est le média phy qui transporte les VC et VP

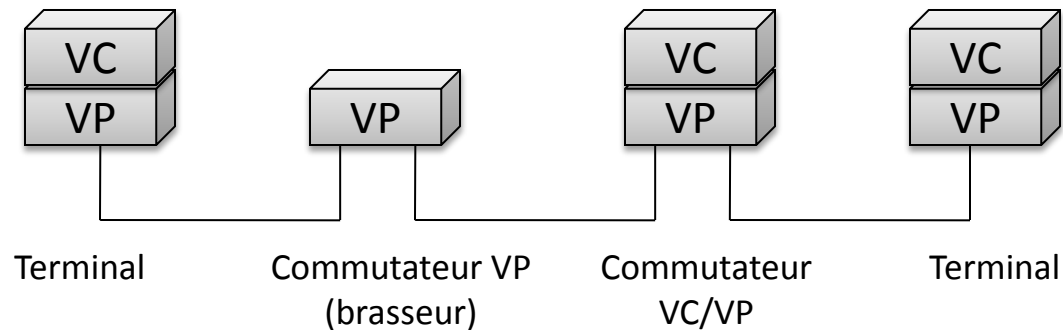


- brasseur de VP: tous les VCs du VP commutés simultanément
- on a donc intérêt à regrouper en un VP les VCs qui vont vers la même destination
- > simplifie les pbs de commutation à l'intérieur du réseau



ATM connections: Virtual Circuits

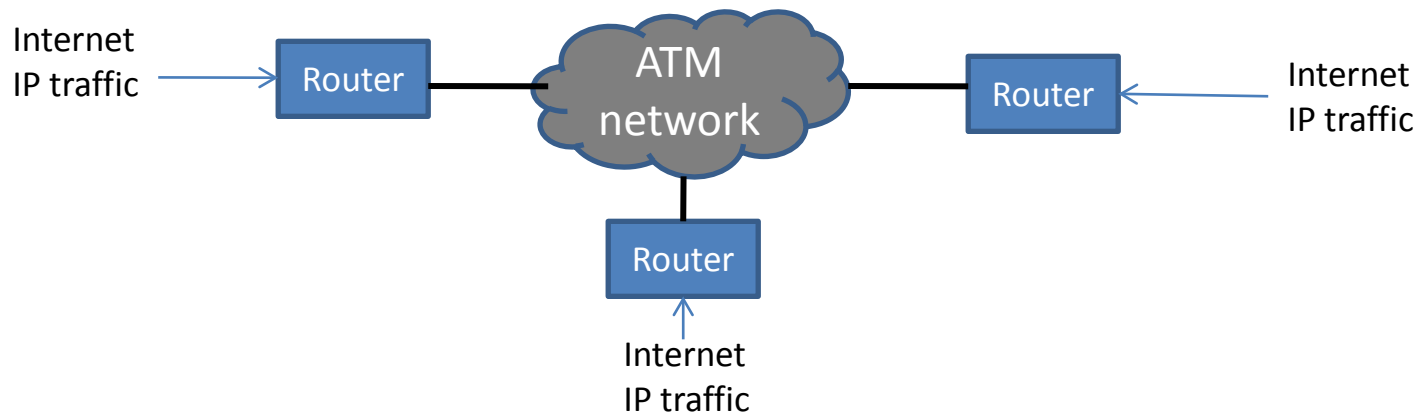
- Des connexions multipoint sont prévues dans la normalisation: associer à une ligne et à une ref en entrée plusieurs lignes et ref en sortie
- Dans un switch ATM, on commute une cell en utilisant les 2 ref. Dans un brasseur, on ne se sert que d'une ref, celle du conduit.
- Par ex, on peut commuter un ens de VC en une seule fois en ne se préoccupant que du VP = brasseur de conduit, ou *cross-connect* (on ne redescend pas au niveau du VC)



ATM connections: Virtual Circuits

IP over ATM

- un backbone ATM avec 3 points entrée/sortie (routeur) pour du trafic IP
- un backbone ATM peut s'étendre sur un continent et avoir des 100aines de switches ATM
- En général, les backbones ATM ont un PVC entre chaque paire de points entrée/sortie
(Recall that ATM uses the jargon "virtual channel" for "virtual circuit".)
- En utilisant des PVCs, les cellules ATM sont commutées d'un point d'entrée à un point de sortie sans avoir à établir et démanteler les VCs.
- Mais PVCs faisables que sur un nombre limité de entry/exit points
(For n entry points, $n(n-1)$ permanent VCs are necessary.)
- Chaque interface de routeur connectée à un réseau ATM aura 2 adresses: @IP et @ATM (layer 3 and 2)
- L'émetteur maintient table de correspondance entre @ATM et VCIs.



ATM connections: Virtual Circuits

-Le routeur d'entrée:

1. Examine l'@IP de destination du datagramme.
2. Détermine l'@IP du routeur de sortie (i.e., the next router in its route).
3. Le routeur d'entrée voit ATM juste comme un autre protocole de couche 2. (possède table de corresp. @IP/@ATM)
4. IP dans le entry router passe le datagramme à LL (i.e., ATM) avec l'@ATM du exit router.

- Après ces 4 étapes, uniquement ATM se charge de transférer le datagramme à l'@ATM de sortie (Step 3 above):

1. Détermine le VCI+VPI pour le VC qui mène à l'@ATM de destination.
2. Segmente le datagramme en cellules côté émetteur du VC (i.e., at the entry router), et ré-assemble les cellules côté récepteur du VC (i.e., at the exit router).

--> introduction to the 3 layers to answer to "How does ATM efficiently segment and reassemble IP datagrams that are sent across an ATM backbone ?"

ATM: La couche physique

- Le modèle ITU a 3 couches :

- BAS ↓
- la couche prenant en charge le transport des cell sur un support physique
 - la couche se préoccupant de l'acheminement des cell de bout en bout
- HAUT ↓
- la couche chargée de l'interface avec les couches sup et regroupant les cell pour les délivrer à l'ut

-La couche la plus basse concerne les protocoles de niveau physique, divisée en 2:

- couche PMD (*Physical Medium Dependent*): transmission sur le support phy et pbs d'horloge, ne reconnaît pas les cell, spécifiée selon le media physique (fiber, copper, etc.)

- couche TC (*Transmission Convergence*): découplage du taux de transmission des cell, génération et vérification de la zone de détection d'erreur de l'entête, le HEC, de la délimitation des cellules, de l'adaptation de la vitesse de transmission, génération et récupération des cell sur le support physique

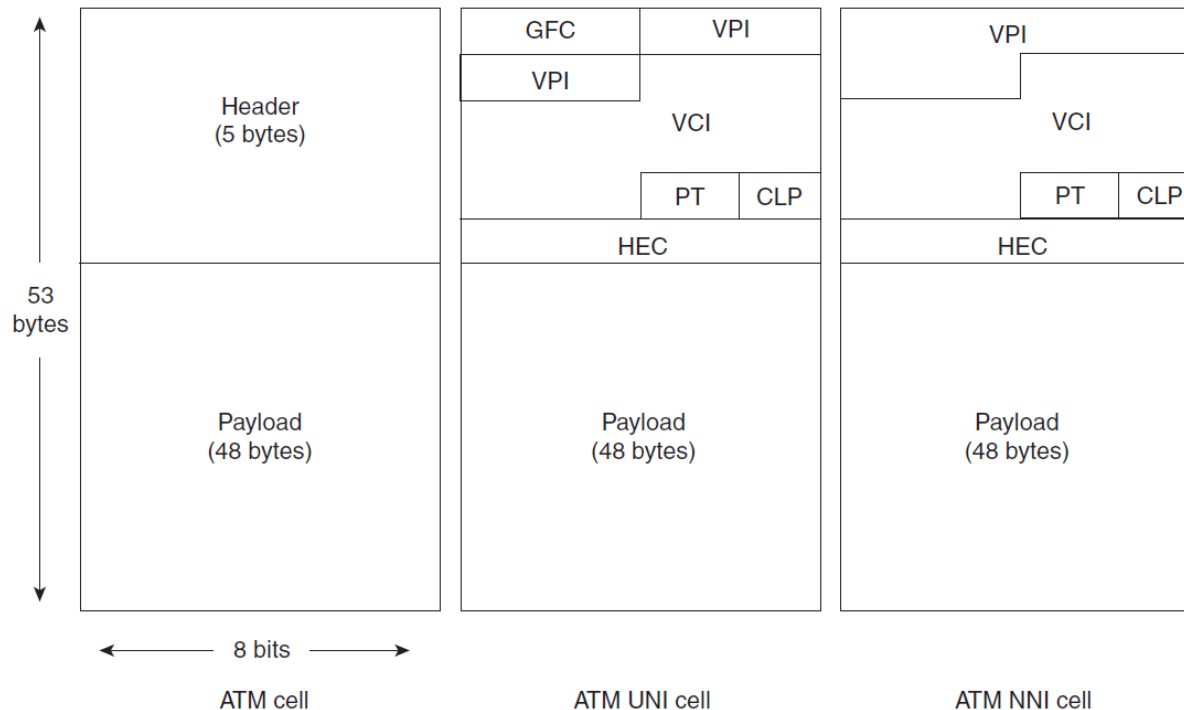
 - émission: génère byte HEC pour corriger toutes les err d'1 bit dans header -> prévient mauvais routage

 - réception: délimite les cell si PMD ne le fait pas, envoie une cell d'attente (*idle cell*) marqué dans PT, quand la couche ATM n'envoie pas de cell, pour flux continu

- La 2^e couche est celle de l'ATM proprement dite. Cette couche gère le transport de bout en bout de la cell.

ATM: La couche ATM

- 53B = 48B+5B
- zone de données: fragment d'un paquet utilisateur, généralement un fragment d'un paquet IP
- Sur les 48B provenant de la couche sup, jusqu'à 4B peuvent concerner la supervision -> la fragmentation du paquet est faite en blocs de 44B (4B de AAL).
- Entête de la cell ATM différente selon l'interface UNI ou NNI :
 - l'interface NNI (*Network Node Interface*) entre 2 nœuds du réseau
 - l'interface UNI (*User Network Interface*), utilisée pour rentrer dans le réseau ou en sortir



ATM: La couche ATM

PTI (Payload Type Identifier) : Type des données (AAL1. . .) et **indication de congestion (Explicit Forward Congestion Indication)**

CLP (cell loss priority) : priorité de suppression de cellule

GFC (Generic Flow Control) : non utilisé

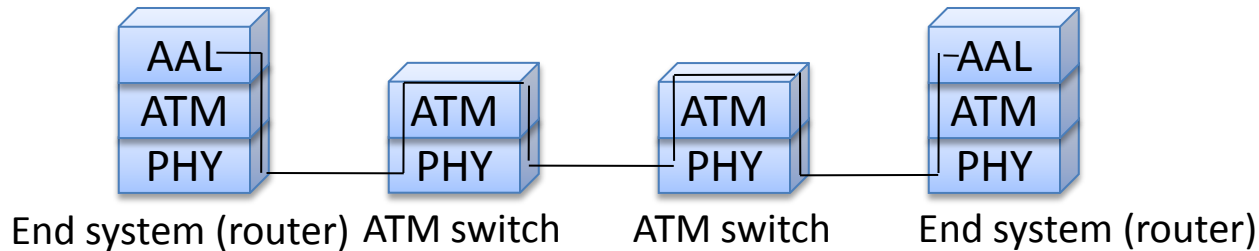
HEC (Header Error Control) : CRC sur l'entête.

Le champ CLP (*Cell Loss Priority*)

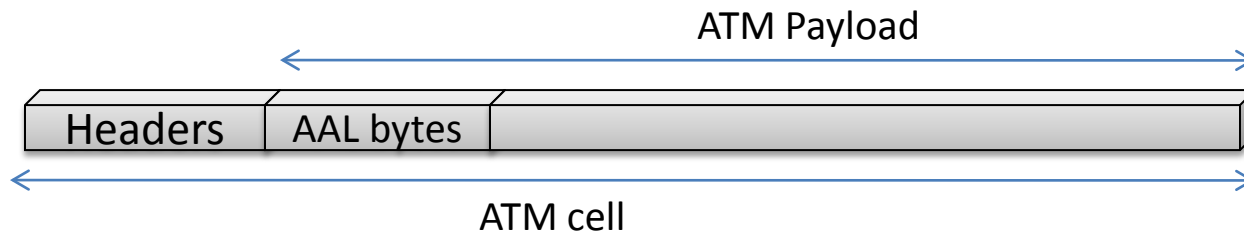
- indique si la cell peut être perdue (CLP=1), ou si elle est importante
- sa fonction est d'aider au contrôle de congestion: avant d'émettre une cell dans le réseau, il faut respecter un débit d'entrée, négocié au moment de l'ouverture du VC
- toujours possible de faire rentrer cell en surnombre, mais avec indicateur permettant de les perdre pour préserver le transport des infos entrées dans le cadre de l'abonnement

ATM: La couche AAL

- But: permettre aux protocoles (e.g., IP) et applis (e.g., constant bit rate video) existants de tourner au dessus d'ATM
- AAL est implanté dans les terminaux ATM (e.g., entry and exit routers in an Internet backbone), pas dans les switchs ATM intermédiaires -> analogue en ce sens à la couche transport de la pile IP



- La couche AAL a son propre champ d'entête, occupant une partie du payload de la cell ATM:



- Divisée en 2 sous-couches:
 - CS (*Convergence Sublayer*): pour l'interfonctionnement avec la couche du dessus
 - SAR (*Segmentation and Reassembly sublayer*): pour segmentation et ré-assemblage message-cellules

ATM: couche AAL et classes de services

- L'ITU répartit les services du réseau ATM en 4 classes, fondées sur la relation de temps entre la source et le destinataire, le débit constant ou variable et le mode de connexion:
 - classe A: débit constant, service en mode avec connexion et contrainte de délai
ex: le service de type parole téléphonique à 64Kbits/s.
 - classe B: débit variable et contrainte de délai
ex: parole téléphonique ou une vidéo compressée
 - classe C: débit variable et pas de contrainte de délai, en mode connexion
 - classe D: débit variable et pas de contrainte de délai, en mode sans connexion
ex de C et D: applications de transfert de données

	Classe A	Classe B	Classe C	Classe D
Synchro. source récepteur	Forte		Faible	
Flux	Constant	Variable		
Type de connexion	Orienté connexion			Sans connexion

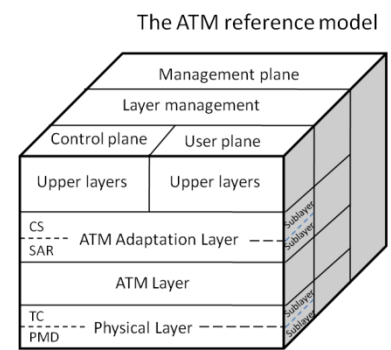
- 4 classes de service -> 4 classes de protocoles (numérotées de 1 à 4) puis 3 (1993)

ATM: couche AAL et classes de services

-L'ITU recommande 4 types de protocoles AAL pour supporter ces classes de services :

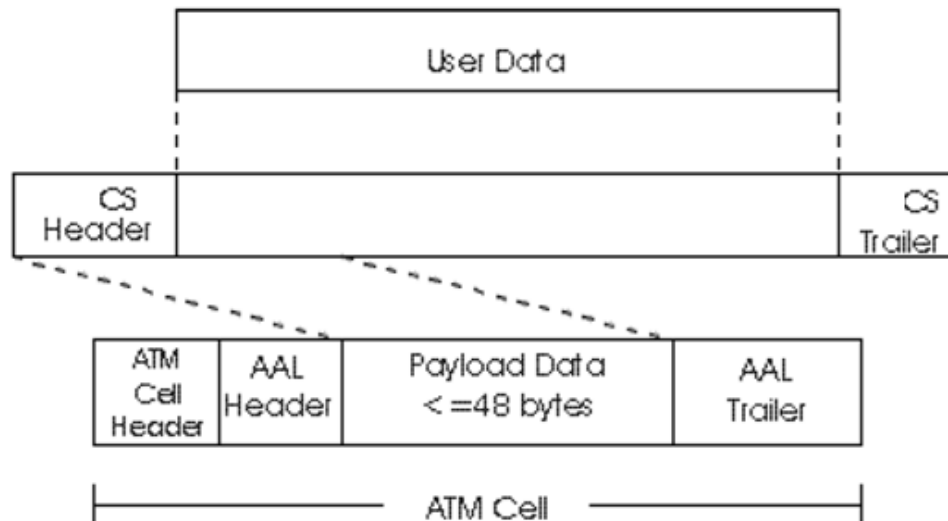
- **AAL-1**: pour services de la **classe A** -> service d'émulation de circuit
Le service rendu par l'AAL-1 s'appelle **CBR (Constant Bit Rate)**.
- **AAL-2**: défini au départ pour les services de la **classe B** (ex: service vidéo à débit variable)
Le service rendu par cette classe s'appelle **VBR (Variable Bit Rate)**.
Ce protocole est utilisé par ex sur la partie accès de l'UMTS, pour permettre le multiplexage de plusieurs connexions bas débit sur une connexion ATM de façon à tenir compte au mieux des contraintes temporelles.
- **AAL-5**: aka SEAL (*Simple Efficient Adaptation Layer*): pour trames de données (paquets IP) en mode avec connexion (**classe C**).
Service élastique et utilise le service **ABR (Available Bit Rate)**.

ATM: exemple avec AAL 5

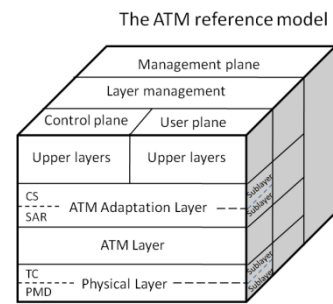


AAL structure

- Les données utilisateur (e.g., an IP datagram) sont d'abord encapsulées dans un CS-PDU avec CS header et CS trailer.
- CS-PDU trop grande pour le payload d'une cell ATM
- > le CS-PDU doit être segmenté à la source ATM et ré-assemblé à la destination ATM.
- La sous-couche SAR segmente le CS-PDU et ajoute un header et un trailer AAL qui sera le payload des cellules ATM.
- (Selon les types AAL, les headers and trailers CS et AAL peuvent être vides.)



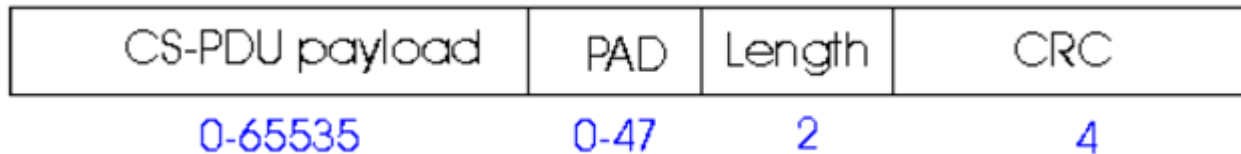
ATM: exemple avec AAL 5



AAL 5 (Simple and Efficient Adaptation Layer - SEAL)

- AAL5 est un AAL léger utilisé pour le transport de datagrammes IP sur des réseaux ATM

- Un datagramme IP occupe le CS-PDU payload (1 à 65 535 bytes). The AAL5 CS-PDU:



-Le PAD assure que le CS-PDU est un multiple de 48 bytes.

- Le champ longueur identifie la taille du payload CS-PDU, pour pouvoir enlever le PAD au récepteur.

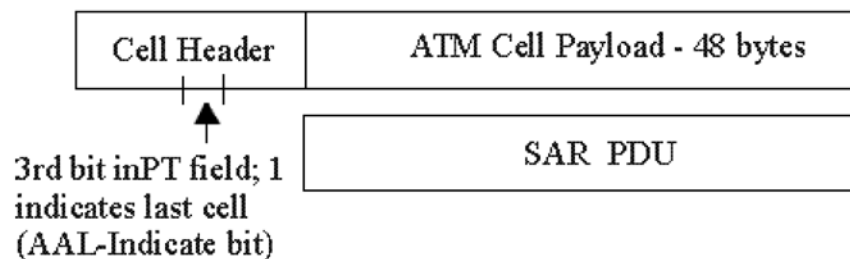
- **A la source ATM**, le SAR de AAL5 découpe le CS-PDU en segments de 48 bytes. Un bit dans le champ PT de l'entête de la cellule ATM, qui est 0 par défaut, est mis à 1 pour la dernière cellule du CS-PDU.

- **A la destination ATM**, la couche ATM dirige les cellule avec un VCI spécifique vers un buffer de la sous-couche SAR.

- Les entêtes de la cellule ATM sont retirées, et le bit du champ PT est utiliser pour délimiter les CS-PDUs.

- Une fois que le CS-PDU est délimité, il est passé à la sous-couche AAL.

- A la sous-couche CS, le champ *length* est utilisé pour extraire le payload du CS-PDU (ex : un pkt IP)



QoS definition

QoS = Collection of technologies which allow applications/users to request and receive **Predictable Services Levels**

In term of → **Bandwidth** [or throughput]
 → **Delays** [End-to-end + Jitter]
 → **Data Integrity** [Loss + Errors]

Provided through Smart Management + Unequal sharing of Network Resources
(often called "Unfairness")

Alternatives to QoS → Dedicated networks (PSTN, leased lines)
 → Over-dimensionning

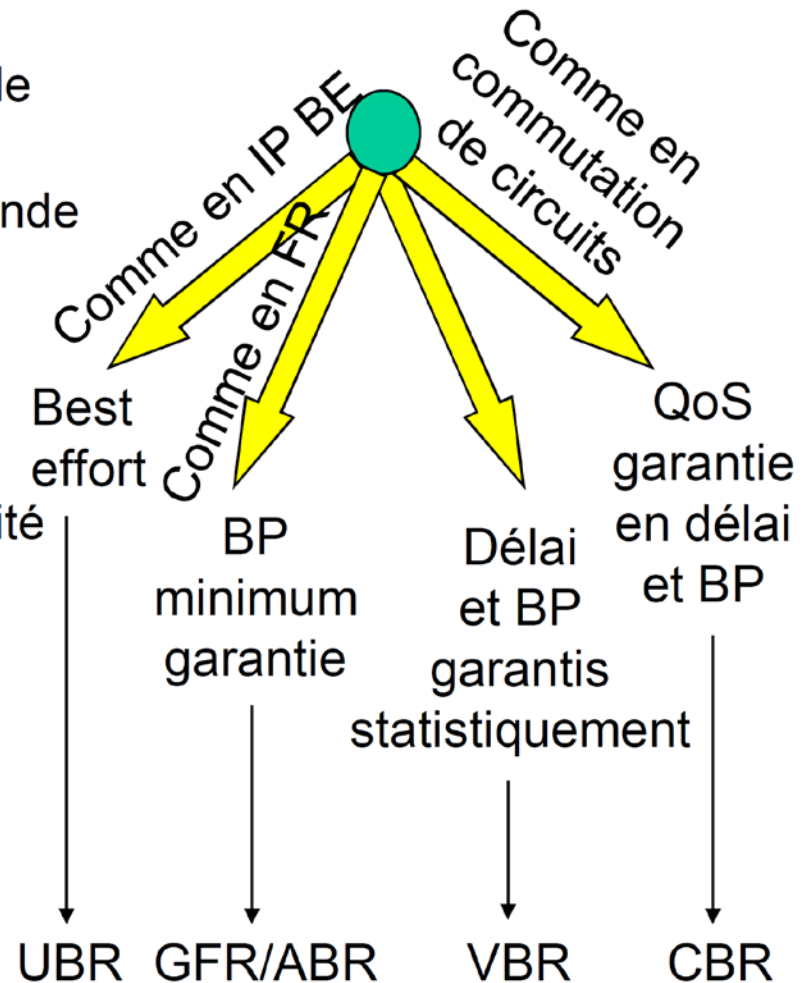
(over-subscribing Vs over-engineering)

Catégories de service

- Chaque circuit virtuel aura la catégorie de service adaptée aux besoins de l'application qui l'utilisera

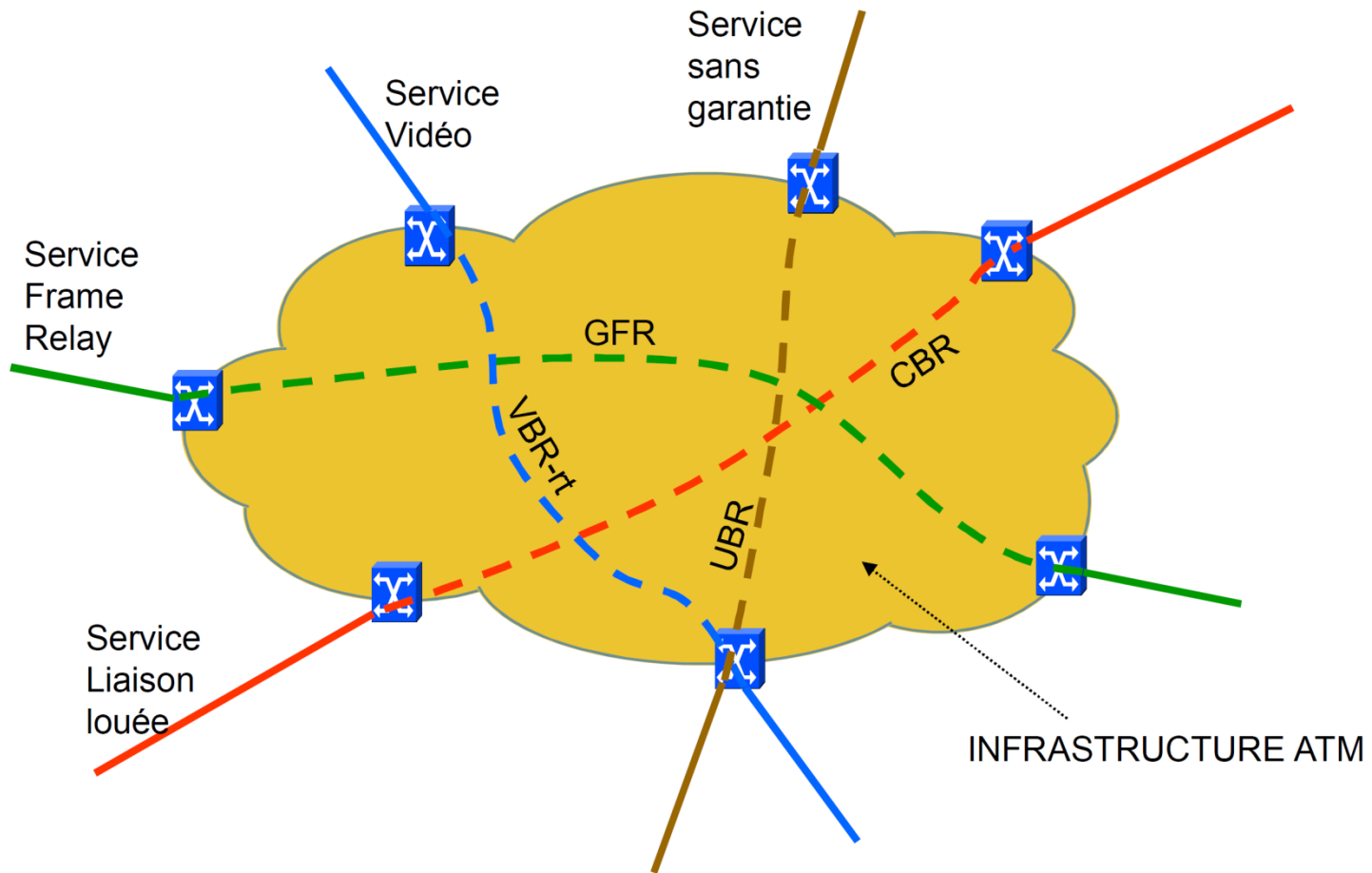
- Garantie absolue en délai et en bande passante : CBR
- Garantie statistique en délai et en bande passante : VBR
- Besoin d'un minimum de bande passante (applications élastiques) : GFR ou ABR
- Pas de traitement spécifique de qualité de service (« best effort ») : UBR

CBR : Constant Bit Rate
VBR : Variable Bit Rate
ABR : Available Bit Rate
GFR : Guaranteed Frame Rate
UBR : Unspecified Bit Rate



Exemple d'utilisation des catégories de service

- L'utilisation des différentes catégories de service permet à l'opérateur de mutualiser son infrastructure pour offrir des services différents



ATM: Qualité de Service (QoS)

- ATM apporte un gain économique grâce au multiplexage statistique.
 - Mais multiplexage statistique de trafic en rafale peut provoquer congestion.
 - Travaux de l'ITU et ATM Forum ont visé à minimiser cette congestion et à **maximiser le taux d'utilisation du réseau, tout en garantissant la QoS spécifiée par l'utilisateur.**
- Or c'est la congestion qui est le seul obstacle à la QoS

--> ATM gère la congestion avec :

- *Call Admission Control (CAC)*: pour garantir QoS, on préfère ne pas admettre de nouveaux clients qui pourraient dégrader la QoS des autres – CAC déterministe et statistique selon la QoS du VC à établir
- On essaye au maximum d'éviter la congestion avec CAC, si elle arrive, **CLP** pour abandon de cellules et PTI pour *notification de congestion*

ATM: Qualité de Service (QoS)

- ATM supporte garanties QoS comprenant **contrat de trafic, mise en forme de trafic et *traffic policing***:

- **Contrat de niveau de service (SLA)** : spécifie une enveloppe pour le flux prévu. Avec BW pic, BW moyenne, taille de rafale. Quand périph ATM se connecte au réseau ATM, il entre dans le cadre d'un contrat, basé sur paramètres QoS achetés.

- **Mise en forme de trafic (*shaping*)** : usage de files pour contraindre les rafales de données, limiter débits pic et lisser la gigue pour que le trafic rentre dans l'enveloppe prévue.

- **Traffic policing** : action prise sur les paquets directement (et non pas seulement leur rythme come en *shaping*) : marquage ou abandon.

Utilisé par les switches pour faire respecter le contrat. Le switch peut mesurer le trafic réel et le comparer à l'enveloppe payée. Le switch peut activer le bit cell-loss priority (CLP) des cellules en excès.

--> Tout switch traversé par cette cellule est autorisé à l'abandonner durant les périodes de congestion.

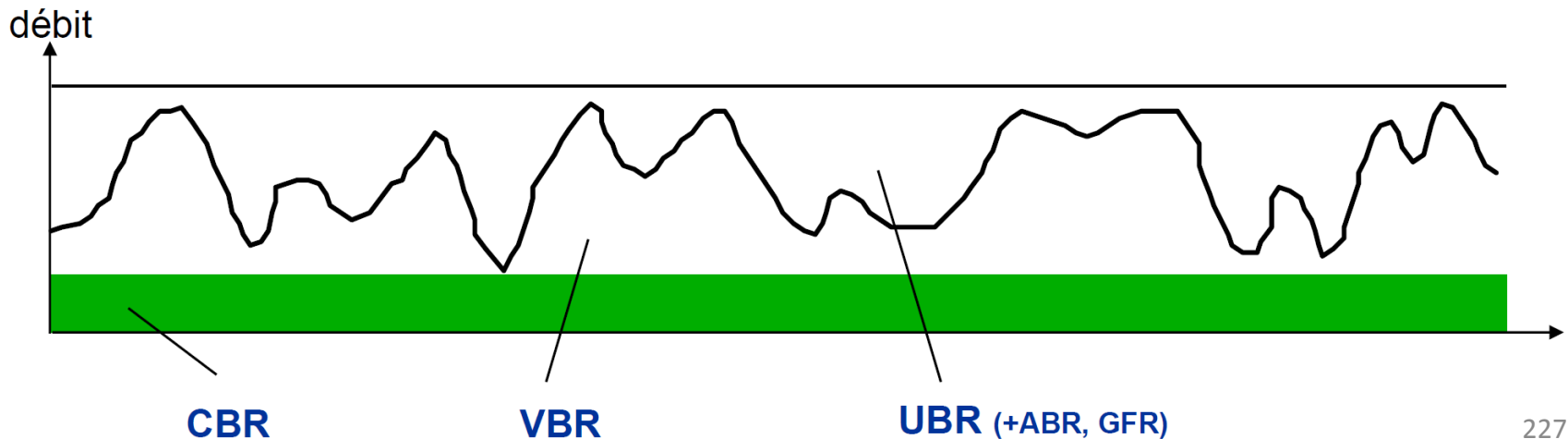
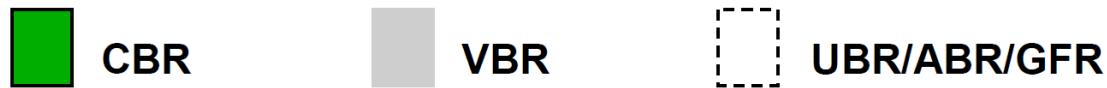
ATM-TM: Classes de service

CBR Constant Bit Rate (téléphonie, son, fax, video à débit constant)

VBR Variable Bit Rate (voix compressée, data temps-réel)

UBR (+ABR, GFR) Unspecified Bit Rate (data non-critique)

Chaque connection (VC), selon sa classe de service, sera caractérisée par des **paramètres de trafic** (PCR, SCR, MCR, MBS) et de **QoS** (CDV, Max CTD, CLR)



ATM-TM: Paramètres de trafic et de QoS

Une source de trafic (Application) s'identifie au réseau par un ensemble de paramètres décrivant plus ou moins précisément l'utilisation du réseau ATM que compte faire cette source en terme de trafic et de qualité de service.

Paramètres de trafic

- . Peak Cell Rate **PCR**
- . Sustainable Cell Rate **SCR**
- . Maximum Burst Size **MBS**
- . Minimum Cell Rate **MCR**

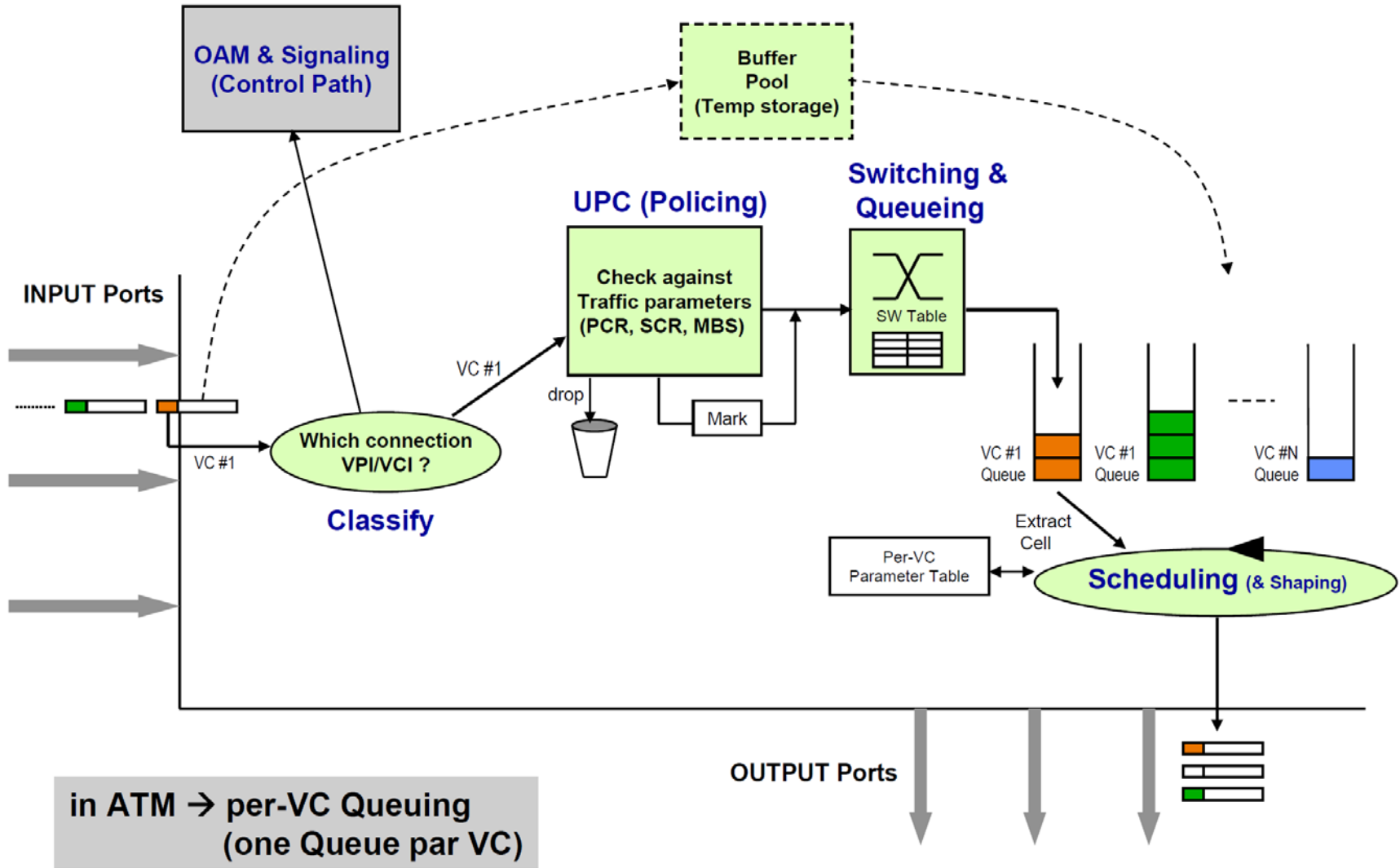
Paramètres de qualité de service

- . Cell Delay Variation **CDV**
- . Maximum Cell Transfer Delay **Max CTD**
- . Cell Loss Ratio **CLR**

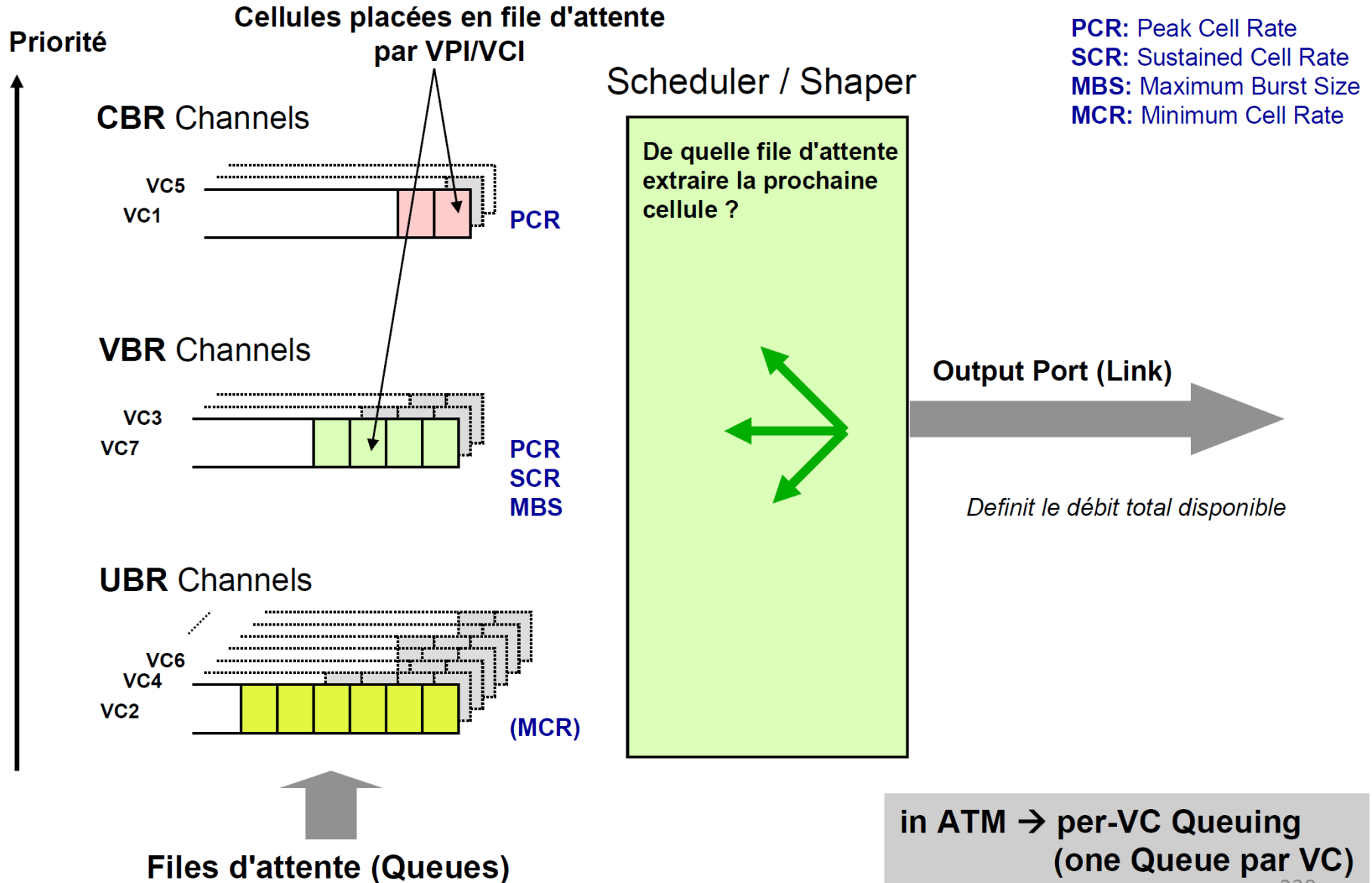
- Ces paramètres sont échangés à l'interface UNI (User-Network) lors de la phase d'initialisation d'une connection. Ils peuvent être explicites ou implicites (définis par défaut par le réseau).
- La prise en compte de ces paramètres se fera par des mécanismes appropriés (file d'attente, scheduling, ...) mis en oeuvre pour chaque connection (per-VC ou per-flow) dans les équipements ATM du réseau.

Paramètres		Classes de service					
		CBR	VBR-rt	VBR-nrt	ABR	UBR	GFR
Paramètres de QoS							
CTD	<i>Cell Transfer Delay</i>	•	•	•			
CDV	<i>Cell Delay Variation</i>	•	•				
CLR	<i>Cell Loss Ratio</i>	•	•	•	•		
Paramètres de Trafic							
PCR	<i>Peak Cell Rate</i>	•	•	•	•		
SCR	<i>Sustained Cell Rate</i>		•	•			
MBS	<i>Max Burst Size</i>		•	•			
MCR	<i>Minimum Cell Rate</i>				•		•

TM/QoS in ATM Switch: Functional description



ATM Queuing-Scheduling: Principle



ATM: Conclusion

- Les réseaux de niveau trame sont au nombre de 3: FR, Ethernet et ATM. Si le 1^{er} est en baisse et que le 2^e monte, le transfert ATM reste stable, malgré de nombreuses prédictions prévoyant sa chute à partir de 2005.
- On peut expliquer cette stabilité de l'ATM par la grande confiance des opérateurs de télécoms à son égard: cette technique est aujourd'hui parfaitement maîtrisée, et on est capable de bien la dimensionner.
- De plus, elle offre des garanties de QoS qui lui confèrent un atout supplémentaire.
- Nous n'avons pas décrit la signalisation du réseau ATM, car celle d'origine a été remplacée par une signalisation IP afin de passer à la techno MPLS, décrite après.
- Nous verrons alors que l'ATM reste une technique très importante dans cette nouvelle génération de réseaux.

Plan

I. Présentation des WAN

II. Les interfaces de la couche physique

III. Protocoles de niveau 2 dans les WAN

IV. MPLS : commutation par VC dans le monde IP

IV.1. Fonctionnement de MPLS

IV.2. Ingénierie de trafic avec MPLS : MPLS-TE

IV.3. Offres de service MPLS : les VPN basés sur MPLS

IV.3.a. IP-VPN

IV.3.b. Ethernet-VPN : VPLS

V. Qualité de service

VI. Technologies xDSL

Cours de J. Drouot (ESIL)

D'ATM vers MPLS

- **Quelle technologie va servir de base pour l'infrastructure unique de convergence pour les réseaux d'opérateurs?**
- **ATM était le choix naturel**
 - Solution éprouvée
 - Investissements souvent déjà engagés
 - Possibilité de haut débit grâce à son fonctionnement hardware
 - Fonctions riches pour assurer différents niveaux de qualité de service
 - Selon le type de trafic ou le type de service offert au client de l'opérateur
 - Possibilités d'ingénierie de trafic
 - Agrégation de trafics sur des PVC respectant des contraintes
- **Mais l'environnement technique a changé depuis la conception d'ATM**
 - IP est devenu le protocole de niveau 3 incontournable
 - Le hardware est monté en puissance
 - La bande passante est plus abondante et moins chère
 - Les stations d'extrémité sont plus intelligentes

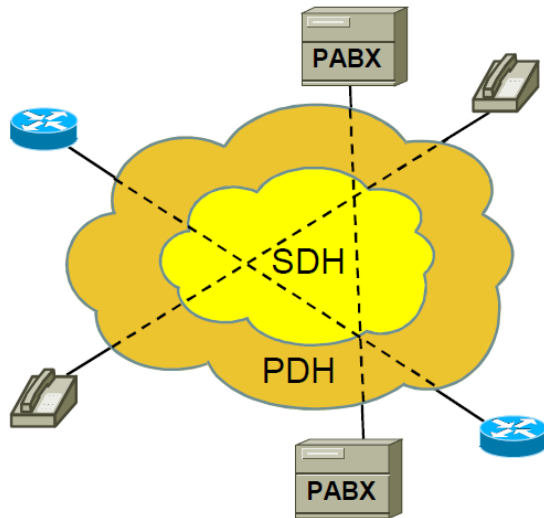
D'ATM vers MPLS

- **Dans le contexte actuel, ATM présente des inconvénients**
 - Il cohabite mal avec IP
 - Conversion d'adresses, mode multicast différent
 - Duplication des protocoles de routage
 - Le hardware permet maintenant le traitement de paquets de longueur variable
 - Les petites cellules ont moins d'intérêt à très haut débit
 - Et pénalisent même le traitement (plus de cellules à traiter)
 - ATM va trop loin dans les possibilités de qualité de service
 - Les stations d'extrémité peuvent s'adapter à une qualité de service un peu moins bonne
 - La qualité de service native est meilleure à très haut débit
- **De nombreux constructeurs ont proposé des solutions de commutation IP faisant la synthèse de la commutation ATM et du routage IP**
 - IP switching (Nokia), ARIS (IBM), Tag Switching (Cisco), etc...
- **MPLS (MultiProtocol Label Switching) est la synthèse IETF de ces propositions**

Evolution des infrastructures réseau des opérateurs

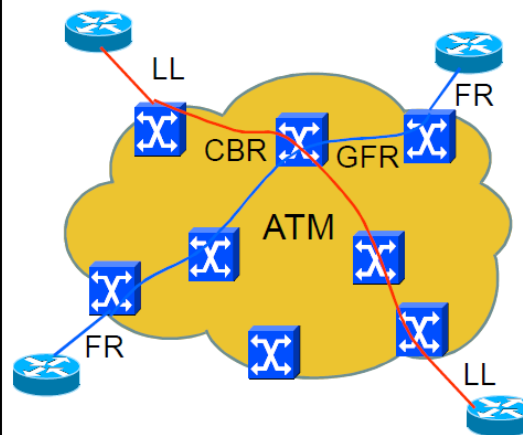
- L'infrastructure des opérateurs a subi des profondes migrations

Infrastructure de niveau 1



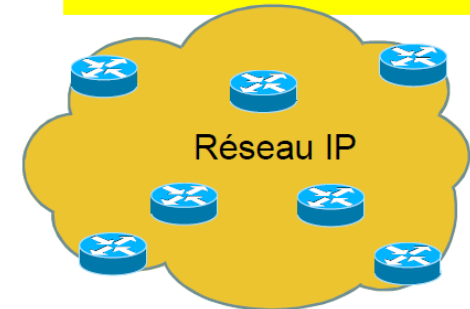
- **Services de niveau 1**
 - Liaisons louées
 - Téléphonie classique
 - Interconnexion de PABX

Infrastructure de niveau 2



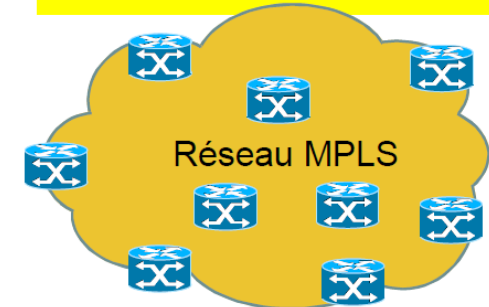
- **Services de niveau 1 et 2**
 - Liaisons louées (CBR)
 - Frame Relay (GFR)
 - Vidéo (VBR-rt)
 - RNIS-Large Bande

Infrastructure de niveau 3



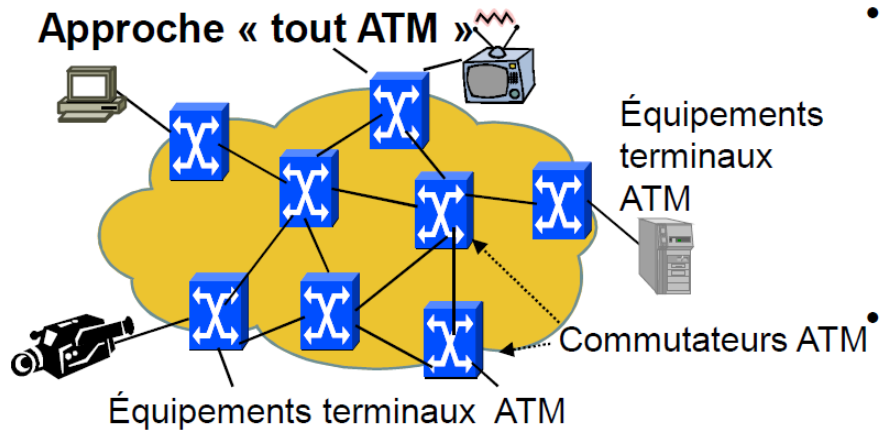
- **Services de niveau 3**
 - Accès Internet
 - VPN IPsec

Infrastructure de niveau 2/3

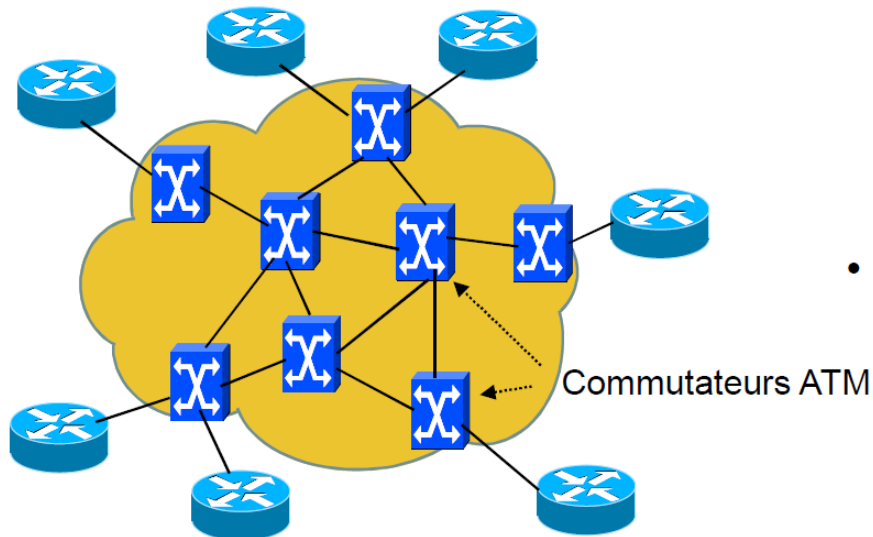


- **Services de niveau 1, 2 et 3**
 - Différents types de VPN

Les approches possibles des opérateurs



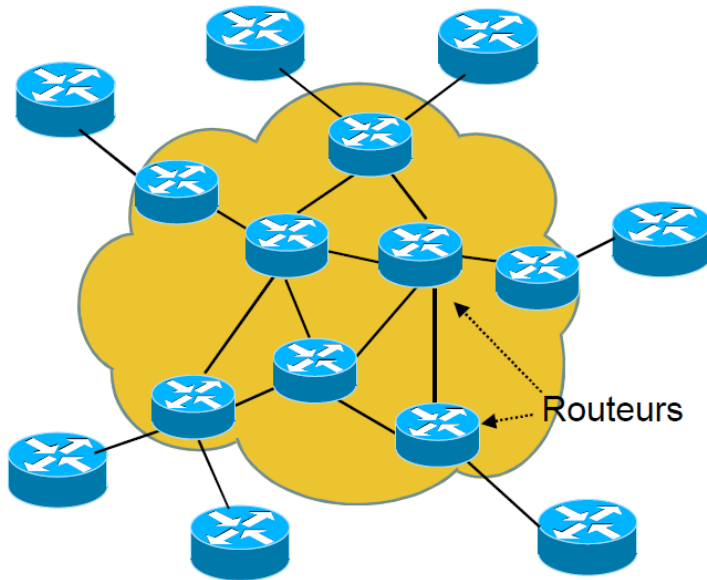
Approche de superposition : IP sur ATM



- **Les opérateurs avaient choisi une approche « tout ATM » sans IP**
 - ATM « sans couture »
 - Le succès d'Ethernet et d'IP a éliminé cette approche
- **Les opérateurs ont alors utilisé leur infrastructure ATM pour transporter les paquets IP**
 - Le mode circuit virtuel d'ATM permet aux opérateurs de faire de l'ingénierie de trafic
 - Choisir sur quel circuit virtuel transporter tel type de trafic
- **Cohabitation de deux technologies**
 - Non conçues pour interopérer
 - Besoin de doubles compétences

Les approches possibles des opérateurs

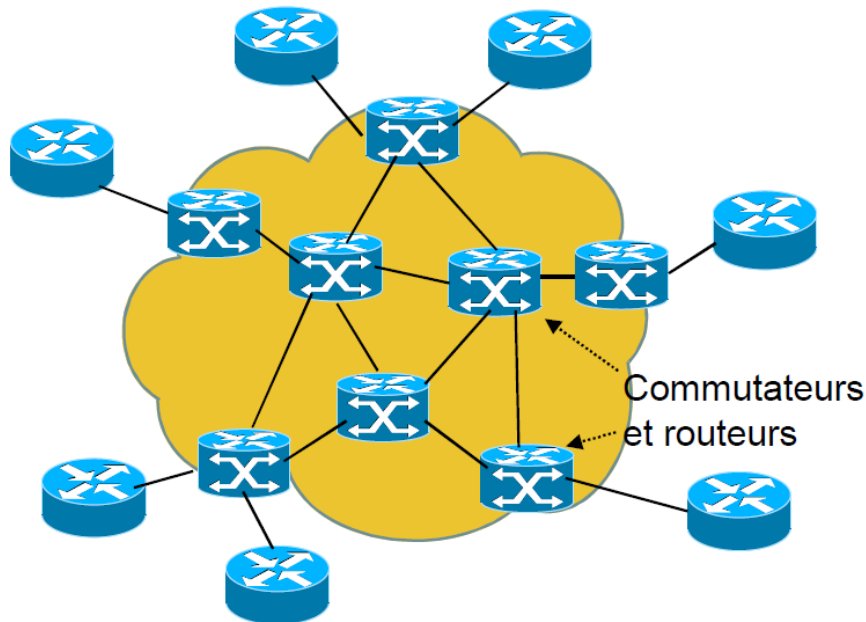
Approche IP pur sans ATM



- **Les opérateurs ont alors envisagé une approche « tout IP »**
 - Une seule compétence
- **Le routage dans le réseau de l'opérateur est celui du mode datagramme IP**
 - Basé sur l'adresse destinataire du paquet IP
 - Tous les paquets sont envoyés sur la meilleure route IP
- **Les routeurs au départ étaient plus lents que les commutateurs ATM**
 - Mais les routeurs rapides ont corrigé ce problème
- **Pas de possibilité d'ingénierie de trafic et d'équilibrage de trafic**

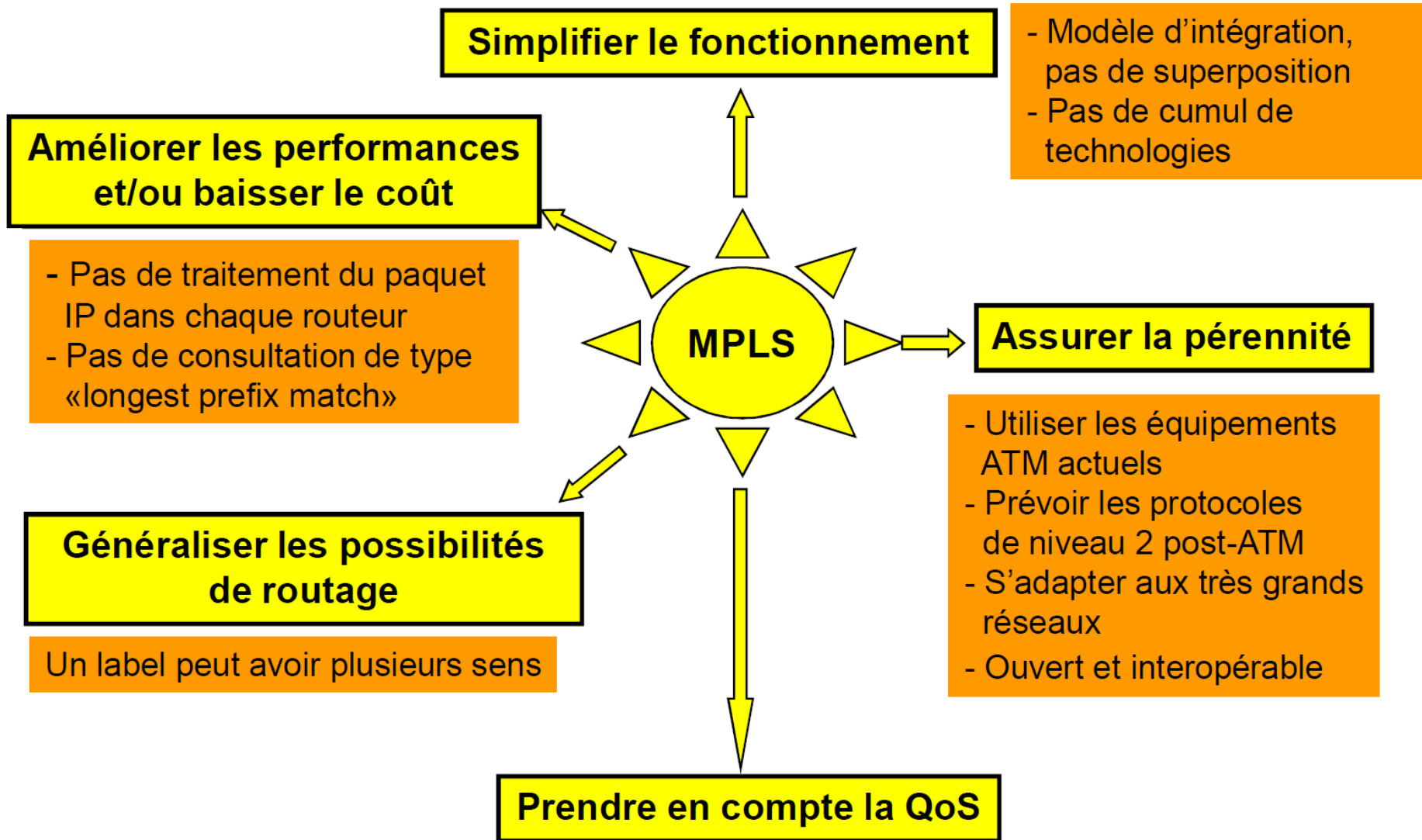
Les approches possibles des opérateurs

Approche d'intégration : MPLS



- **Une approche intermédiaire d'intégration a été proposée**
 - Un seul plan d'adressage IP
 - Les équipements internes de l'opérateur sont des équipements hybrides
 - Ils peuvent fonctionner comme des routeurs IP
 - Ils peuvent aussi fonctionner dans un mode proche du circuit virtuel en commutant selon un numéro de label
- **Le routage n'est plus forcément corrélé à l'adresse destinataire IP**
 - L'ingénierie de trafic est possible
- **IP et MPLS sont des technologies proches conçues pour interopérer**

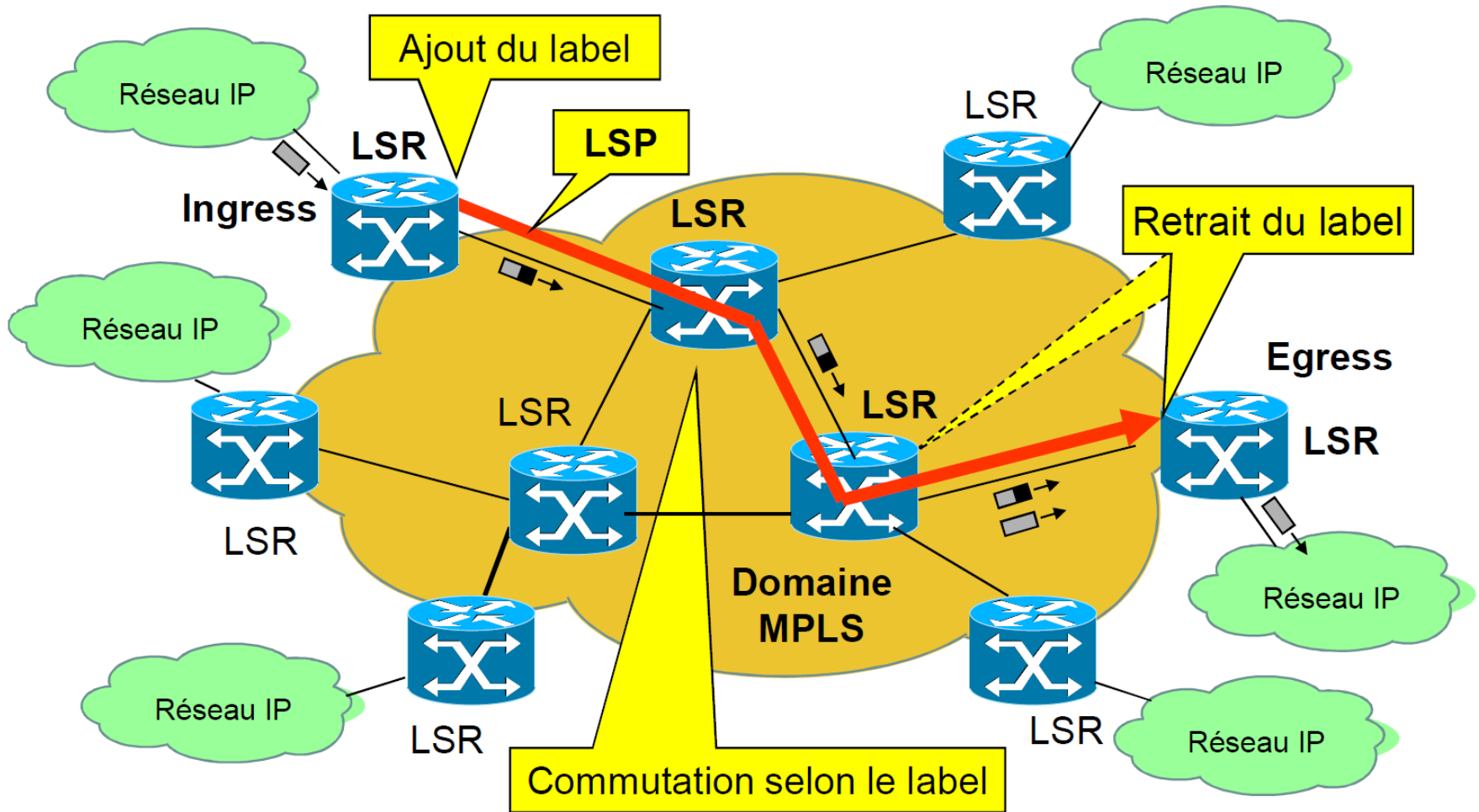
Objectifs de MPLS



Principes de MPLS

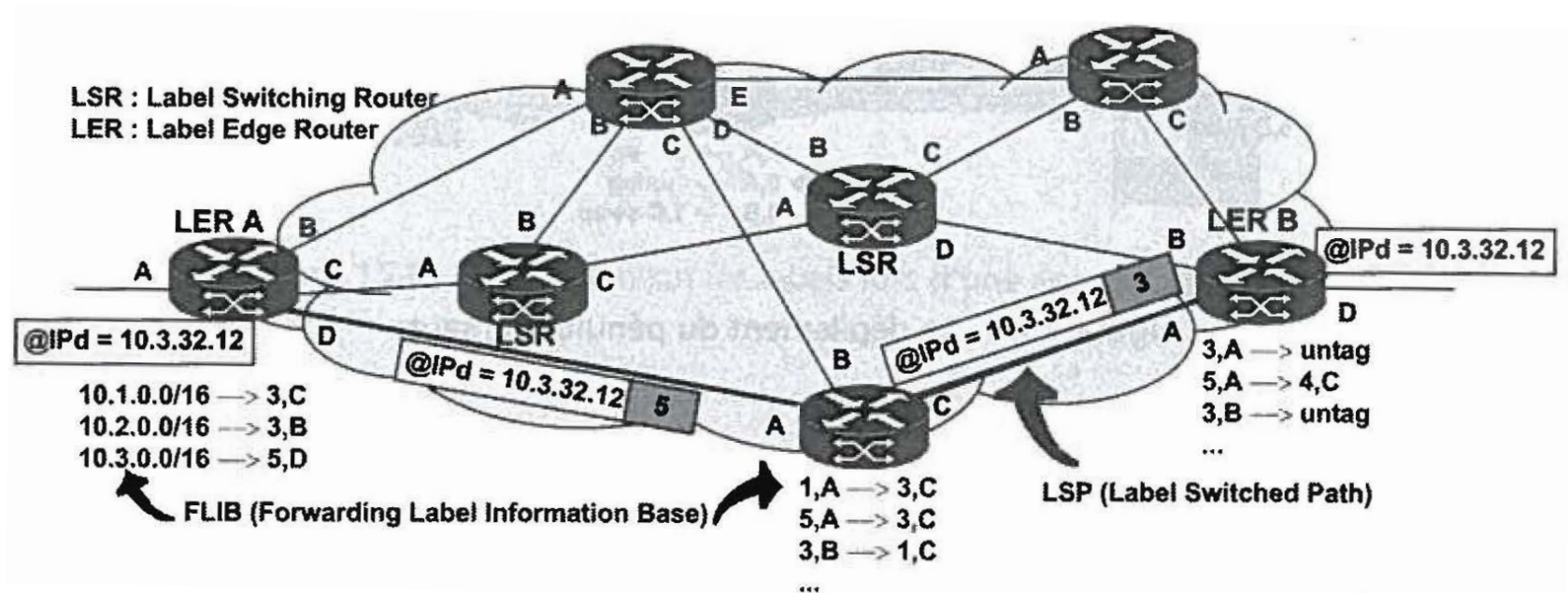
- **Des chemins prédéfinis relient les points d'extrémité du réseau**
 - Les LSP (Label Switched Path)
 - Un LSP est unidirectionnel
 - Les LSP sont établis par un protocole de signalisation en suivant la route déterminée par les protocoles de routage IP
 - Les LSP peuvent être établis à l'initiative de l'administrateur (proche des circuits virtuels permanents)
 - Ou ils sont établis automatiquement à l'initiative d'un point d'extrémité du réseau dès qu'il apprend par les protocoles de routage l'existence d'un nouveau préfixe IP
- **Les équipements MPLS s'appellent des LSR (Label Switch Router)**
- **A l'entrée du réseau, le 1er LSR (« Ingress LSR ») analyse le paquet IP**
 - Il choisit alors le LSP et insère un label devant le paquet IP
- **Les équipements suivants (les LSR du cœur de réseau) relaient le paquet en se basant seulement sur le label**
- **Le LSR de sortie (« Egress LSR) retire le label**
 - Dans certaines implémentations, c'est l'avant dernier LSR qui retire le label
- **A la sortie le paquet est routé selon le fonctionnement IP traditionnel**

Principes de MPLS



Principes de MPLS

Acheminement d'un datagramme IP dans un réseau MPLS:



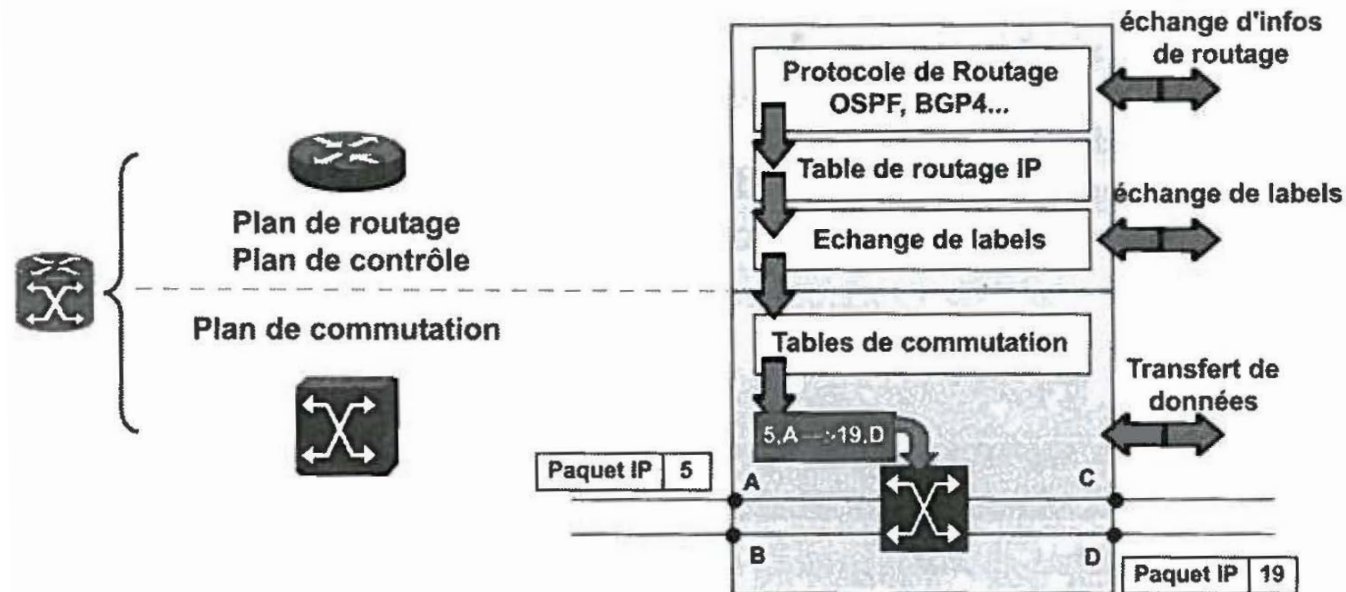
Dans un réseau MPLS, un même paquet MPLS peut recevoir plusieurs labels (Push tag).

L'empilement de labels permet de définir une **agrégation de routes** en interne dans le réseau et des VPN.

L'opération **Pop tag** permet de supprimer le label de haut de pile, alors que **Untag** supprime le dernier label.

Principes de MPLS

Structure d'un LSR:

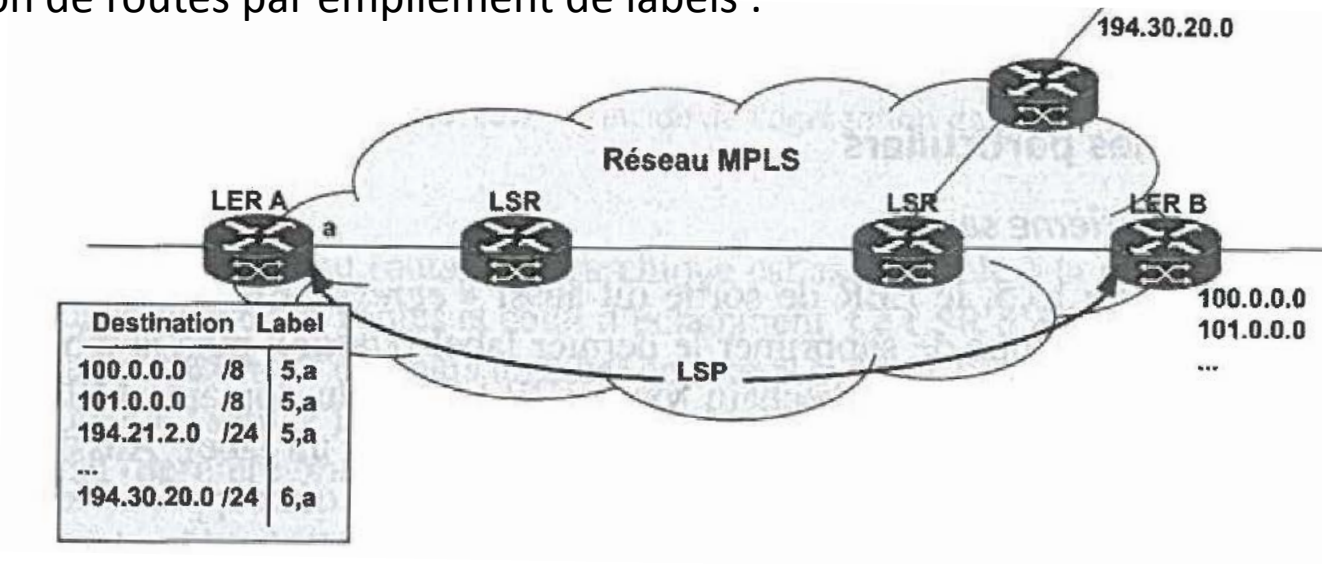


- Un *Label Switching Router (LSR)* correspond à l'association d'un routeur et d'un commutateur.
- En principe un switch FR ou ATM peut évoluer en LSR par une simple mise à jour du logiciel.

- Le plan de routage ou plan de contrôle met en œuvre un protocole de routage IP
- Un protocole spécifique distribue les labels aux LSR voisins : **LDP, Label Distribution Protocol**.
- Tous les paquets à destination d'un même nœud de sortie reçoivent le même label et subissent donc le même traitement dans le réseau.
- > **agrégation de routes** à la périphérie: allège les tables et participe à l'amélioration des performances.

Principes de MPLS

Agrégation de routes par empilement de labels :



- Croissance du réseau facilitée
- Augmentation du nombre de sites transparente au cœur du réseau: toutes les ad réseau connues du LER B reçoivent en entrée le même label
- **L'ensemble des datagrammes qui reçoivent un même label forme une FEC.**
- Le circuit virtuel défini pour une classe d'équivalence est appelé LSP.

Principes et composantes: la FEC

Définition

- Un ensemble de paquets à traiter de la même façon
- Ils sont tous envoyés au même prochain saut
- Une FEC est identifiée par un label

Forwarding Equivalent Class (FEC)

Exemples

- Paquets unicast dont l'adresse destinataire a le même préfixe
- Paquets unicast dont l'adresse destinataire a le même préfixe et le même champ ToS (ou DS)
- Paquets unicast faisant l'objet d'une décision d'ingénierie de trafic
- Paquets appartenant à un même VPN
- Paquets multicast de même source et mêmes destinataires

Granularité

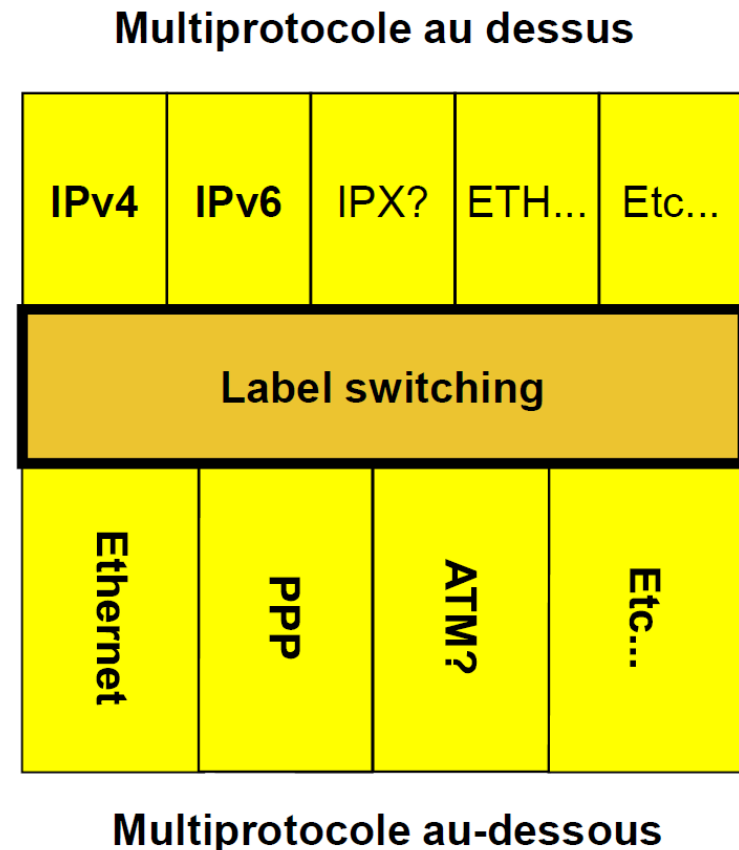
- Peut être quelconque
- Grossière si la FEC regroupe des adresses destinataires de même préfixe
- Fine si la FEC correspond au flux d'une application entre 2 machines

MPLS forwarding

- At ingress LSR:
 - Find the appropriate FEC from packet header
 - Bind label to FEC
 - Encapsulate IP packet in a MPLS packet
- In the core:
 - Perform label switching
 - Send packet on output link
- At egress LSR:
 - De-encapsulate IP packet from MPLS packet
 - Use the FIB to find the next hop

Réseaux d'infrastructure supportés

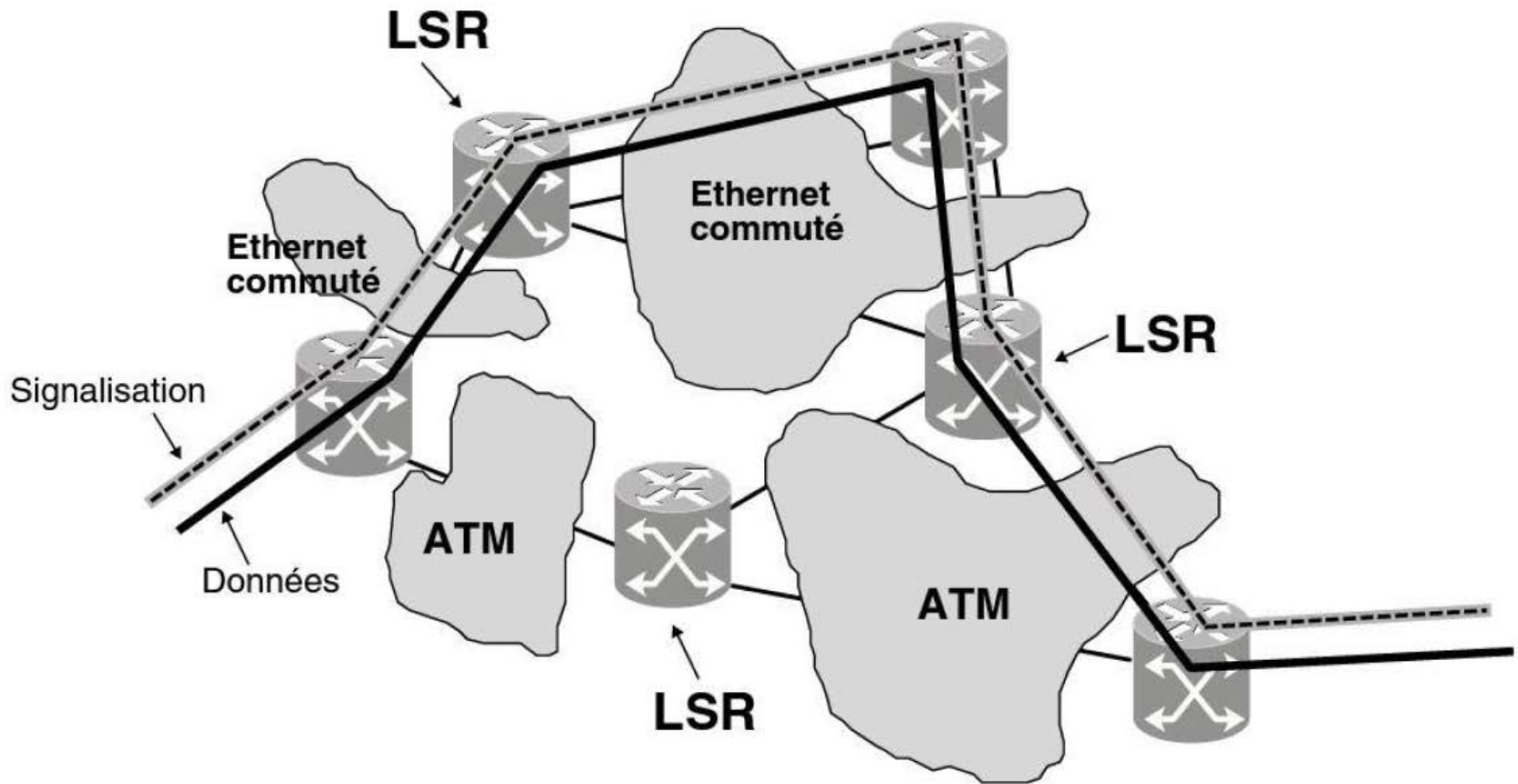
- **Protocole supérieur quelconque**
 - IPv4 ou IPv6 (niveau 3)
 - Ethernet (pour service VPLS)
- **Protocole de niveau 2 quelconque**
 - ATM (pour migration)
 - PPP (sur liaisons Sonet/SDH)
 - Ethernet 1 ou 10 Gbps
 - Combinaison des approches précédentes
- **MPLS est donc flexible**
 - Peut utiliser l'infrastructure ATM existante, puis migrer vers Ethernet ou autre
 - Peut évoluer facilement vers IPv6
 - Peut transporter n'importe quel trafic
 - Par ex. des trames Ethernet (VPN de niveau 2 (VPLS))



VPLS : Virtual Private LAN Service

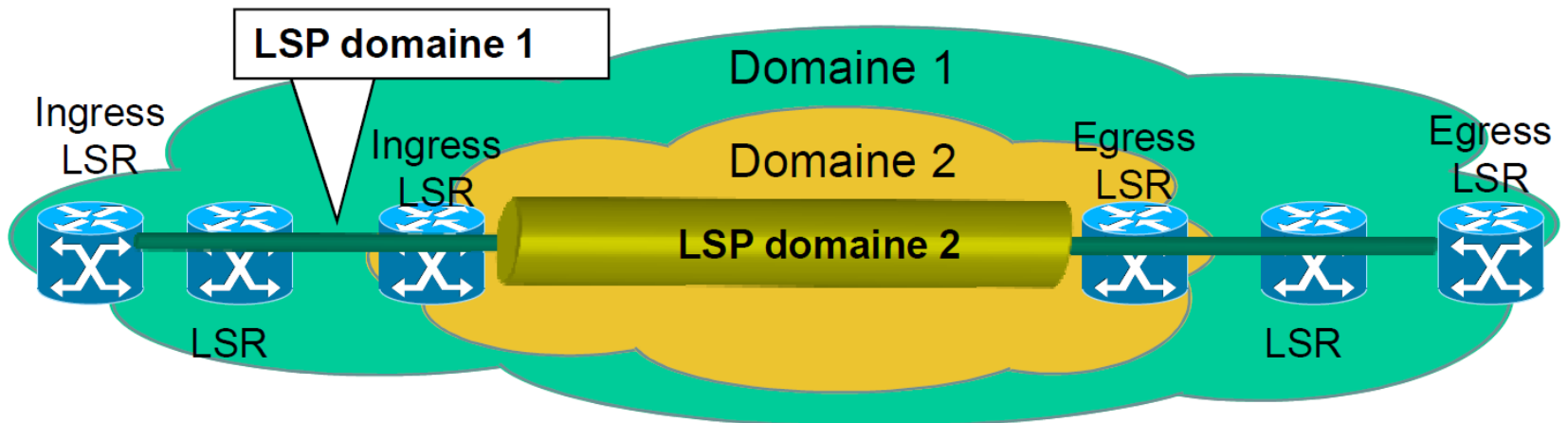
Réseau MPLS de transition

Traversée de plusieurs réseaux spécifiques formant un réseau MPLS afin d'illustrer la transition entre les réseaux de génération ATM et MPLS:

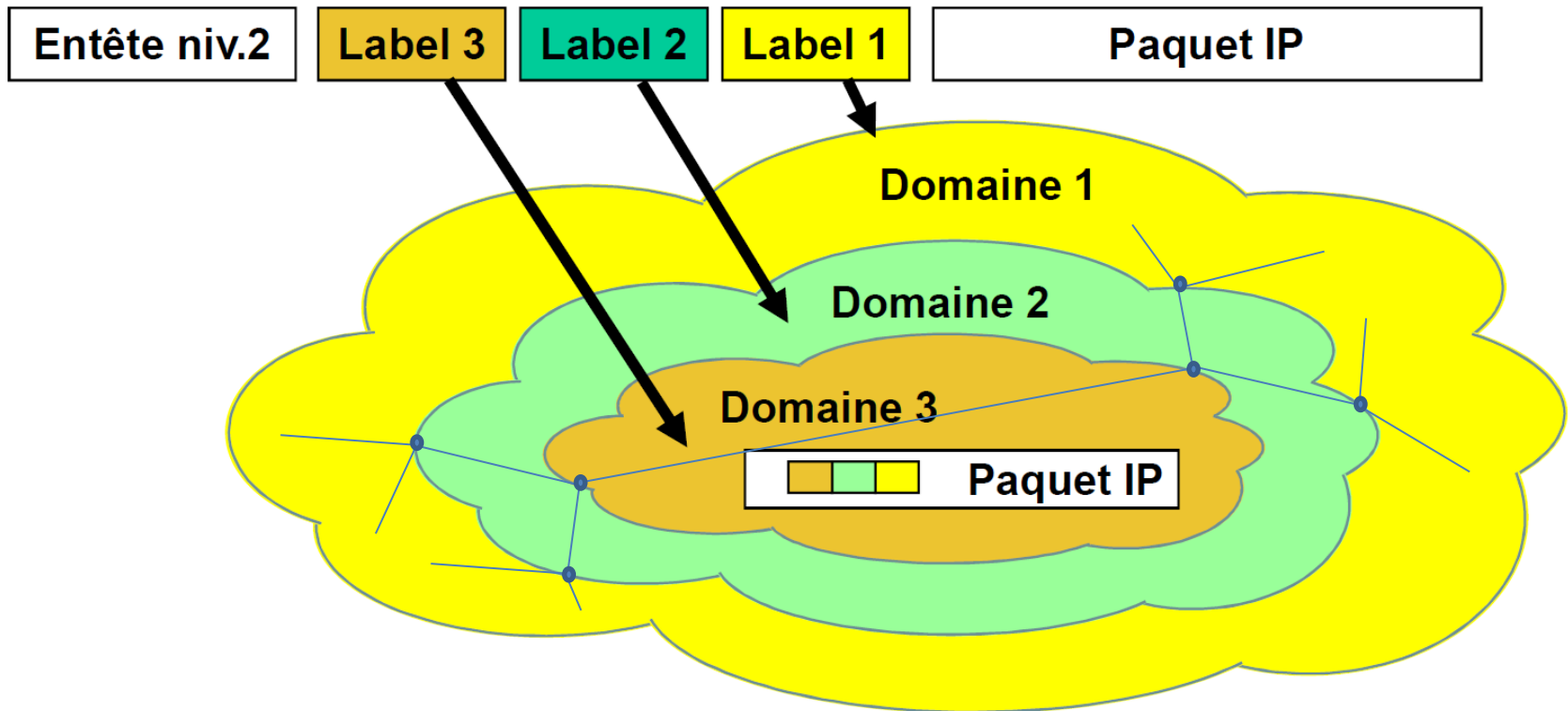


Domaines MPLS

- **Le réseau peut être découpé en domaines administratifs**
 - Ces domaines peuvent être hiérarchisés
- **Relais entre les domaines**
 - Entre ses LSR d'extrémité, le LSP du domaine 2 sert de tunnel au LSP du domaine 1
 - Le paquet est alors précédé d'une pile de 2 labels
 - La pile peut contenir un nombre quelconque de labels
 - Similaire aux conduits ATM, mais plus de 2 niveaux de hiérarchie
 - Permet de réaliser des niveaux d'agrégation dans le cœur de réseau



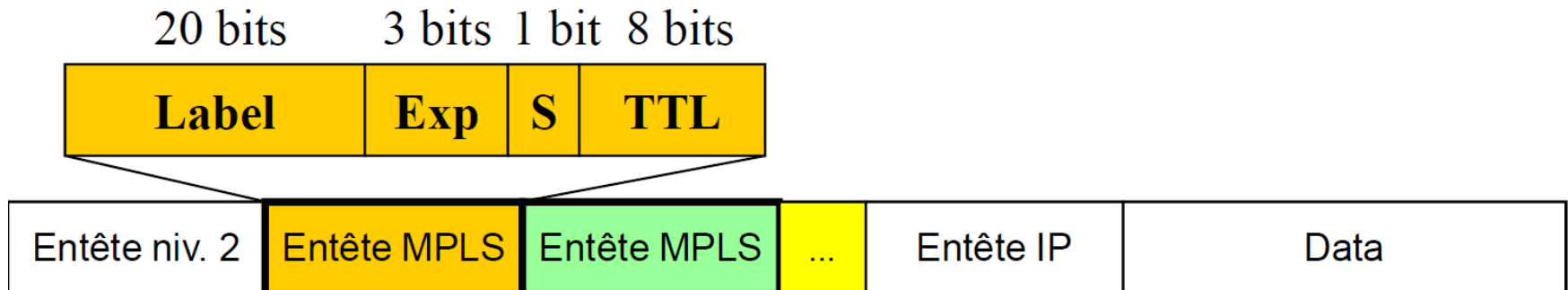
Domaines MPLS hiérarchisés



- **Les domaines MPLS peuvent être hiérarchisés grâce aux piles de labels**
 - Pour augmenter les performances au cœur du réseau
 - Pour permettre les interactions entre opérateurs
- **Les piles de labels sont aussi utilisées pour garantir l'étanchéité des VPN**

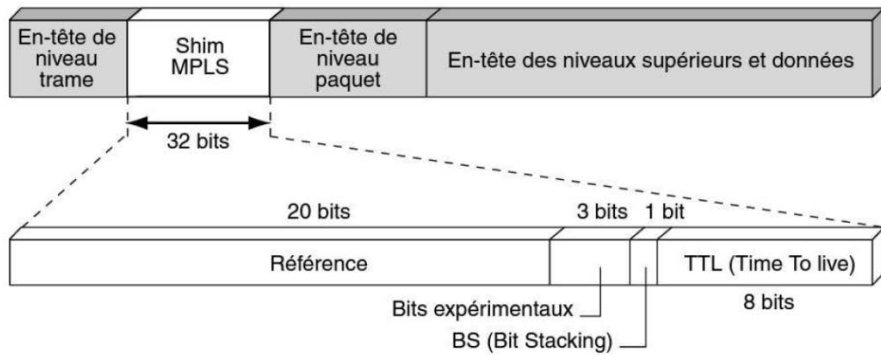
Labels MPLS

- **L'en-tête MPLS est inséré entre le niveau 2 et l'en-tête IP**
 - Label : numéro sur 20 bits (Valeurs 0 à 16 réservées)
 - S sert à gérer des labels hiérarchisés (Stack)
 - Marque le dernier label avant l'entête IP
 - Exp peut être utilisé pour traiter la QoS : files d'attente et rejet
 - Fonctionnement conforme à DiffServ
 - TTL a le même rôle que dans IP (détection de boucles)
- **Opérations sur les labels**
 - Swap (dans les LSRs), push (dans ingress LSR), pop (dans egress LSR)
- **Le label peut éventuellement être implicite**
 - Par exemple une longueur d'onde

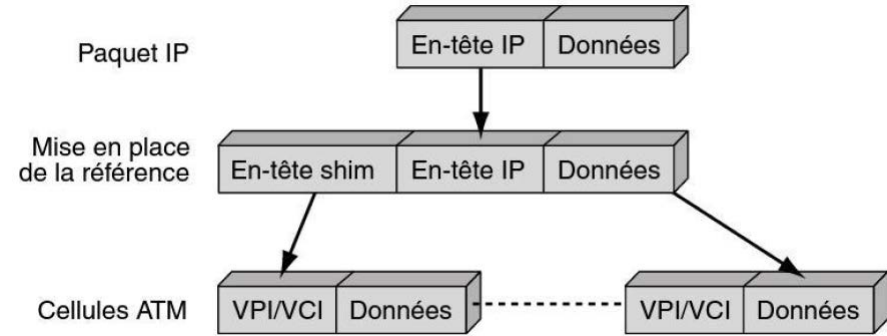


MPLS et les infrastructure existantes

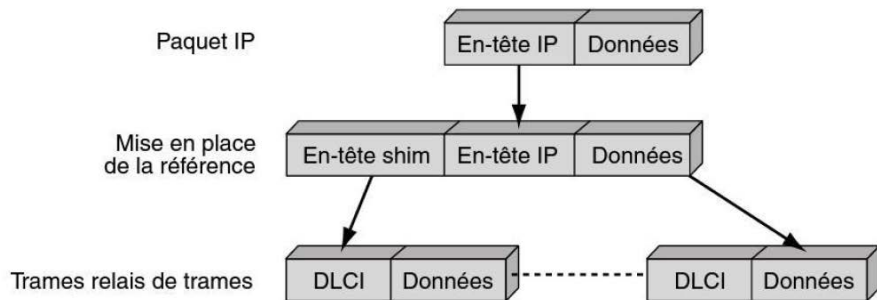
- Quand MPLS est utilisé sur une infrastructure de commutation traditionnelle, il utilise les techniques de la technologie sous-jacente : ceci confère à MPLS une grande facilité d'adaptation puisqu'il ne remet pas en cause les investissements réalisés.
- Dans ces réseaux, la valeur du premier label MPLS affecté est utilisée comme étiquette de commutation : DLCI ou VPi/VCi.
- Un protocole de routage IP traditionnel et un protocole de distribution des labels se substituent à la signalisation d'origine.



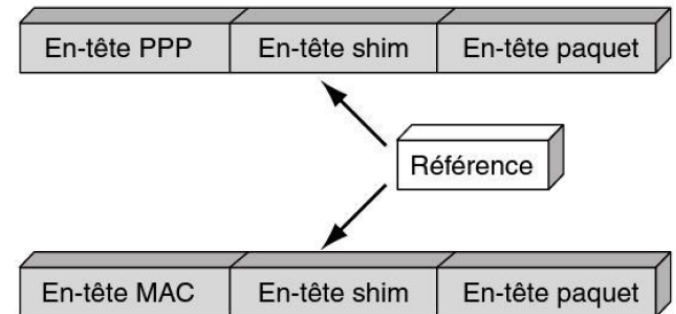
Format générique d'un label (ref) dans MPLS



Mise en place des labels dans ATM



Mise en place des labels dans FR



Mise en place des labels dans PPP et Ethernet

Modes de fonctionnement de MPLS

Modes de fonctionnement (et de signalisation)

Mode datagramme pur

- Les LSR se comportent comme des routeurs
- Quand un label n'est pas attribué à la FEC ou avant qu'un label soit attribué

Mode circuit virtuel « mou »

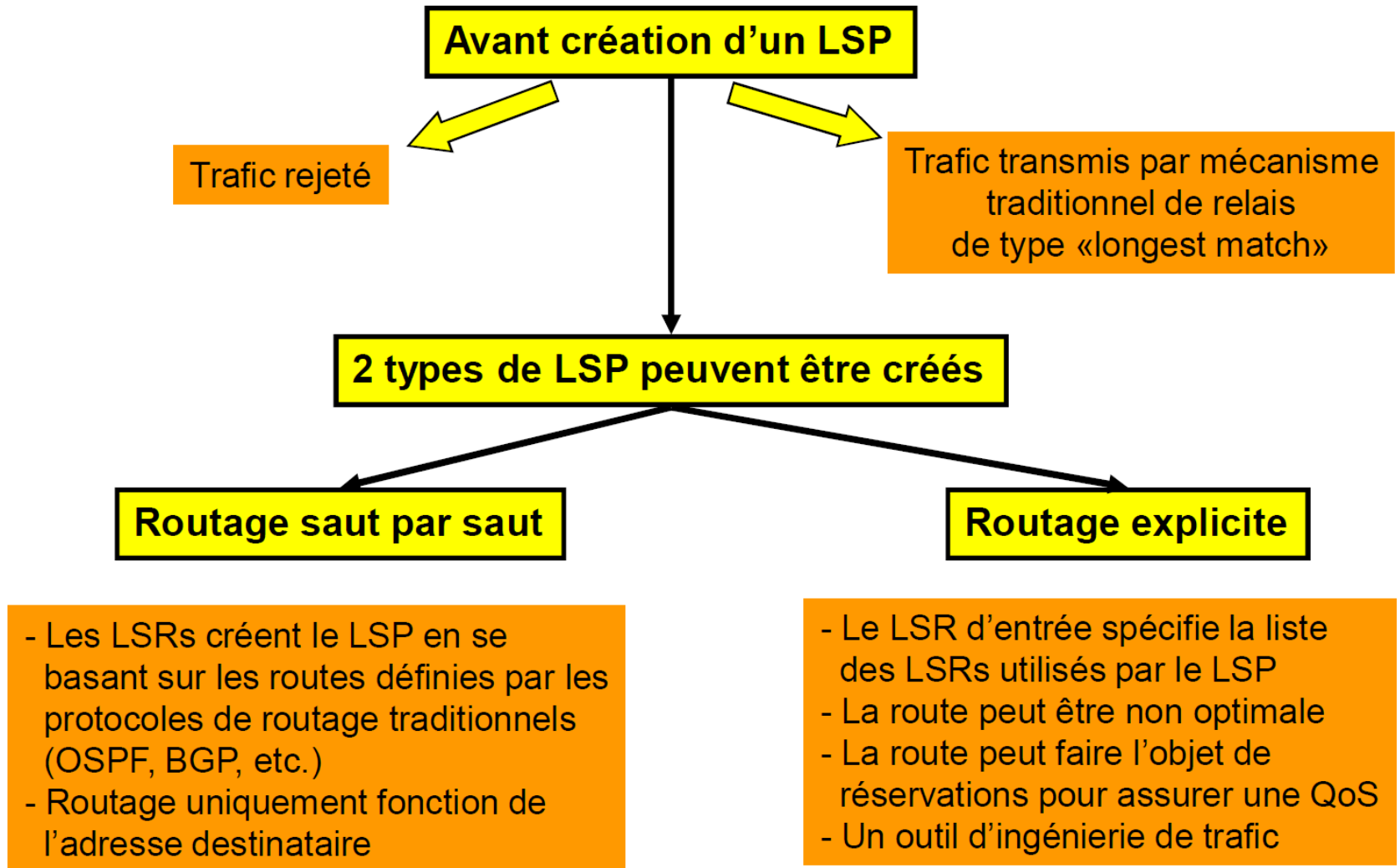
- La création du LSP est déclenchée par l'annonce d'un nouveau préfixe IP par les protocoles de **routing IP**
- Le LSP est créé le long de la meilleure route IP vers le préfixe IP
- Si la meilleure route change, le LSP se reconfigure automatiquement
- Le protocole de signalisation est alors **LDP (Label Distribution Protocol)**

Mode circuit virtuel pur

- La signalisation est déclenchée à l'initiative de l'administrateur
- Le LSP est créé selon une route respectant des contraintes spécifiques
- **Routing explicite** défini par le LSR d'entrée
- Les protocoles de routing sont alors spécifiques (C-OSPF par exemple)
- Le protocole de signalisation est **CR-LDP** ou **RSVP-TE**
- Une réservation de bande passante peut avoir lieu à la création du LSP

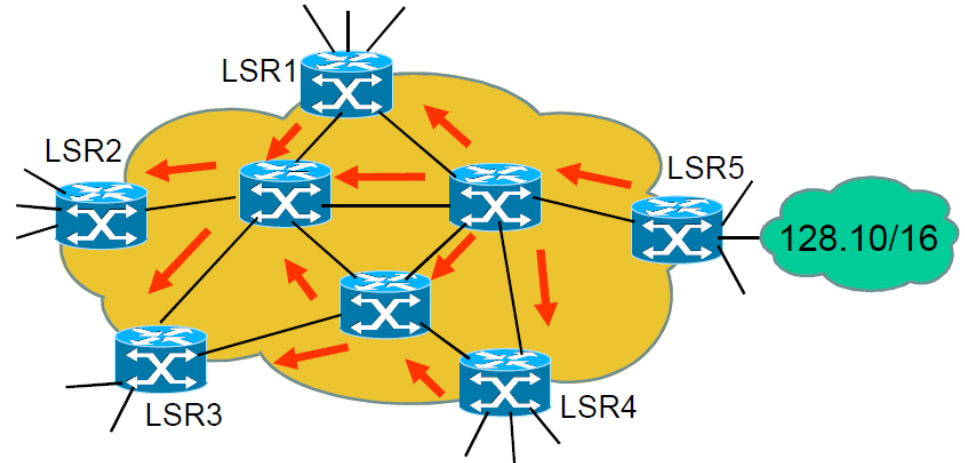
Besoin de signalisation : créer les LIB le long de la route
Le label est attribué par le LSR aval et transmis au LSR amont

Création d'un LSP

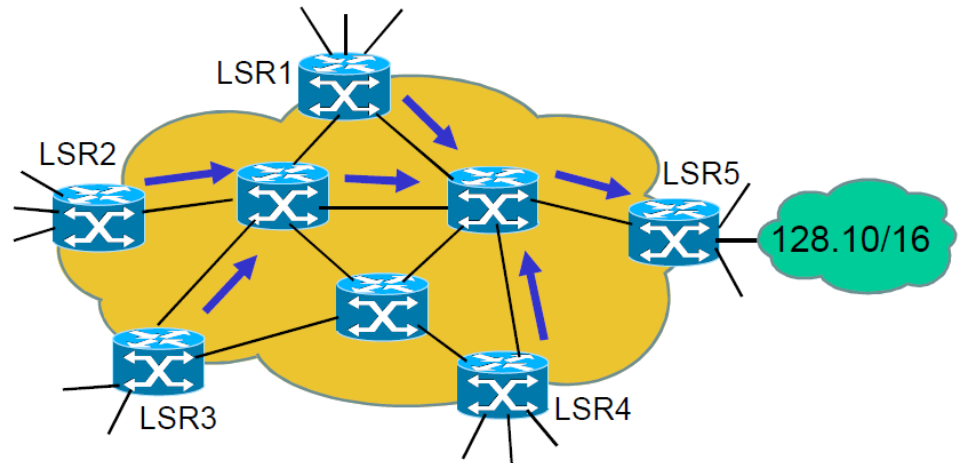


Exemple de signalisation par LDP

- Le préfixe 128.10/16 est annoncé par le protocole de routage
 - Par les messages OSPF →
 - Les LSR d'entrée (LSR1, LSR2, LSR3, LSR4) apprennent l'existence du préfixe 128.10/16



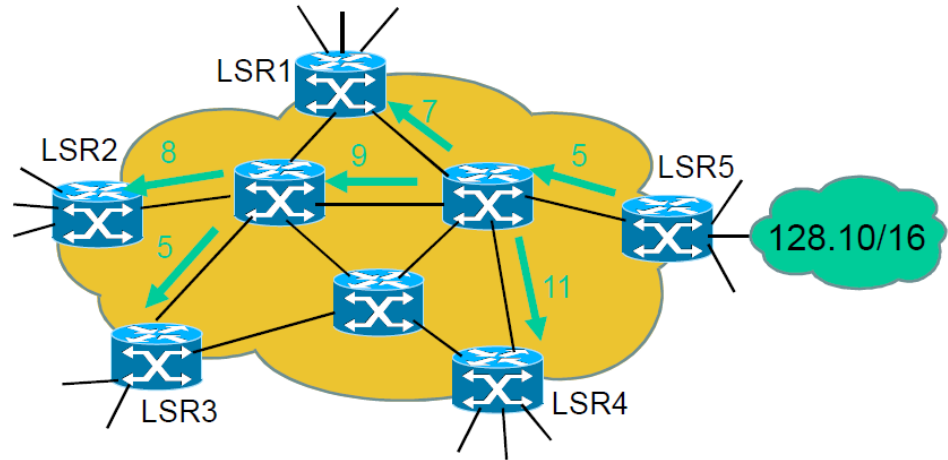
- Les LSR d'entrée (LSR1, LSR2, LSR3 et LSR4) demandent l'établissement d'un LSP vers 128.10/16
 - Par des messages *Label Request* de LDP →
 - Ces messages suivent la meilleure route IP vers 128.10/16



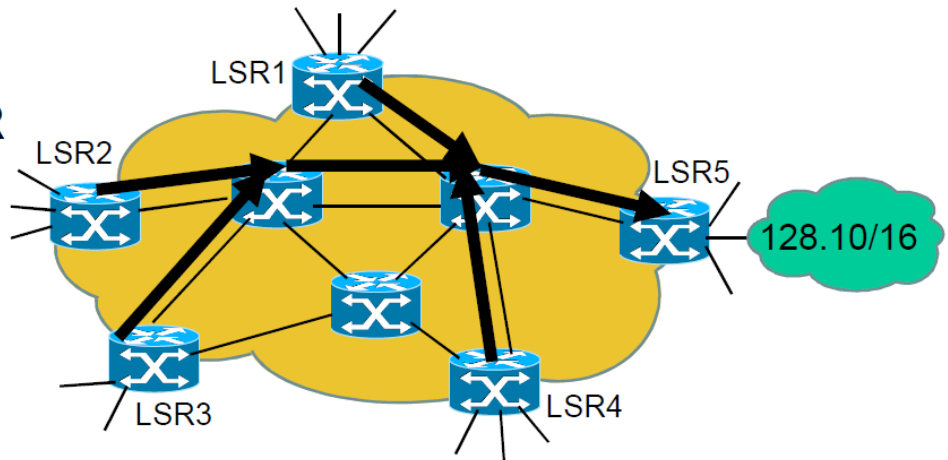
Exemple de signalisation par LDP

- **Les labels sont attribués en commençant par l'aval**

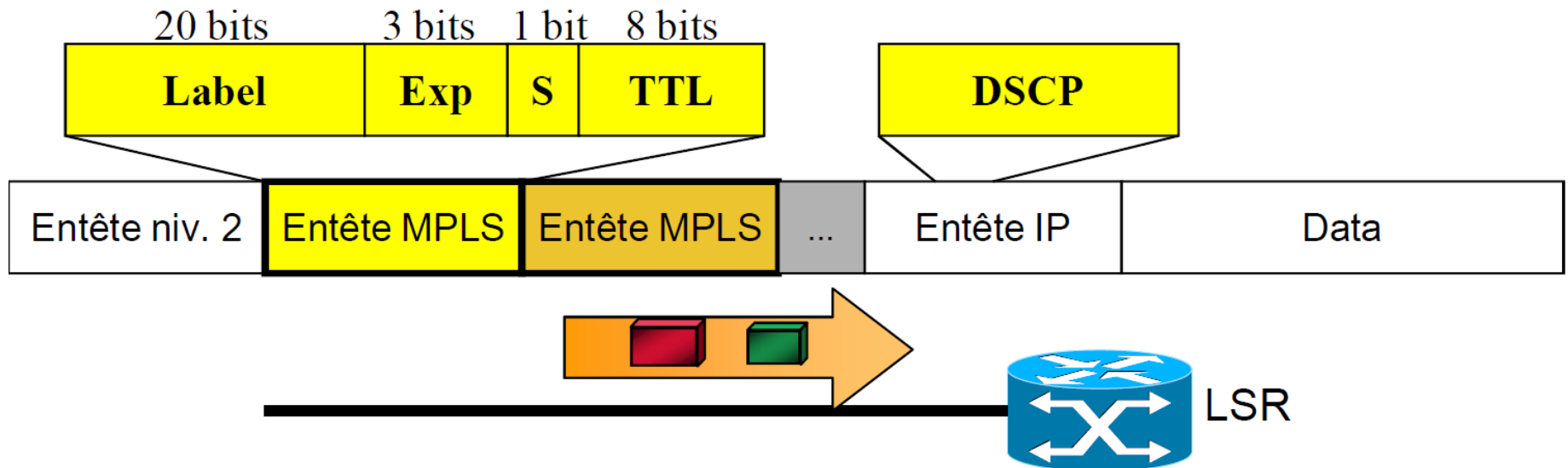
- En partant de l'égress LSR (LSR5), chaque LSR répond au message *Label Request* par un message *label mapping* contenant un n° de label →
- Les Ingress LSR reçoivent leur label



- **Le LSP (multipoint à point) est établi, depuis chaque ingress LSR vers 128.10/16**



MPLS et DiffServ (RFC 3270)



- **Les LSR doivent appliquer le traitement de QoS demandé dans le champ DSCP des paquets IP entrants**
 - Mais le DSCP est dans l'entête IP et ne sera donc plus visible
 - Le LSR Ingress marque le champ Exp (CoS) de l'entête MPLS
 - Il ne peut y avoir que 8 PHB au plus (3 bits)!
- **Les LSR MPLS utilisent DiffServ de la même façon que les routeurs**

Plan

I. Présentation des WAN

II. Les interfaces de la couche physique

III. Protocoles de niveau 2 dans les WAN

IV. MPLS : commutation par VC dans le monde IP

IV.1. Fonctionnement de MPLS

IV.2. Ingénierie de trafic avec MPLS : MPLS-TE

IV.3. Offres de service MPLS : les VPN basés sur MPLS

IV.3.a. IP-VPN

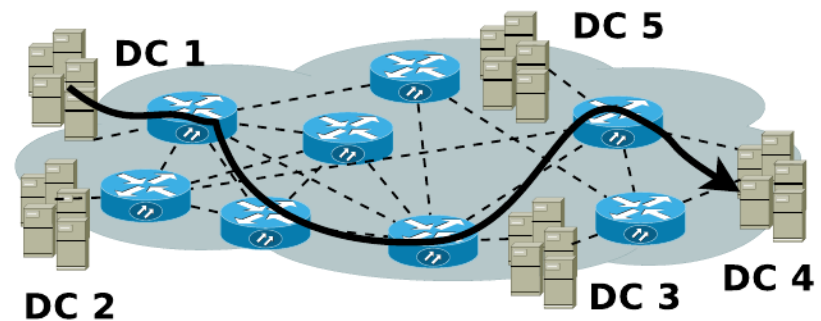
IV.3.b. Ethernet-VPN : VPLS

V. Qualité de service

VI. Technologies xDSL

MPLS Traffic Engineering (MPLS-TE)

- **Ingénierie de trafic (TE)** : processus de décision de comment router/répartir le trafic à travers le réseau du SP
- Le but est de satisfaire une matrice de trafic donnée (des routeurs d'entrée aux routeurs de sortie) tout en optimisant pour les critères de performance tel que délai et taux de pertes.
- Les mécanismes de TE permettent d'utiliser efficacement les ressources du réseau tout en maintenant de bonnes performances pour le trafic.
- MPLS permet de choisir entièrement le chemin suivi par le trafic, alors que TE basé sur le routage (OSPF) ne permet que d'employer le plus court chemin -> pas souvent optimal
- Le TE basé sur MPLS est le plus répandu aujourd'hui, et supporté par les fabricants majeurs tels que Cisco et Juniper.



Caractéristiques des LSP en MPLS-TE

- Un LSP a plusieurs attributs : chemin, bande-passante, priorité, etc.
- 2 types de LSP :
 - statique : allocation d'un chemin et d'une BP lors de l'établissement du LSP, restent constants ensuite
 - dynamique : surveille en continu le débit du trafic à travers ce LSP, et adapte sa BP en fonction. Il peut changer de chemin quand il y a des changements dans sa BP allouée, ou dans la BP disponible du réseau.

Algorithmes MPLS-TE

- Après qu'un chemin est sélectionné, le LSP réserve la BP requise sur l'interface de sortie de chaque routeur du chemin. Chaque interface de sortie de routeur maintient un compteur pour sa BP courante réservable.
- L'information de BP réservable et la topologie du réseau (TED) est périodiquement disséminée sur le réseau (=graphe de connexions avec BP réservable sur chaque branche).
- **Priorité et préemption** : Chaque LSP est configuré avec 2 valeurs de priorité : priorité d'établissement et priorité de maintien.
 - La **priorité d'établissement** détermine si un nouvel LSP peut être établi en préemptant un LSP existant.
 - La **priorité de maintien** détermine dans quelle mesure un LSP existant peut garder sa réservation.
 - Un nouvel LSP avec une haute priorité d'établissement peut préempter un LSP existant avec une basse priorité de maintien si : (a) il n'y a pas assez de BP réservable dans le réseau; ou (b) le nouvel LSP ne peut pas être établi à moins qu'un LSP existant ne soit effacé.

Algorithmes MPLS-TE

- **CSPF** : trie les LSP selon leurs priorités et sélectionne le plus court chemin pour chaque LSP.
 - Commence avec le LSP de plus haute priorité, élague le TED en enlevant les liens qui n'ont pas une BP réservable suffisante,
 - Assigne ensuite le chemin le plus court dans ce TED élagué au LSP et met à jour la BP réservable sur les liens affectés.
 - Ce processus se poursuit jusqu'à ce qu'il ne reste plus de LSP.
- **Ré-optimisation** : CSPF est lancé périodiquement pour ré-assigner à chaque LSP un meilleur chemin si possible.
- **AutoBP** : MPLS ne contrôle pas le débit (BP) utilisé par le trafic sur un LSP : un LSP peut porter tout débit de trafic indépendamment de sa BP réservée.
 - A la place de ce possible contrôle, un mécanisme d'autoBP permet à un LSP d'ajuster sa BP réservée au débit courant.
 - Pour utiliser autoBP, un LSP a besoin de plusieurs paramètres en plus : seuil d'ajustement, intervalle d'ajustement et intervalle d'échantillonnage.
 - Chaque intervalle d'échantillonnage (ex : 5 min), un LSP mesure le débit moyen qu'il supporte. Chaque intervalle d'ajustement (ex : 15 min), il calcule le max du débit moyen mesuré sur chaque intervalle d'éch.
 - Si le max du débit utilisé diffère de la BP réservée courante de plus que le seuil d'ajustement, alors le LSP invoque CSPF avec le max du débit comme nouvelle BP à réserver.

MPLS : quelques chiffres

- 7% des AS utilisent MPLS, le plus gros déploiement chez les fournisseurs de tiers-1
- 90% des LSP avec 7 sauts ou moins, certains avec plus de 15
- 25% de tous les chemins en 2011 traversent au moins 1 tunnel MPLS, 4% plus d'un
- Il semble que beaucoup d'AS emploient de la classification de trafic et de l'ingénierie dans leurs tunnels.

Plan

I. Présentation des WAN

II. Les interfaces de la couche physique

III. Protocoles de niveau 2 dans les WAN

IV. MPLS : commutation par VC dans le monde IP

IV.1. Fonctionnement de MPLS

IV.2. Ingénierie de trafic avec MPLS : MPLS-TE

IV.3. Offres de service MPLS : les VPN basés sur MPLS

IV.3.a. IP-VPN

IV.3.b. Ethernet-VPN : VPLS

V. Qualité de service

VI. Technologies xDSL

at&t Enterprise

PRODUCTS & SERVICES NETWORKING EXCHANGE NEWS & INSIGHTS SUPPORT

Application Services Content Delivery Hosting Services Mobility Services Network Security Network Services Unified

Products & Services : Network Services : IP VPN

IP VPN

AT&T MPLS: Maximizing Performance over Your IP VPN
[10:20]

NETWORK MANAGEMENT

Ethernet

- Metro Ethernet
- Wide Area Ethernet

Frame Relay

Internet Connectivity

- Business DSL
- Managed Internet Service
- AT&T Wi-Fi Services, Formerly Wayport, Inc.

IP VPN

- Remote Access VPN

Private Line

Ring Services

- SONET Ring
- WaveLength Ring

and other business applications. IP VPNs provide the foundation for a highly secure, reliable network that can connect your corporate headquarters, data centers, branch offices, and remote and mobile workers to each other, and to the applications they need to be productive.

To be effective, employees need access to your mission critical applications

MPLS ET OFFRES DE SERVICE

Sources:

- *VPLS Technical Tutorial*, Technology White Paper, Alcatel-Lucent, 2010
- *Enabling High-Performance Data Services with Ethernet WAN and IP VPN*, IDC White Paper, 2011
- The CCIE R&S: <http://aitaseller.wordpress.com/2012/09/10/mpls-layer-3-vpns/>

Une application de MPLS:

Différents types de VPN basés MPLS

MPLS permet une application très répandue: le support des Virtual Private Networks (VPNs) aux opérateurs, pour que les clients puissent avoir des sites géographiques éloignés connectés au travers du réseau de l'opérateur.

Différents types de VPN basés MPLS:

- Layer 3 VPNs:
 - le SP participe au routage niveau 3 du client.
 - Le routeur CE du client sur chaque site communique avec un protocole de routage (tel que BGP ou OSPF) avec les routeur PE du SP. Les préfixes IP annoncés par chaque site client sont portés par le réseau du SP.
- Layer 2 VPNs:
 - Sites clients interconnectés par techno niveau 2 (ATM, FR ou Ethernet).
 - Le client est seul en charge du routage.
- Virtual Private LAN Service:
 - Le réseau du SP est vu comme un switch Ethernet par le client.
 - Les clients voient le WAN comme un réseau local avec un techno de réseau local bien connue: Ethernet.
 - Contrairement aux services MetroEthernet, des sites clients à l'échelle du continent ou de la planète peuvent être interconnectés par VPLS.
 - Donc un client avec des sites à Londres, Moscou, Hong Kong, Seattle, et New York peut les connecter avec ce qui lui apparaît comme étant un seul switch Ethernet.

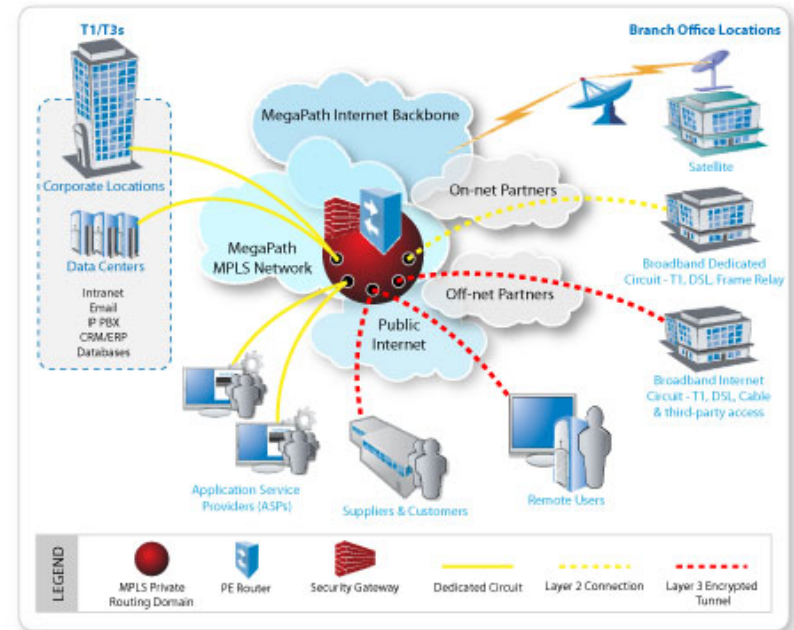
Principe d'un VPN

- “Virtual” de VPN: les services individuels donnent l'impression d'être séparés entre les clients, mais sont en fait fournis par une même infrastructure: le réseau MPLS.

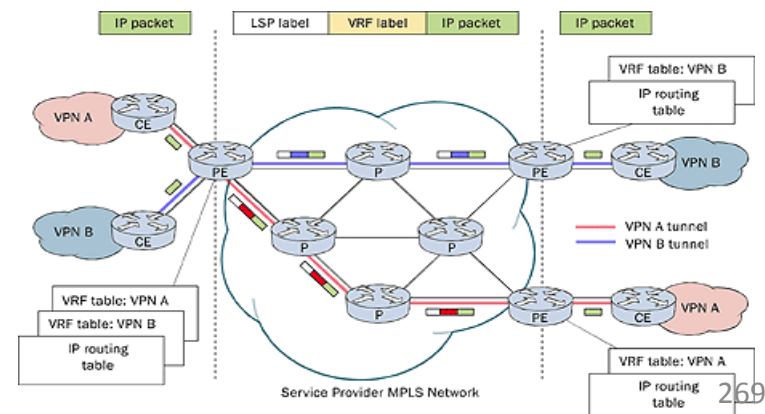
--> Optimisation de l'utilisation des ressources du SP

- “Private” de VPN: les réseaux des clients doivent rester séparés les uns des autres pour la sécurité:

- Clients A et B, en L3 VPNs, ne doivent pas voir les préfixes IP de l'autre. Leurs espaces d'adressage peuvent même se chevaucher car le SP garde les préfixes IP séparés.
- Clients C et D, en L2 VPNs, ne doivent pas voir les adresses de couche 2 de l'autre.
- Clients E et F en VPLS, ne doivent pas voir qu'ils sont connectés au même switch Ethernet (virtuel).

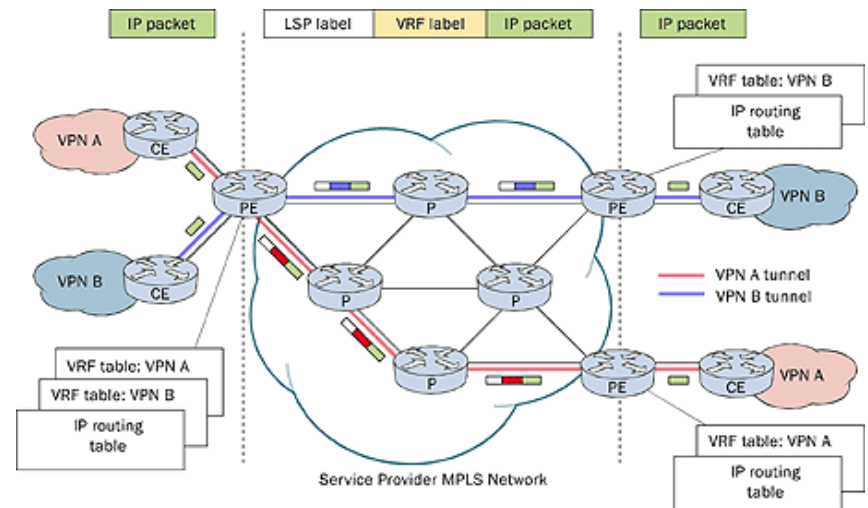


Site-to-Site MPLS VPN



Principe de fonctionnement : la séparation des tables de routage ou d'adressage

- Pour la confidentialité entre VPNs: les sites clients (leurs tables) interconnectés par des LSP MPLS différents
- La table dépend du type de VPN:
 - L3 VPN : les tables contiennent les préfixes IP et s'appellent Virtual Routing and Forwarding Tables (VRF). Les VRFs sont simplement des tables de routage dédiées.
 - L2 VPN : Virtual Forwarding Tables (VFT), contiennent les adresses de couches 2, ou les DLCI de FR, etc...
 - VPLS : contiennent les adresses MAC Ethernet, et les VLAN IDs si VLAN, mappées aux LSPs menant aux autres sites. Même rôle que les MAC tables dans les switches Ethernet.



Les avantages des VPN basés MPLS

- **Service sans connection** : Internet doit son succès à la techno TCP/IP basique: pas d'action nécessaire avant la communication entre 2 hôtes. Un VPN basé MPLS supprime le besoin du tunnels et d'encryption pour assurer la confidentialité, donc beaucoup moins de complexité.
- **Passage à l'échelle** : seuls les routeurs PE mémorisent les routes des VPN qu'ils gèrent. Les routeurs P non. Donc pas d'augmentation de complexité dans le coeur du réseau avec l'augmentation de clients.
- **Sécurité** : Les paquets d'un VPN ne peuvent pas par erreur aller dans un autre VPN:
 - Sur le bord, assure que les paquets d'un client sont placés dans le bon VPN.
 - Dans le coeur, le trafic des VPN reste séparé. Le spoofing (essai d'avoir accès à un routeur PE) quasi-impossible car les paquets reçus des clients sont IP. Ces paquets IP doivent être reçus sur une interface ou sous-interface particulière attachée à un seul label VPN.
- **Adressage flexible** : beaucoup de clients utilisent des plages d'adresses privées, et ne veulent pas les convertir en public (temps et argent). Les VPN MPLS permettent à ces clients de continuer à utiliser ces adresses privées sans besoin de NAT.
- **Qualité de service** : permet de satisfaire 2 contraintes importantes pour les VPN:
 - Performance prédictible et implémentation de politiques pour SLA
 - Supporte plusieurs niveaux de service dans un VPN MPLS

Le trafic est classifié et labellisé au bord pour être traité de façon différenciée selon les classes (avec différents délais ou proba d'abandon par exemple).

Plan

I. Présentation des WAN

II. Les interfaces de la couche physique

III. Protocoles de niveau 2 dans les WAN

IV. MPLS : commutation par VC dans le monde IP

IV.1. Fonctionnement de MPLS

IV.2. Ingénierie de trafic avec MPLS : MPLS-TE

IV.3. Offres de service MPLS : les VPN basés sur MPLS

IV.3.a. IP-VPN

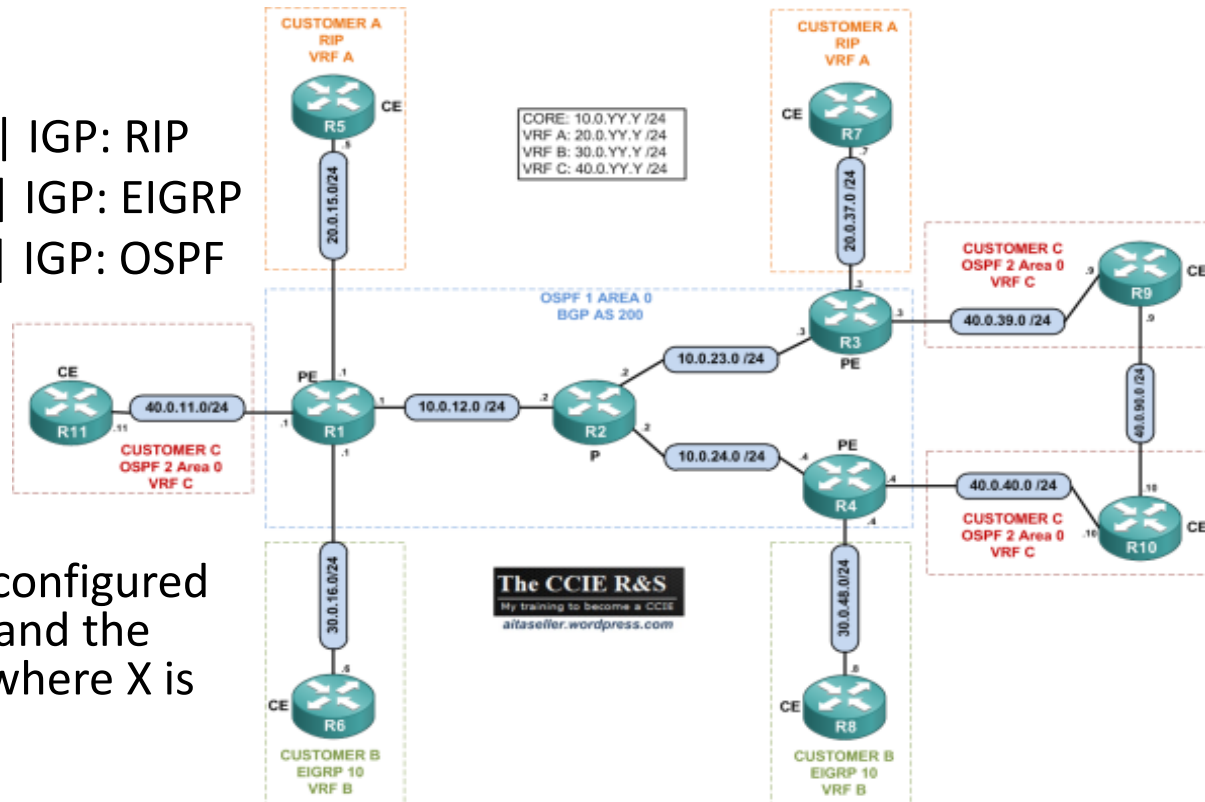
IV.3.b. Ethernet-VPN : VPLS

V. Qualité de service

VI. Technologies xDSL

Configuration d'un IP-VPN basé MPLS sur un exemple Cisco

- Platform/IOS: Cisco 691/12.4(15)
- VRFs:
 - Customer A: VRF A | IGP: RIP
 - Customer B: VRF B | IGP: EIGRP
 - Customer C: VRF C | IGP: OSPF
 - ISP: Core IGP: OSPF
MP-BGP AS 200
- Addressing:
 - All the routers are configured with a Loopback IP and the format X.X.X.X /32 where X is the router number.



Les VPN MPLS sont une combinaison de différents protocoles et technologies: ils s'appuient sur MPLS et peuvent gérer différents protocoles de routage pour les clients. Ces VPN s'appuient sur le protocole MP-BGP (multiprotocol BGP) pour échanger les routes VPN. MP-BGP est une évolution de BGP gérant les VRF. MP-BGP gère une nouvelle famille d'adresses nommée "VPNv4" (VPN IPv4).

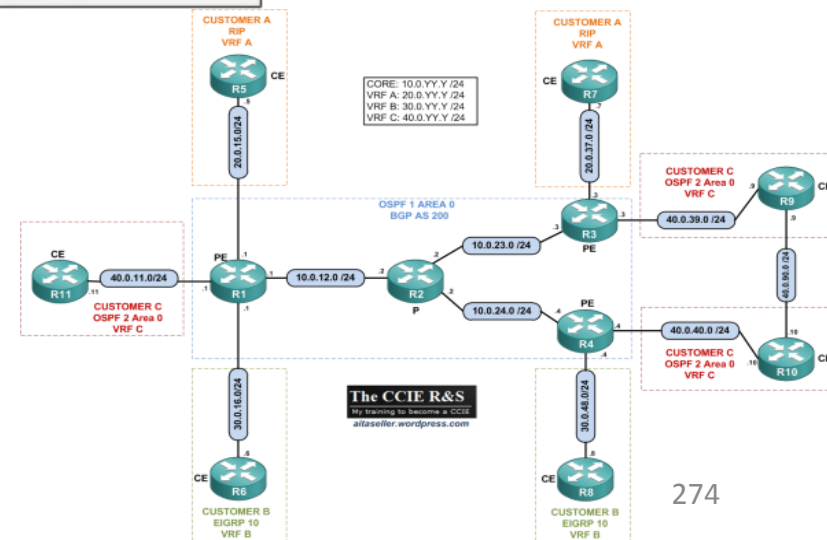
1. Configuration MPLS du coeur de l'ISP

Activer LDP sur tous les routeurs du coeur:

```
R1-R4
conf t
router ospf 1
!!!ENABLE LDP on all OSPF interfaces!!!
mpls ldp autoconfig
```

Les voisins LDP échangent préfixes et labels associés, constituant la FLIB :

```
R1#sh mpls forwarding-table
Local   Outgoing   Prefix          Bytes tag  Outgoing     Next Hop
tag     tag or VC  or Tunnel Id    switched  interface
16      Pop tag    2.2.2.2/32      0         Fa1/0        10.0.12.2
17      17         3.3.3.3/32      0         Fa1/0        10.0.12.2
18      18         4.4.4.4/32      0         Fa1/0        10.0.12.2
19      Untagged   10.0.24.0/24    0         Fa1/0        10.0.12.2
20      Untagged   10.0.23.0/24    0         Fa1/0        10.0.12.2
```

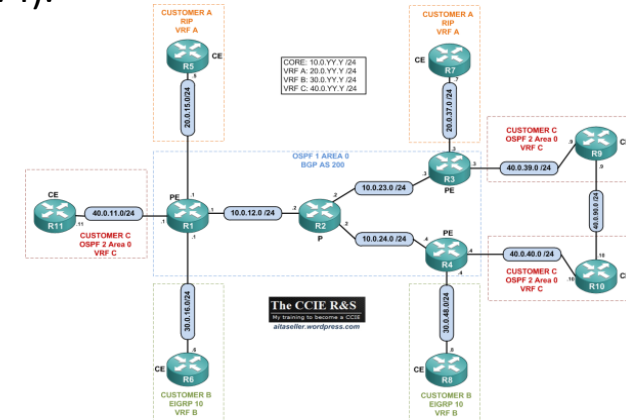


2. Etablissement des sessions MP-BGP entre les PE

Etablissons les sessions MP-BGP entre les PE (pour ensuite échanger les routes entre les CE).

On établit un maillage complet de sessions MP-BGP entre les 3 PE en désactivant la famille d'@ IPv4 unicast address-family (car ici on échangera seulement des préfixes VPNv4).

```
R1,R3,R4
conf t
router bgp 200
no bgp default ipv4-unicast
bgp log-neighbor-changes
neighbor X.X.X.X remote-as 200
neighbor X.X.X.X update-source Loopback0
!
address-family vpnv4
neighbor X.X.X.X activate
neighbor X.X.X.X send-community extended
```



On vérifie sur R1 que les sessions sont établies entre tous les PE:

```
R1#sh bgp vpnv4 unicast all summary
BGP router identifier 1.1.1.1, local AS number 200
BGP table version is 1, main routing table version 1

Neighbor      V    AS MsgRcvd MsgSent  TblVer  InQ  OutQ Up/Down  State/PfxRcd
3.3.3.3       4   200    16     17      1     0    0 00:13:33 0
4.4.4.4       4   200    15     15      1     0    0 00:11:51 0
```

Etape suivante: configurer les VRF respectifs sur les différents PE, et les protocoles de routage CE-PE.

3. Configuration des VRF

- Pour créer un nouveau VRF: commande `ip vrf <VRF_NAME>` pour entrer en mode config de VRF.
- Puis configuration d'un *Route Distinguisher (RD)* pour chaque VRF avec `rd X:Y` où X et Y sont 32 bits.
Le RD est un préfixe de 64 bits ajouté à chaque route dans sa table VRF respective.
- Le format du RD est usuellement ASN:NN (Autonomous System Number et NN est le numéro du VRF) ou IP-Address-PE:NN.
- Dans cet exemple: - VRF A: rd=200:1 - VRF B: rd=200:2 - VRF C: rd=200:3
- Le RD a un sens local au PE et ne peut pas être utilisé pour établir l'appartenance des routes aux VPN.
- L'attribut *Route Target (RT)* (64 bits) détermine l'appartenance d'une route à un VPN, le RT est attaché à chaque route exportée.
- Un préfixe IPv4 avec un préfixe RT en plus est un préfixe VPNv4 de 96 bits (32+64).
- Quand un routeur PE reçoit un préfixe, le routeur regarde le RT attaché et vérifie s'il a un VRF qui correspond au RT attaché à la route :
 - Si le PE a ce RT dans les RT à importer, le préfix VPNv4 est importé dans la VRF correspondante.
 - Sinon le préfixe est abandonné.
- RT définis dans le mode de config VRF: `route-target export X:Y`

- Dans notre exemple, on utilise les RT suivants pour les VRF:
VRF A: rt=200:1 pour import et export
VRF B: rt=200:2 pour import et export
VRF C: rt=200:3 pour import et export

D'où la configuration des différents VRF sur les PE :

```
R1
!
ip vrf VRFA
rd 200:1
route-target export 200:1
route-target import 200:1
!
ip vrf VRFB
rd 200:2
route-target export 200:2
route-target import 200:2
!
ip vrf VRFC
rd 200:3
route-target export 200:3
route-target import 200:3

R3
!
ip vrf VRFA
rd 200:1
route-target export 200:1
route-target import 200:1
!
ip vrf VRFC
rd 200:3
route-target export 200:3
route-target import 200:3
!

R4
!
ip vrf VRFB
rd 200:2
route-target export 200:2
route-target import 200:2
!
ip vrf VRFC
rd 200:3
route-target export 200:3
route-target import 200:3
```

On associe ensuite chaque VRF à l'interface CE correspondante: `ip vrf forwarding <VRF NAME>`

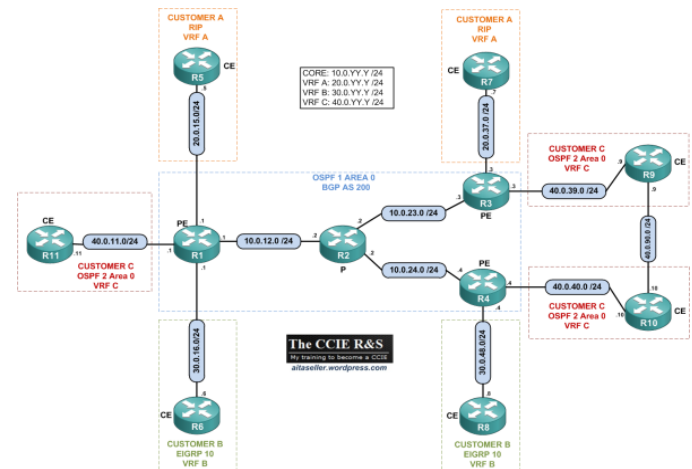
```
R1#sh ip vrf interfaces
Interface      IP-Address      VRF      Protocol
Fa0/0          20.0.15.1       VRFA     up
Fa0/1          30.0.16.1       VRFB     up

R3#sh ip vrf interfaces
Interface      IP-Address      VRF      Protocol
Fa1/0          20.0.37.3       VRFA     up
Fa0/1          40.0.39.3       VRFC     up

R4#sh ip vrf interfaces
Interface      IP-Address      VRF      Protocol
Fa0/1          30.0.48.4       VRFB     up
Fa1/0          40.0.40.4       VRFC     up
```

Chaque routeur CE est placé dans la bonne VRF.

Prochaine étape : Configurer les protocoles de routage PE-CE de chaque site pour que l'ISP et les différents clients puissent échanger leurs préfixes.



4. Configuration des protocoles de routage PE-CE

On utilise ici RIP, EIGRP et OSPF. Chaque CE est déjà configuré et annonce son adresse de loopback.

Commençons avec la config du process RIP tenant compte des VRF :

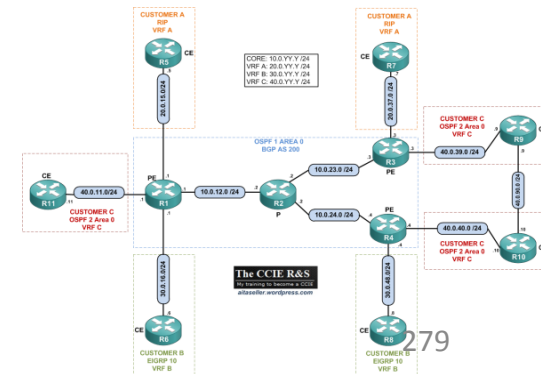
```
R1#sh run | sec rip
router rip
version 2
no auto-summary
!
address-family ipv4 vrf VRFA
network 20.0.0.0
no auto-summary
exit-address-family
```

On vérifie que R1 a appris l'adresse de loopback de R5 par une mise à jour RIP :

```
R1#sh ip route vrf VRFA 5.5.5.5
Routing entry for 5.5.5.5/32
Known via "rip", distance 120, metric 1
Redistributing via rip
Last update from 20.0.15.5 on FastEthernet0/0, 00:00:01 ago
Routing Descriptor Blocks:
* 20.0.15.5, from 20.0.15.5, 00:00:01 ago, via FastEthernet0/0
Route metric is 1, traffic share count is 1
```

Activation de RIP sur R3 et on vérifie que R3 a appris l'adresse de loopback de R7 :

```
R3#sh ip route vrf VRFA 7.7.7.7
Routing entry for 7.7.7.7/32
Known via "rip", distance 120, metric 1
Redistributing via rip
Last update from 20.0.37.7 on FastEthernet1/0, 00:00:14 ago
Routing Descriptor Blocks:
* 20.0.37.7, from 20.0.37.7, 00:00:14 ago, via FastEthernet1/0
Route metric is 1, traffic share count is 1
```



Pareil pour EIGRP :

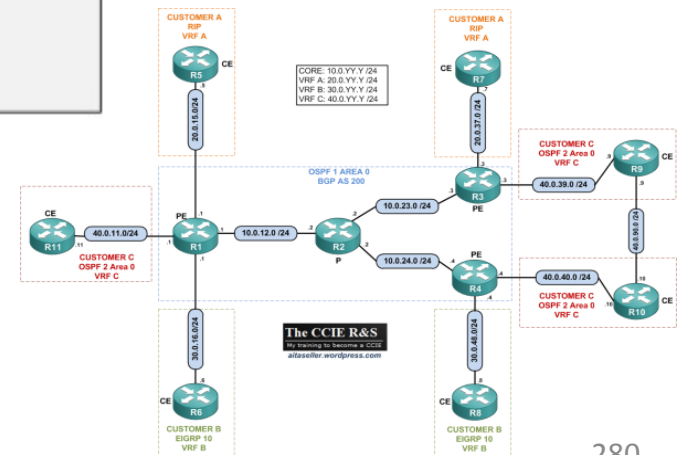
```
R1
router eigrp 1
no auto-summary
!
address-family ipv4 vrf VRFB
network 30.0.16.1 0.0.0.0
auto-summary
autonomous-system 10      -> specify the AS in the routing context
exit-address-family
```

Et on vérifie que R1 a appris l'adresse de loopback de R6 :

```
R1#sh ip route vrf VRFB 6.6.6.6
Routing entry for 6.6.6.6/32
  Known via "eigrp 10", distance 90, metric 156160, type internal
  Redistributing via eigrp 10
  Last update from 30.0.16.6 on FastEthernet0/1, 00:00:27 ago
  Routing Descriptor Blocks:
  * 30.0.16.6, from 30.0.16.6, 00:00:27 ago, via FastEthernet0/1
  !!!OUTPUT OMITTED!!!
```

Idem pour R4 et R8 :

```
R4#sh ip route vrf VRFB 8.8.8.8
Routing entry for 8.8.8.8/32
  Known via "eigrp 10", distance 90, metric 156160, type internal
  Redistributing via eigrp 10
  Last update from 30.0.48.8 on FastEthernet0/1, 00:00:20 ago
  Routing Descriptor Blocks:
  * 30.0.48.8, from 30.0.48.8, 00:00:20 ago, via FastEthernet0/1
  !!!OUTPUT OMITTED!!!
```



OSPF: On configure un processus OSPF pour certaines VRF. Pour configurer OSPF comme un protocole de routage PE-CE, il faut un process OSPF pour chaque VRF où on veut de l'OSPF. Coeur de l'ISP utilise OSPF process 1 -> on prend process 2 pour la configuration PE-C.

```
R3
router ospf 2 vrf VRFC
router-id 3.3.3.3
```

Vérifions que R3 apprend bien l'adresse de loopback de R9 :

```
R3#sh ip route vrf VRFC 9.9.9.9
Routing entry for 9.9.9.9/32
  Known via "ospf 2", distance 110, metric 2, type intra area
  Last update from 40.0.39.9 on FastEthernet0/1, 00:16:33 ago
  Routing Descriptor Blocks:
    * 40.0.39.9, from 40.0.90.9, 00:16:33 ago, via FastEthernet0/1
      Route metric is 2, traffic share count is 1
```

On configure un process OSPF sur R4 et on vérifie que R4 apprend l'adresse de loopback de R10:

```
R4
router ospf 2 vrf VRFC
router-id 4.4.4.4
```

```
R4#sh ip route vrf VRFC 10.10.10.10
Routing entry for 10.10.10.10/32
  Known via "ospf 2", distance 110, metric 2, type intra area
  Last update from 40.0.40.10 on FastEthernet1/0, 00:17:53 ago
  Routing Blocks:
    * 40.0.40.10, from 10.10.10.10, 00:17:53 ago, via FastEthernet1/0
      Route metric is 2, traffic share count is 1
```

Ok, tous ces protocoles de routage PE-CE sont configurés pour les différents sites.

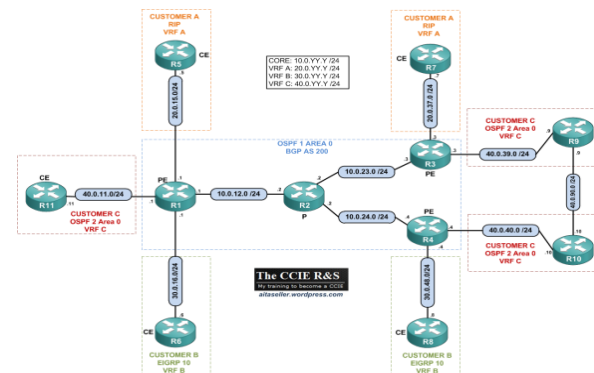
Maintenant il faut configurer l'échange des préfixes VPNv4 entre les PEs dans le but d'échanger les routes des clients entre les différents sites.

5. Configurer l'échange des préfixes VPNv4 avec MP-BGP

- On a juste besoin de redistribuer chaque protocole de routage CE dans BGP pour le VRF spécifique, et redistribuer BGP dans chaque CE pour le VRF spécifique.
- Redistribution mutuelle entre RIP et BGP pour la VRFA :

```
R1
router bgp 200
!
address-family ipv4 vrf VRFA
 redistribute rip
 no synchronization
 exit-address-family
```

- Dès qu'on redistribue RIP dans le process BGP, R1 annonce les préfixes du client A à tous ses voisins MP-BGP.
- On peut voir ce paquet MP-BGP de mise à jour VPNv4 envoyé par R1 vers R3 et R4 pour le préfixe 20.0.15.0/24 :



- Le RT configuré est attaché au préfixe.
 - Cette update est envoyée dans le coeur avec MPLS : label 17 correspondant à la loopback de R3
- > Le routeur de coeur P (R2 ici) ne fait que du label switching et pas de routage IPv4.

```

# Frame 73: 239 bytes on wire (1912 bits), 239 bytes captured (1912 bits)
# Ethernet II, Src: c0:05:21:c0:00:10 (c0:05:21:c0:00:10), Dst: c0:03:21:c0:00:00 (c0:03:21:c0:00:00)
# MultiProtocol Label Switching Header, Label: 17, Exp: 6, S: 1, TTL: 255
# Internet Protocol Version 4, Src: 1.1.1.1 (1.1.1.1), Dst: 3.3.3.3 (3.3.3.3)
# Transmission control Protocol, Src Port: 64339 (64339), Dst Port: bgp (179), Seq: 39, Ack: 20, Len: 181
# Border Gateway Protocol
  # UPDATE Message
    Marker: 16 bytes
    Length: 90 bytes
    Type: UPDATE Message (2)
    unfeasible routes length: 0 bytes
    Total path attribute length: 67 bytes
    # Path attributes
      # ORIGIN: INCOMPLETE (4 bytes)
      # AS_PATH: empty (3 bytes)
      # MULTI_EXIT_DISC: 0 (7 bytes)
      # LOCAL_PREF: 100 (7 bytes)
      # EXTENDED_COMMUNITIES: (11 bytes)
        # Flags: 0xc0 (Optional, Transitive, Complete)
          Type code: EXTENDED_COMMUNITIES (16)
          Length: 8 bytes
        # Carried Extended communities
          UnknownRoute Target: 200:1
      # MP_REACH_NLRI (35 bytes)
        # Flags: 0x80 (Optional, Non-transitive, Complete)
          Type code: MP_REACH_NLRI (14)
          Length: 32 bytes
          Address family: IPv4 (1)
          Subsequent address family identifier: Labeled VPN unicast (128)
      # Next hop network address (12 bytes)
        Next hop: Empty Label Stack RD=0:0 IPv4=1.1.1.1 (12)
        Subnetwork points of attachment: 0
      # Network layer reachability information (15 bytes)
        # Label Stack=21 (bottom) RD=200:1, IPv4=20.0.15.0/24
          MP Reach NLRI Prefix length: 112
          MP Reach NLRI Label stack: 21 (bottom)
          MP Reach NLRI Route Distinguisher: 200:1
          MP Reach NLRI IPv4 prefix: 20.0.15.0 (20.0.15.0)
    
```

Regardons si R3 et R4 reçoivent les préfixes annoncés par R1 :

```
R3
41.574: BGP(2): 1.1.1.1 rcvd UPDATE w/ attr: nexthop 1.1.1.1, origin ?,
localpref 100, metric 0, extended community RT:200:1
41.586: BGP(2): 1.1.1.1 rcvd 200:1:20.0.15.0/24
41.602: BGP(2): 1.1.1.1 rcvd UPDATE w/ attr: nexthop 1.1.1.1, origin ?,
localpref 100, metric 1, extended community RT:200:1
41.610: BGP(2): 1.1.1.1 rcvd 200:1:5.5.5.5/32
```

```
R3#sh bgp vpnv4 unicast vrf VRFA
!!!OUTPUT OMITTED!!!
```

Network	Next Hop	Metric	LocPrf	Weight	Path
Route Distinguisher: 200:1 (default for vrf VRFA)					
*>i5.5.5.5/32	1.1.1.1	1	100	0 ?	
*>i20.0.15.0/24	1.1.1.1	0	100	0 ?	

```
R4
02.098: BGP(2): 1.1.1.1 rcvd 200:1:5.5.5.5/32 -- DENIED due to: extended
community not supported;
02.106: BGP(2): 1.1.1.1 rcvd UPDATE w/ attr: nexthop 1.1.1.1, origin ?,
localpref 100, metric 0, extended community RT:200:1
02.114: BGP(2): 1.1.1.1 rcvd 200:1:20.0.15.0/24 -- DENIED due to: extended
community not supported;
```

R4 reçoit les updates mais n'en accepte aucune des 2 puisque on n'a pas configuré de RT d'import en 200:1 sur R4, ce qui est normal car 200:1 correspond au client A, et R4 n'est lié qu'aux clients B et C.

Redistribuons RIP dans BGP sur R3 et vérifions que R1 reçoit les routes et les ajoute à sa table de routage VRFA:

```
R1
27.614: BGP(2): 3.3.3.3 rcvd UPDATE w/ attr: nexthop 3.3.3.3, origin ?,
localpref 100, metric 0, extended community RT:200:1
27.622: BGP(2): 3.3.3.3 rcvd 200:1:20.0.37.0/24
27.638: BGP(2): 3.3.3.3 rcvd UPDATE w/ attr: nexthop 3.3.3.3, origin ?,
localpref 100, metric 1, extended community RT:200:1
27.646: BGP(2): 3.3.3.3 rcvd 200:1:7.7.7.7/32
30.770: BGP(2): Revise route installing 1 of 1 routes for 7.7.7.7/32 ->
3.3.3.3(main) to VRFA IP table
30.770: BGP(2): Revise route installing 1 of 1 routes for 20.0.37.0/24 ->
3.3.3.3(main) to VRFA IP table
```

Redistribution de RIP dans BGP pour que le client A obtienne les routes des 2 sites.
Configurons ça sur R1 et R3 :

```
R1,R3
router rip
!!!OUTPUT OMITTED!!!
!
address-family ipv4 vrf VRFA
 redistribute bgp 200 metric transparent
!!!OUTPUT OMITTED!!!
```

Vérifions que R5 et R7 reçoivent les routes:

```
R5
43.246: RIP: received v2 update from 20.0.15.1 on FastEthernet0/0
43.246: 7.7.7.7/32 via 0.0.0.0 in 2 hops
43.254: 20.0.37.0/24 via 0.0.0.0 in 1 hops

R5#sh ip route rip
 20.0.0.0/24 is subnetted, 2 subnets
R   20.0.37.0 [120/1] via 20.0.15.1, 00:00:13, FastEthernet0/0
 7.0.0.0/32 is subnetted, 1 subnets
R   7.7.7.7 [120/2] via 20.0.15.1, 00:00:13, FastEthernet0/0
```

```
R7#sh ip route rip
 20.0.0.0/24 is subnetted, 2 subnets
R   20.0.15.0 [120/1] via 20.0.37.3, 00:00:07, FastEthernet0/0
 5.0.0.0/32 is subnetted, 1 subnets
R   5.5.5.5 [120/2] via 20.0.37.3, 00:00:07, FastEthernet0/0
```

Le coeur MPLS du réseau apparaît comme un seul saut. R7 annonce une métrique de 1 pour 7.7.7.7/32 et R5 reçoit 7.7.7.7/32 avec une métrique de 2.

RIP ajoute une métrique de 1 quand une update est envoyée, et pas quand elle est reçue.

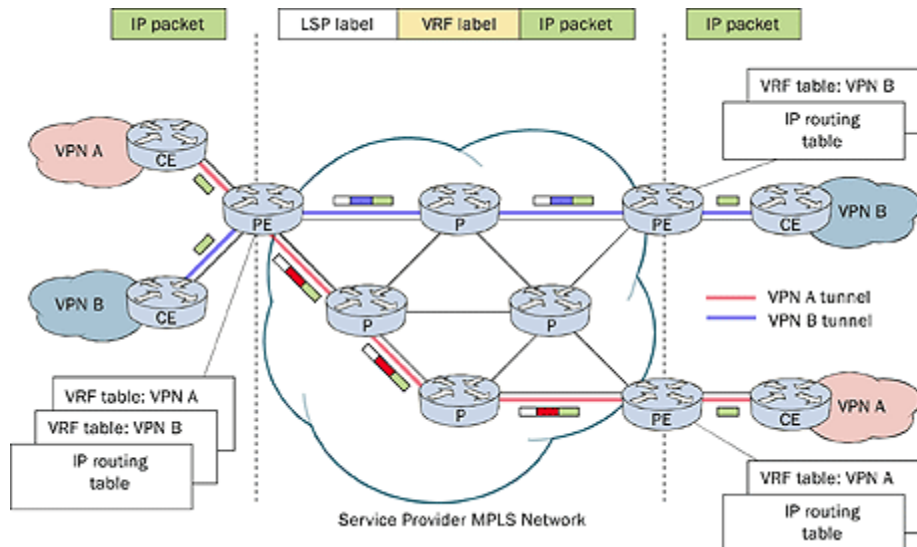
Il semble que les sites du client A peuvent maintenant communiquer. Testons :

```
R5#traceroute 7.7.7.7

Type escape sequence to abort.
Tracing the route to 7.7.7.7

 0  20.0.15.1  36 msec  32 msec  16 msec
 1  10.0.12.2  [MPLS: Labels 17/22 Exp 0]  80 msec  64 msec  76 msec
 2  20.0.37.3  [MPLS: Label 22 Exp 0]  72 msec  52 msec  52 msec
 3  20.0.37.7  116 msec *  128 msec
```

Ok. Label 22 : le label externe 17 est le label de transport, utilisé pour joindre le prochain saut BGP 3.3.3.3, vient de la FLIB. Quand R1 doit joindre l'@ de loopback de R7, il a besoin d'encoder cette info dans un label MPLS sinon R3 ne saurait pas dans quelle VRF regarder : c'est le **label VPN**.



Un paquet de client porte donc 2 niveaux de labels dans le coeur :

1. Label externe pour diriger le paquet vers le bon PE dest.
2. Label interne pour indiquer au PE côté dest comment transférer ce paquet au bon routeur CE.

```

R1#sh ip bgp vpnv4 vrf VRFA 7.7.7.7
BGP routing table entry for 200:1:7.7.7.7/32, version 11
Paths: (1 available, best #1, table VRFA)
Not advertised to any peer
Local
  3.3.3.3 (metric 12) from 3.3.3.3 (3.3.3.3)
    Origin incomplete, metric 1, localpref 100, valid, internal, best
    Extended Community: RT:200:1
    mpls labels in/out nola/22

```

Donc quand R2 retire le label de transport 17, R3 reçoit un paquet MPLS avec label 22 et sait qu'il doit chercher le routage à effectuer dans la table de routage VRFA.

```

R3#sh mpls forwarding-table
Local  Outgoing  Prefix          Bytes tag  Outgoing  Next Hop
tag    tag or VC  or Tunnel Id    switched   interface
22     Untagged  7.7.7.7/32[V]  684       Fa1/0     20.0.37.7
!!!OUTPUT OMITTED!!!

```

Les étapes suivantes correspondent à suivre la même procédure pour les autres clients utilisant d'autres protocoles de routage.:

- Redistribution mutuelle entre EIGRP et BGP pour VRFB
- Redistribution mutuelle entre OSPF et BGP pour VRFC

Plan

I. Présentation des WAN

II. Les interfaces de la couche physique

III. Protocoles de niveau 2 dans les WAN

IV. MPLS : commutation par VC dans le monde IP

IV.1. Fonctionnement de MPLS

IV.2. Ingénierie de trafic avec MPLS : MPLS-TE

IV.3. Offres de service MPLS : les VPN basés sur MPLS

IV.3.a. IP-VPN

IV.3.b. Ethernet-VPN : VPLS

V. Qualité de service

VI. Technologies xDSL

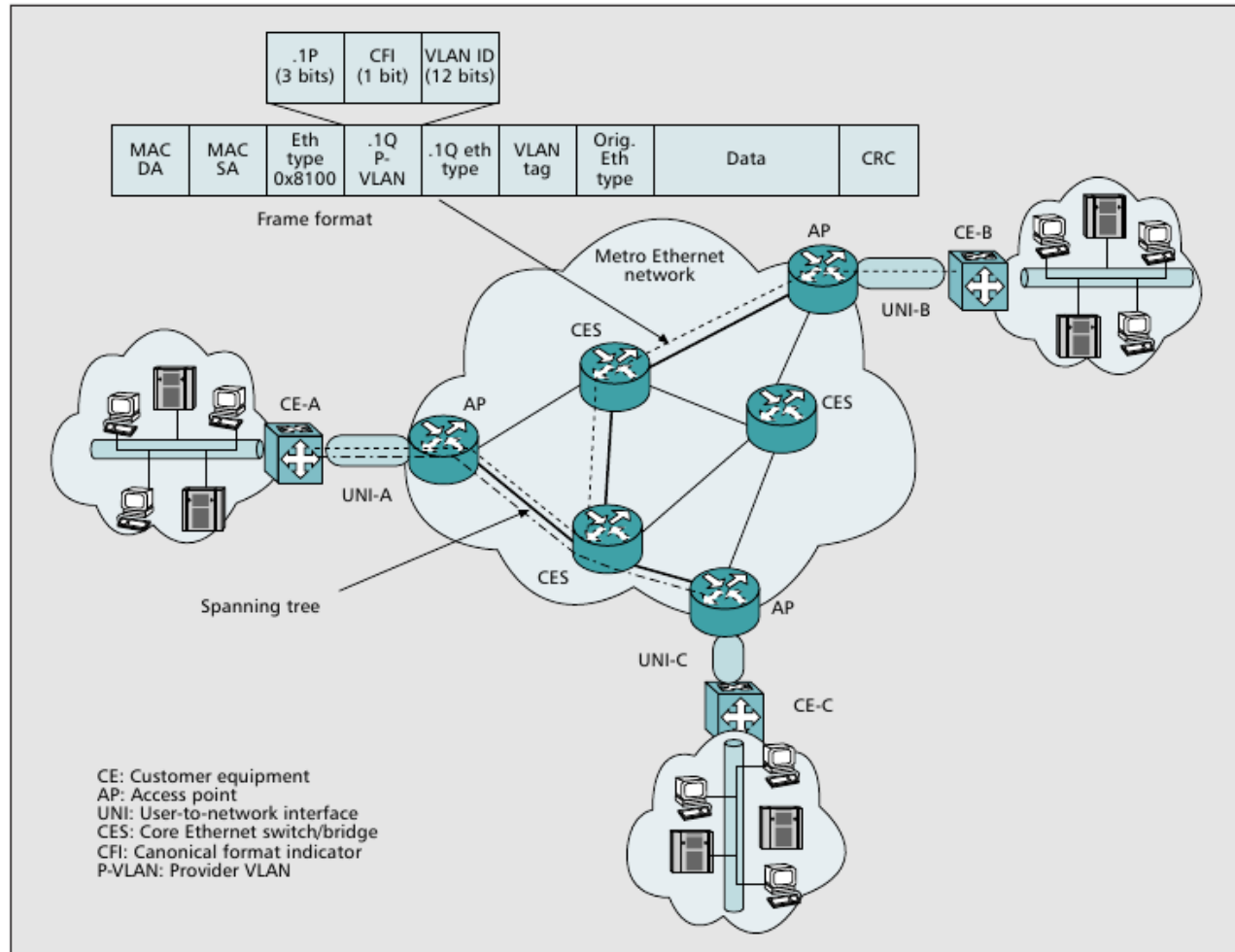
Ethernet dans le WAN

- Plusieurs architectures possibles pour porter des trames Ethernet dans le WAN :
 - Extension du protocole Ethernet natif
 - Utilisation de MPLS

Extension du protocole Ethernet natif

- Dans le réseau metro (IEEE 802.1): *Provider Bridged Networks*
 - Le réseau metro comprend des bridges/switches Ethernet
Un protocol ST est utilisé pour établir un ou plusieurs arbres couvrant.
 - Chaque arbre fournit un chemin entre chaque sites client du même VLAN.
 - Problème : le passage à l'échelle dans le domaine metro :
 - seulement un nombre limité de VLAN est supporté
 - explosion de la taille des tables d'adressage (*MAC adress table*)

Extension du protocole Ethernet natif



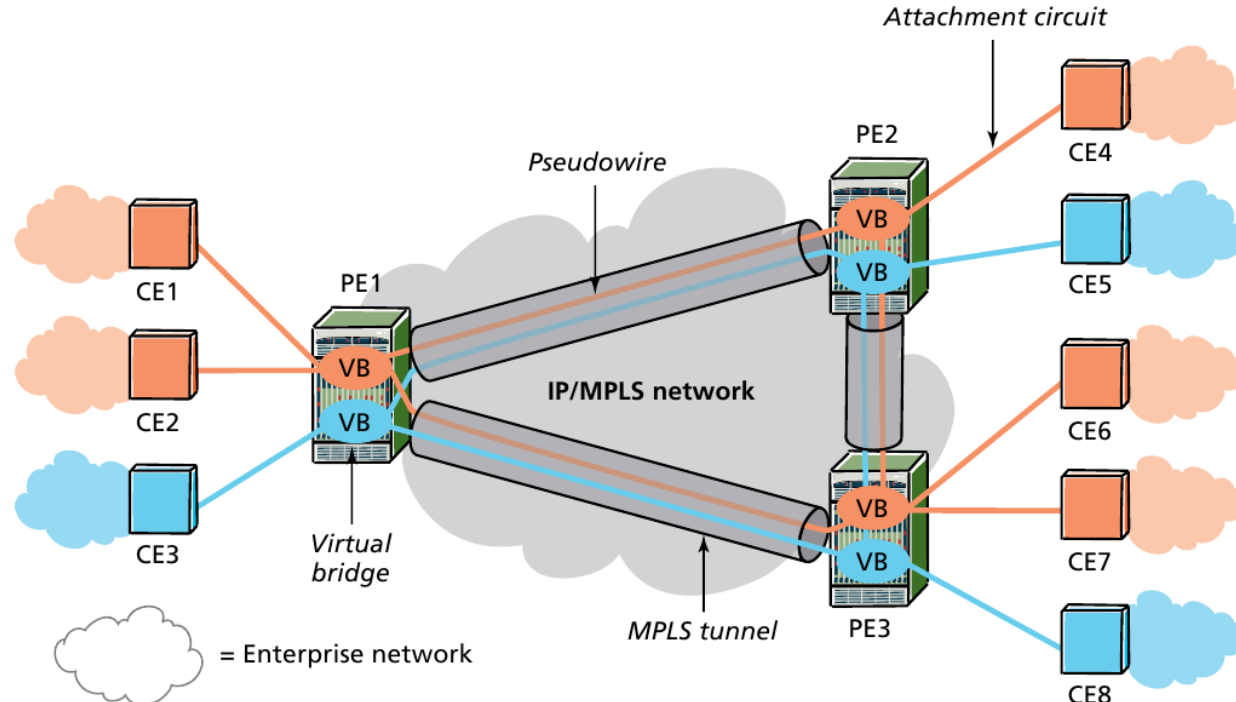
■ Figure 2. Network scenario 2: a provider bridged network.

WAN Ethernet basé sur MPLS : Virtual Private LAN Services - VPLS

- VPLS est un type de VPN multi-point de couche 2
- Tous les sites d'un client donné, dans un VPN VPLS, apparaissent comme étant sur le même LAN
- VPLS utilise l'interface Ethernet du client
- Un réseau VPLS comprend des CE, PE et un coeur MPLS:
 - Le CE est routeur ou switch localisé dans les locaux du client. Ethernet est l'interface entre le CE et le PE.
 - Les VPN sont gérés par les PE.
 - Comme VPLS est un service de couche 2 (Ethernet), les PE doivent assurer l'apprentissage des adresses MAC, la commutation et la diffusion par VPN.
 - Le coeur MPLS interconnecte les PE, ne participe pas à la gestion des VPN. Le trafic est juste commuté par les labels MPLS.

WAN Ethernet basé sur MPLS : Virtual Private LAN Services - VPLS

- Un maillage complet de LSP bi-directionnels (appelés *Pseudo-wires*) est créé entre tous les PE d'une instance VPLS.



WAN Ethernet basé sur MPLS : Virtual Private LAN Services - VPLS

- PW = une paire de 2 LSPs dans des directions opposées
 - > Permet à un PE d'apprendre les @ MAC: quand un PE reçoit une trame Ethernet avec un @MAC source inconnue, le PE sait sur quel PW elle est arrivée, et donc cette adresse sera joignable.
- Le PE implémente un switch pour chaque instance VPLS :
 - Grâce à la FLIB pour chaque instance VPLS,
 - La FLIB est remplie des correspondances @MAC/labels LSP (PW)

VPLS : comment ça marche ?

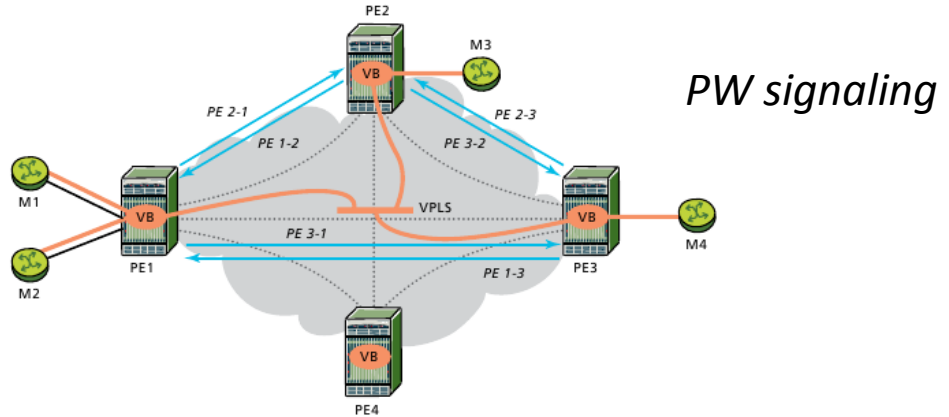
- Création des PWs:

Une instance VPLS

identifiée par

Service-identifiant 101

(Svc-id 11) -> créer les PW entre PE1, PE2 et PE3



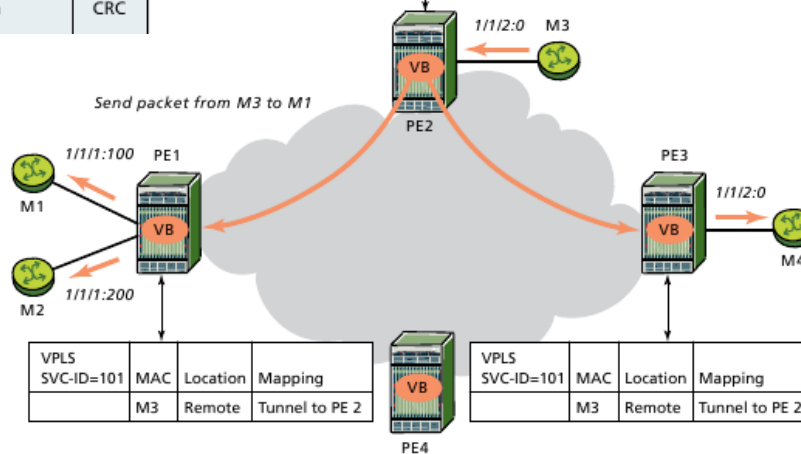
PE1 -> PE2: For SVC-ID 101 use VC label PE 2-1
 PE2 -> PE1: For SVC-ID 101 use VC label PE 1-2
 PE1 -> PE3: For SVC-ID 101 use VC label PE 3-1
 PE3 -> PE1: For SVC-ID 101 use VC label PE 1-3
 PE3 -> PE2: For SVC-ID 101 use VC label PE 2-3
 PE2 -> PE3: For SVC-ID 101 use VC label PE 3-2

- MAC learning and packet forwarding

Tunnel label	VC label	MAC DA	MAC SA	VLAN tag	Eth type	Data	CRC
--------------	----------	--------	--------	----------	----------	------	-----

Packet walkthrough for VPLS service-ID 101

VPLS SVC-ID=101	MAC	Location	Mapping
	M3	Local	1/1/2:0

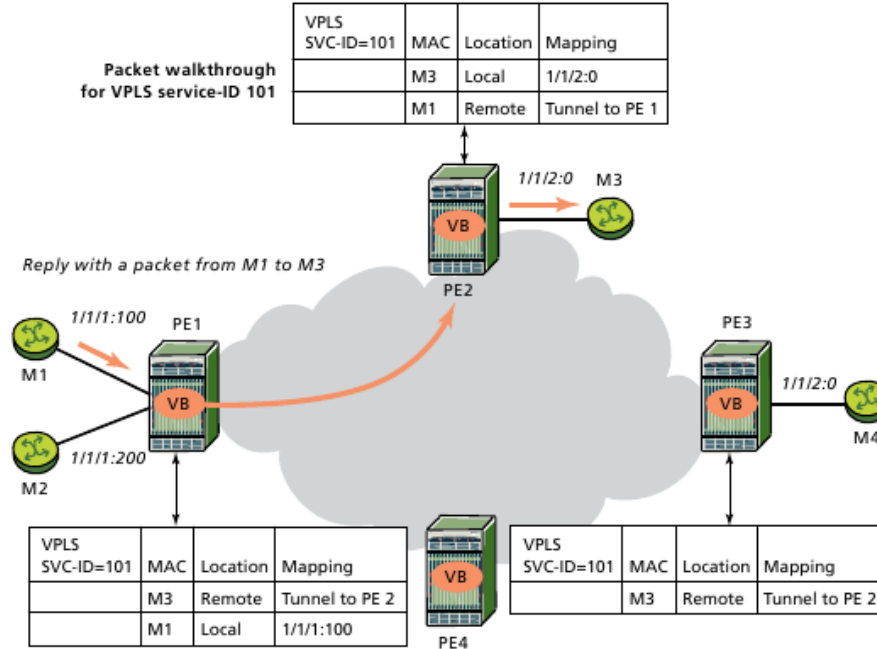


VPLS SVC-ID=101	MAC	Location	Mapping
	M3	Remote	Tunnel to PE 2

VPLS SVC-ID=101	MAC	Location	Mapping
	M3	Remote	Tunnel to PE 2

VPLS : comment ça marche ?

- VPLS packet forwarding:



Comparaison des VPN basés sur MPLS, aux niveaux 2 et 3

Choisir son service VPN : Ethernet ou IP VPN, ou les 2 ? Critères et bénéfices

- Bénéfices des IP-VPNs:
 - **Externalisation du control du routage** : le SP applique des priorités aux différents types de trafic en les classant dans des CoS différentes.
 - **Accès flexible**
 - **Passage à l'échelle** : supportent de très grands et nombreux réseaux d'entreprise (avec 100aines ou milliers de sites)
 - **Portée étendue**: offerts par un grand nombre de SP donc couverture géographique étendue
 - **Sécurité**: tables de routages séparées

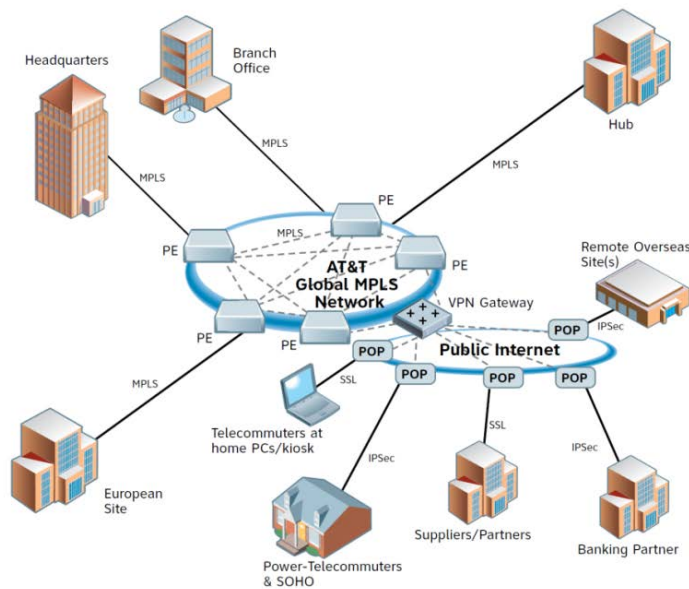
Choisir son service VPN : Ethernet ou IP VPN, ou les 2 ? Critères et bénéfices

- Bénéfices des WAN Ethernet :
 - **Contrôle du routage** : quand l'entreprise préfère gérer elle-même son routage
 - **Transparent pour le protocole de couche 3**
 - **Bande passante plus élevée**: de 1MBps à 10GBps

Choisir son service VPN : Ethernet ou IP VPN, ou les 2 ? Critères et bénéfices

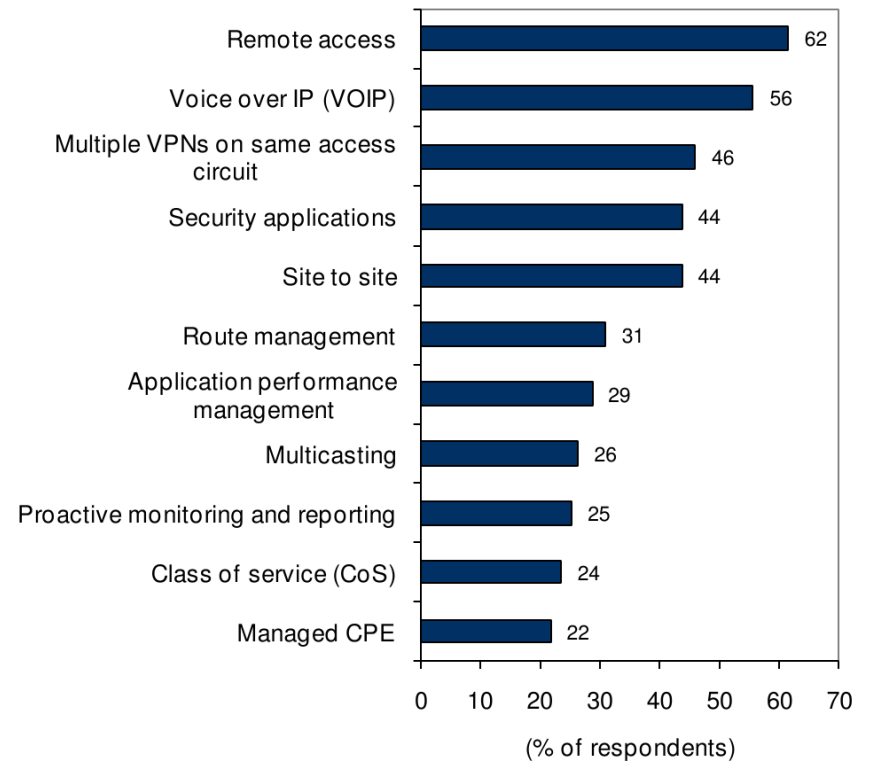
- 62% des entreprises avec IP VPNs. 56% pour de la VoIP : 25% de plus qu'en 2009
- IP VPNs plutôt pour les “petits” sites, et WAN Ethernet pour les gros sites ou les datacenters avec accès fibre.

Choisir son service VPN : Ethernet ou IP VPN, ou les 2 ? Critères et bénéfices



Multiple VPN technology choices working together

Key IP VPN Adoption Criteria



U.S. only n = 174

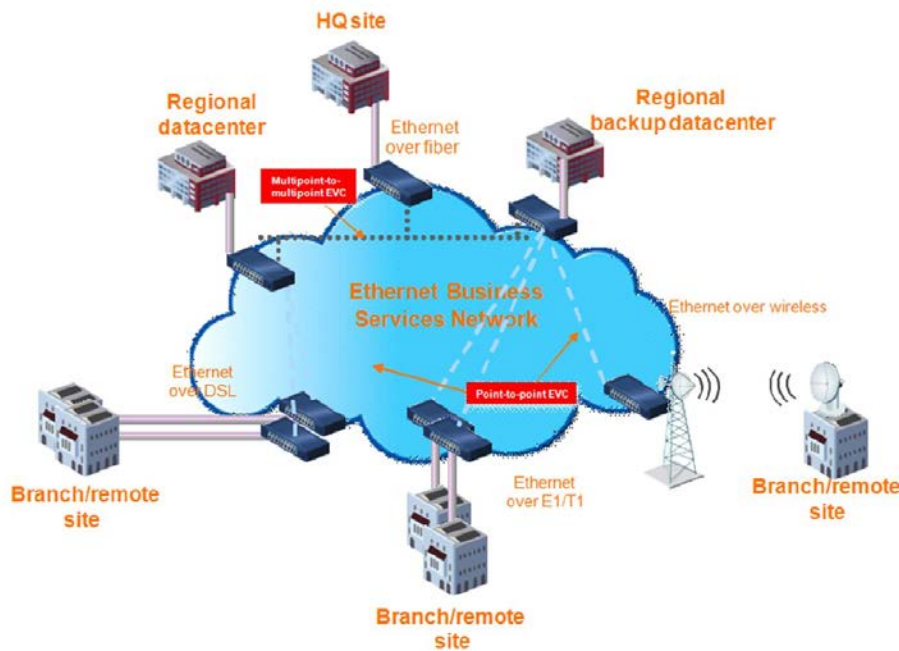
Source: IDC's WAN Manager Survey, 2010

Choisir son service VPN : Ethernet ou IP VPN, ou les 2 ? Critères et bénéfices

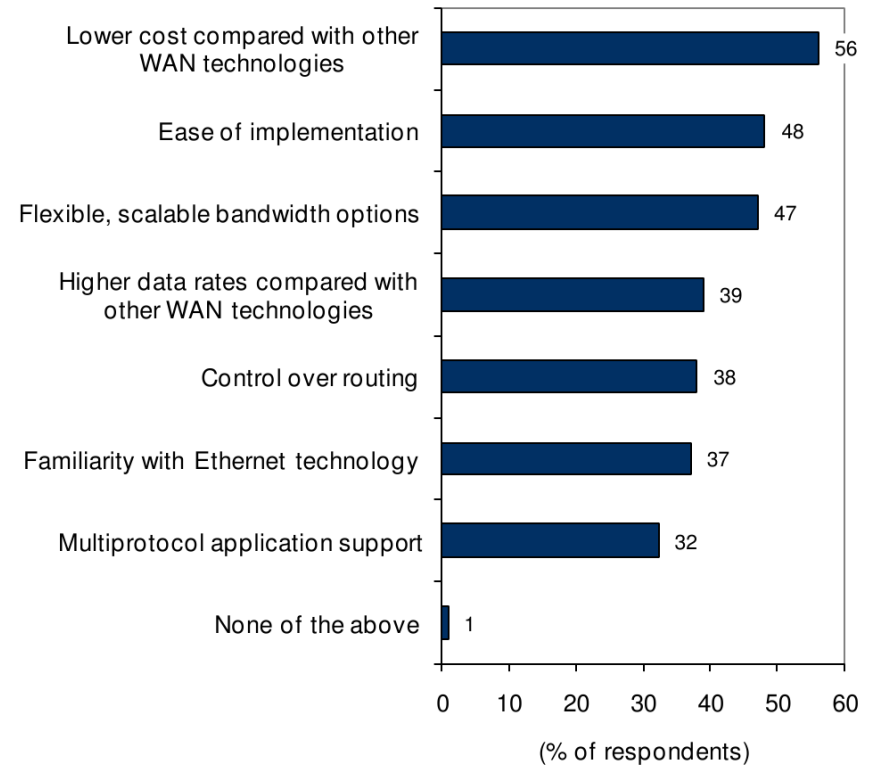
- Adoption de WAN Ethernet par les entreprises pour le coût, la facilité d'implémentation et la familiarité avec Ethernet
- 58% des entr utilisent une solution hybride Ethernet/IP VPN, et augmentation de 33% environ par an.

Choisir son service VPN : Ethernet ou IP VPN, ou les 2 ? Critères et bénéfices

Ethernet WAN



Key Ethernet WAN Adoption Criteria



n = 432

Source: IDC's WAN Manager Survey, 2010

Plan

I. Présentation des WAN

II. Les interfaces de la couche physique

III. Protocoles de niveau 2 dans les WAN

IV. MPLS : commutation par VC dans le monde IP

V. Qualité de service

V.1. TCP et le contrôle de congestion dans le réseau

V.1.a. Rappels : transfert fiable et contrôle de flux

V.1.b. Principe du contrôle de congestion

V.1.c. Le contrôle de congestion par TCP

V.2. Classification des applications et besoin de QoS

V.2.a. Classification

V.2.b. Paramètres-clé de la QoS

V.2.c. Stratégies pour la QoS

V.3. Techniques de traitement de la QoS

V.3.a. Les outils

V.3.b. Traitements au niveau 2

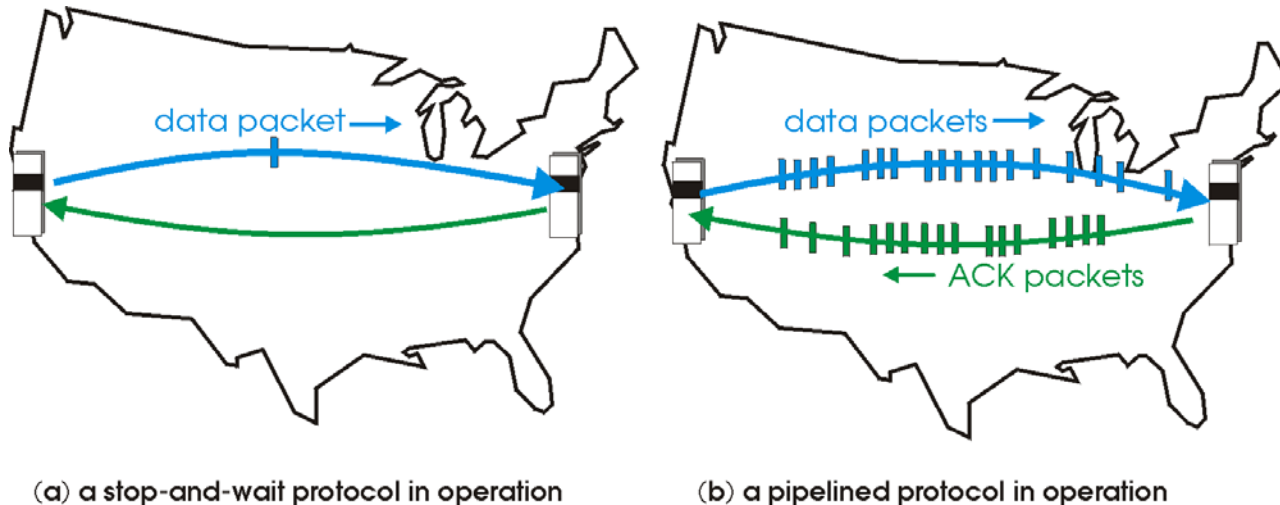
V.3.c. Traitements au niveau 3

VI. Technologies xDSL

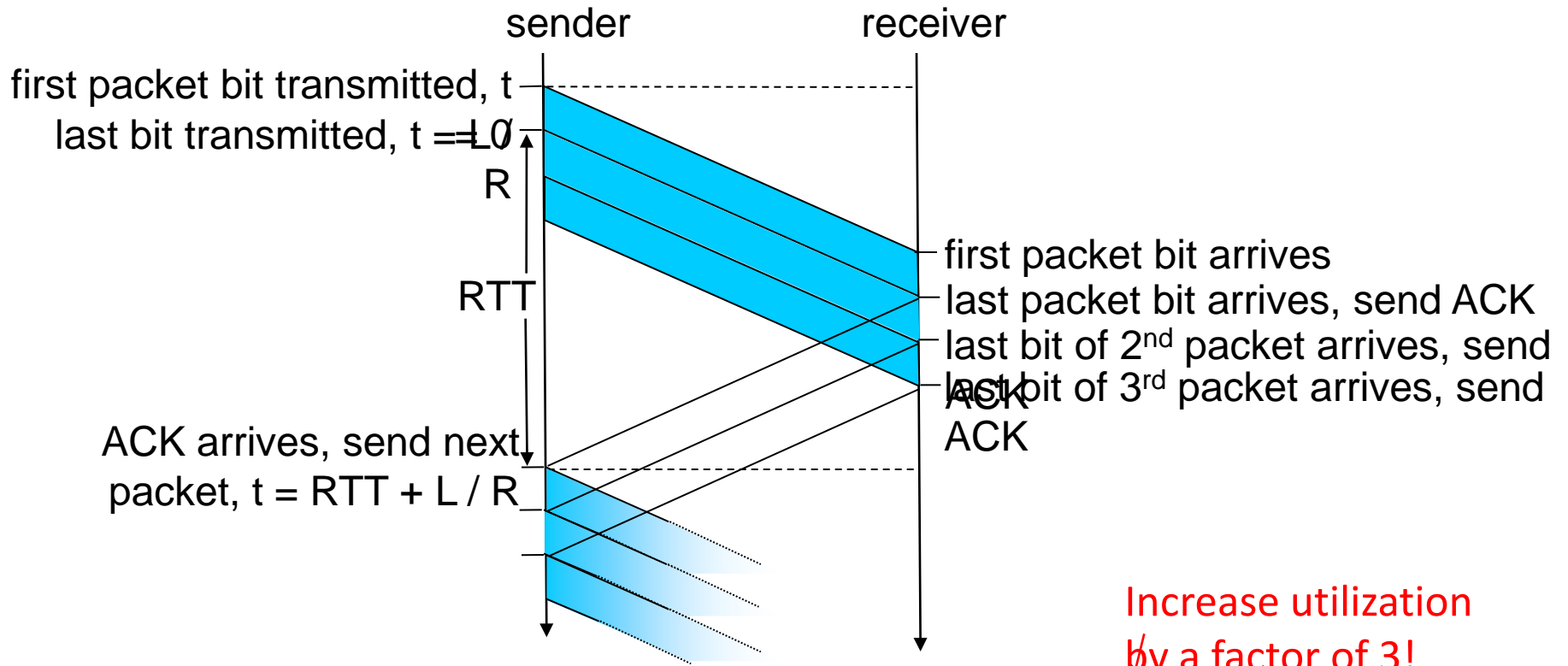
La classe de protocoles à laquelle TCP appartient: les protocoles en pipeline

Pipelining: l'émetteur envoie plusieurs paquets sans attendre sans attendre l'ACK du premier

- La plage de numéros de séquence doit être augmentée
- Mise en mémoire à l'émetteur et au récepteur



Pipelining: augmente l'utilisation



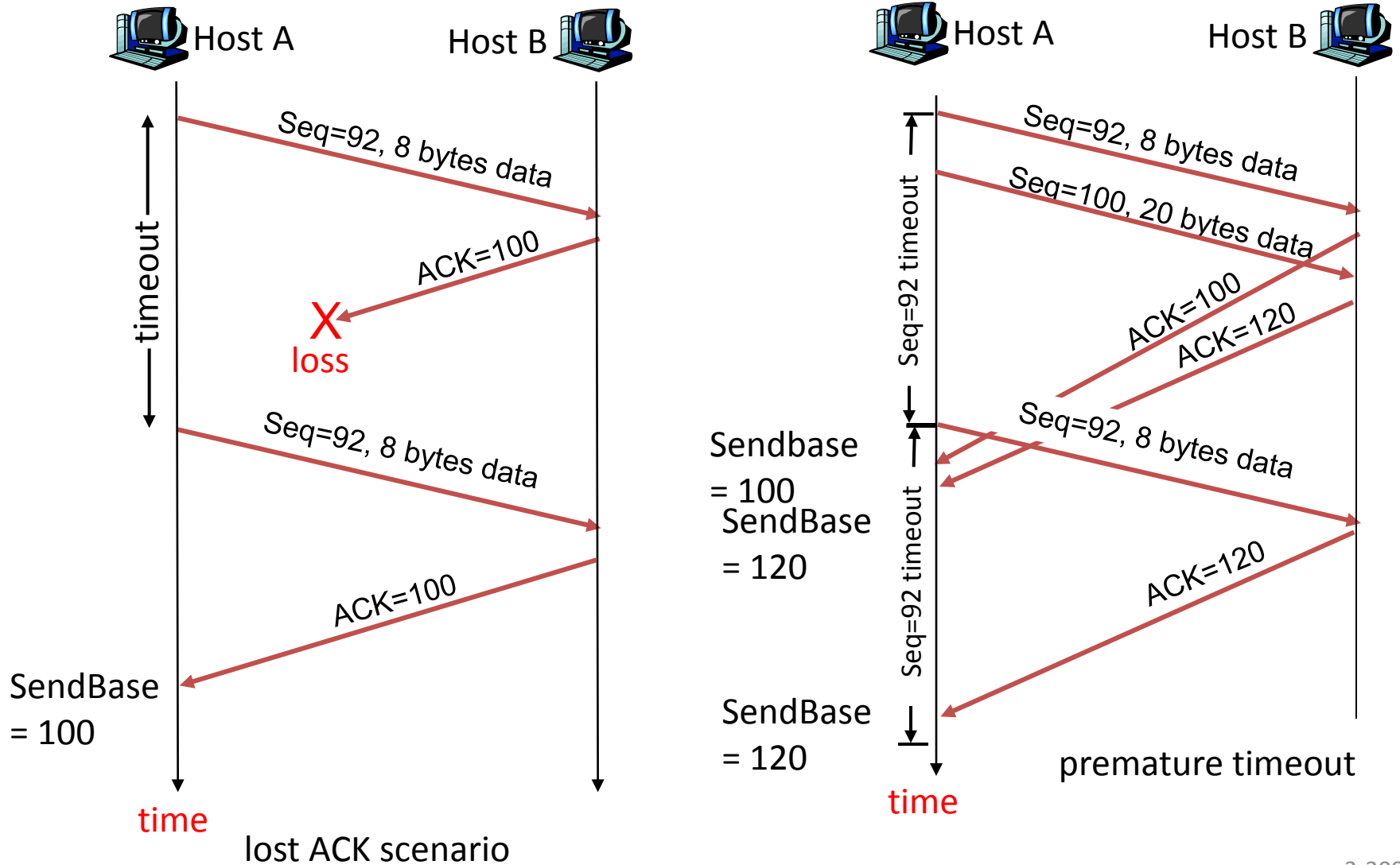
Increase utilization
by a factor of 3!

$$U_{\text{sender}} = \frac{3 * L / R}{RTT + L / R} = \frac{.024}{30.008} = 0.0008$$

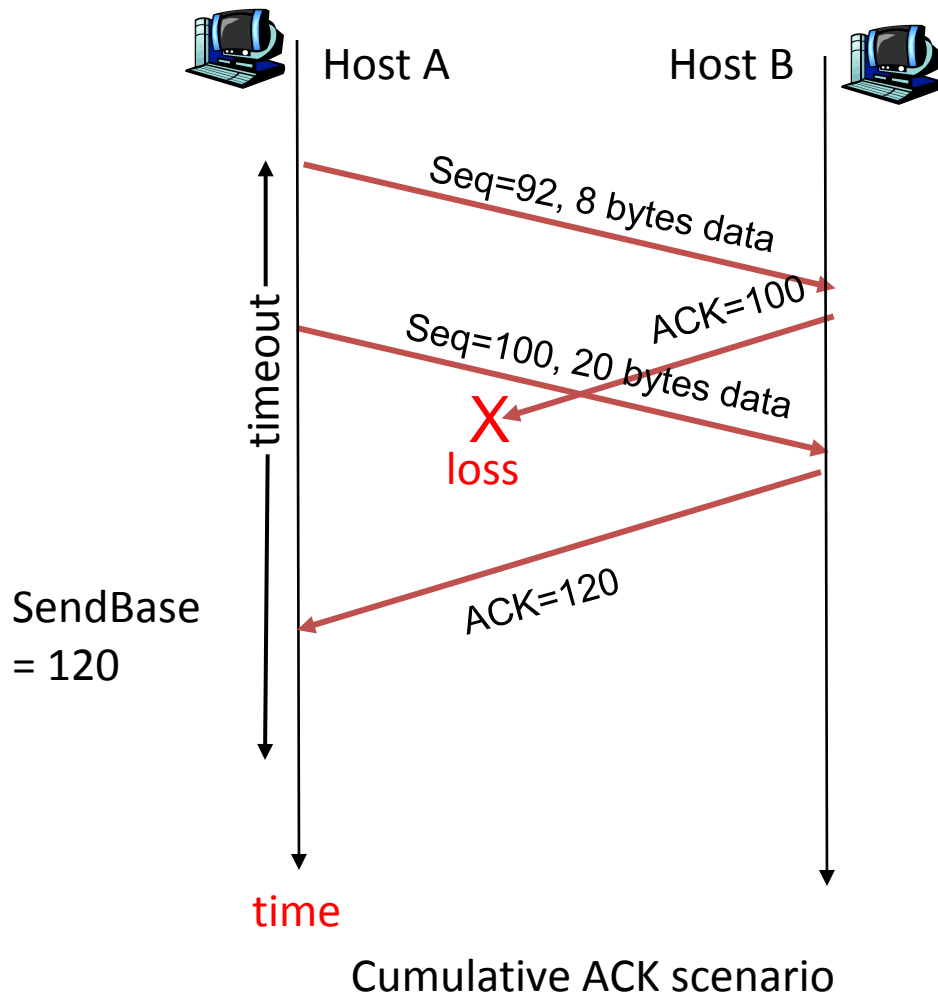
Transfert fiable TCP

- TCP crée un service de tf au dessus du service non-fiable de IP
- Protocole en pipeline
- Acks cumulatifs
- Timer de retransmission
- Retransmissions déclenchées par :
 - Événement de timeout
 - Acks dupliqués

Scenarios de retransmission TCP



Scenarios de retransmission TCP



Fast Retransmit

- Période de timeout souvent assez longue :
 - long délai avant ré-émission d'un paquet perdu
- Détection de segments perdus via ACKs dupliqués.
 - L'émetteur envoie souvent plusieurs segments à la suite.
 - Si un segment est perdu, il y aura probablement des ACKs dupliqués.
- Si l'émetteur reçoit 4 ACKs demandant le même paquet, il suppose que le segment a été perdu:
 - **fast retransmit**: renvoyer le segment avant que le timer de timeout expire

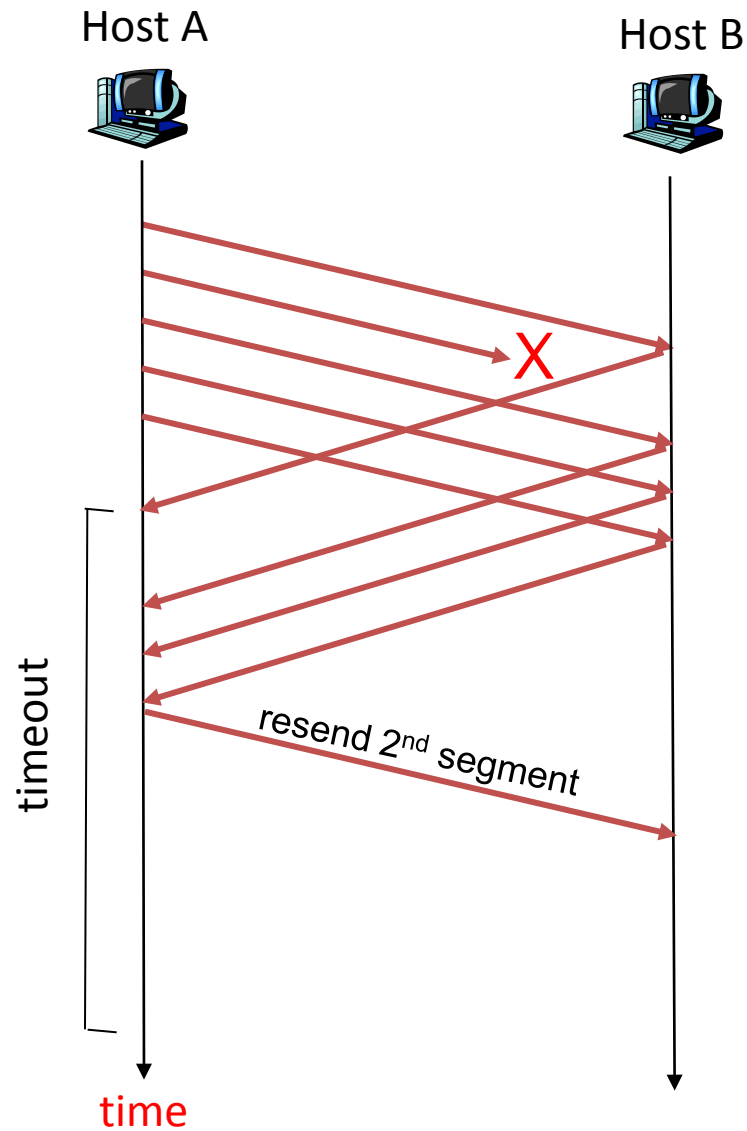
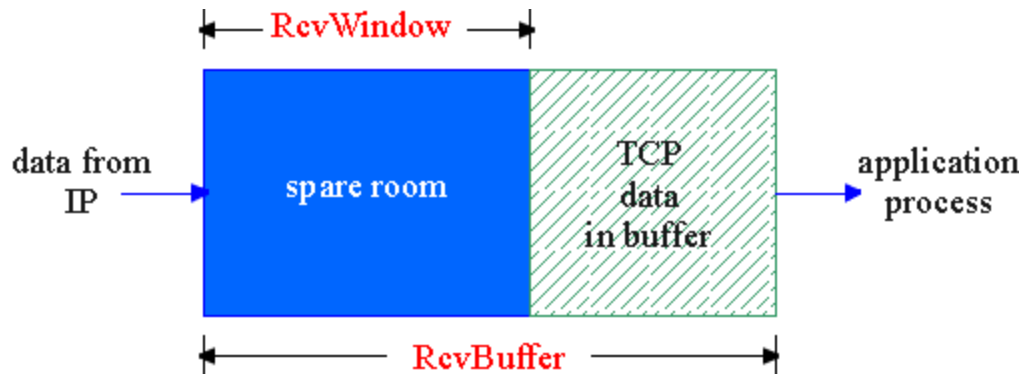


Figure 3.37 Resending a segment after triple duplicate ACK

Contrôle de flux TCP

- Le récepteur TCP a un buffer de réception:



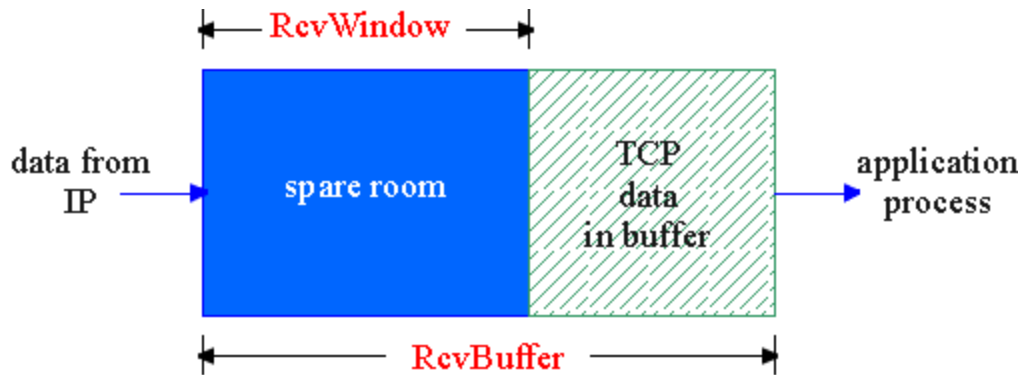
Contrôle de flux

L'émetteur ne va pas submerger le buffer du récepteur en envoyant trop et trop vite

- Il faut faire correspondre le débit d'émission avec le débit auquel l'appli peut lire les données

- r Le processus application peut lire les données du buffer lentement

TCP Flow control: how it works



- Rcvr annonce la valeur **RcvWindow** dans l'entête TCP des segments renvoyés vers l'émetteur
- L'émetteur limite le nombre de paquets envoyés non encore accusés (ACKés) à **RcvWindow**
 - Garantie que le buffer de réception ne sature pas

Plan

I. Présentation des WAN

II. Les interfaces de la couche physique

III. Protocoles de niveau 2 dans les WAN

IV. MPLS : commutation par VC dans le monde IP

V. Qualité de service

V.1. TCP et le contrôle de congestion dans le réseau

V.1.a. Rappels : transfert fiable et contrôle de flux

V.1.b. Principe du contrôle de congestion

V.1.c. Le contrôle de congestion par TCP

V.2. Classification des applications et besoin de QoS

V.2.a. Classification

V.2.b. Paramètres-clé de la QoS

V.2.c. Stratégies pour la QoS

V.3. Techniques de traitement de la QoS

V.3.a. Les outils

V.3.b. Traitements au niveau 2

V.3.c. Traitements au niveau 3

VI. Technologies xDSL

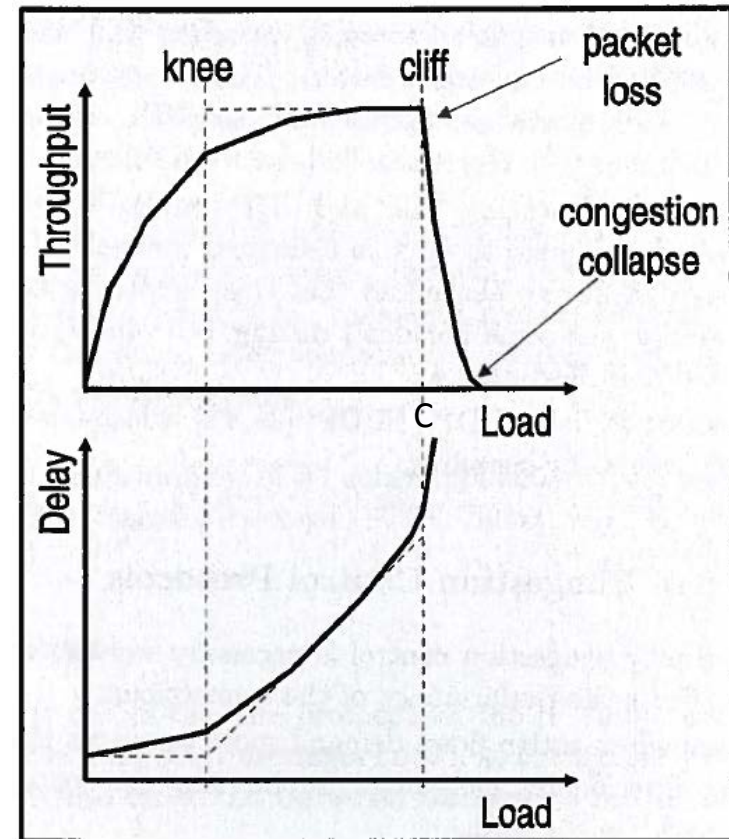
Le problème de la congestion dans le réseau

- La congestion apparaît quand des flows demandent plus de ressources que les liens et équipements du réseau ne peuvent fournir:
Sending rate > capacity of the bottleneck
- > D'abord mise en file d'attente des paquets
- > Puis perte si le débit ne décroît pas
- => Le **contrôle de congestion permet d'éviter le *congestion collapse***: effondrement du débit causé par un grand nombre d'abandon de paquets

Le problème de la congestion dans le réseau

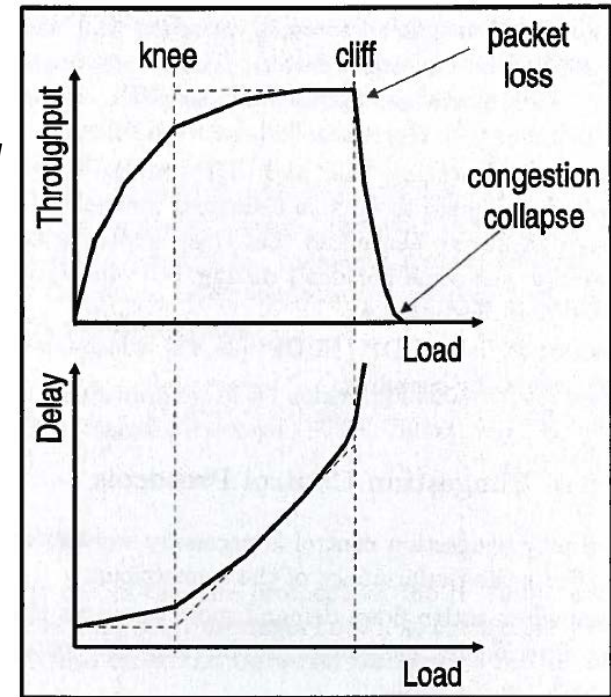
2 points importants avant congestion collapse :

- *Knee* : la charge commence à excéder la capacité du lien et les buffers se remplissent
Après le *knee* : le délai croît exponentiellement
- *Cliff* : après le *cliff*, les buffers sont pleins et drop des paquets



Importance des protocoles de contrôle de congestion

- Reprise sur erreur sans contrôle de congestion: TCP sans CC avec correction d'erreur:
 - Plusieurs sessions (flows) TCP
 - Le débit total agrégé est variable, autour de la moyenne *load*
 - Plus la moyenne *load* augmente, plus souvent on dépasse C
 - --> la mise en file d'attente commence
 - ---> quand le buffer est complètement plein, des paquets sont perdus
 - TCP sans CC ne diminue pas le débit qu'il met en entrée du réseau, il se contente de faire de la correction: au bout d'un timeout, supposé > temps de congestion, on retransmet
 - La durée de la congestion augmente avec le nombre de sessions
 - si le timeout est trop court, le débit nominal d'entrée ne diminue pas, on ne fait que re-transmettre, le débit utile de sortie s'effondre



Buts du contrôle de congestion

- Problème : gérer le débit appliqué en entrée du réseau par le protocole de transport
- 2 buts principaux de TCP avec CC:
 - Maximiser l'utilisation de la capacité des liens tout en évitant la congestion dans le réseau (i.e., maintenir la charge en dessous du *knee*)
 - Résoudre rapidement les situations de congestion pour éviter le congestion collapse (i.e., éviter impérativement le *cliff*)
- ET partager équitablement les ressources entre tous les utilisateurs
- ET transport fiable: basé ACKs

Approches pour le contrôle de congestion

2 grandes classes d'approches du contrôle de congestion:

Contrôle de congestion de bout-en-bout (*end-to-end*):

- pas de retour explicite du réseau
- congestion inférée à partir des pertes et du délai vu par l'hôte d'extrémité (*end host*)
- C'est l'approche prise par TCP

Contrôle de congestion assisté par le réseau:

- les routeurs fournissent un retour aux end hosts
 - Un bit indiquant la congestion (FR, ATM, TCP ECN)
 - Routeurs ERN

Plan

I. Présentation des WAN

II. Les interfaces de la couche physique

III. Protocoles de niveau 2 dans les WAN

IV. MPLS : commutation par VC dans le monde IP

V. Qualité de service

V.1. TCP et le contrôle de congestion dans le réseau

V.1.a. Rappels : transfert fiable et contrôle de flux

V.1.b. Principe du contrôle de congestion

V.1.c. Le contrôle de congestion par TCP

V.2. Classification des applications et besoin de QoS

V.2.a. Classification

V.2.b. Paramètres-clé de la QoS

V.2.c. Stratégies pour la QoS

V.3. Techniques de traitement de la QoS

V.3.a. Les outils

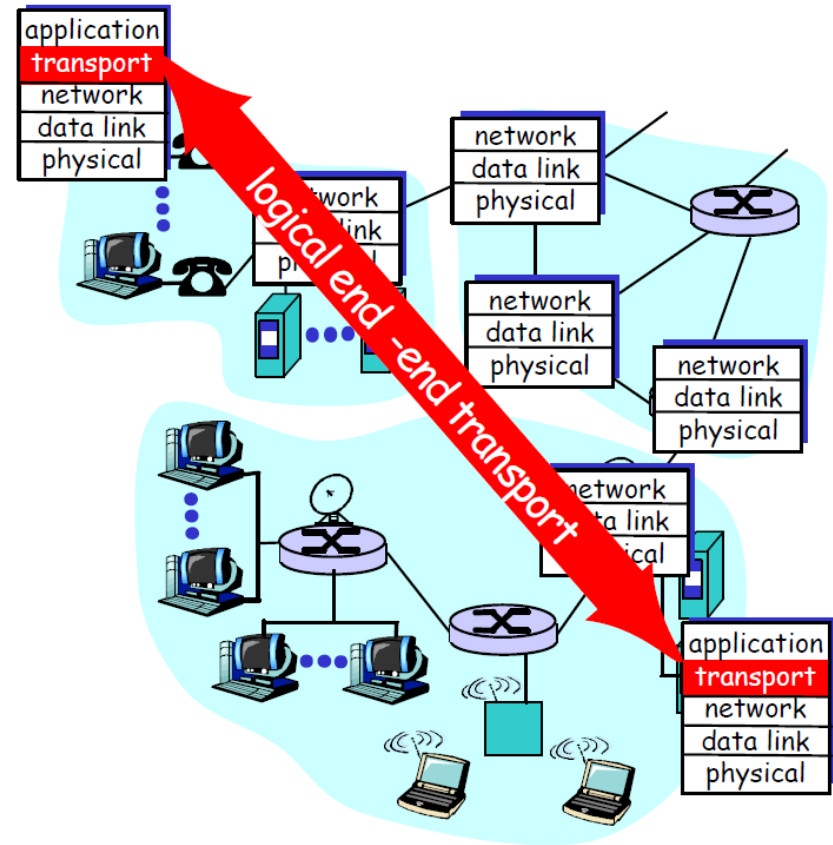
V.3.b. Traitements au niveau 2

V.3.c. Traitements au niveau 3

VI. Technologies xDSL

Protocole de contrôle de congestion standard: TCP et ses premières versions

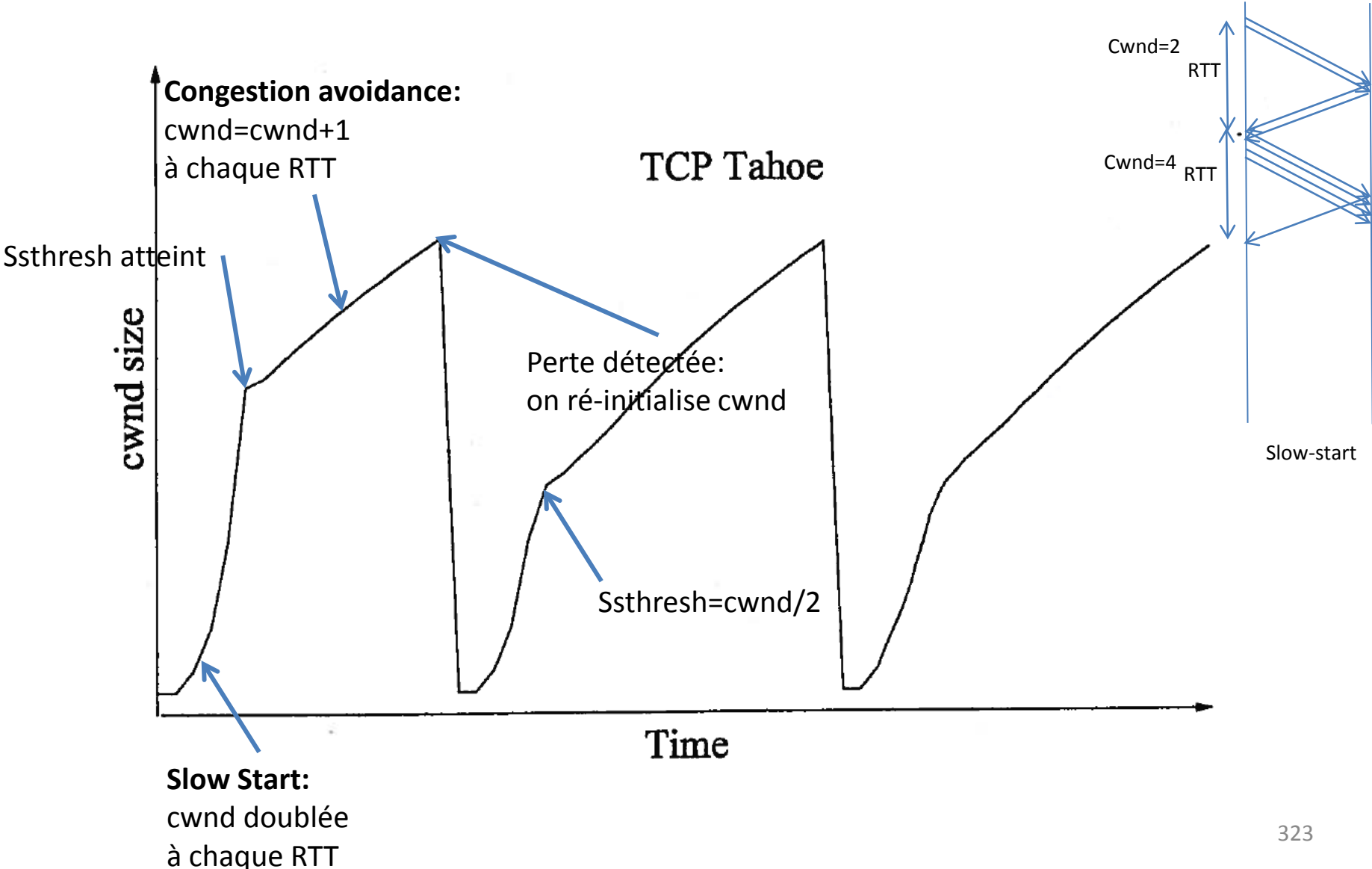
- L'étude du contrôle de congestion dans les réseaux IP a débuté en 1986, avec les premiers congestion collapse sur Internet (dû à un nombre croissant de flows)
- 1988: Van Jacobson propose le 1^{er} protocole de contrôle et évitement de congestion: TCP Tahoe
- Fonctionnement End-to-End (E2E): exécution du protocole qu'aux extrémités



Principe de TCP

- Principe: pour chaque connexion, TCP maintient une *congestion window (cwnd)*, qui est le nombre de segments TCP envoyés non encore acknowledged.
- Paramètres importants :
 - *RTT* : temps d'aller-retour
 - *RTO* : temps au bout duquel, si pas de retour d'ACK, on déclare le segment perdu
 - *ssthresh* : seuil fixé à ~64KB initialement
 - > Ces paramètres sont constamment ré-évalués au cours du temps

TCP Tahoe: 1^{ère} version de TCP



Contrôle de congestion TCP : détails

- L'émetteur limite le débit de transmission par la limitation du nombre d'octets envoyés à **cwnd**
- A peu près,

$$\text{Débit} = \frac{\text{cwnd}}{\text{RTT}} \text{ Bytes/sec}$$

- **cwnd** est dynamique, fonction de la congestion du réseau perçue

Comment l'émetteur détecte la congestion ?

- Événement de perte = timeout *ou* 3 acks dupliqués
- L'émetteur TCP réduit le débit (**cwnd**) après une perte

3 mécanismes:

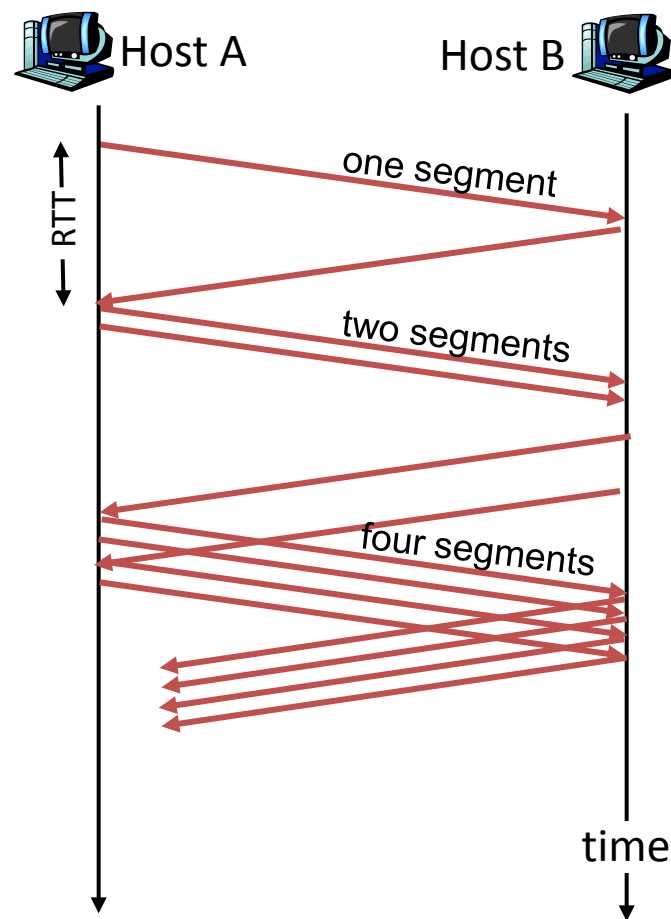
- AIMD
- slow start
- conservatif après timeout

Slow Start TCP

- Quand la connexion commence, **cwnd** = 1 MSS
 - Exemple: MSS = 500 bytes & RTT = 200 msec
 - Débit initial = 20 kbps
- Mais la BP disponible peut être \gg MSS/RTT
 - désirable d'accroître rapidement le débit à un niveau proche de la BP dispo
- r Quand la connexion commence, augmenter le débit exponentiellement vite jusqu'à ce que la première perte (due à la congestion) se produise

Slow Start TCP (more)

- Quand la connexion commence, augmenter le débit exponentiellement vite jusqu'à ce que la première perte (due à la congestion) se produise :
 - doubler **cwnd** chaque RTT
 - fait en augmentant **cwnd** d'un MSS à chaque ACK reçu
- En résumé: le débit initial est faible mais il augmente exponentiellement vite



Raffinement: slow-start + congestion avoidance + détection de perte améliorée

- But: atteindre un débit élevé tout en évitant le plus longtemps possible la congestion
- Après 3 dup ACKs :
 - **cwnd** diminuée de moitié (*Fast recovery*)
 - recommence à croître linéairement
- Mais après un événement de timeout :
 - **cwnd** ré-initialisé à 1 MSS;
 - slow-start (croissance exp)
 - jusqu'à un seuil, puis croissance linéaire
- La phase de croissance linéaire de s'appelle la phase de *congestion avoidance*

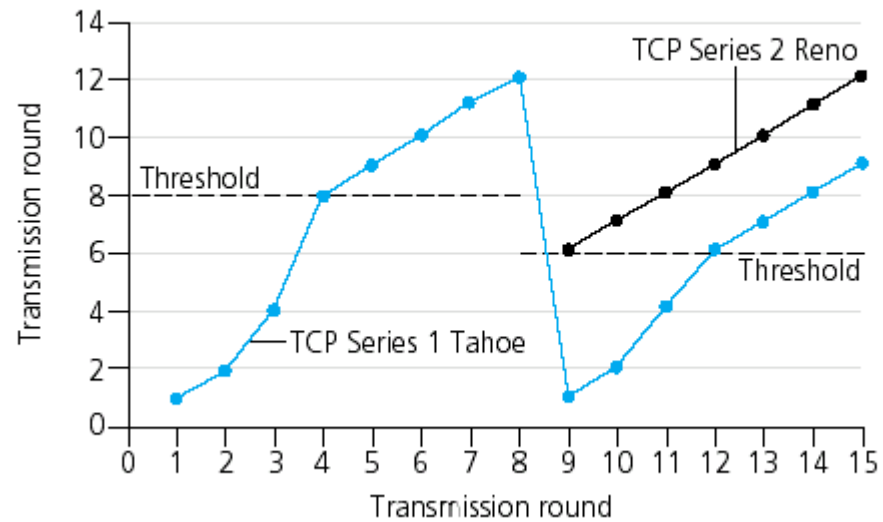
Philosophie :

- ❑ 3 dup ACKs indiquent un réseau capable de délivrer des segments
- ❑ un timeout indique un problème de congestion plus grave

Raffinement

Q: Quand l'augmentation exponentielle doit basculer en linéaire ?

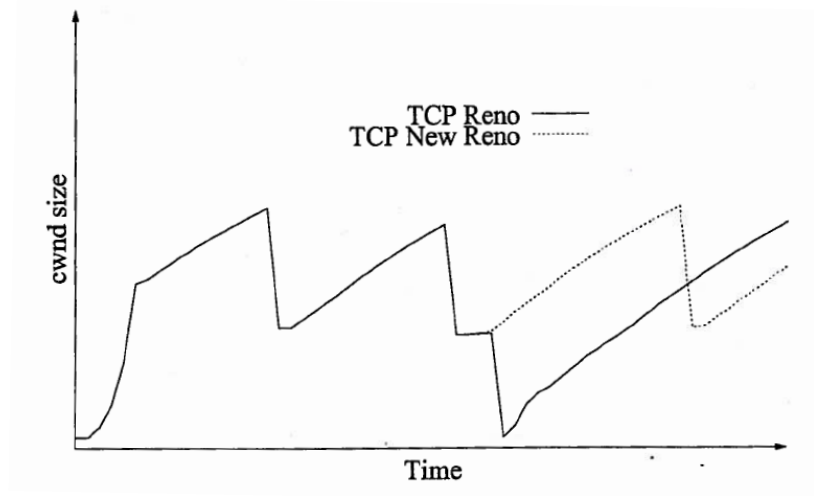
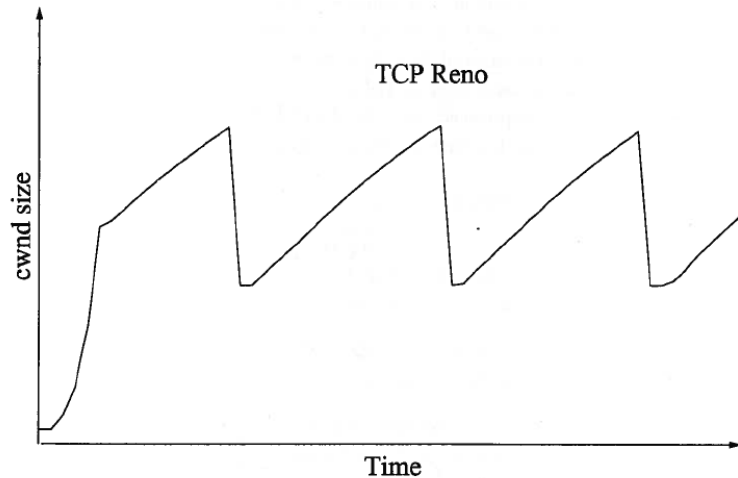
A: Quand **cwnd** atteint 1/2 de sa valeur avant timeout.



Versions de TCP

- Evolutions:

1. **TCP Tahoe** : seulement RTO et cwnd remise à 1 à chaque perte
2. Evolution de TCP Tahoe : **Fast retransmit** utilisé en plus de RTO
3. **TCP Reno: Fast recovery**: $cwnd = cwnd/2$ au lieu de $cwnd = 1$ après perte
4. **TCP New Reno**: seulement 1 FR/FR après 2 pertes de paquets de la même fenêtre



Résumé : Contrôle de congestion TCP

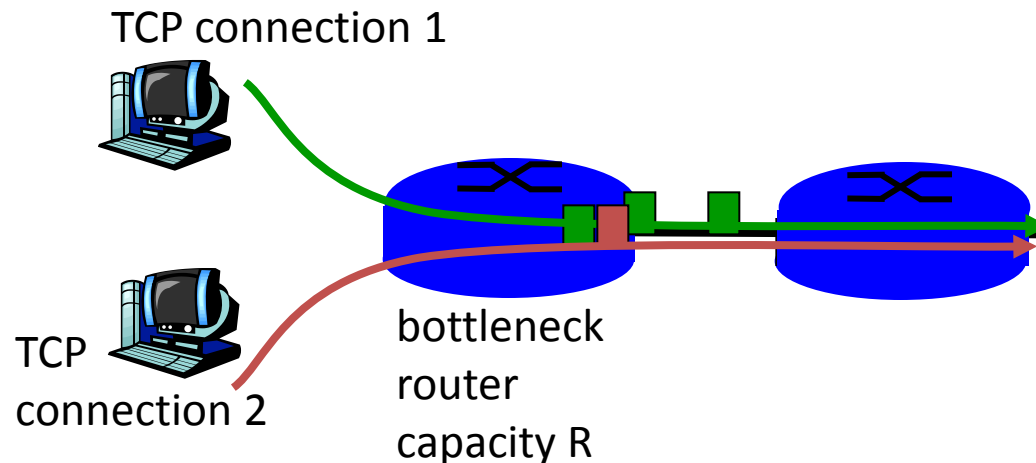
- Quand **cwnd** est en dessous de **ssthresh**, l'émetteur est dans la phase de **slow-start**, la fenêtre croît exponentiellement.
- Quand **cwnd** est au dessus de **ssthresh**, l'émetteur est dans la phase de **congestion-avoidance**, la fenêtre croît linéairement.
- Quand un **triple duplicate ACK** se produit, **ssthresh** est mis à **cwnd/2** and **cwnd** est mise à **ssthresh**.
- Quand un **timeout** se produit, **ssthresh** est mis à **cwnd/2** and **cwnd** est mise à 1 MSS.

TCP sender congestion control

State	Event	TCP Sender Action	Commentary
Slow Start (SS)	ACK receipt for previously unacked data	$cwnd = cwnd + MSS$, If ($cwnd > ssthresh$) set state to "Congestion Avoidance"	Resulting in a doubling of $cwnd$ every RTT
Congestion Avoidance (CA)	ACK receipt for previously unacked data	$cwnd = cwnd + MSS * (MSS/cwnd)$	Additive increase, resulting in increase of $cwnd$ by 1 MSS every RTT
SS or CA	Loss event detected by triple duplicate ACK	$ssthresh = cwnd / 2$, $cwnd = ssthresh$, Set state to "Congestion Avoidance"	Fast recovery
SS or CA	Timeout	$ssthresh = cwnd / 2$, $cwnd = 1 MSS$.	Enter slow start

L'équité de TCP

But de l'équité : si K sessions TCP partagent le même goulot d'étranglement de BP R , chacune doit obtenir un débit de R/K



Equité

Equité et UDP

- Les appli multimedia souvent n'utilisent pas TCP
 - Ne veulent pas être bridées ou étouffées par le CC
- Utilisent UDP à la place :
 - injectent audio/video à un débit constant, tolèrent des pertes de paquets
- Champ de recherche : gentil avec TCP

Equité et connexions TCP parallèles

- rien n'empêche les appli d'ouvrir plusieurs connexions en parallèle entre 2 hôtes
- les Web browsers font ça
- Exemple: lien de BP R supportant 9 connexions;
 - une nouvelle appli demande 1 TCP, obtient un débit de $R/10$
 - une nouvelle appli demande 10 TCPs, obtient $R/2$!

Plan

I. Présentation des WAN

II. Les interfaces de la couche physique

III. Protocoles de niveau 2 dans les WAN

IV. MPLS : commutation par VC dans le monde IP

V. Qualité de service

V.1. TCP et le contrôle de congestion dans le réseau

V.1.a. Rappels : transfert fiable et contrôle de flux

V.1.b. Principe du contrôle de congestion

V.1.c. Le contrôle de congestion par TCP

V.2. Classification des applications et besoin de QoS

V.2.a. Classification

V.2.b. Paramètres-clé de la QoS

V.2.c. Stratégies pour la QoS

V.3. Techniques de traitement de la QoS

V.3.a. Les outils

V.3.b. Traitements au niveau 2

V.3.c. Traitements au niveau 3

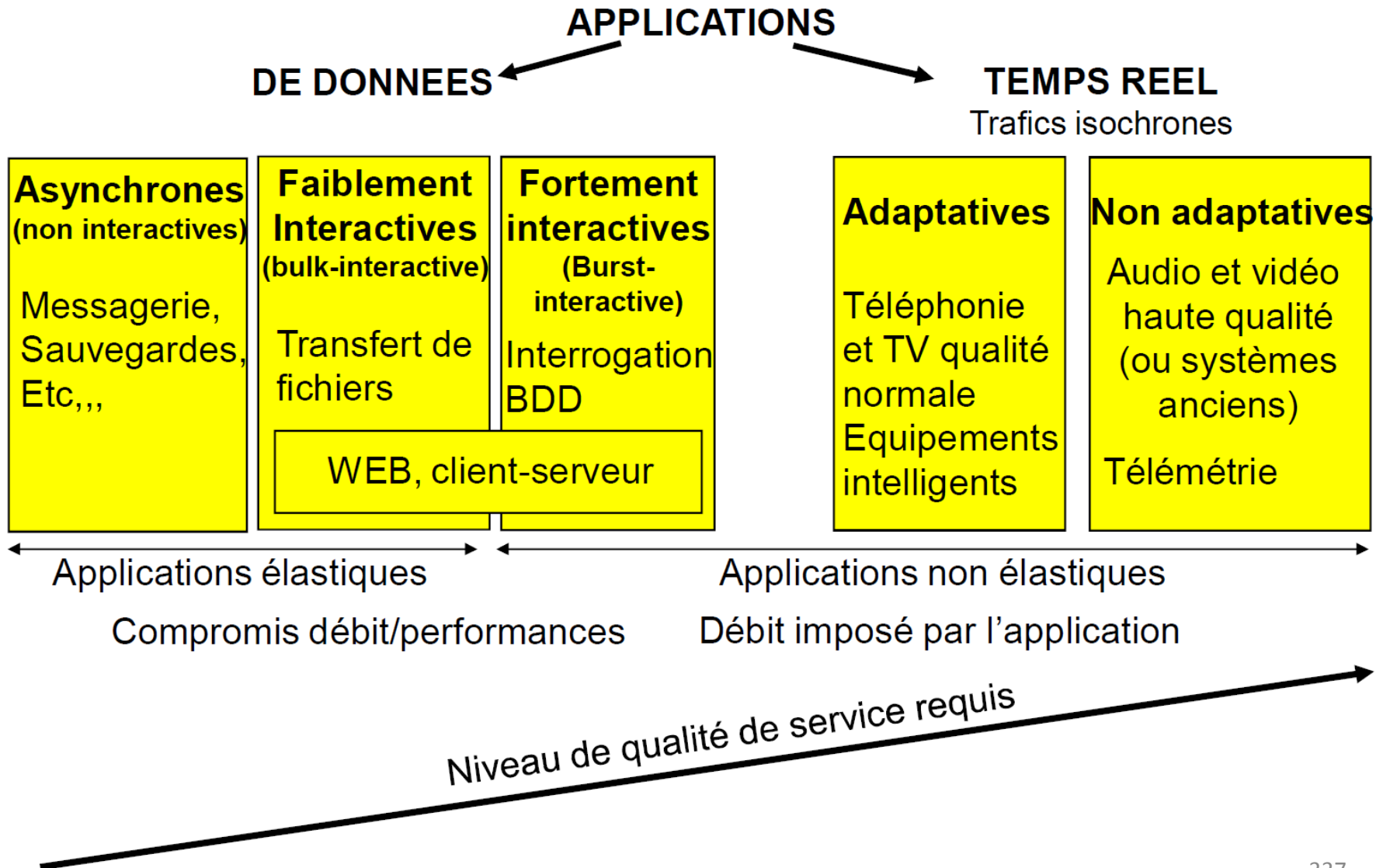
VI. Technologies xDSL

Source: Cours de J. Drouot (ESIL)

Classification des applications

Application	Pertes	Débit	Sensibilité au délai
file transfer	no loss	elastic	
e-mail	no loss	elastic	no
Web documents	no loss	elastic	no
real-time audio/video	loss-tolerant	audio: 5kbps-1Mbps video: 10kbps-5Mbps	no yes, 100's msec
stored audio/video	loss-tolerant	same as above	
interactive games	loss-tolerant	few kbps up	yes, few secs
instant messaging	no loss	elastic	yes, 100's msec
			yes and no

Classification des applications



Classification des applications

- Le débit et le délai peuvent fluctuer, faisant varier le niveau de confort de l'utilisateur
 - Les applications non interactives (**asynchrones**) sont insensibles à ces fluctuations
 - Les applications peu interactives (**bulk**) y sont peu sensibles
 - Les applications interactives (**burst**) y sont les plus sensibles
- Les applications ayant des gros transferts (bulk) et utilisant TCP accélèrent dès qu'elles le peuvent : elles sont dites « élastiques »
 - Du fait du fonctionnement de TCP
 - Ces applications, bien que peu exigeantes en général, sont dangereuses pour les autres applications
 - Il faut donc les identifier

Applications non-adaptatives

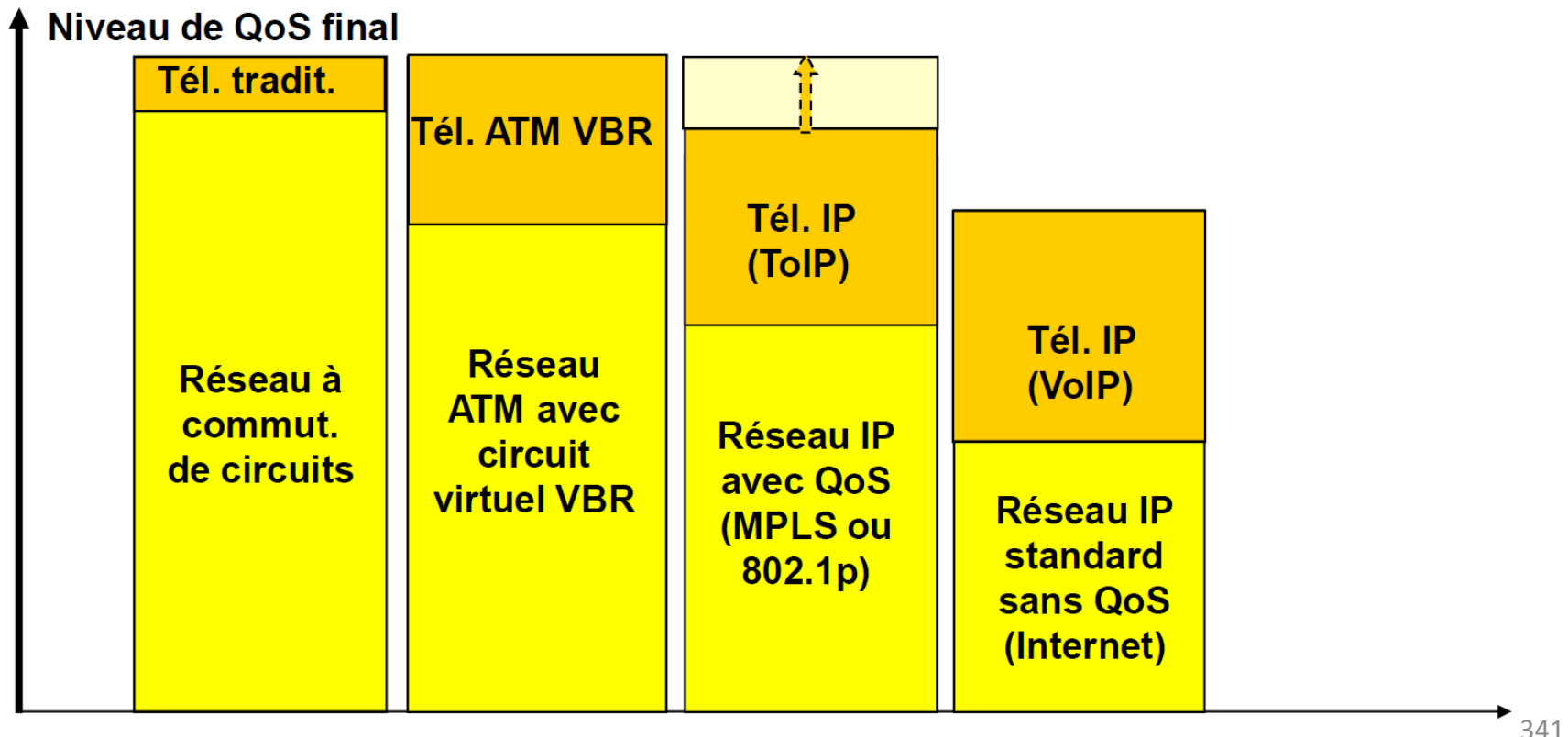
- **Les applications temps réel (voix, vidéo) ont un rythme imposé (*isochrone*) qui doit se maintenir de la source au destinataire**
 - Elles s'adaptent beaucoup plus mal à l'état de congestion du réseau
 - Le débit spécifié doit être assuré par le réseau sous peine de non fonctionnement
 - Ce débit était constant dans le cas des codecs sans compression
 - Le débit est variable quand les techniques de compression sont plus évoluées
 - Le délai doit être faible pour les applications temps réel interactives
 - Téléphonie ou vidéoconférence
 - Le délai doit en tout cas être le plus constant possible
 - La variation de délai (la ***gigue*** ou ***jitter***) doit être faible
 - Les pertes de paquet ne sont pas récupérées par retransmission
 - Ces applications utilisent UDP, qui ne tient pas compte de l'état de congestion du réseau
 - Ces applications doivent donc être protégées

Applications adaptatives

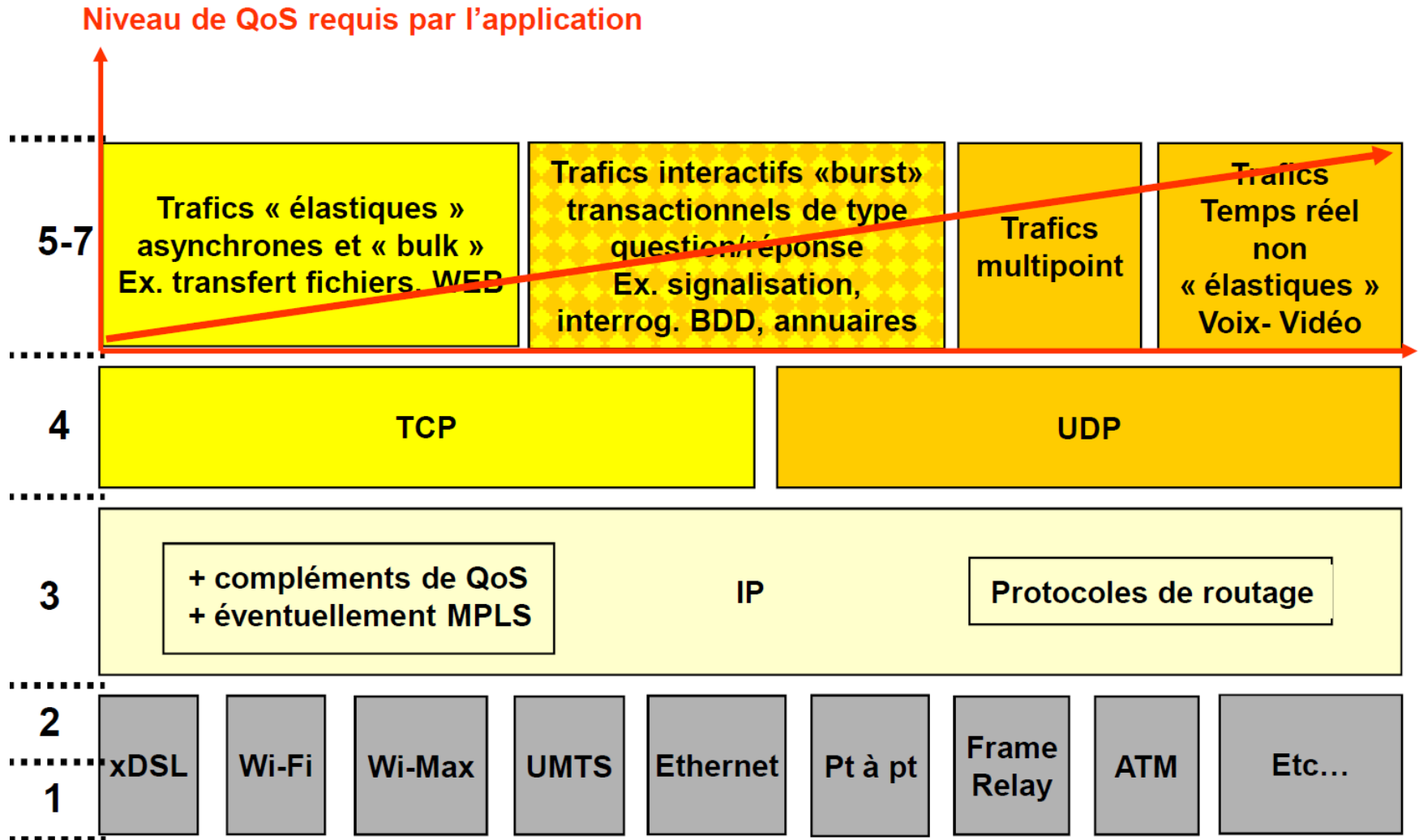
- **Les applications de données sur TCP s'adaptent à l'état de congestion du réseau**
 - Contrôle de flux et récupération de paquets perdus par TCP
 - L'allongement du délai n'est en général pas un problème
 - Les applications bulk sont peu interactives
- **Les applications de données de type burst ne s'adaptent pas à l'allongement du délai**
 - Mécontentement des utilisateurs
- **Les applications temps réel traditionnelles n'avaient pas à s'adapter**
 - Elles utilisaient un réseau à commutation de circuits
 - Délai très court, gigue très faible, débit dédié
- **Les applications temps réel modernes deviennent adaptatives**
 - Pour s'adapter aux fluctuations d'un réseau à commutation de paquets
 - Buffer de stockage à l'arrivée pour supprimer la gigue
 - Si la gigue est inférieure à un plafond, et au détriment du délai
 - Interpolation en cas de paquets perdus

Applications adaptatives

- **Les équipements d'extrémité sont de plus en plus intelligents**
 - Ils participent de plus en plus au niveau de QoS final obtenu
 - Et demandent moins de QoS au réseau
- **Tendance vers un réseau plus simple donc plus rapide et des stations plus intelligentes**



Utilisation de TCP ou UDP



A-t-on vraiment besoin de traiter la QoS ?

- **La bande passante au niveau LAN devient énorme et bon marché**
 - 100 Mbps, 1Gbps, 10 Gbps, ...
 - On peut se permettre de surdimensionner les liaisons
- **La bande passante interne aux WAN devient énorme aussi**
 - Jusqu'à des Térabps dans une même fibre grâce à DWDM!
 - Les cœurs de réseau sont aujourd'hui surdimensionnés
- **La bande passante à l'interface LAN-WAN est en train d'exploser**
 - Grâce à ADSL (de 512 Kbps à 20 Mbps) puis FTTH (50 à 100 Mbps)
- **Les commutateurs et routeurs sont de plus en plus puissants**
 - Jusqu'à des dizaines de millions de paquets/s

Pourquoi ne pas simplement profiter du surdimensionnement des lignes et des équipements?

- **Sans ajouter un traitement de QoS qui risque de freiner les performances et augmenter le coût!**

Oui, le traitement de la QoS est nécessaire

- **Les différents types d'applications induisent des flux qui se contrarient**
 - Les transferts de gros volumes (par exemple les transferts de fichiers) sont élastiques, et prennent toute la bande passante disponible
 - Que ce soit 64 Kbps ou 100Mbps!
 - Les applications interactives (question/réponse) consomment une bande passante prévisible, mais exigent des délais courts
 - Elles sont pénalisées par les transferts de fichiers
 - Les applications temps réel (téléphonie ou vidéo) ne sont pas élastiques (besoin borné en bande passante), mais elles doivent avoir un débit garanti, et un délai court et fixe
 - Elles sont pénalisées par les applications de gros transferts
- **Avoir une bande passante surdimensionnée ne suffit pas**
 - Il faut empêcher les applications élastiques de prendre toute la bande passante
- **Avoir beaucoup de bande passante permet juste de simplifier le traitement de la qualité de service**
 - Besoin de mécanismes de QoS simples, implémentés en hardware

Plan

I. Présentation des WAN

II. Les interfaces de la couche physique

III. Protocoles de niveau 2 dans les WAN

IV. MPLS : commutation par VC dans le monde IP

V. Qualité de service

V.1. TCP et le contrôle de congestion dans le réseau

V.1.a. Rappels : transfert fiable et contrôle de flux

V.1.b. Principe du contrôle de congestion

V.1.c. Le contrôle de congestion par TCP

V.2. Classification des applications et besoin de QoS

V.2.a. Classification

V.2.b. Paramètres-clé de la QoS

V.2.c. Stratégies pour la QoS

V.3. Techniques de traitement de la QoS

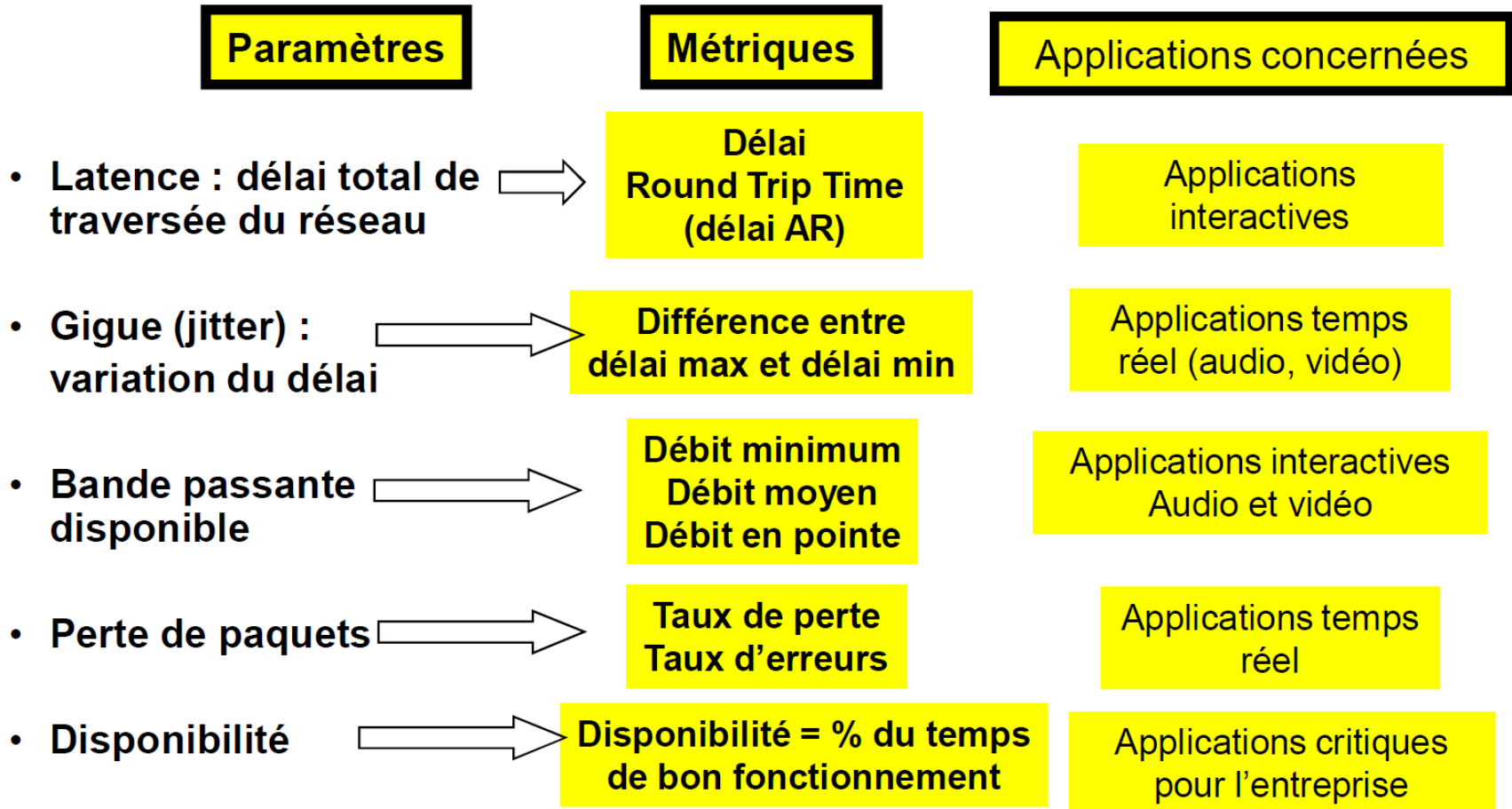
V.3.a. Les outils

V.3.b. Traitements au niveau 2

V.3.c. Traitements au niveau 3

VI. Technologies xDSL

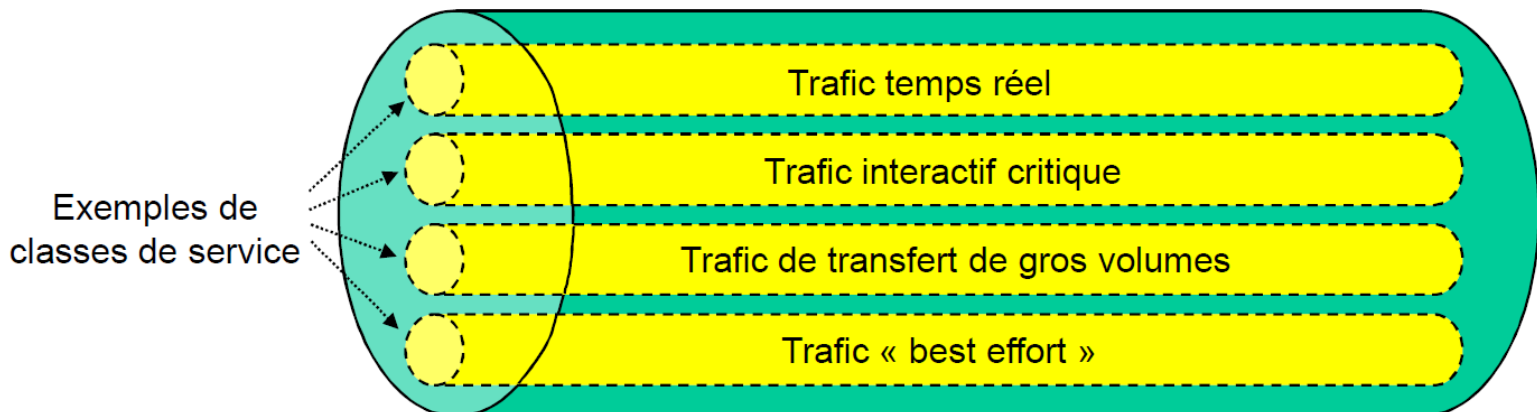
Paramètres-clé de la QoS



C'est la congestion qui est responsable de la plupart des dégradations de QoS

Définition de la qualité de service (QoS)

- **C'est l'assurance pour un élément (application, hôte, routeur, commutateur) que son trafic sera acheminé dans les conditions voulues et prévisibles**
 - Le délai doit être compatible avec les besoins de l'application
 - La bande passante doit être disponible
 - Le taux de perte de paquets doit être compatible avec l'application
 - La QoS se focalise sur les périodes de congestion
- **Le trafic doit être réparti en classes de service de façon à isoler les applications qui se contrarient**
 - Cela suppose d'analyser les flux qui doivent transiter sur le réseau
 - Chaque classe de service doit avoir les performances qui lui conviennent



Plan

I. Présentation des WAN

II. Les interfaces de la couche physique

III. Protocoles de niveau 2 dans les WAN

IV. MPLS : commutation par VC dans le monde IP

V. Qualité de service

V.1. TCP et le contrôle de congestion dans le réseau

V.1.a. Rappels : transfert fiable et contrôle de flux

V.1.b. Principe du contrôle de congestion

V.1.c. Le contrôle de congestion par TCP

V.2. Classification des applications et besoin de QoS

V.2.a. Classification

V.2.b. Paramètres-clé de la QoS

V.2.c. Stratégies pour la QoS

V.3. Techniques de traitement de la QoS

V.3.a. Les outils

V.3.b. Traitements au niveau 2

V.3.c. Traitements au niveau 3

VI. Technologies xDSL

Stratégies de traitement de la qualité de service

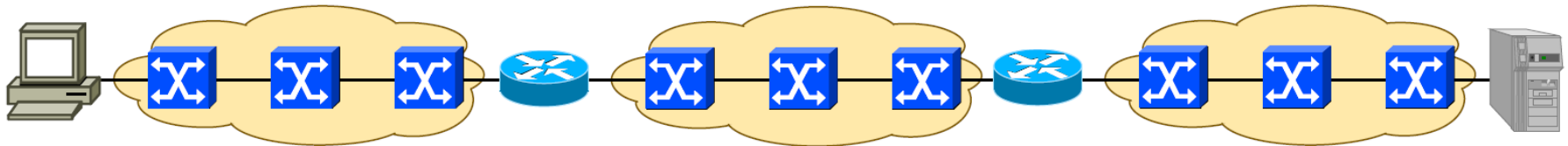
- **Cinq moyens complémentaires d'assurer la qualité de service**
- **1. Surdimensionnement de la capacité du réseau**
- **2. Utiliser des applications adaptatives**
 - Interpolation de données manquantes (temps réel)
 - Émettre à débit variable en fonction de la congestion
 - Buffers de réception pour compenser la gigue, ...
- **3. Traitement sélectif du trafic sans réservation préalable**
 - Le trafic est classifié, et le traitement différencié (DiffServ)
 - Chaque classe a son traitement spécifique
 - Files d'attente séparées
 - Traitement spécifique en cas de congestion
 - Les trafics à privilégier sont prioritaires
- **4. Réservation dynamique de ressources**
 - Frame Relay, ATM, IntServ - RSVP
- **5. Ingénierie de trafic**
 - Répartir le trafic dans le réseau en fonction de la bande passante disponible



-> **MPLS-TE**

Stratégies de traitement de la qualité de service

- **Dans quelle couche OSI doit-on traiter la qualité de service?**
- **Traitement au niveau des couches supérieures?**
 - Oui si on veut compenser les imperfections résiduelles de QoS
 - Par TCP (applications élastiques) ou par les applications adaptatives (VoIP)
- **Traitement au niveau 3?**
 - Oui si on veut conserver une QoS sur l'ensemble du parcours
 - Traitement dans les routeurs
- **Traitement au niveau 2?**
 - Oui si on veut que la QoS soit homogène de bout en bout
 - Traitement dans chaque commutateur de chaque sous-réseau multipoint
- **Le traitement de la qualité de service est réparti dans toutes les couches**
 - La répartition des rôles est variable selon les modèles, c'est le résultat final qui compte!
 - Exemples : RTC, VoIP sur Internet, ToIP en entreprise



RTC : Réseau Téléphonique commuté VoIP : Voice over IP ToIP : Telephony over IP

Plan

I. Présentation des WAN

II. Les interfaces de la couche physique

III. Protocoles de niveau 2 dans les WAN

IV. MPLS : commutation par VC dans le monde IP

V. Qualité de service

V.1. TCP et le contrôle de congestion dans le réseau

V.1.a. Rappels : transfert fiable et contrôle de flux

V.1.b. Principe du contrôle de congestion

V.1.c. Le contrôle de congestion par TCP

V.2. Classification des applications et besoin de QoS

V.2.a. Classification

V.2.b. Paramètres-clé de la QoS

V.2.c. Stratégies pour la QoS

V.3. Techniques de traitement de la QoS

V.3.a. Les outils

V.3.b. Traitements au niveau 2

V.3.c. Traitements au niveau 3

VI. Technologies xDSL

Principales composantes du traitement de la QoS

Traitements sur les données

- Classification des flux
- Prévention de la congestion
 - Conditionnement à l'entrée
 - shaping, policing, dropping
- Gestion de la congestion
 - Traitement des files d'attente
- Adaptation de l'application
 - Buffer de gigue
 - Interpolation données perdues

Plan de données

Actions de réservation préalable

- Configuration statique
- Signalisation par flux agrégés
- Signalisation par micro-flux

Suppose une forme de circuit virtuel
Frame Relay, ATM, RSVP, MPLS

Plan de contrôle

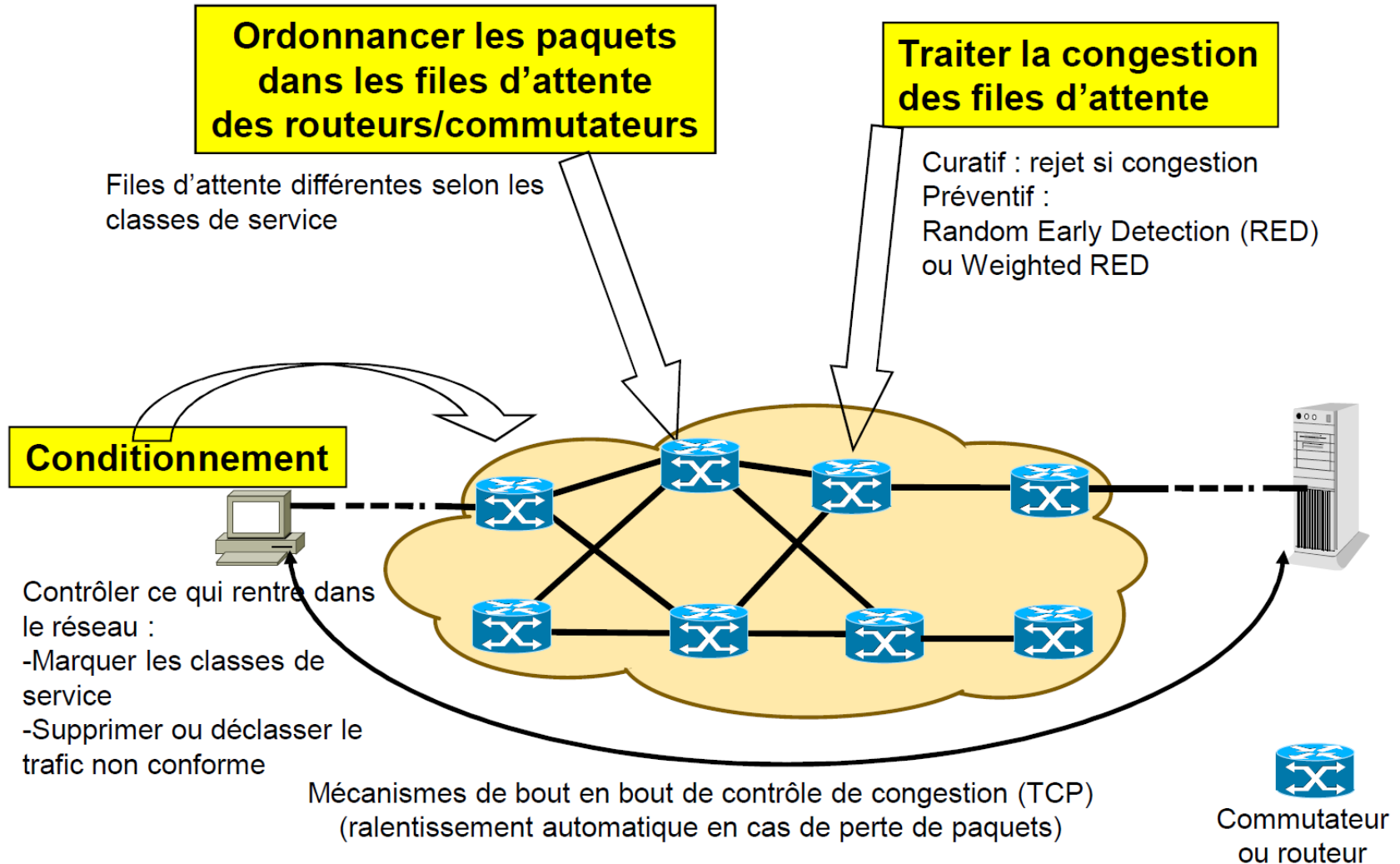
QoS

- **Routage par chemin le plus court (IP)**
- **Ingénierie de trafic**
Routage par contraintes
pour des flux agrégés

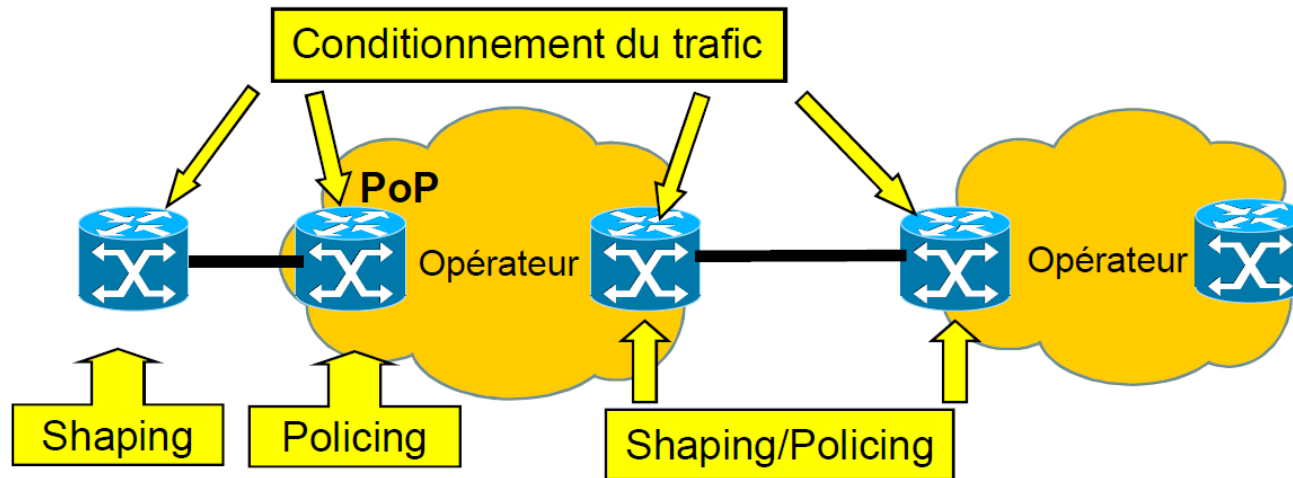
Plan de routage

Routage et QoS sont traités indépendamment dans IP : routage basé sur l'adresse destination (tout le trafic est envoyé sur la meilleure route)

Plan de données: actions sur les données



Outils de conditionnement de trafic



- **Objectif : rendre le trafic compatible avec un profil de trafic pré-défini**
 - Profil accepté par le réseau
 - Débit moyen, débit en pointe, taille de rafale
 - Profil défini dans le contrat (SLA) passé entre l'utilisateur et l'opérateur
- **Les techniques employées pour la mesure et la mise en forme sont propriétaires**
 - Elles sont locales à un équipement
 - Les techniques les plus courantes sont le seau percé et le seau à jetons

PoP : Point Of Presence

Leaky bucket (saut percé)

- **Un seau par flux ou classe de trafic**

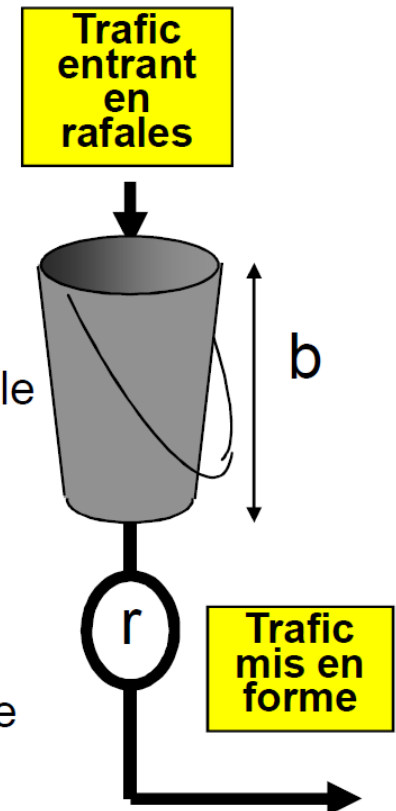
- Taille du seau : b octets
- Le seau fuit au débit de r octets/s
- Les octets d'un paquet entrant sont placés dans le seau
- Un paquet qui ferait déborder le seau est rejeté
- Quand le paquet de taille d est au fond du seau, on le retient pendant d / r avant de l'envoyer
- La taille du seau b détermine la taille maximale de la rafale

- **Utilisation pour le shaping**

- Le trafic en entrée est en rafales (bornées par la taille du seau), le trafic en sortie est régulier

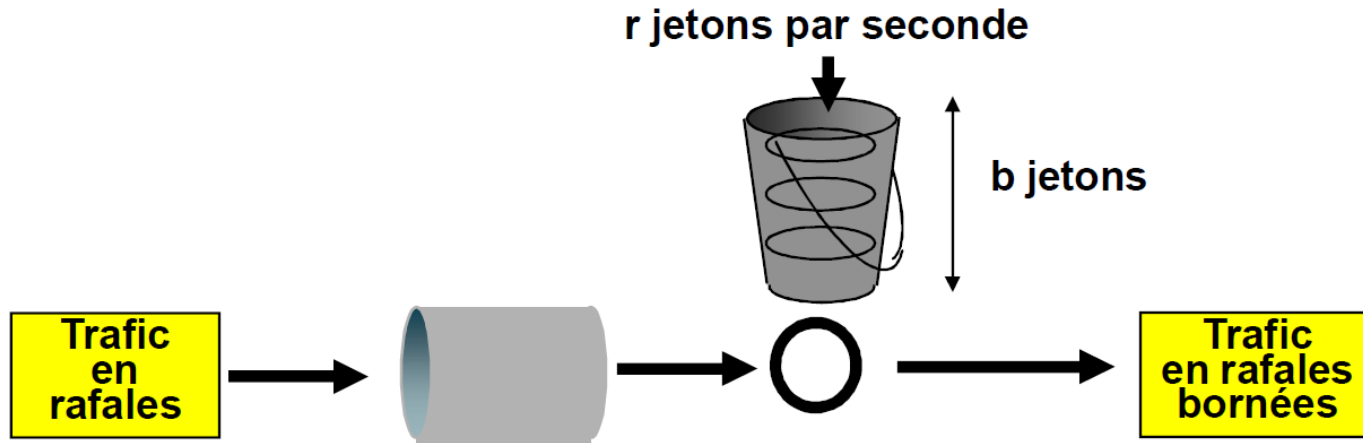
- **Utilisation pour le policing**

- Permet de surveiller le débit moyen (r) et la taille de rafale (b) du trafic entrant
 - Pour chaque paquet conforme, on ajoute d octets dans le seau
 - Un paquet qui ferait déborder le seau n'est pas conforme



==> Débit d'entrée écriété à r . Permet d'autoriser rafale de taille $(\text{debit_raf}-r).\text{tps_raf} \leq b$ bits, ou encore $\Delta r \leq b/\Delta t$.

Token bucket (saut à jetons)



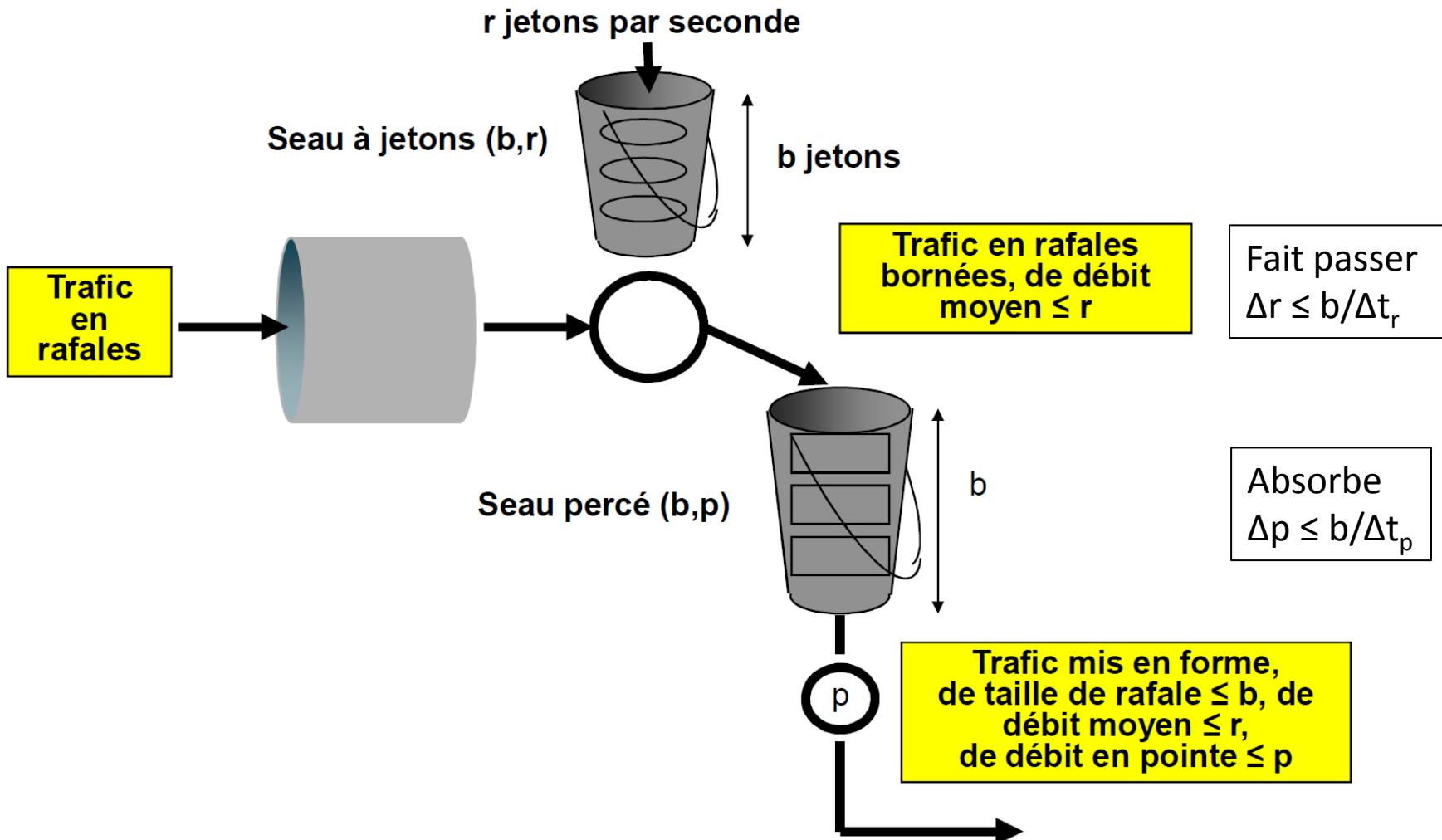
- **On place des jetons dans le seau avec un débit r**
 - La capacité du seau est de b jetons
 - Le trafic de données ne passe pas dans le seau
 - Les jetons sont rejetés si le seau est plein
 - Pour émettre un paquet de taille d octets, on doit enlever d jetons du seau
- **Le seau à jetons permet de borner les rafales**

==> Débit de sortie peut dépasser r de Δr pendant Δt pourvu que: $(r+\Delta r)\Delta t \leq r\Delta t + b$, ou encore $\Delta r \leq b/\Delta t$.

Pour recharger le saut de b jetons, il faut redescendre à un débit de $(r-x)$ pendant au moins t sec, (t,x) tel que: $(r-x)t \geq b$

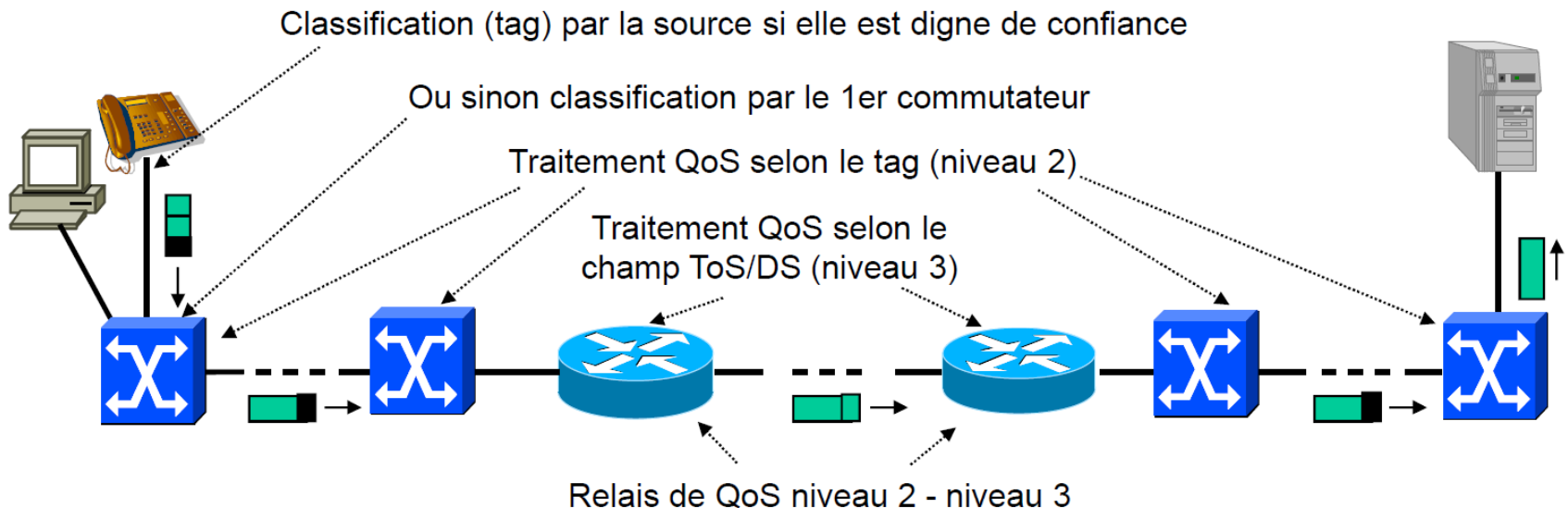
--> Le débit moyen sur une longue période est toujours $\leq r$.

Utilisation combinée de *leaky* et *token buckets*



Outils de traitement des files d'attente

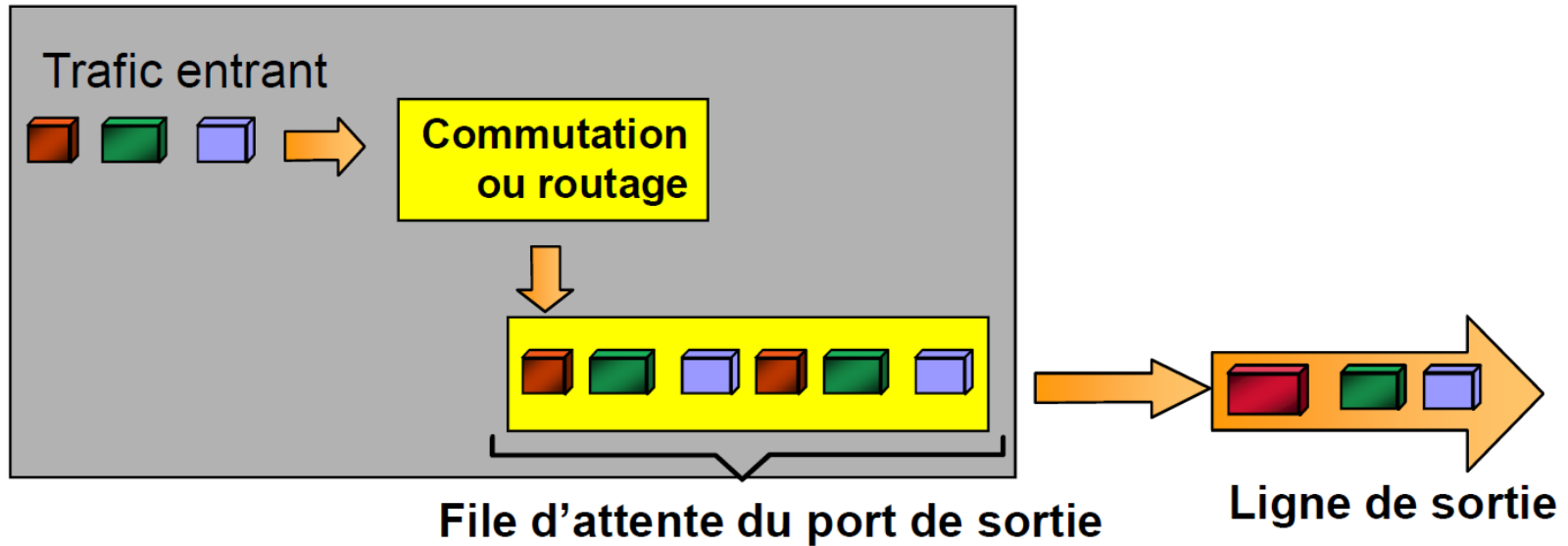
- **Objectifs des techniques de traitement des files d'attente**
 - Diminuer le délai de certains trafics prioritaires
 - Assurer l'équité des trafics
 - Empêcher que certains trafics en occultent d'autres
 - Répartir la bande passante entre les trafics
- **Les techniques de gestion des files d'attente sont propriétaires**
- **Ces outils de traitement des files d'attente sont mis en œuvre dans les commutateurs Ethernet (au niveau 2) et dans les routeurs (au niveau 3)**



Files d'attente de type FIFO

- **FIFO (First-In-First-Out)**

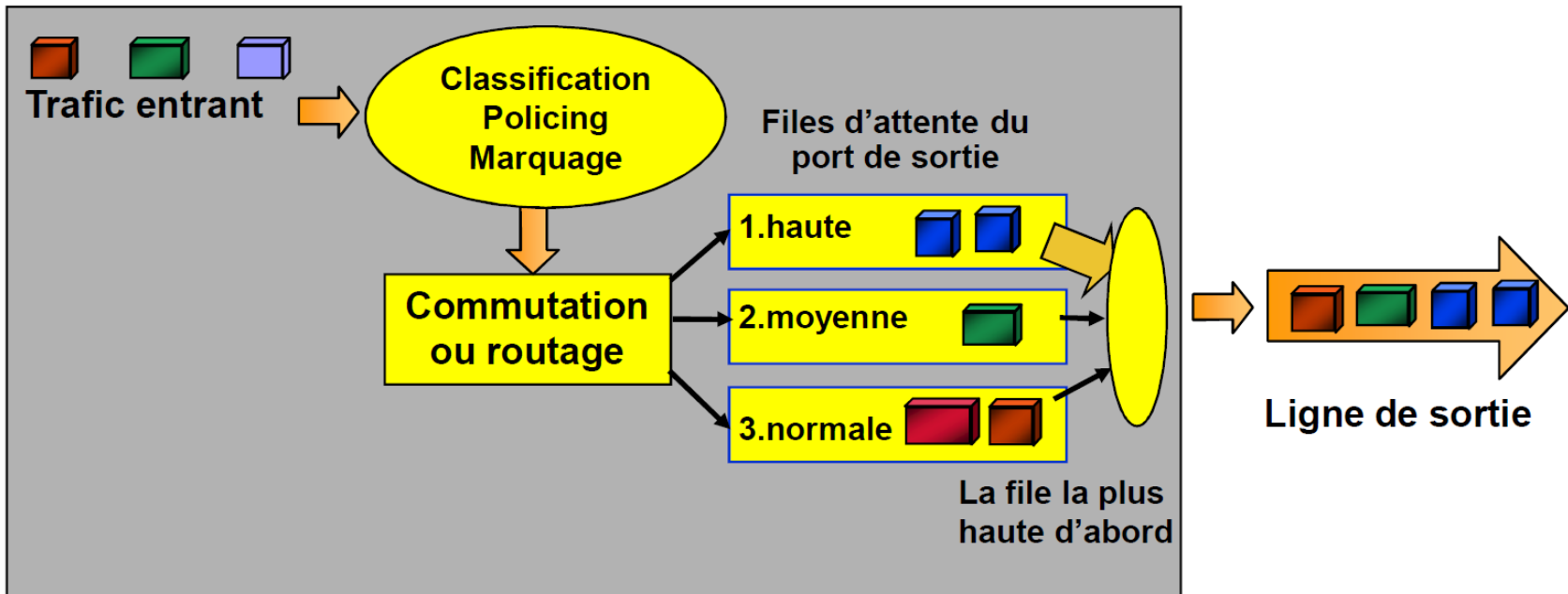
- La plus simple et la plus courante
- Fonctionne bien en absence de congestion
 - Rejet de paquets excédentaires en cas de congestion



- **Un transfert de fichiers peut monopoliser toute la bande passante**

Files d'attente *Priority Queuing*

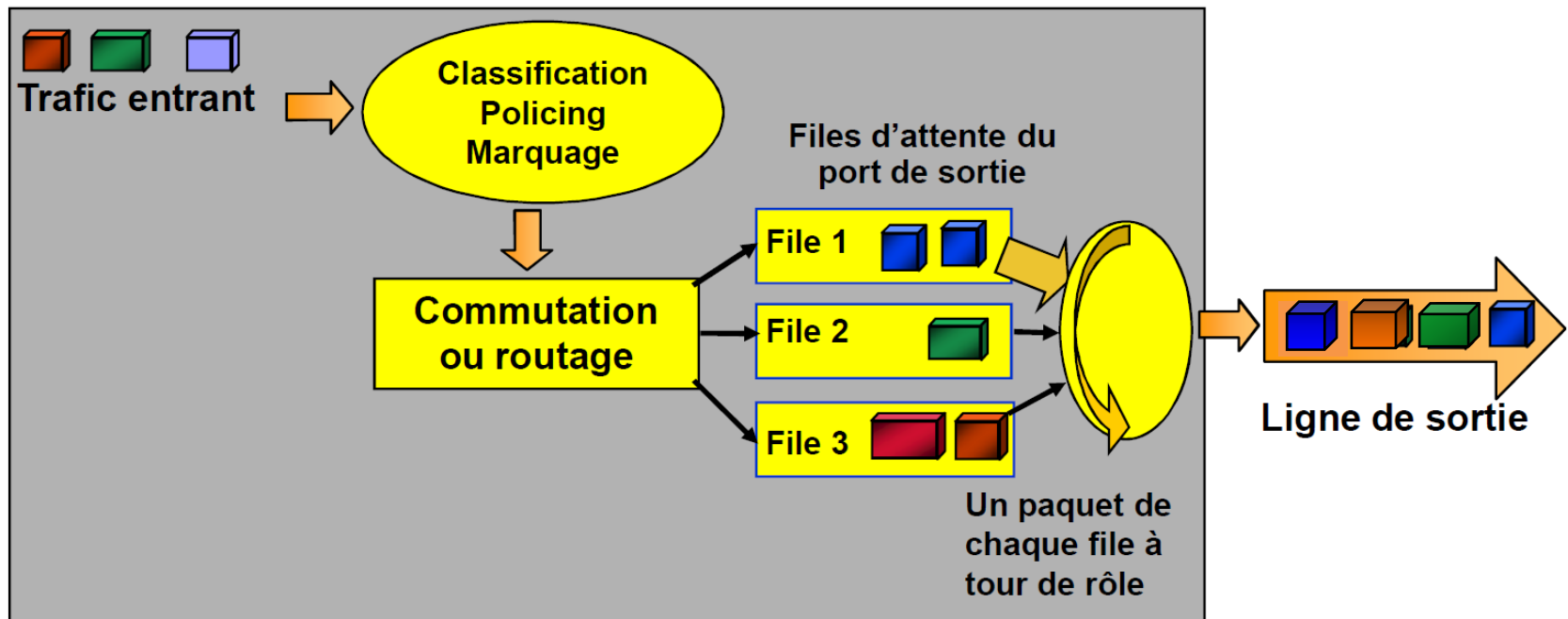
- **Files d'attente par priorités (priority queuing)**
 - Files d'attente différentes selon les classes de trafic
 - Les files d'attente sont traitées dans l'ordre des priorités
 - Une file d'attente n'est servie que si les files de plus haute priorité sont vides



- **Un type de trafic peut dominer les autres**
 - Si une file d'attente prioritaire ne se vide pas

Files d'attente *Round-robin* Queuing

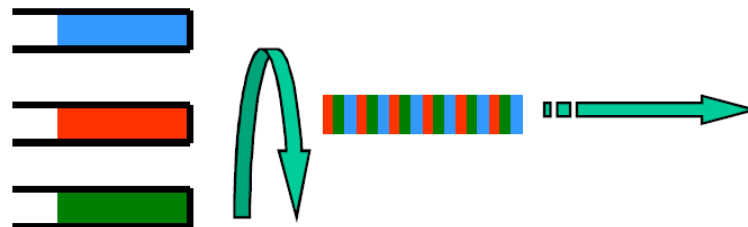
- On sert un paquet de chaque file non vide à tour de rôle
- Version pondérée (*Weighted RRQ*) : on sert plus d'un paquet par visite



- Empêche les trafics de se « cannibaliser »
- Mais favorise les flux ayant des paquets longs

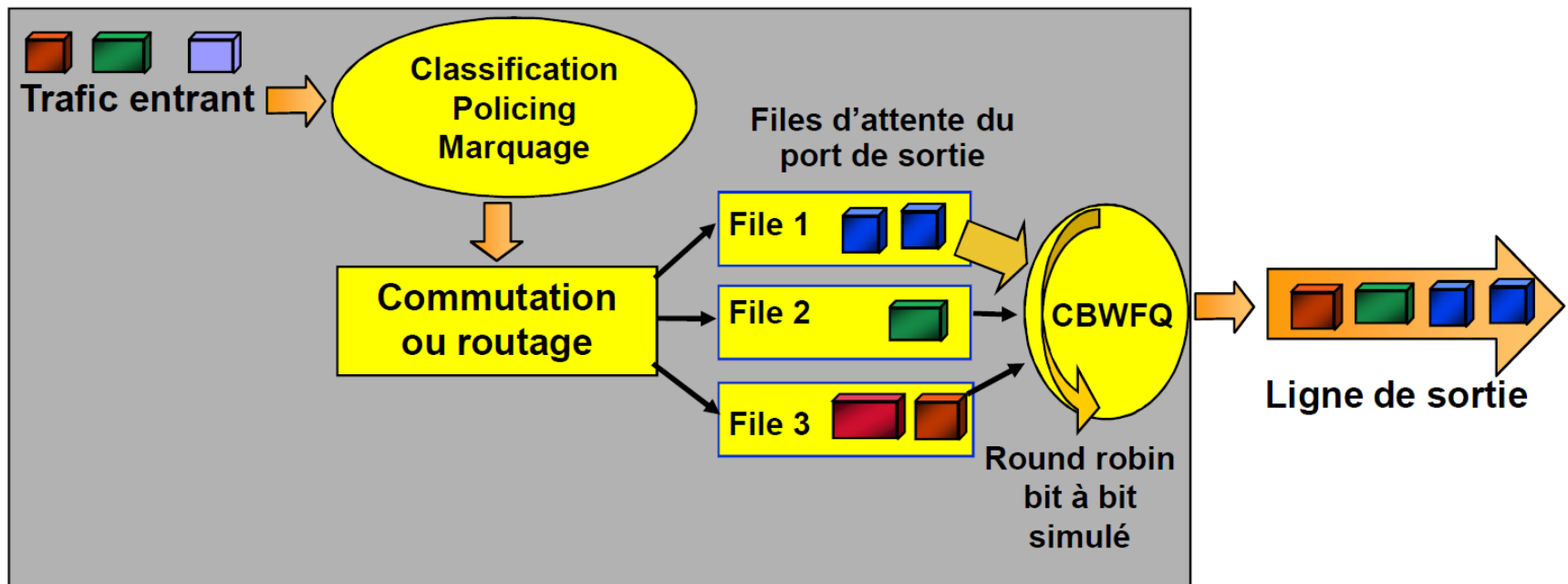
Vers une politique d'ordonnancement « idéale »

- **Les solutions Priority Queuing (PQ) et Round Robin Queuing (RRQ) ne satisfont pas tous les besoins**
 - PQ est bien adapté aux flux nécessitant une priorité stricte
 - A condition que ces flux ne soient pas élastiques
 - RRQ est équitable, mais privilégie les grands paquets
- **Il manque une solution simple, équitable et permettant de garantir des performances minimales**
 - Class-Based Weighted Fair Queuing (CB-WFQ) est une adaptation de Weighted RRQ
 - On simule un service cyclique bit par bit
 - Les paquets sont émis dans l'ordre correspondant au temps auquel leur dernier bit aurait été transmis en émission bit à bit
 - On ne défavorise pas les flux de petits paquets



Class-Based Weighted Fair Queuing

- **Multiplexage temporel (tranches de temps allouées cycliquement)**
 - Les conversations à faible volume ont donc une priorité effective
 - Les conversations à fort volume ne monopolisent pas la bande passante
 - Des poids permettent d'attribuer plus de BP aux trafics sensibles au délai



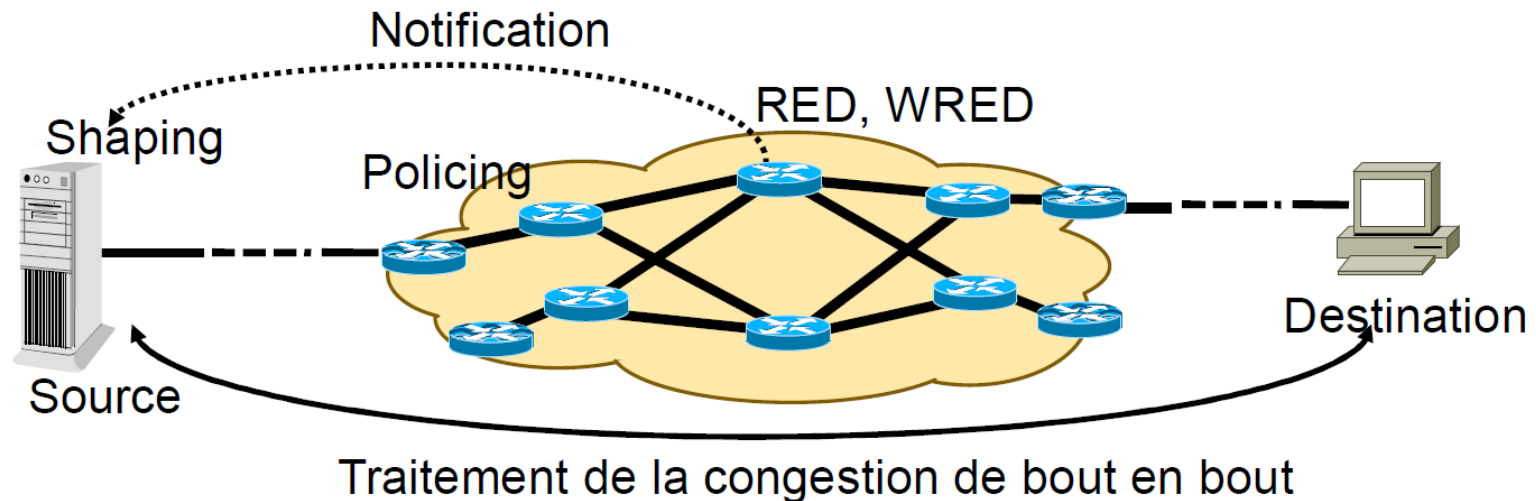
- **Permet de répartir la bande passante de façon équitable**

Performances du Class-Based Weighted Fair Queuing

- **Débit alloué à la classe i , pendant tout intervalle de temps où il y a des paquets de classe i à envoyer**
 - $d_i = D * w_i / (\sum w_j)$
 - w_i = poids associé à une classe i , D = débit disponible en sortie
- **Théorème de Parekh et Gallager**
 - Il permet de calculer le délai maximum de traversée d'un paquet pour un flux conditionné à l'entrée du réseau (par un seau à jetons), en fonction de la bande passante réservée dans chaque WFQ.
- **On peut donc utiliser CBWFQ pour faire de la réservation de bande passante**
 - Et garantir un délai maximum de traversée

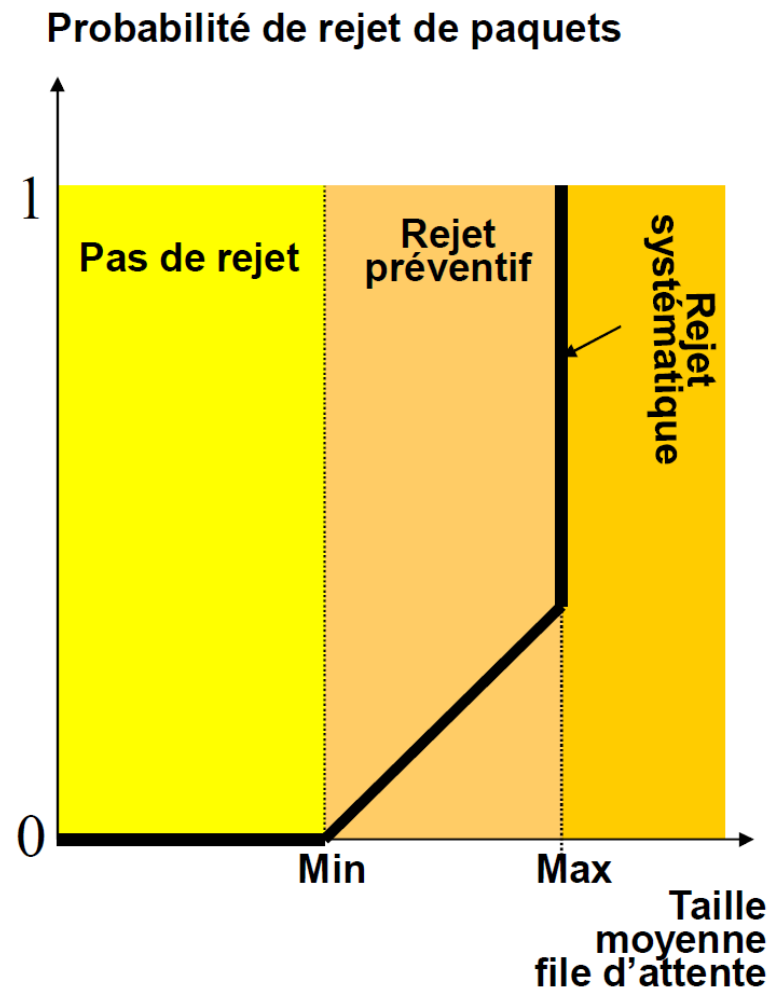
Les outils de traitement de la congestion

- La congestion a un impact important sur des paramètres clés de la QoS
 - Le taux de pertes de paquets
 - Le délai et la variation de délai
- **3 moyens de traiter la congestion**
 - Préventivement par *shaping / policing* (voir précédemment)
 - De façon curative de bout en bout (par TCP)
 - Préventivement par les équipements réseau : RED et WRED
 - Avec ou sans notification explicite à la source



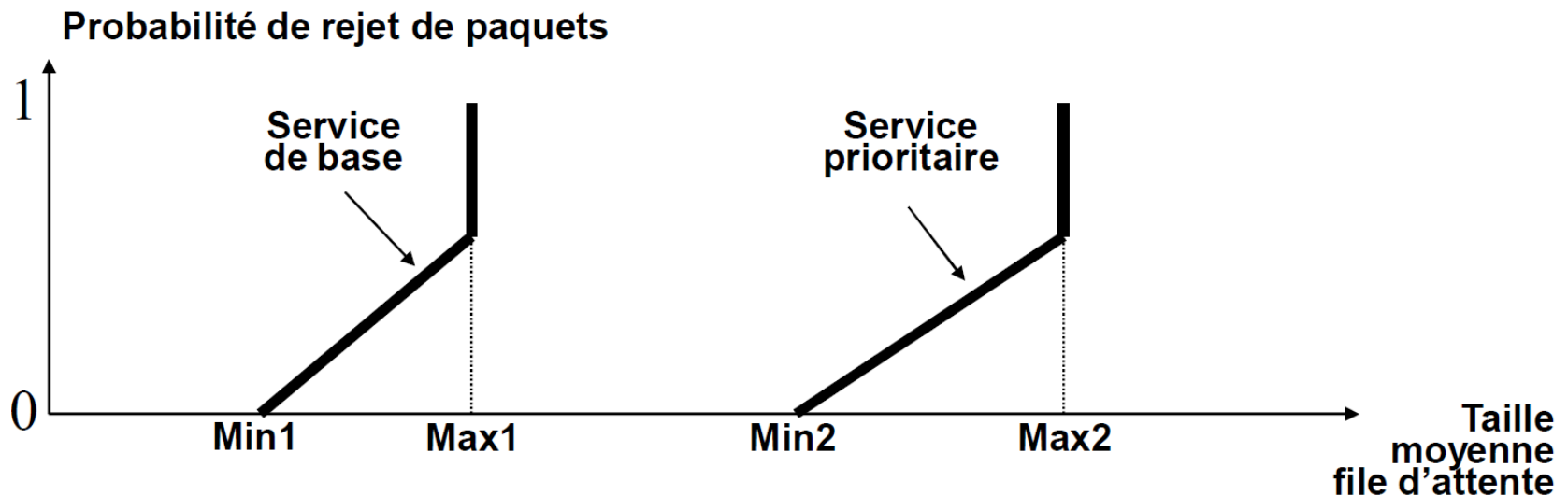
Random Early Detection (RED)

- **Le traitement de la congestion par TCP est curatif**
 - Il provoque la synchronisation des connexions TCP
 - *Slow-start* synchronisés des différentes connexions TCP
- **RED permet un traitement préventif**
 - Un paquet perdu est un signal de congestion pour TCP, qui provoque un ralentissement (*congestion avoidance*)
 - On rejette des paquets après un seuil mais avant la congestion
 - Rejet aléatoire entre les différentes connexions
 - Ce qui lisse la taille de la file d'attente tout en évitant la synchronisation globale
 - RFC 2309



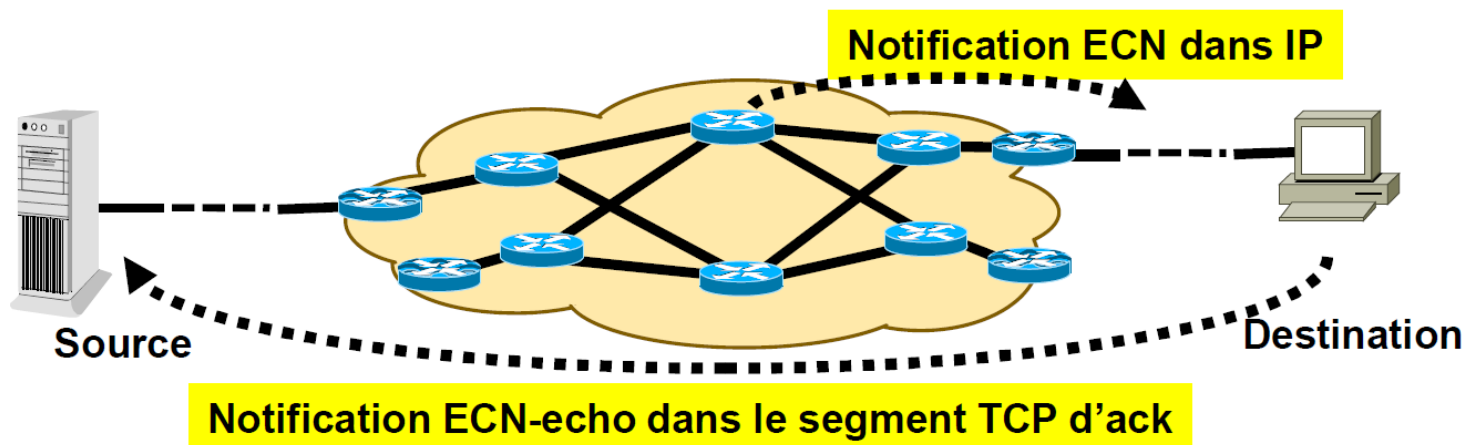
Weighted RED

- **Les seuils à partir desquels on commence à rejeter des paquets peuvent être différents selon les classes de service**
 - Exemple : 30% de la taille du buffer pour le service de base, et 60% pour le service prioritaire (priorité en cas de congestion)
 - La priorité peut être marquée dans le champ ToS /DS
- **RED est équitable et simple, mais efficace seulement avec les trafics TCP**



Notification explicite de congestion

- Utilisation conjointe de RED et ECN (Explicit Congestion Notification)
 - RFC 2481
 - Un routeur RED positionne le bit ECN au lieu de jeter le paquet
 - Le bit ECN est recopié dans l'entête TCP d'ack (ECN-echo)
 - Un seul paquet marqué ECN provoque une réaction à la congestion
 - Un 2e bit peut indiquer si TCP est compatible ECN
 - Selon ce bit le marquage RED est un rejet ou le bit ECN



Plan

I. Présentation des WAN

II. Les interfaces de la couche physique

III. Protocoles de niveau 2 dans les WAN

IV. MPLS : commutation par VC dans le monde IP

V. Qualité de service

V.1. TCP et le contrôle de congestion dans le réseau

V.1.a. Rappels : transfert fiable et contrôle de flux

V.1.b. Principe du contrôle de congestion

V.1.c. Le contrôle de congestion par TCP

V.2. Classification des applications et besoin de QoS

V.2.a. Classification

V.2.b. Paramètres-clé de la QoS

V.2.c. Stratégies pour la QoS

V.3. Techniques de traitement de la QoS

V.3.a. Les outils

V.3.b. Traitements au niveau 2

V.3.c. Traitements au niveau 3

VI. Technologies xDSL

Qualité de service aux niveaux 2 et 3

- **Différentes technologies de réseau ont introduit des mécanismes pour assurer un niveau de qualité de service au niveau 2**
 - Frame Relay, Token ring, FDDI
 - Et surtout ATM
 - Qualité de service complète (trop?)
- **Dans un contexte d'interconnexion de réseaux, les mécanismes de traitement de la QoS au niveau 2 ne peuvent assurer une QoS de bout en bout**
 - Il faut aussi traiter la QoS au niveau 3
- **L'infrastructure de niveau 2, de façon native ou par le biais de mécanismes de traitement de la QoS, ne doit pas freiner les trafics que les routeurs traitent de façon prioritaire au niveau 3**
- **Les mécanismes de QoS des niveaux 2 et 3 sont donc complémentaires et doivent être cohérents**

Bilan des traitements de QoS au niveau 2

	Besoin de QoS
PPP	Néant : le traitement de QoS de niveau 3 suffit
Ethernet	Besoins assez faibles : la bande passante est abondante et bon marché. Surdimensionnement. Il suffit de privilégier le délai des applications temps réel, de veiller à l'équité entre les classes de flux, et de se protéger des flux élastiques.
Frame Relay	Qualité de service prévue pour assurer un débit minimum à un circuit virtuel en cas de congestion. Une seule classe de service par circuit virtuel Mécanismes de réservation à l'établissement de connexion : bande passante chère et limitée
ATM	Réseau prévu pour être universel : réseau d'accès, de distribution, et cœur de réseau Tous les niveaux de QoS sont disponibles. Une seule classe de service par circuit virtuel : le traitement de la QoS n'est plus effectif si IP est au dessus d'ATM

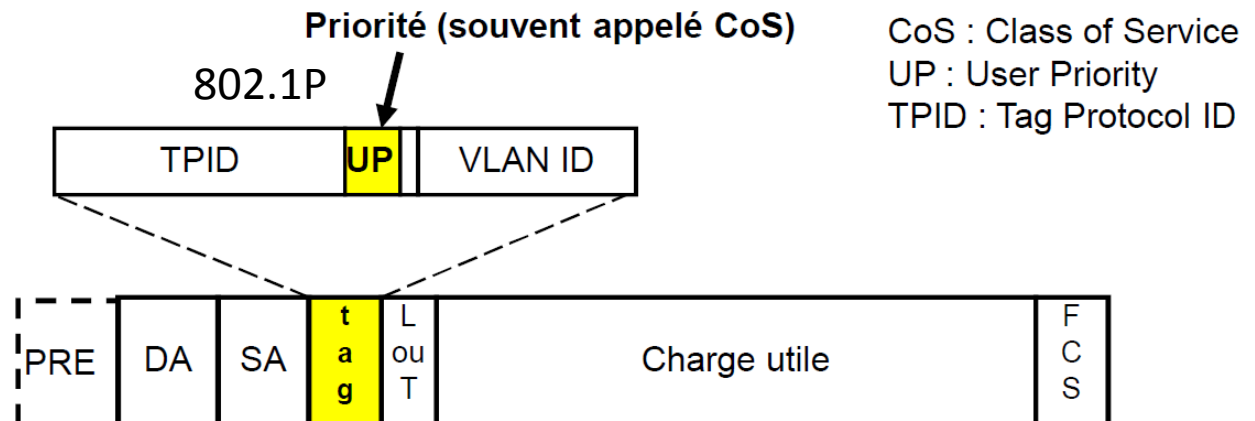
Bilan des traitements de QoS au niveau 2

	Plan de données	Plan de contrôle	Plan de routage
PPP	Néant	Néant	Néant
Ethernet	Classification et marquage : tags 802.1 P Traitement des files d'attente Congestion : rejet préventif	Néant	Néant
Frame Relay	Conditionnement : CIR/EIR Marquage des trames en entrée Rejet du trafic excédent en entrée Congestion : rejet curatif	Signalisation (si SVC) Configuration statique (PVC) Réservation de débit minimum	Néant
ATM	Classification, marquage, policing, traitement des files d'attente, congestion : rejet curatif selon priorités	Signalisation Q.2931 Toutes politiques de réservation	Routage en fonction de la QoS

SVC : Switched Virtual Circuit PVC : Permanent Virtual Circuit

802.1p : Priorité des trames Ethernet

- La gestion des priorités du commutateur nécessite que les trames véhiculent une information de priorité
- Les trames Ethernet natives n'ont pas d'indication de priorité
- Une étiquette (tag) 802.1Q doit être ajoutée
 - Cette étiquette comporte un champ priorité (3 bits)
 - Le tag peut être inséré par le premier commutateur selon des critères prédéfinis, ou par une station digne de confiance
 - En général une file d'attente de priorité stricte : téléphonie et vidéo
 - Et des files d'attente standard (souvent de type RRQ) qui empêchent les flux de se cannibaliser



802.1p : Priorité des trames Ethernet

- **Le tableau suivant donne un exemple d'utilisation du champ CoS**
 - Les commutateurs sont souvent limités à quatre files d'attente de sortie
 - Files d'attente de type Priority Queuing ou Round Robin Queuing
 - Mais les noms diffèrent selon les constructeurs
 - Exemple SRR (Shaped Round Robin Queuing) chez Cisco

Priorité	Nom	Type de trafic
7	Network control	Administration de réseau
5 et 6	Vidéo et audio	Voix ou multimédia (priorité stricte)
3 et 4	Excellent effort et Controlled load	Niveaux de priorité intermédiaires
2	Reserved	Réservé
1	Background	Trafic bulk non urgent
0	Best effort	Trafic LAN standard

Plan

I. Présentation des WAN

II. Les interfaces de la couche physique

III. Protocoles de niveau 2 dans les WAN

IV. MPLS : commutation par VC dans le monde IP

V. Qualité de service

V.1. TCP et le contrôle de congestion dans le réseau

V.1.a. Rappels : transfert fiable et contrôle de flux

V.1.b. Principe du contrôle de congestion

V.1.c. Le contrôle de congestion par TCP

V.2. Classification des applications et besoin de QoS

V.2.a. Classification

V.2.b. Paramètres-clé de la QoS

V.2.c. Stratégies pour la QoS

V.3. Techniques de traitement de la QoS

V.3.a. Les outils

V.3.b. Traitements au niveau 2

V.3.c. Traitements au niveau 3

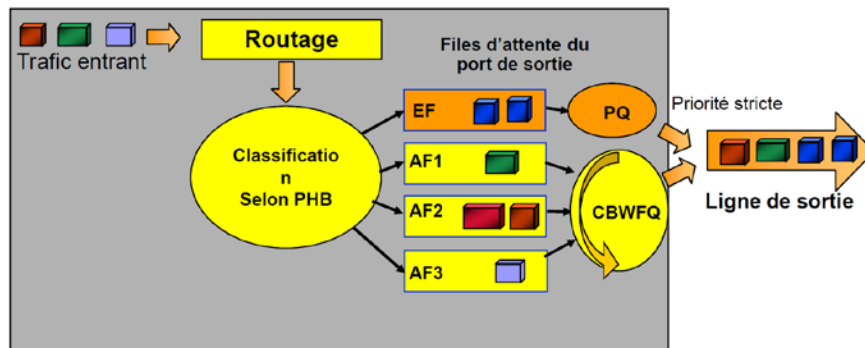
VI. Technologies xDSL

Principe de DiffServ

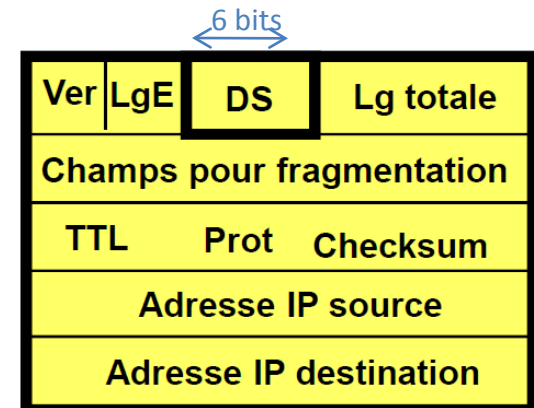
- Dans l'Internet traditionnel, tous les flows sont traités de la même façon
 - Avec ATM, on peut offrir des garanties en terme de QoS au prix de plus de signalisation, et de décisions d'acceptation/rejet de nouveaux flows pour maintenir le service des flows présents.
 - En effet, ressources limitées -> besoin de rejeter des flows pour maintenir le niveau de service
- > contraire à la nature *Best-effort* de l'Internet où il n'y a pas de contrôle d'admission
- Mais important de différencier les classes de flows : un abonné qui voudrait payer plus pourrait avoir un plus haut débit ou un plus petit délai (appli temps-réel tels que voix, vidéo,...).
- > introduction de Diffserv : basé sur le marquage des paquets aux bord du réseau selon le niveau de performance que le SP veut leur fournir, et traitement différencié de ces paquets dans le coeur du réseau.

Principe de DiffServ

- 4 classes de flows définies, et les paquets de flows de classes différentes mis dans des files différentes
- Différenciation supplémentaire des paquets dans la même classe : 3 niveaux intra-classe pour les paquets d'un même flow. La combinaison d'une classe et d'un niveau dans la classe est appelée ou *Per-Hop Behavior – PHB*.
- Chacun des 12 PHB correspond à un code point affecté au paquet à son entrée dans le réseau.
- Un niveau intra-classe est aussi appelé *drop precedence* : probabilité d'abandon fonction de ce niveau si saturation de la file affectée à cette classe (par ex les paquets de synchro TCP).



CBWFQ : Class-Based Weighted Fair Queuing



Mode de fonctionnement de DiffServ

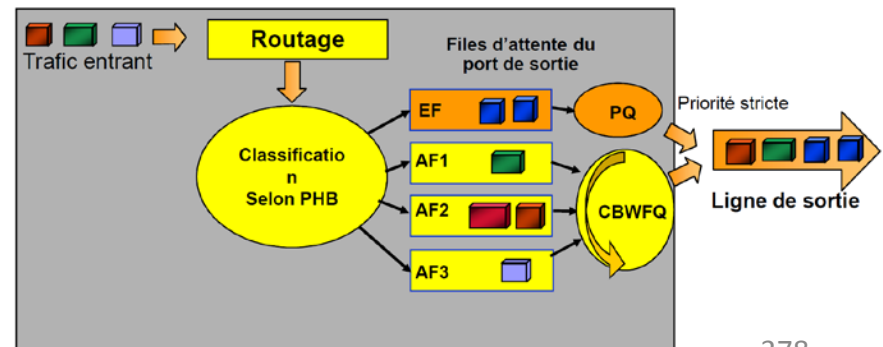
L'architecture Diffserv a 2 composants :

1. Routeur de bord de l'ISP :

- Politiques d'affectation de priorités aux paquets : décidées par le SP sur la base du SLA passé avec le client. Dépend notamment du comportement de la source du flow (quel est son débit courant par rapport à son débit moyen et de crête prévus dans le SLA).
- Assignation du DiffServ code point (DSCP) à chaque paquet.

2. Routeurs de coeur : appliquer des traitement différents aux paquets en fonction de leurs DSCP.

Traitement différents: en termes de décisions d'ordonnancement et d'abandon.

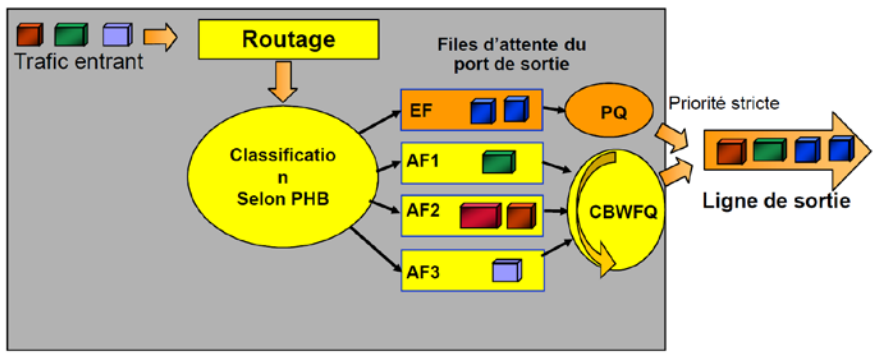


Format du champ DS

- DSCP = 0 associé au Best-effort
- 1 valeur de DSCP associée au PHB EF (Expedited Forwarding)
- 12 valeurs de DSCP associées aux PHB AF (Assured Forwarding)

6 bits
↔

Ver	LgE	DS	Lg totale
Champs pour fragmentation			
TTL	Prot	Checksum	
Adresse IP source			
Adresse IP destination			



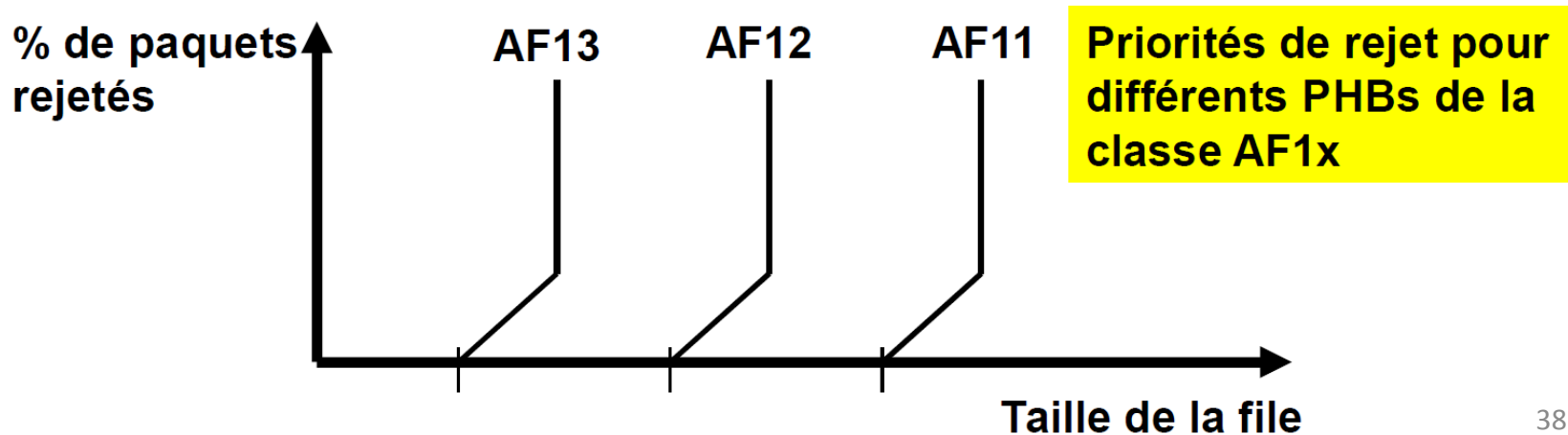
CBWFQ : Class-Based Weighted Fair Queuing

Le PHB EF (Expedited Forwarding)

- **Le PHB EF (appelé auparavant premium) est conçu pour des flux avec**
 - Faible taux de perte, faible délai, faible gigue et bande passante garantie
 - Similaire à une liaison spécialisée virtuelle de débit de pointe connu entre deux points extrémité à travers un domaine DS
 - Valeur du code DSCP pour PHB EF = 101110
- **Pour minimiser délai et gigue, les paquets doivent perdre le moins de temps possible dans les files des routeurs**
 - Conditionnement (policing et shaping) du trafic en fonction du débit de pointe en bordure d'un domaine
 - Dimensionnement du réseau de telle sorte que le débit de pointe soit inférieur aux débits des liaisons de sortie de chaque routeur dans le réseau
 - Paquets rangés dans une file de sortie à haute priorité
 - PQ avec priorité fixe préemptive ou WFQ avec un poids important
 - Mais aucun mécanisme particulier n'est imposé
- **RFC 3246 et RFC 3260**

Le PHB AF (Assured Forwarding)

- Pour déterminer les niveaux intra-classe :
 - soit un leaky ou token bucket -> 2 niveaux (paquets in et paquets out)
 - soit CIR et PIR -> 3 niveaux



Plan

I. Présentation des WAN

II. Les interfaces de la couche physique

III. Protocoles de niveau 2 dans les WAN

IV. MPLS : commutation par VC dans le monde IP

V. Qualité de service

VI. Technologies xDSL

VI.1. Principe : tirer le maximum de la paire de fils de cuivre

VI.2. Technique de TS pour xDSL : l'OFDM

VI.3. Fonctionnement protocolaire entre le FAI et l'abonné (cas dégroupé et non-dégroupé)

Références

- Cours basé sur les transparents de J. Stein (*RAD data communications*)
- Cours OFDM de P. Ciblat (Télécoms-ParisTech)
- Site de Christian Caleca

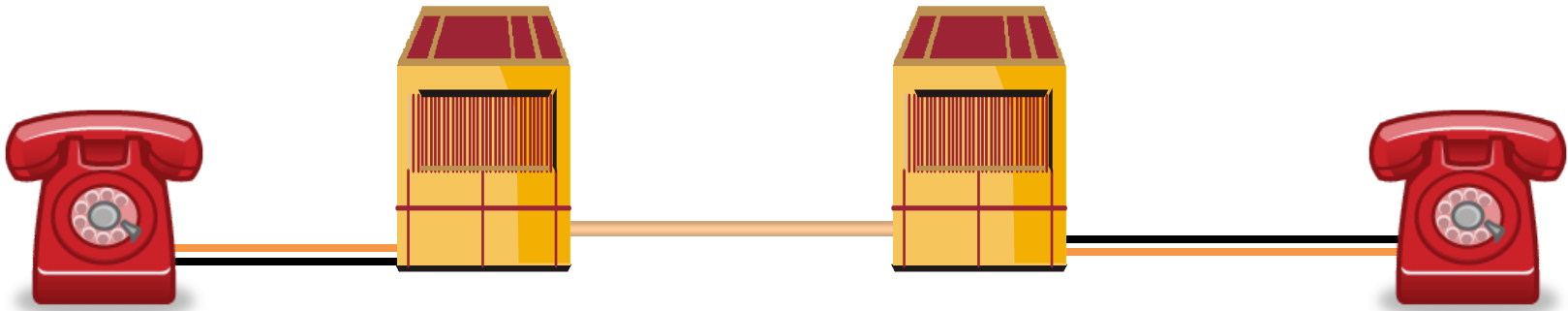
Original PSTN



Manual switching directly connected two *local loops*

Due to microphone technology, audio BW was 4 kHz

Analog switched PSTN

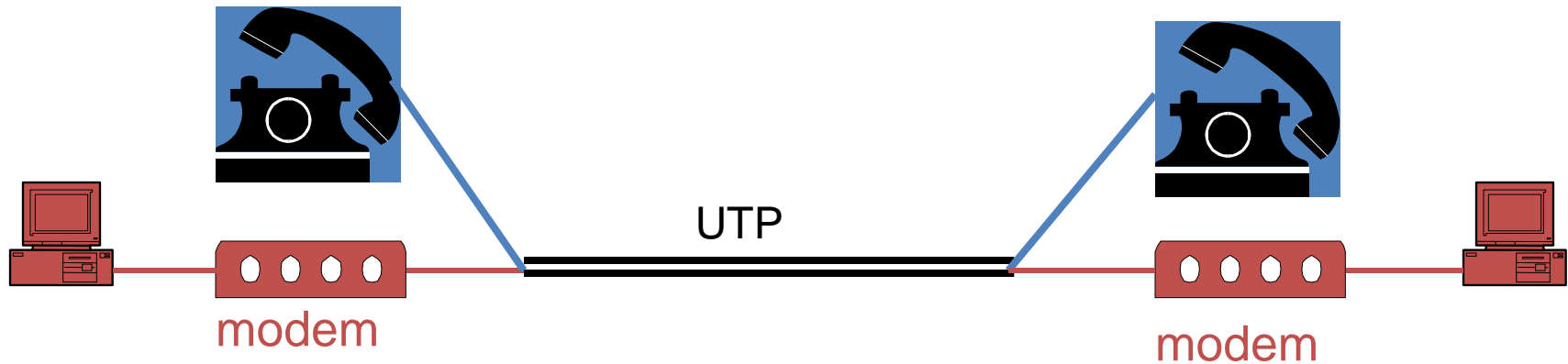


Invention of tube amplifier enabled *long distance*

Between central offices used FDM spaced at 4 kHz
(each cable carrying 1 group = 12 channels)

Developed into hierarchical network of automatic switches
(with supergroups, master groups, supermaster groups)

Data supported via voice-grade modems

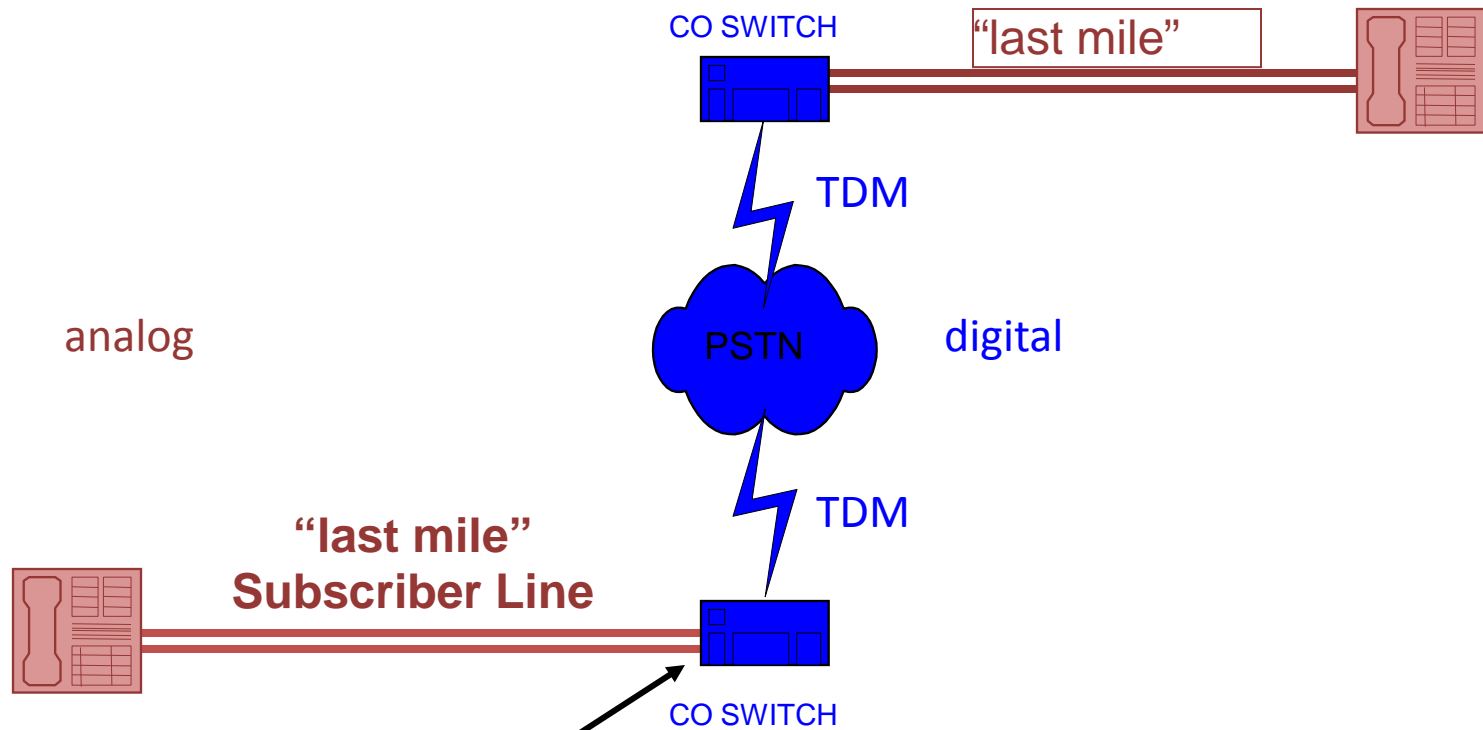


To send data, it is converted into 4 kHz audio (modem)

Data rate is determined by *Shannon's capacity theorem*

- *there is a maximum data rate (bps) called the "capacity" that can be reliably sent through the communications channel*
- *the capacity depends on the BW and SNR*

Digital PSTN



LP filter to 4 kHz at input to CO switch (before A/D converter)

Where is the limitation ?

A 4 kHz analog channel is presented to subscriber

The 4 kHz limitation is enforced by LP filter

at input to CO switch (before 8 kHz sampling)

The actual subscriber line is not limited to 4 kHz

Is there a better way

to use the subscriber line for digital transmissions ?

What is UTP?

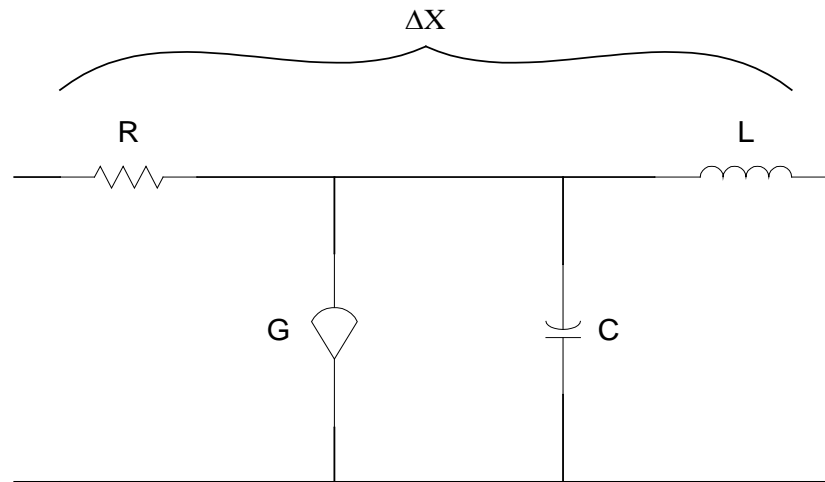
The achievable data rate is limited by physics of the subscriber line

The subscriber line is an Unshielded Twisted Pair of copper wires

- Two plastic insulated copper wires (two directions over single pair)
- Twisted to reduce crosstalk
- Supplies DC power and audio signal
- Physically, UTP is
 - distributed resistances in series
 - distributed inductances in series
 - distributed capacitances in parallelso the attenuation increases with frequency
- Various other problems exist (splices, loading coils, etc.)

UTP characteristics

- Resistance per unit distance
- Capacitance per unit distance
- Inductance per unit distance
- Cross-admittance (assume pure reactive) per unit distance



Propagation loss

Voltage decreases as travel along cable

Each new section of cable reduces voltage by a factor



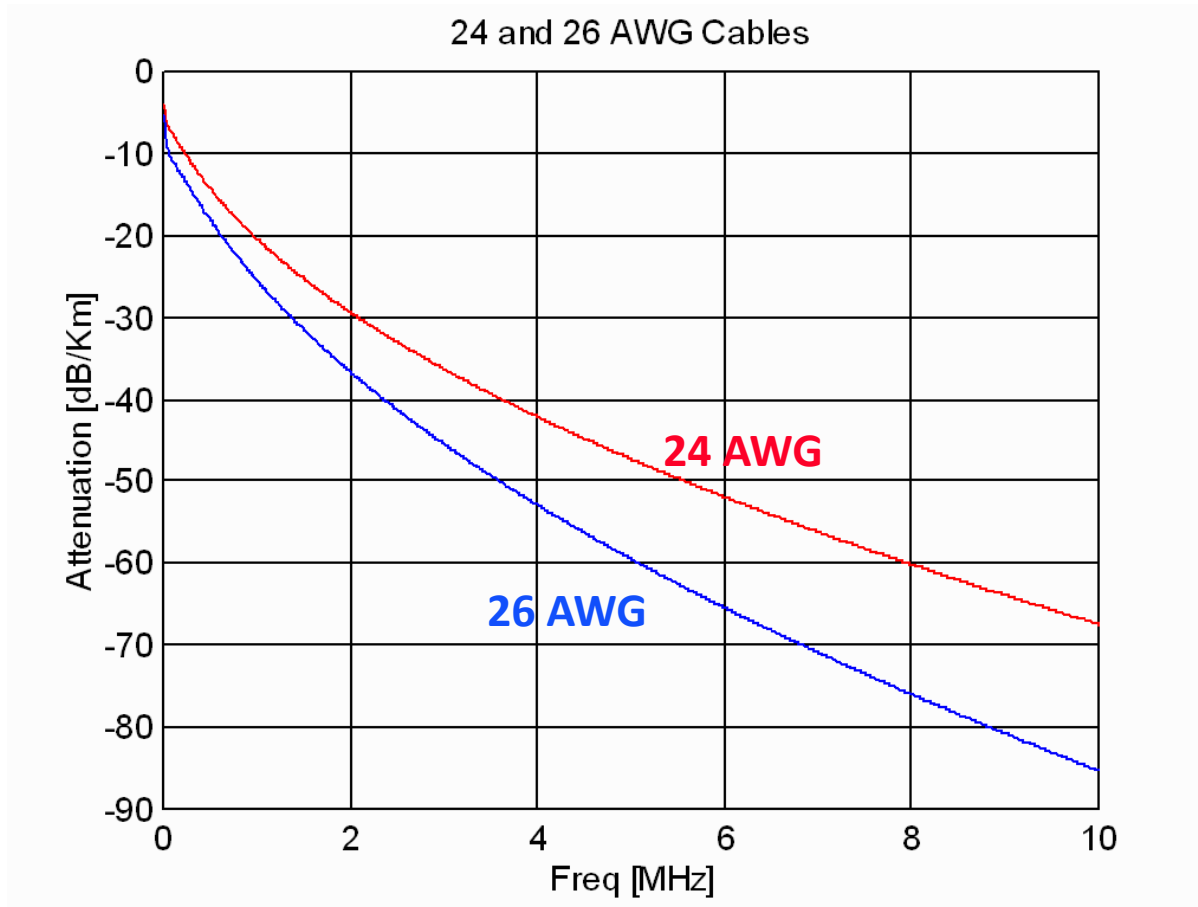
So the decrease is exponential

$$V_a / V_b = e^{-\gamma x} = H(f, x)$$

where x is distance between points a and b

We can calculate γ , and hence the loss, directly from the RCLG model

Attenuation vs. frequency

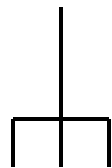
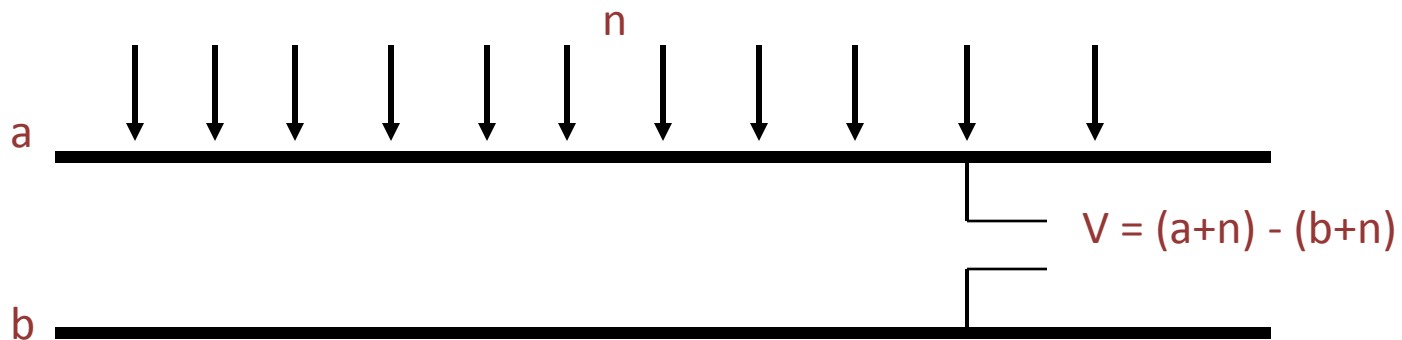


Why twisted?

from Alexander Graham Bell's 1881 patent

To place the direct and return lines close together.

To twist the direct and return lines around one another so that they should be absolutely equidistant from the disturbing wires

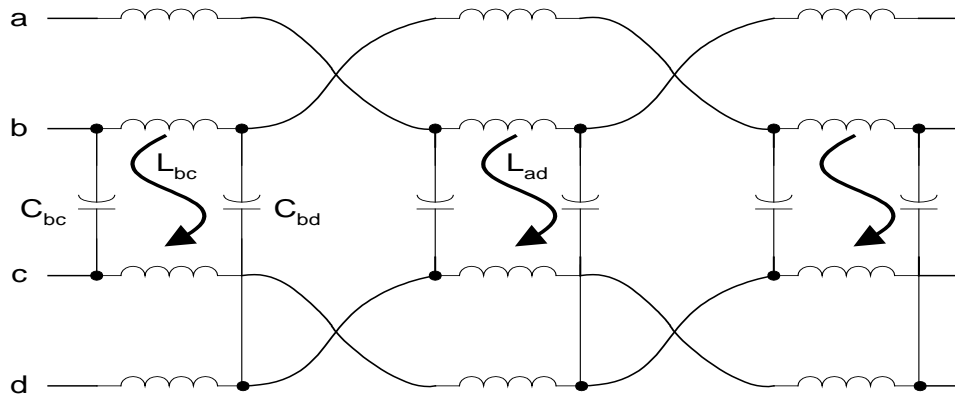


Why twisted? - continued

So don't need shielding, at least for audio (**low**) frequencies

But at higher frequencies UTP has **cross-talk**: when two pairs are gathered, one **interferes on the other**

George Campbell was the first to model (see BSTJ 14(4) Oct 1935)



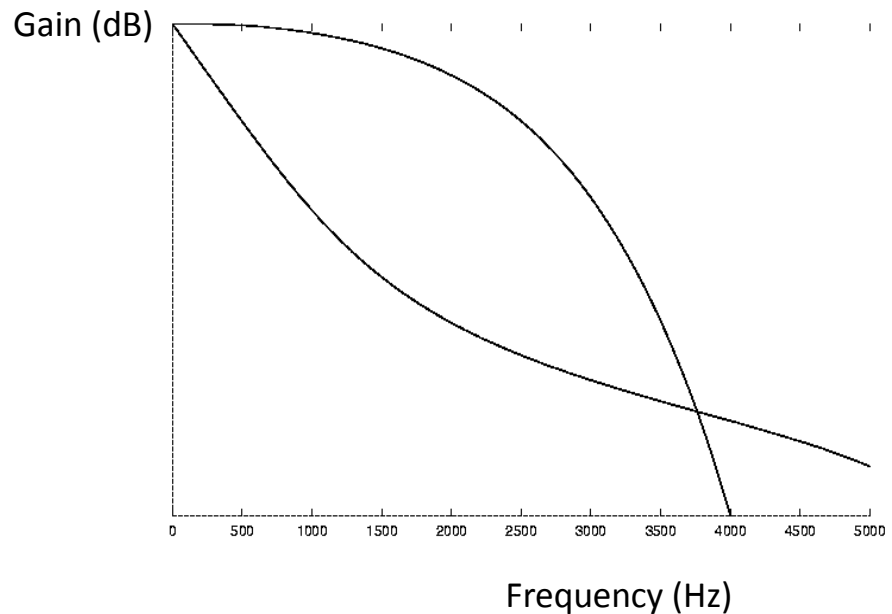
Cross-talk due to capacitive and/or inductive mismatch

$$|I_2| = Q f V_1 \quad \text{where} \quad Q \sim (C_{bc} - C_{bd}) \quad \text{or} \quad Q \sim (L_{bc} - L_{ad})$$

Loading coils

Long loops have loading coils to prevent voice distortion

What does a loading coil do?



Flattens response in voice band

Attenuates strongly above voice frequencies

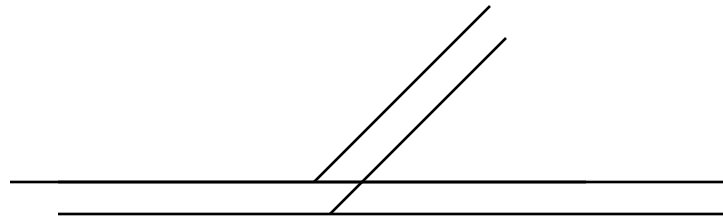
loops longer than 6 Km need loading coils: 88 mH every 2 Km starting 1 Km

Bridge taps

There may also be *bridged taps* (from Party lines before 1940)

Parallel run of unterminated UTP

- unused piece left over from old installation
- placed for subscriber flexibility



High frequency signals are reflected from the open end

A bridged tap can act like a notch filter!

Other problems

Splices

Subscriber lines are seldom single runs of cable

In the US, UTP usually comes in 170m lengths

So splices must be made every 170m

Average line has >20 splices

Splices are pressure connections that add to attenuation

Over time they corrode and may spark, become intermittent, etc.

Gauge changes

US binder groups typically start off at 26 AWG

Change to 24 AWG after 3 Km

In rural areas they may change to 19 AWG after that

Binder groups

UTP are not placed under/over ground individually

In central offices they are in cable *bundles*
with 100s of other UTP

In the outside plant they are in binder groups
with 25 or 50 pairs per group



These pairs interfere with each other
a phenomenon called cross-talk (XTALK)

CSA guidelines

1981 AT&T Carrier Service Area guidelines
advise as follows for new deployments

- No loading coils
- Maximum of 3 Km of 26 gauge (including bridged taps)
- Maximum of 4 Km of 24 gauge (including bridged taps)
- Maximum of 800m bridged taps
- Maximum single bridged tap 600m
- Suggested: no more than 2 gauges

In 1991 more than 60% of US lines met CSA requirements

Present US PSTN

We will see that for DSL - basically four cases

- Loaded line - no DSL possible
- Resistance design unloaded <6 Km $<1300 \Omega$ - ADSL
- CSA reach - HDSL
- DA (distribution area) 1-2 Km - VDSL

Higher rate - lower reach

(because of attenuation and noise!)

xDSL

What problems to overcome?

What goals to reach?

Alternatives for data services

Fiber, coax, Hybrid Fibre-Coax

COST: \$10k-\$20k / mile

TIME: months to install

T1/E1

COST: >\$5k/mile for *conditioning*

TIME: weeks to install

DSL

COST: $\cong 0$ (just equipment price)

TIME: $\cong 0$ (just setup time)

xDSL

Need for higher speed digital connection to subscribers

Not feasible to replace UTP in the last mile

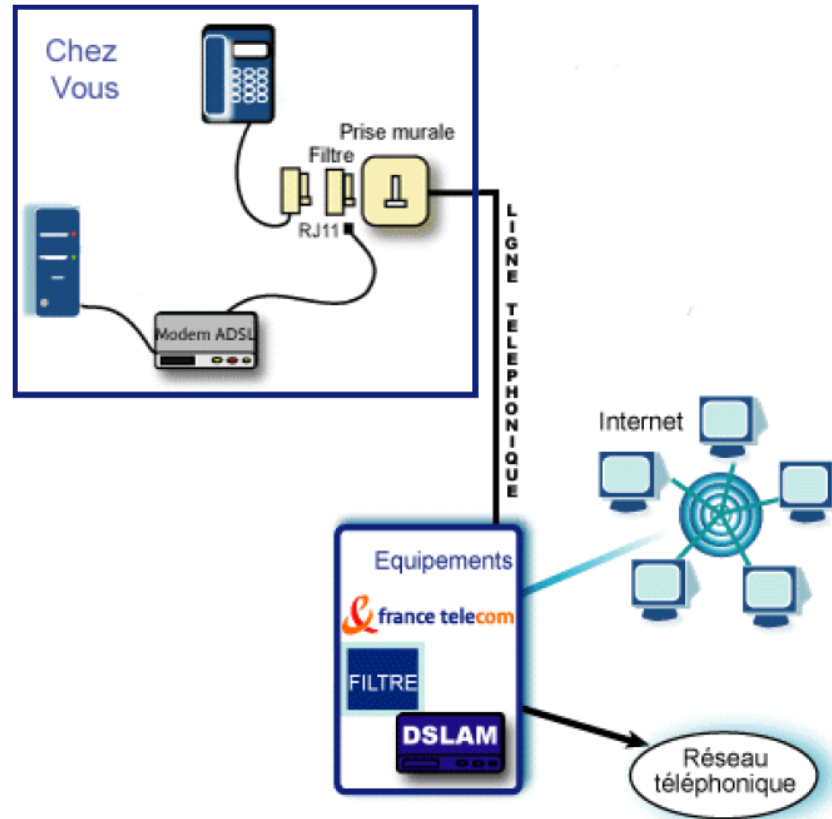
Older voice grade modems assume 4kHz analog line

Newer (V.90) modems assume 64kbps digital line

DSL modems don't assume anything

Use whatever the physics of the UTP allows

xDSL System Reference Model



Why is DSL better than a voice-grade modem?

Analog telephony modems are limited to 4 KHz bandwidth
Shannon's channel capacity theorem gives the maximum transfer rate

$$C = Bw \log_2 (SNR + 1)$$

So by using more BW we can get higher transfer rates if SNR does not decrease

But what is the BW of UTP?

Maximum reach

To use Shannon's capacity theorem we need to know how much noise there is

One type of noise that is always present (above absolute zero temperature) is thermal noise

Maximum reach is the length of cable for reliable communications at a given data rate, ASSUMING ONLY THERMAL NOISE

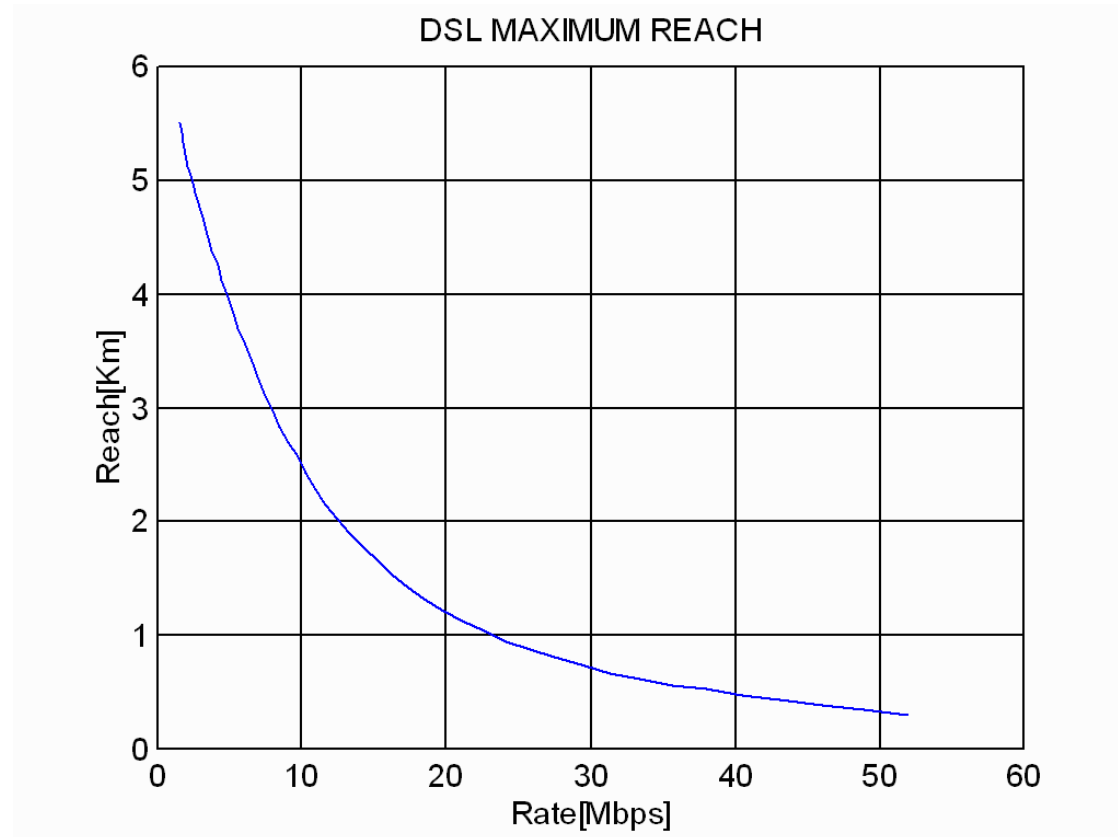
Belcore study in residential areas (NJ) found

- -140 dBm / Hz
- white (i.e. independent of frequency)

is a good approximation

We can compute the maximum reach from known UTP attenuation

xDSL - Maximum Reach



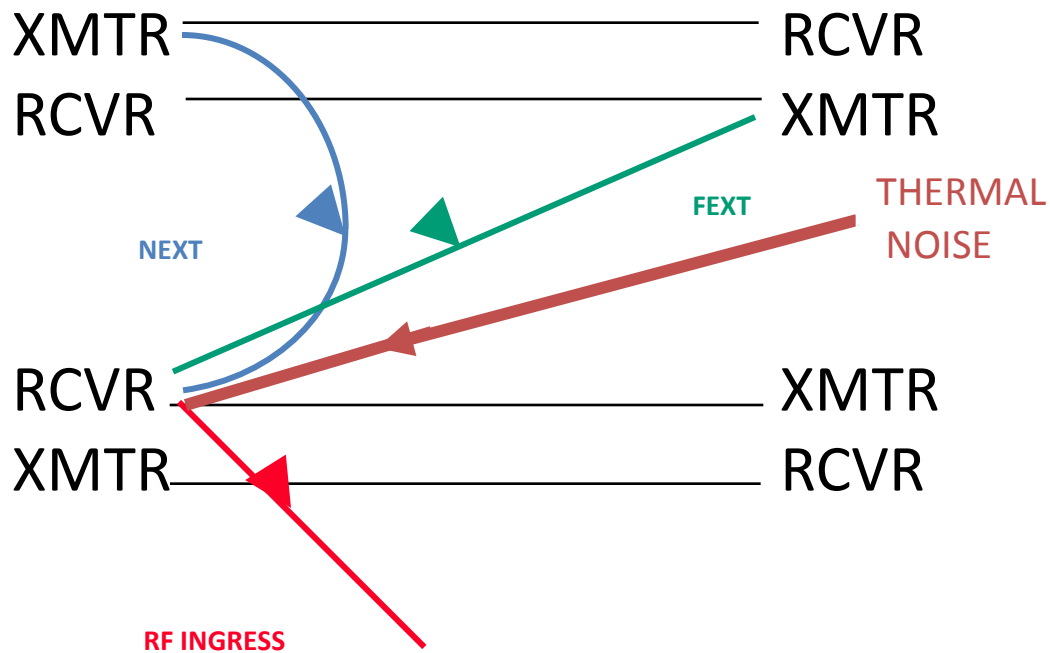
Other sources of noise

But real systems have other sources of noise,
and thus the SNR will be lower
and thus will have lower reach

There are three other commonly encountered types
of noise

- RF ingress
- Near End Cross Talk (NEXT)
- Far End Cross Talk (FEXT)

Sources of Interference



Duplexing

Up to now we assumed that only one side transmits

Bidirectional (full duplex) transmission

requires some form of ***duplexing***

For asymmetric applications we usually speak of

DS downstream and **US** upstream

Four methods are in common use:

- Half duplex mode
- Echo cancellation mode (ECH)
- **Time Domain Duplexing** (requires syncing all binder contents)
- **Frequency Domain Duplexing**



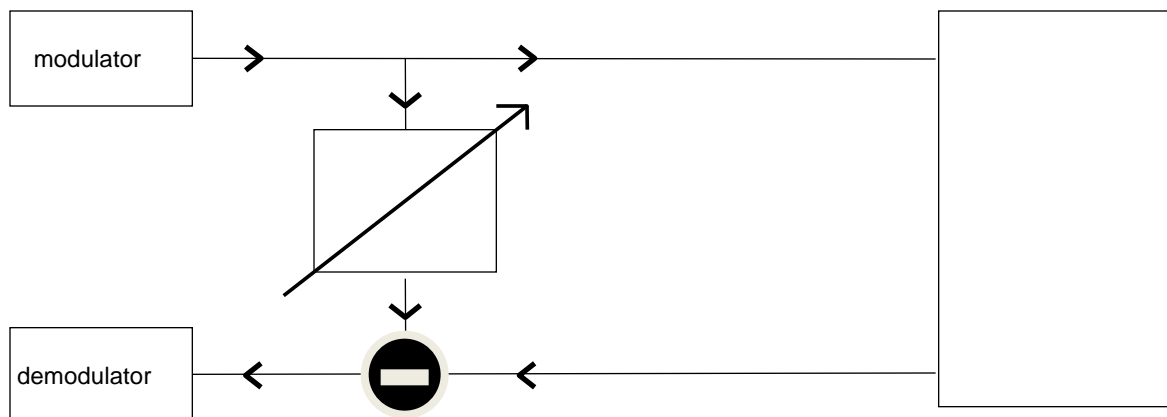
(Adaptive) echo cancellation

Signal transmitted is known to transmitter

It is delayed, attenuated and distorted in the round-trip

Using adaptive DSP algorithms we can

- find the delay/attenuation/distortion
- subtract



Plan

I. Présentation des WAN

II. Les interfaces de la couche physique

III. Protocoles de niveau 2 dans les WAN

IV. MPLS : commutation par VC dans le monde IP

V. Qualité de service

VI. Technologies xDSL

VI.1. Principe : tirer le maximum de la paire de fils de cuivre

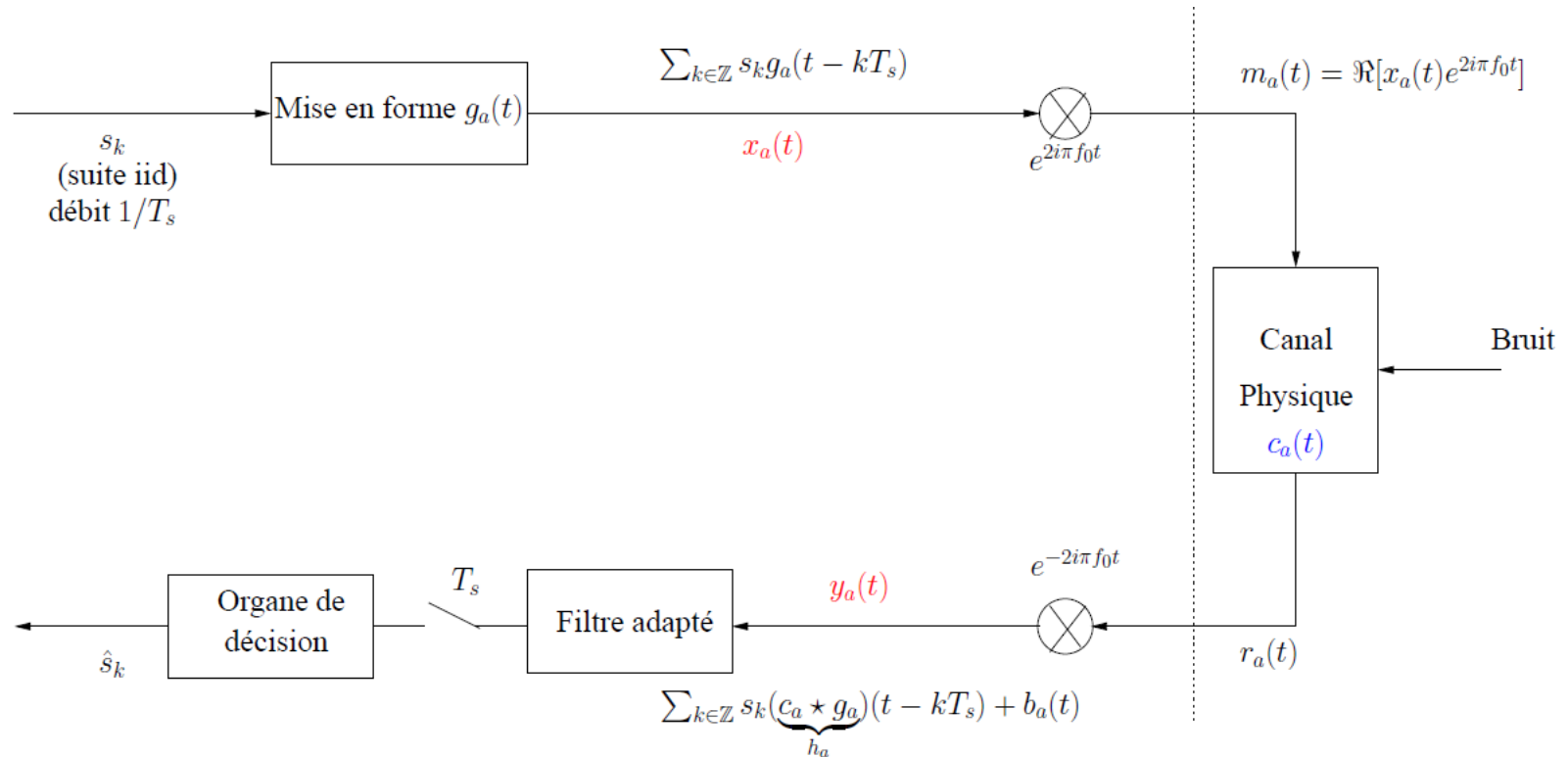
VI.2. Technique de TS pour xDSL : l'OFDM

VI.3. Fonctionnement protocolaire entre le FAI et l'abonné (cas dégroupé et non-dégroupé)

Principe de l'OFDM:
Orthogonal Frequency Division
Multiplexing

Systeme mono-porteuse

- Modulation lineaire



Canal $c_a(t) \neq \delta(t) \Rightarrow \tilde{h}_a(t)$ different de Nyquist.

=> Interference entre symboles (ISI)

Canaux difficiles: Interférence entre symboles

$$y_a(t) = c_a \star x_a(t)$$

- Si $c_a(t) = \lambda\delta(t)$, alors $y_a(t) = \lambda x_a(t) + b_a(t)$
- Si $c_a(t) = \sum_{l=1}^{L_c} \lambda_l \delta(t - \tau_l)$ (cas multi-trajets),
alors $y_a(t) = \sum_{l=1}^{L_c} \lambda_l x_a(t - \tau_l)$ (somme de versions retardées)

→ Interference entre symboles possible !! (IES)

Interférence entre symboles

- L'IES n'arrive pas si

$$\tau_{max} \ll T_s \quad (1)$$

- Or on a (théorème de Shannon): $\frac{1}{T_s} > 2f_{max} \rightarrow T_s < \frac{1}{BW_{signal}}$.

Donc (1) est assuré si:

$$\tau_{max} \ll \frac{1}{BW_{signal}}$$

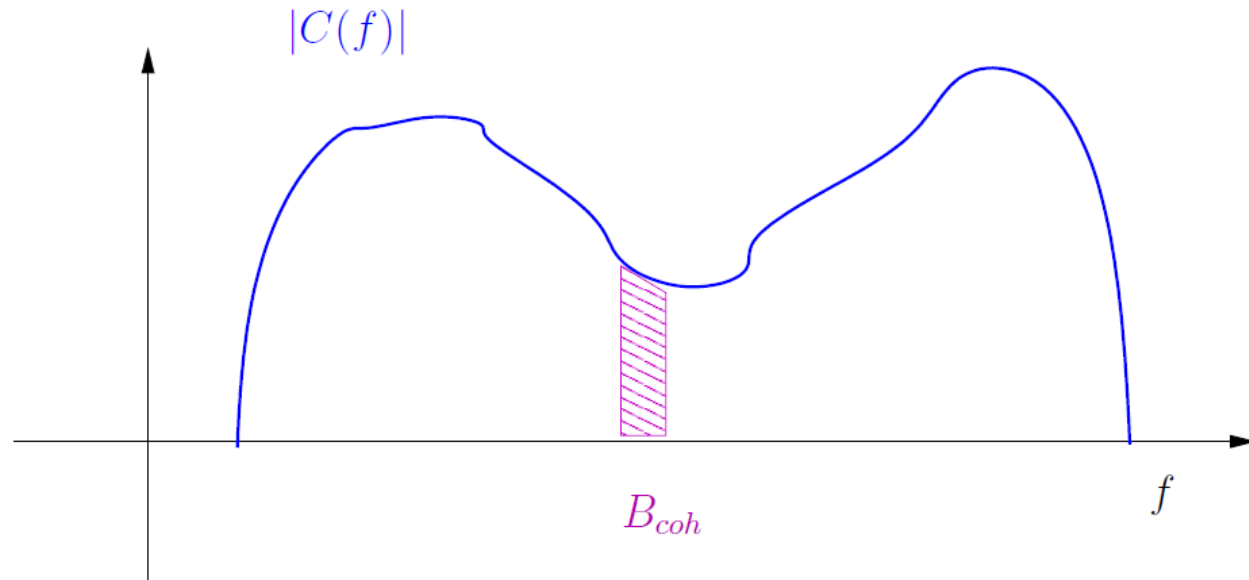
Soit la bande de cohérence du canal $B_{coh} = \frac{1}{\tau_{max}}$

- Alors les IES sont évitées si

$$BW_{signal} \ll B_{coh}$$

Le canal $c_a(t)$ (1/2)

Canal multi-trajets : $c_a(t) = \sum_{l=1}^{L_c} \lambda_l \delta(t - \tau_l)$.

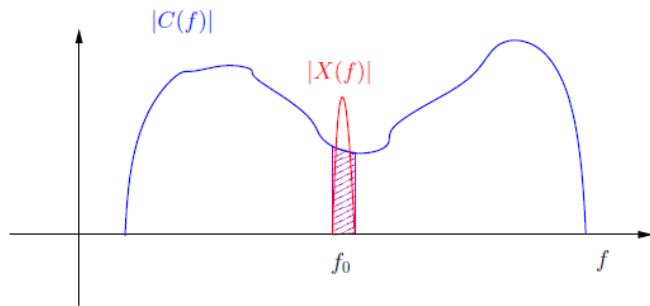


B_c : bande de cohérence du canal.

Le canal $c_a(t)$ (2/2)

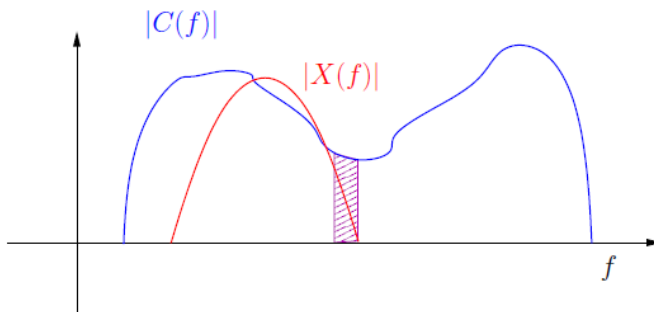
Soit B la bande du signal émis :

- $B < B_c$: seulement atténuation et déphasage



$$Y(f) \approx C(f_0)X(f) \Rightarrow y_a(t) \approx C(f_0)x_a(t)$$

- $B > B_c$: IES dû au canal physique $c_a(t)$.



$$Y(f) = C(f)X(f) \Rightarrow y_a(t) = c_a(t) \star x_a(t)$$

Comment se retrouver dans une configuration $B < B_c$?

Principe du multi-porteuses

Rappel : B requise = Débit-symbole ($1/T_s$)

Idée naïve : Diviser la suite des symboles en N sous-suites de symboles (de période $T = NT_s$) telles que

$$\frac{1}{T} < B_c.$$

Chaque sous-suite n étant émise sur une sous-bande différente associée à une sous-porteuse f_n .

Intérêt : Pour chaque sous-bande, pas d'IES.

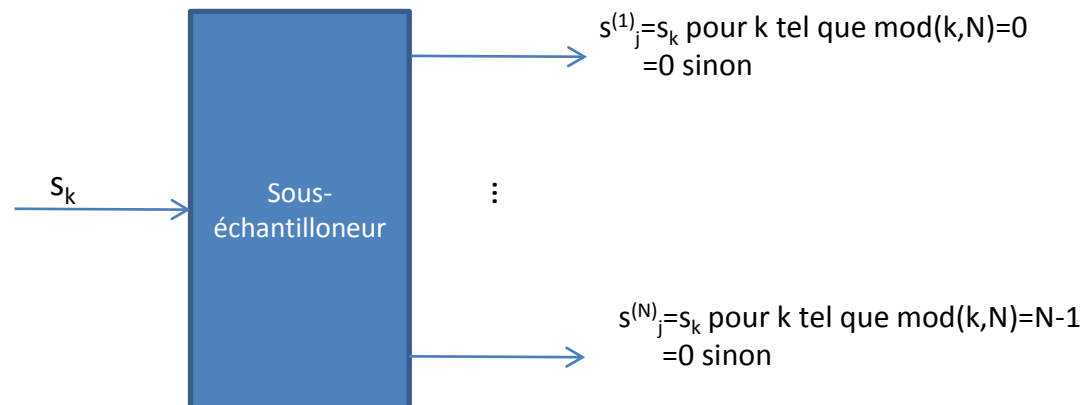
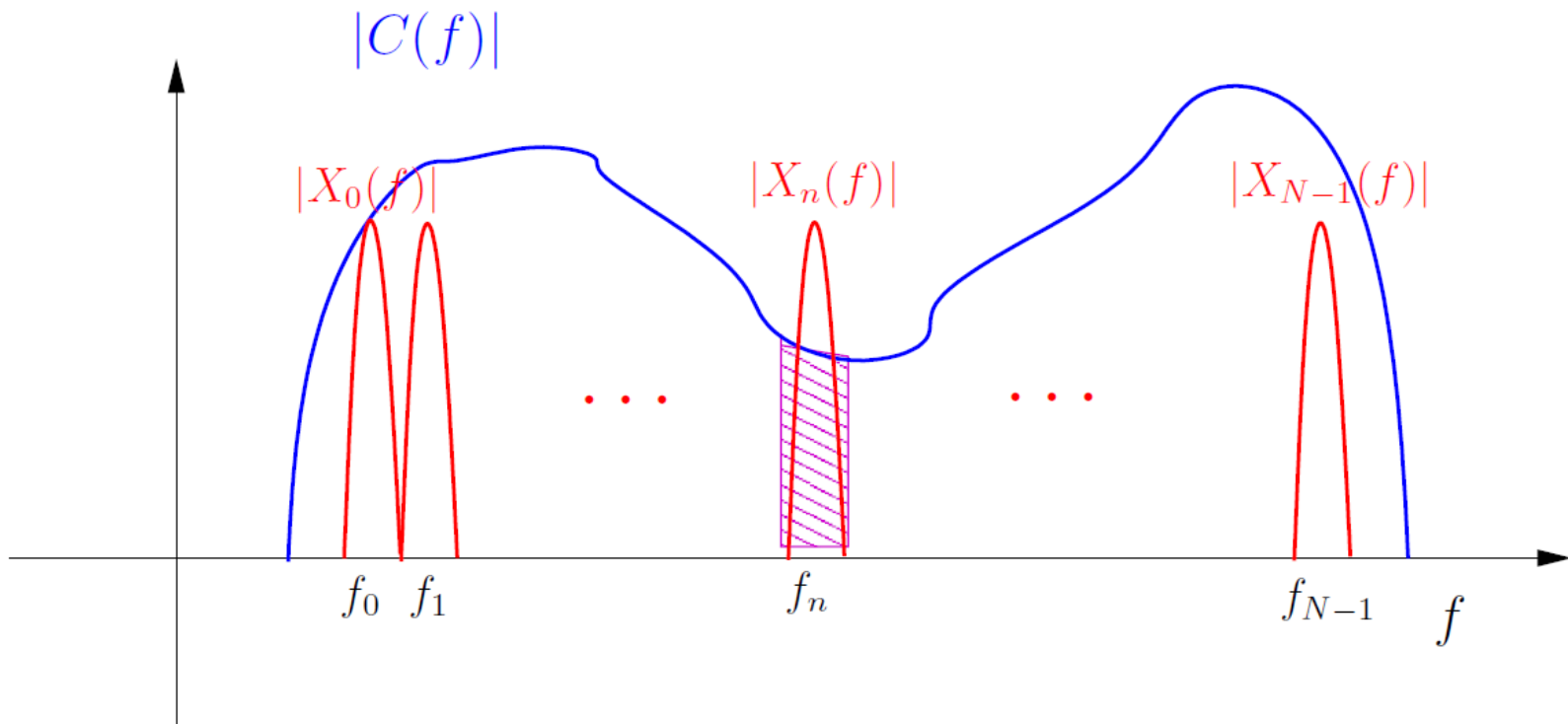
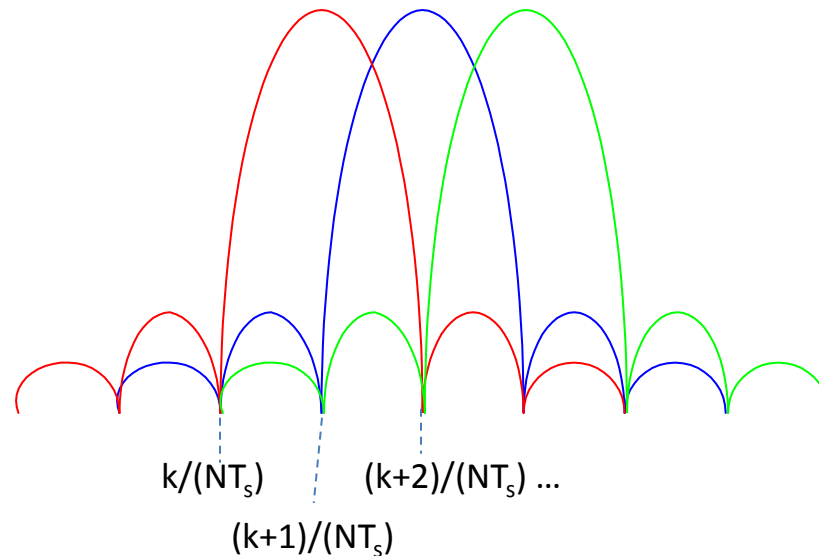


Schéma récapitulatif

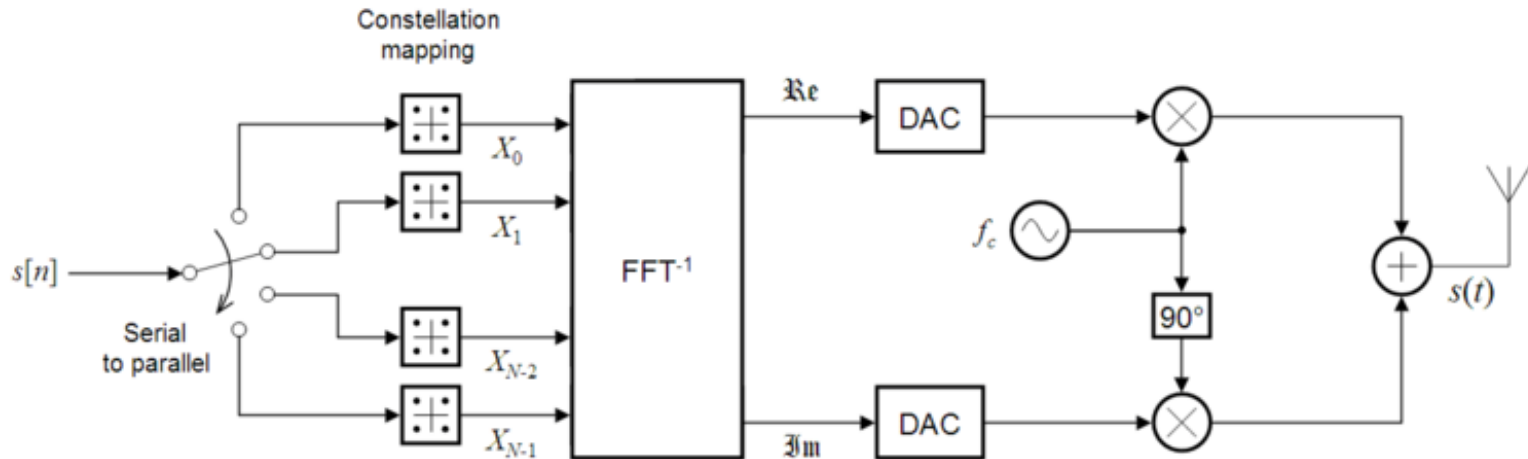


OFDM



- Sinc function has zero at center of nearby modem
- This implies that the signals are orthogonal - no ICI
- No guard frequencies are needed
- Don't need N independent modems
 - efficient digital implementation by **FFT** algorithm

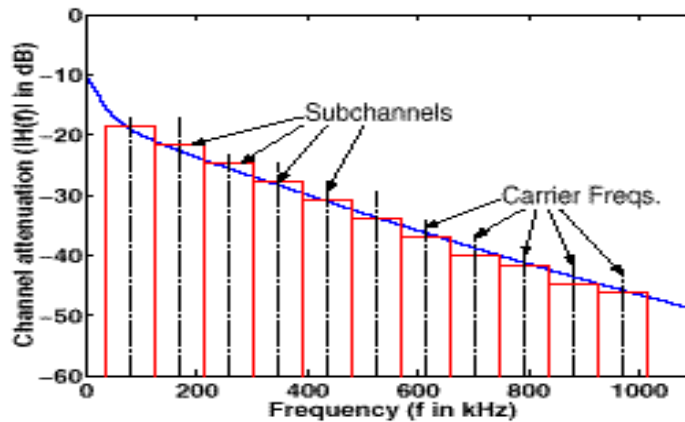
OFDM Transmitter



- Chaque séquence X_i résultant du sous-échantillonnage de $s[n]$ est mise sur une porteuse différente
- Chaque porteuse est espacée de $1/(NT_s)$ si $s[n]$ provient d'un échantillonnage à la période T_s

Discrete Multi-Tone (DMT)

- Measures SNR(f) during initialization
- Water fill QAM signals according to SNR(f)
- Symbol duration $>$ channel impulse response time --- no ISI
- No equalizer required



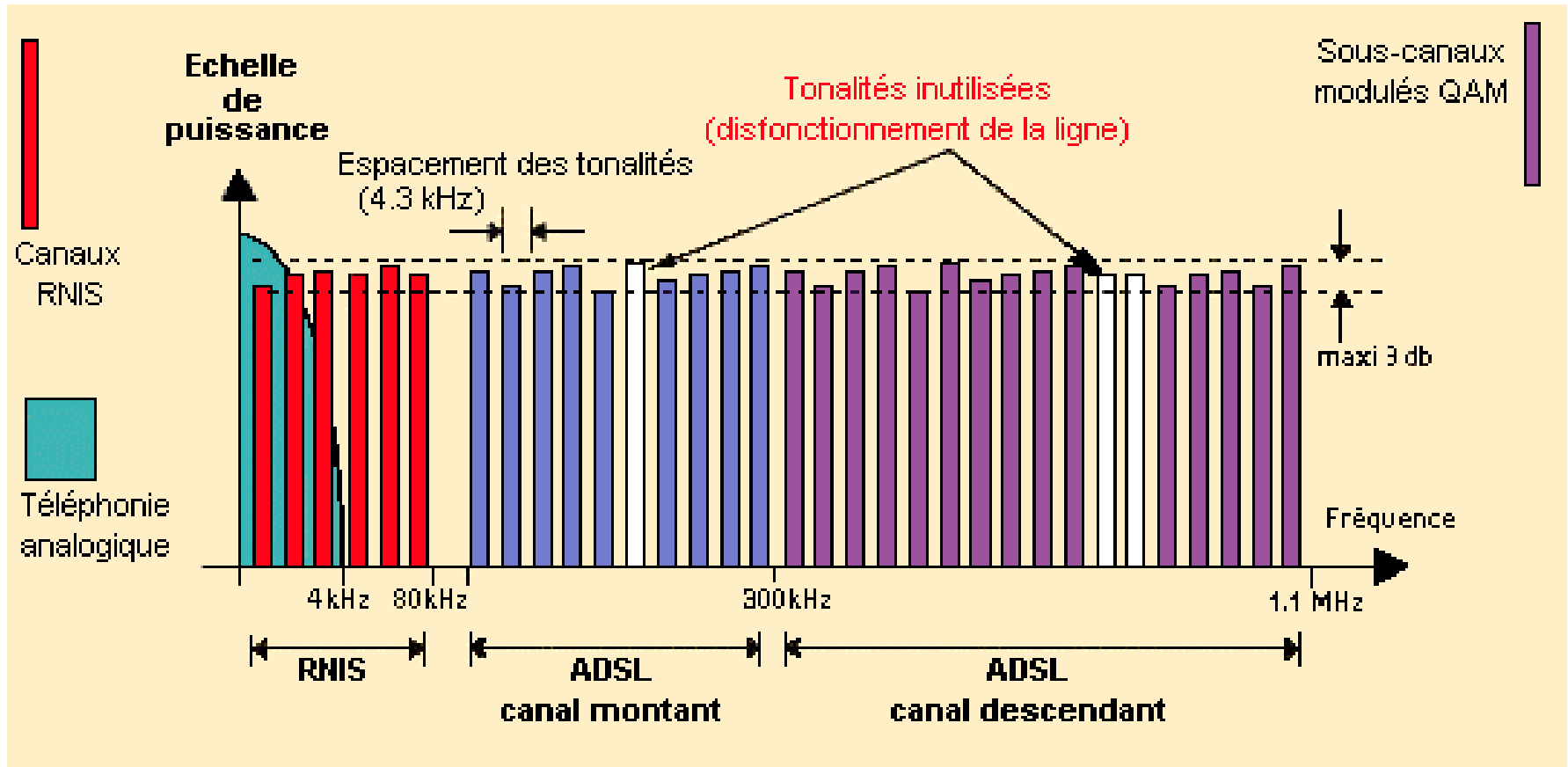
xDSL

Modems et débits

Le modem ADSL

- La technologie ADSL a été normalisée par l'UIT-T sous la recommandation G.992.1.
- Une extension a été apportée dans la recommandation G. 992.3 déterminant l'ADSL2.
- Des extensions permettant l'amélioration de l' ADSL2 sont adoptées pour allonger la distance entre le client et le DSLAM. Ces améliorations ont permis l'adoption de l'ADSL2+ ou LDSL (Long-reach DSL) ou encore READSL (Range Extended ADSL).
- Les modems ADSL offrent une bande montante de 4 à 100 kHz, qui est utilisée pour des débits de 0,64 Mbit/s. La bande descendante utilise une bande comprise entre 100 kHz et 1,1 MHz, qui permet d'atteindre le débit de 8,2 Mbit/s.
- La parole analogique, entre 0 et 4 kHz, passe en même temps que les données utilisant le modem.

Spectre de signal sur ligne téléphonique



Modulation et débits

- La méthode DMT (Discrete MultiTone) :
 - partie US du spectre divisée en 20 sous-bandes de 4,3 kHz
 - chaque sous-bande est capable de transporter de 4 à 15 bits en parallèle
 - On choisit 8 bits par symb (i.e., par intervalle d'horloge)

- 4000 IT/s (4000 Bauds=nb symb/s) -> $4\ 000 \times 8 \text{ bits} = 32 \text{ Kbps}$ par sous-bande
- 20 sous-bandes -> total de $32 \times 20 = 640 \text{ Kbps}$
- 256 sous-bandes pour DS -> total de $4\ 000 \times 8 \text{ bits} \times 256 = 8,2 \text{ Mbps}$
- Débit peut être augmenté en: augmentant le nb de bits par symb et/ou la BW

- Les modems ADSL2+ permettent ainsi de monter jusqu'à 28 Mbps en augmentant fortement la partie du spectre DS (jusqu'à 2,2 MHz).

Les différentes technologies xDSL

	modem	speed	reach	main applications
	ADSL	6 Mbps DS 640 Kbps US	3.5-5.5 km	residential Internet, video-on-demand
	ADSL2	8 Mbps DS 800 Kbps US	> ADSL	Internet access, VoIP
	ADSL2+	16 Mbps DS 800 Kbps US	< 2 km	“
	VDSL	<= 52 Mbps	300m - 1 km	LAN interconnect, HDTV, combined services
	VDSL2	200 Mbps (aggregate)	up to 1.8 km	“
Not DSL	cable modem	10-30Mbps DS shared	50 km	residential Internet
	HPNA	1, 10 Mbps	home wiring	residential networking

Plan

I. Présentation des WAN

II. Les interfaces de la couche physique

III. Protocoles de niveau 2 dans les WAN

IV. MPLS : commutation par VC dans le monde IP

V. Qualité de service

VI. Technologies xDSL

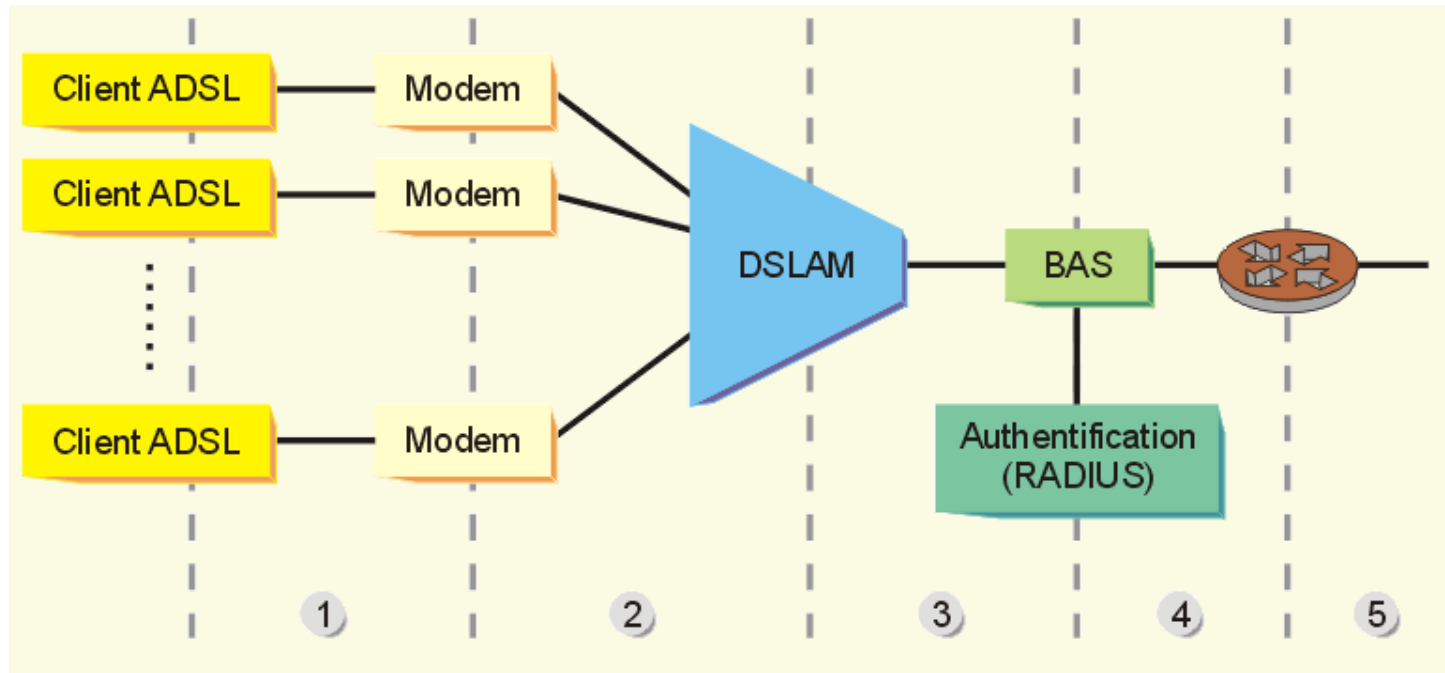
VI.1. Principe : tirer le maximum de la paire de fils de cuivre

VI.2. Technique de TS pour xDSL : l'OFDM

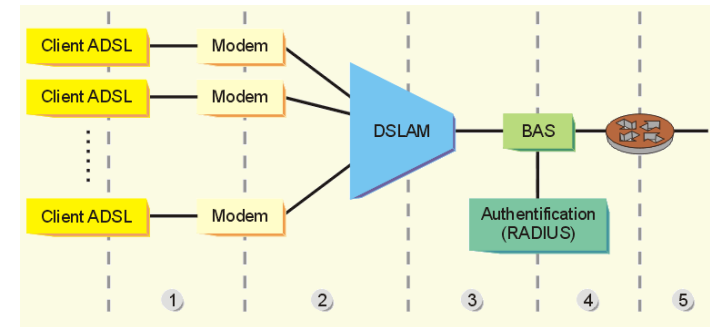
VI.3. Fonctionnement protocolaire entre le FAI et l'abonné (cas dégroupé et non-dégroupé)

Non-dégroupé: Schéma simplifié

Le schéma qui suit, simplifié à l'extrême, n'est pas pour autant faux. Il peut convenir dans le cas du dégroupage

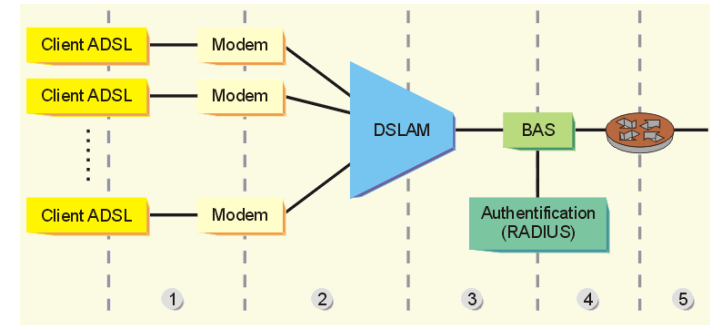


Les composants



- **Client ADSL**
 - La machine que l'abonné connecte à l'internet. Peu important la plate forme matérielle et le système d'exploitation, pourvu que ce dernier supporte le réseau TCP/IP.
- **Modem**
 - Modulateur/Démodulateur. Une boîte dont la fonction est assez similaire à celle du modem RTC, à part qu'ici, elle est conçue pour la technologie DSL.
- **DSLAM**
 - Digital Subscriber Line Access Multiplexer. C'est une sorte d'entonnoir ou de gouttière, qui ramasse les flux numériques de chaque abonné et les fait converger par multiplexage sur un seul lien à fort débit.
- **BAS**
 - Broadband Access Server
 - Lorsque l'on a réussi une connexion avec son FAI, on a établi un lien PPP (Point to Point Protocol) entre son ordinateur et le BAS. Ce lien PPP va transporter les protocoles supérieurs IP, TCP, UDP, ICMP... C'est au niveau du BAS que l'authentification du client va se faire et que les paramètres IP vont être transmis (serveur RADIUS, généralement).
- **Routeur**
 - C'est l'équipement qui va assurer la liaison entre le BAS et le réseau du fournisseur d'accès.
 - Le lien n°4 relie le BAS à ce routeur et les données circulent dans un tunnel de type L2TP (Layer 2 Tunnel Protocol). Il s'agit de construire un VPN (Virtual Private Network : réseau privé virtuel) entre le BAS et le réseau du fournisseur d'accès.

Les liaisons



- 1. Représente le "bout de câble" qui relie votre machine au modem. Ce bout de câble peut être de type :
 - Ethernet, USB, Hertzien (pas de câble, mais une onde électromagnétique), dans le cas d'un modem/routeur WiFi.
- 2. Représente votre ligne téléphonique, c'est une paire de fils de cuivre qui va de votre prise murale jusqu'au concentrateur de l'opérateur de téléphonie. Cette ligne va véhiculer la téléphonie traditionnelle (POTS) et les porteuses ADSL. La séparation des services se fait au moyen d'un filtre séparateur (Splitter) qui peut être extérieur, mais aussi intégré au modem.
- 3. Représente le lien à fort débit (généralement de la fibre optique) qui véhicule les données numériques de l'ensemble des abonnés connectés au même DSLAM.
- 4. Est encore un lien à fort débit, qui relie le BAS au réseau de votre FAI.
- 5. Nous sommes maintenant sur le réseau du fournisseur d'accès.

Les protocoles du réseau

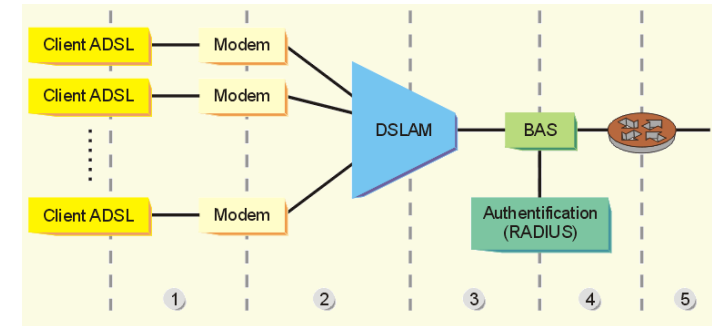
- **ATM**

- Les opérateurs de télécom aiment ATM (Asynchronous Transfert Mode). Pourquoi ? Parce que ATM est très bien adapté au transport de paquets commutés, avec des circuits (virtuels) point à point, avec une gestion de QoS (Quality of Service) fine, autant de services utiles pour passer sur le même réseau de la téléphonie, de la vidéo et des données informatiques.

- **Ethernet**

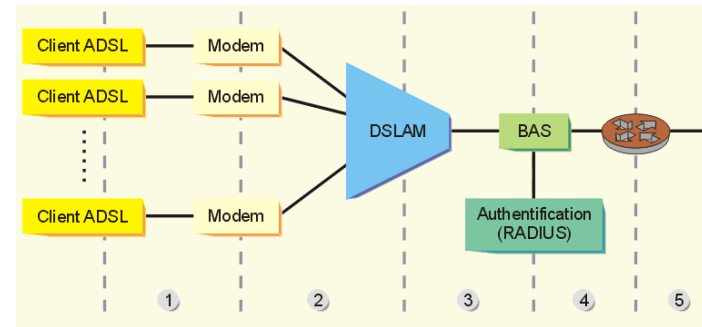
- Comparativement, les réseaux informatiques aiment Ethernet, qui n'a absolument rien à voir avec ATM, si ce n'est que, dans le modèle OSI à 7 couches, les deux protocoles pourraient à la rigueur être situés au même niveau (2). C'est en grande partie faux, ATM peut remplacer non seulement Ethernet mais aussi IP.
- Mais pour ce qui nous intéresse ici, ATM transportera de l'IP ou du PPP et donc jouera un rôle similaire à Ethernet.

Les protocoles



- Le tronçon 3 de l'illustration a comme support ATM.
- Le tronçon 4 est spécifié comme du "réseau IP", mais par quoi est transportée la couche IP ? Seul l'opérateur du réseau pourra le dire. IP peut en effet être transporté par ATM, par Ethernet, par Ethernet sur ATM...
- Ce qui peut paraître surprenant, c'est que le tronçon 2 (entre votre prise téléphonique et le DSLAM) utilise également ATM. Autrement dit, votre modem ADSL est un terminal ATM.
- Entre votre ordinateur et votre modem, ça pourra être :
 - de l'Ethernet si :
 - votre modem dispose d'une prise Ethernet et votre machine d'une interface réseau également Ethernet,
 - votre modem est un modem USB, qui n'est qu'une liaison série, sur laquelle on va simuler un lien Ethernet, grâce au driver à installer avec le modem,
 - de l'ATM si :
 - votre modem dispose d'une prise ATM et votre machine d'une interface réseau également ATM (cas fort peu probable, vu le prix),
 - votre modem est un modem USB, qui n'est qu'une liaison série, sur laquelle on va simuler un lien ATM, grâce au driver à installer avec le modem.

Non-dégroupé: Les protocoles



- **Et par dessus tout ça...**

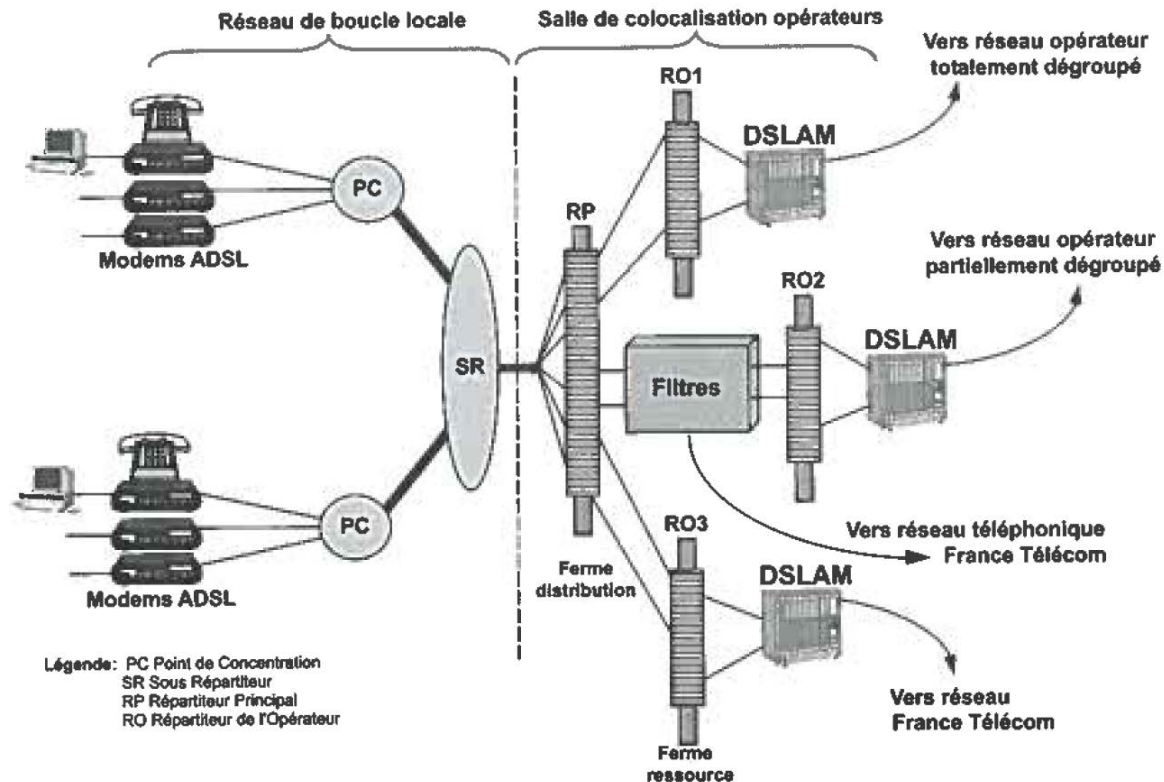
- On va construire un lien PPP, qui doit aller de votre ordinateur jusqu'au BAS, et qui sera porté :
 - par Ethernet (PPPoE : PPP over Ethernet) entre votre machine et le modem, si la liaison en dessous est de type Ethernet,
 - par ATM (PPPoA : PPP over ATM) entre votre machine et le modem, si la liaison en dessous est de type ATM.
- Entre le modem et le BAS, souvent du PPPoA.
- Ce lien PPP transportera IP entre votre ordinateur et le BAS. Comme c'est du PPP, il y a une IP à chaque bout :
 - la vôtre, généralement dynamique, qui vous est attribuée lors de l'établissement de la session PPP par le serveur d'authentification

Dans la pratique: dégroupage et non-dégroupage

- Dans la pratique, ça va être un peu plus compliqué, du moins dans le cas du non-dégroupage
- Qu'est-ce que le dégroupage ?
 - La boucle locale appartient à France Télécom. Les centres de raccordement (NRA) aussi.
 - Ces centres de raccordement sont souvent situés dans des locaux exigus, où il est difficile de laisser de la place à des opérateurs alternatifs. Pourtant, le dégroupage doit en passer par là.
 - Pour dégroupier une ligne, il faut qu'un ou plusieurs opérateurs alternatifs puissent installer leurs propres équipements dans le centre, et y connecter directement les lignes de leurs abonnés. France Télécom se contente de louer la ligne entre le centre et le client.
 - Lorsque ceci n'est pas fait, peu importe la raison, il faut trouver une autre solution pour que des opérateurs alternatifs puissent tout de même proposer des abonnements ADSL.
- **Les offres France Télécom**
 - **L'option 1**
 - Non-dégroupé: France Télécom assure la totalité du transport entre l'abonné et le réseau du FAI.
 - **L'option 2**
 - Dégroupage: FT se contente de louer l'accès à la boucle locale aux FAIs. Les fournisseurs sont donc maîtres de la qualité de leur prestation. Ils ne sont dépendants que de la qualité physique de la boucle locale.

Dégroupage

- Le **répartiteur téléphonique** est le lieu situé dans le CO (ou NRA) où se font toutes les connexions entre la LL et les infrastructures
- Aucun dégroupage: FAI absent du NRA
- Dégroupage partiel: FAI présent au NRA, mais abonnement FT encore possible
- Dégroupage total: FAI présent au NRA, abonnement FT impossible (téléphonie assurée sur spectre ADSL)

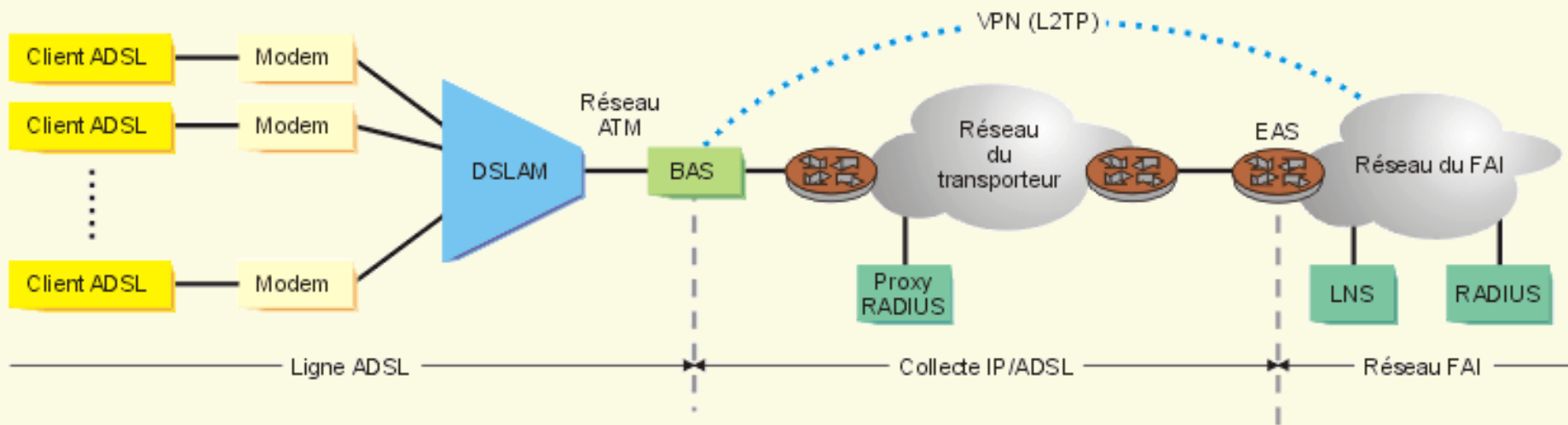


En dégroupé

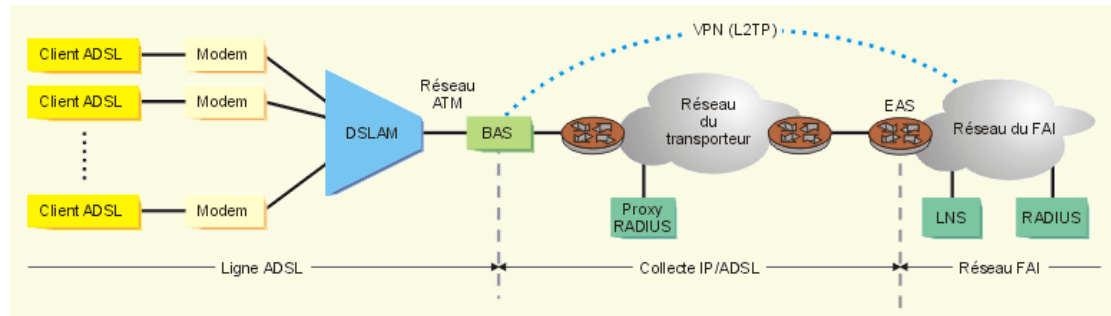
- DSLAM du FAI présent au CO
- IP over ATM entre le modem et le FAI
- Adresse IP souvent fixe --> plus de PPP

Le "vrai" schéma en non-dégroupé

- Nous allons donc détailler le cas de l'option 1.
- L'option 2 se rapproche beaucoup du schéma simplifié, vu plus haut.
- Dans le cas de la collecte IP/ADSL (option 1), c'est à dire le cas où FT prend totalement en charge l'acheminement des données depuis l'abonné jusqu'au FAI, tout ce qui est situé entre le modem de l'abonné et l'EAS (routeur assurant l'interconnexion avec le réseau du FAI) est géré par France Télécom.

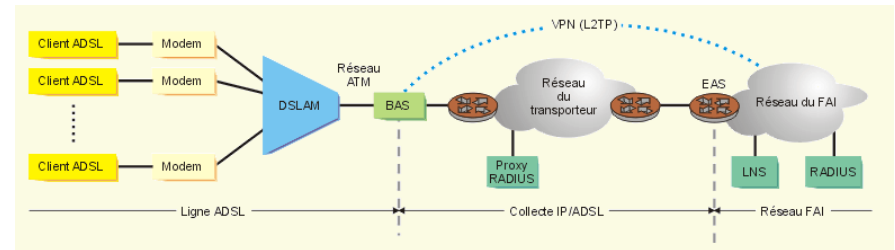


Non-dégroupé: principe



- Permettre la mise en place d'un lien PPP entre l'utilisateur (abonné ADSL) et le serveur d'accès de son FAI à travers le réseau France Télécom.
- Ce lien PPP va être supporté par le réseau ATM entre le modem de l'utilisateur et le BAS, puis par un tunnel L2TP (VPN) entre le BAS et le serveur du FAI.
- Cette méthode va permettre à plusieurs FAI de proposer leurs services aux abonnés à une ligne fixe FT.
- En effet, il est possible de créer dans le réseau IP de FT autant de VPN qu'il sera nécessaire pour connecter les utilisateurs à leur FAI respectif.
- La collecte ADSL a pour but de fournir la structure matérielle nécessaire à l'établissement du tunnel L2TP entre le BAS et les équipements du FAI concerné.

Non-dégroupé: quoi de plus



- Toute la partie "Collecte IP/ADSL". Cette partie a pour objet de créer un tunnel VPN entre le BAS et le réseau du FAI et de faire passer dans ce tunnel le lien PPP qui relie le client à son fournisseur. Pratiquement, ça permet d'utiliser le réseau IP France Télécom pour relier le BAS aux installations du FAI, qui peuvent être distantes, comme si elles étaient directement raccordées au BAS.
- Autrement dit :
 - Le client est authentifié via le proxy RADIUS fourni par FT. Un proxy, encore appelé "serveur mandataire" va servir d'intermédiaire entre le client ADSL, quel que soit son fournisseur, et le serveur RADIUS de son fournisseur,
 - le tunnel VPN est construit sur L2TP (Layer 2 Tunneling Protocol) entre le BAS et le LNS (L2TP Network Server) du fournisseur,
 - ce tunnel va permettre le passage du lien PPP entre le client ADSL et le réseau du FAI, comme si ce lien était établi directement entre le BAS et le réseau du fournisseur, comme on l'a vu dans l'approche simplifiée.
- L'EAS est un routeur fourni par France Télécom, qui permet d'interconnecter le réseau IP FT à celui du fournisseur.
- --> C'est plus compliqué, mais ça ne change strictement rien au fonctionnement de la connexion, à partir de la couche IP.

Pour finir: Etablir PPP côté abonné

- Nous savons maintenant que le lien PPP va voyager "over ATM" entre le modem et le DSLAM. Reste à savoir comment le faire voyager entre votre ordinateur (ou routeur domestique) et votre modem.
- **Vous avez un modem Ethernet**
 - Pas le choix, ayant un lien Ethernet entre la machine et le modem, il faudra utiliser PPPoE.
- **Vous avez un modem USB**

USB est une liaison série. Vous avez ici le choix de la couche de transport de PPP :

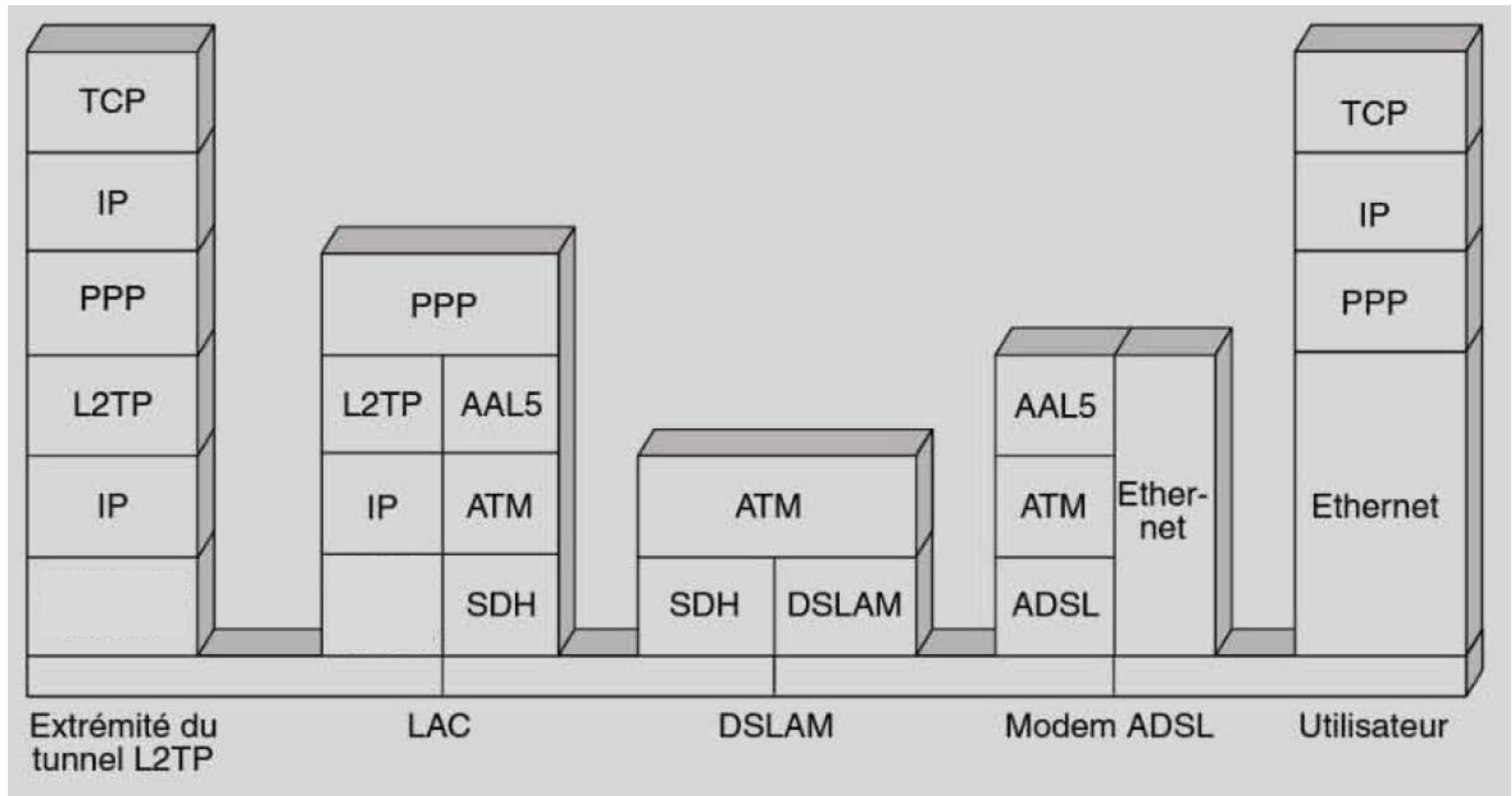
 - créer une couche Ethernet sur la liaison série et utiliser PPPoE,
 - créer une couche ATM sur la liaison série et utiliser PPPoA.
Ceci est possible par l'installation sur l'ordinateur du driver approprié (suivant la disponibilité pour un type de modem donné).
- Q: Puisqu'on est sur une liaison série (USB), pourquoi ne pas faire passer PPP directement dessus, puisque c'est possible, et éliminer une couche inutile ? Elle n'est pas inutile. PPP directement sur une liaison série ne sait pas attribuer d'adresse MAC, adresse utilisable au niveau 2 du modèle OSI, et l'ajout de la couche Ethernet ou ATM contourne cette limite de PPP.
- **Vous avez un modem/routeur intégré**

Vous aurez le choix que vous aura donné le constructeur (généralement PPPoE).

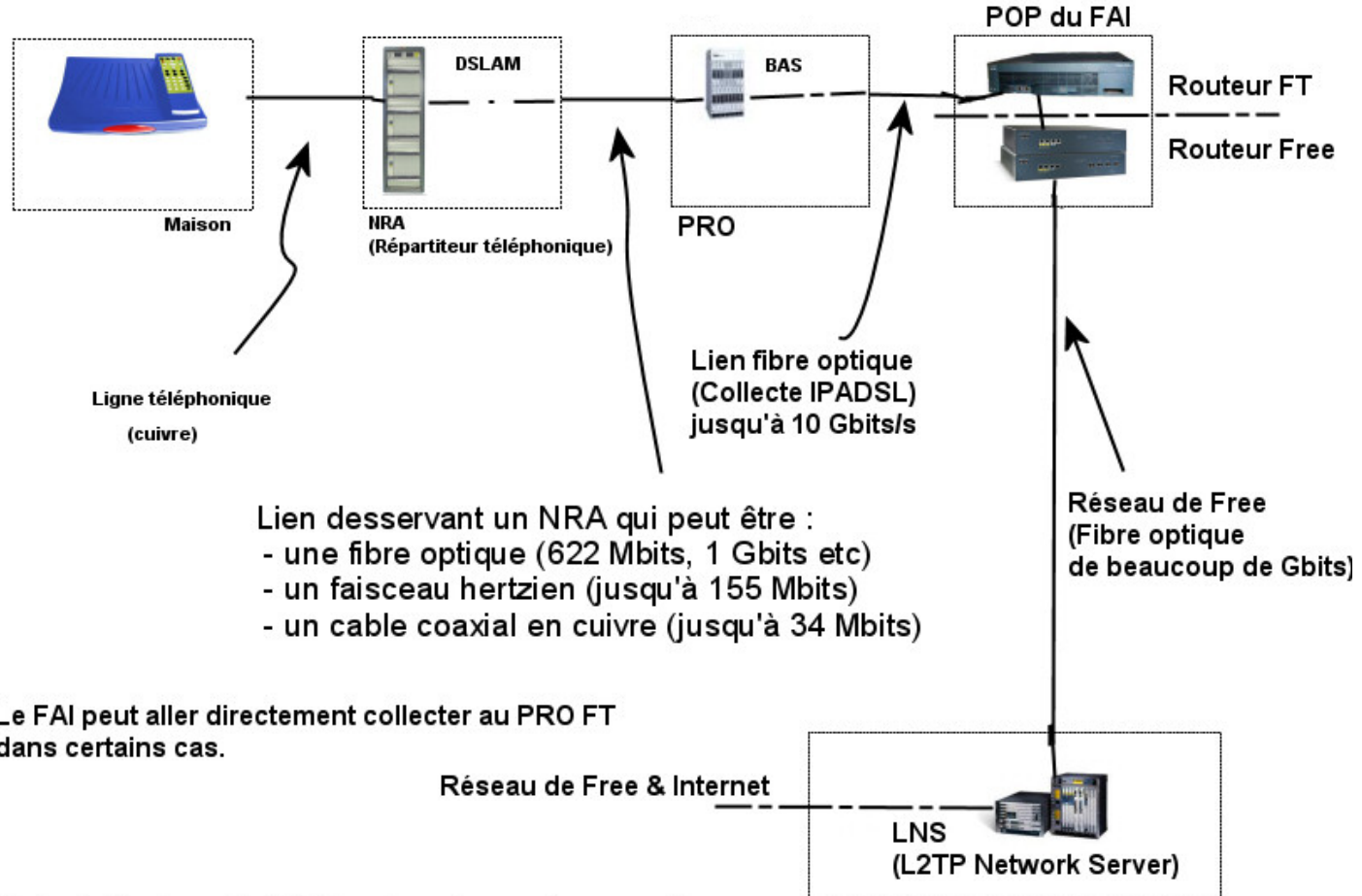
Etablissement d'un tunnel L2TP

- Manque de confidentialité de L2TP -> souvent implémenté avec Ipsec on parle alors de L2TP/Ipsec (standardisé dans IETF RFC 3193)
- On peut alors établir un VPN basé sur L2TP/Ipsec
- Confusion possible dans L2TP/IPsec entre les termes "tunnel" and "secure channel."
 - *Tunnel*: canal permettant de transporter des paquets d'un réseau sur un autre réseau sans les modifier ni nécessiter de connaître leur contenu (pas de lecture, pas d'écriture)
Dans le cas de L2TP/IP, les paquets L2TP/PPP sont transportés sur IP
 - *Secure channel*: connexion dans laquelle la confidentialité de toutes les données est garantie.
Dans le cas de L2TP/IPsec, IPsec fournit un secure channel, puis L2TP fournit un tunnel.

Architecture protocolaire d'une communication ADSL



Free ADSL: schéma en zone non-dégroupée



Lien desservant un NRA qui peut être :

- une fibre optique (622 Mbits, 1 Gbits etc)
- un faisceau hertzien (jusqu'à 155 Mbits)
- un câble coaxial en cuivre (jusqu'à 34 Mbits)

Le FAI peut aller directement collecter au PRO FT dans certains cas.

Entre la Freebox et le BAS les données sont encapsulées en ATM puis entre le BAS et le LNS elles sont encapsulées dans des tunnels L2TP. C'est pourquoi les différents équipements traversés ne sont pas visibles avec un traceroute.

Vocabulaire

- **ATM** : Asynchronous Transfert Mode
- **AAL5** : ATM Abstraction Layer 5
- **EAS** : Equipement d'Acces aux Services
- **L2TP** : Layer two Tunneling Protocol
- **LAC** : L2TP Access Concentrator
- **LNS** : L2TP Network Server
- **PAS** : Plateforme d'Acces aux Services (Proxy RADIUS)
- **PPP** : Point to Point Protocol
- **PPPoA** : PPP over ATM
- **PPPoE** : PPP over Ethernet
- **POTS** : Plain Old Telephone Service
- **RADIUS** : Remote Authentication Dial In User Service

xDSL types and history

DSL Flavors

DSL is often called **xDSL**

since there are many varieties (different **x**)

e.g. ADSL, HDSL, SHDSL, VDSL, IDSL, etc.

There were once many unconnected types

but now we divide them into three main families

The differentiation is by means of the application scenario

- HDSL (symmetric, mainly business, data + telephony)
- ADSL (asymmetric, mainly residential, Internet access)
- VDSL (very high rate, but short distance)

More xDSL flavors

modem	speed	reach	main applications
IDSL	160 (144) Kbps	5.5 km	POTS replacement, videoconferencing, Internet access
HDSL	2 Mbps (4-6W)	3.6-4.5 km	T1/E1 replacement, PBX interconnect, FR
HDSL2	2 Mbps (2W)	3 km	same as HDSL
SHDSL	2.3 Mbps	3 km	same as HDSL
SHDSLbis	4.6 Mbps	3 km	same as HDSL

More xDSL flavors (cont.)

modem	speed	reach	main applications	
ADSL	6 Mbps DS 640 Kbps US	3.5-5.5 km	residential Internet, video-on-demand	
ADSL2	8 Mbps DS 800 Kbps US	> ADSL	Internet access, VoIP	
ADSL2+	16 Mbps DS 800 Kbps US	< 2 km	“	
VDSL	<= 52 Mbps	300m - 1 km	LAN interconnect, HDTV, combined services	
VDSL2	200 Mbps (aggregate)	up to 1.8 km	“	
Not DSL	cable modem	10-30Mbps DS shared	50 km	residential Internet
	HPNA	1, 10 Mbps	home wiring	residential networking

T1 line conditioning

In order for a subscriber's line to carry T1

- Single gauge
- CSA range
- No loading coils
- No bridged taps
- Repeaters every 6 Kft (starting 3 Kft)
- One T1 per binder group
- Labor intensive (expensive) process
- Need something better ... (DSL)

HDSL

1991: HDSL

- Replaced T1/E1 service, but
 - full CSA distance w/o line conditioning / repeaters
- AMI line code replaced with IDSL's 2B1Q line code
- Use 2 UTP pairs, but in ECH mode (DFE)
 - For T1 784 kbps on each pair
 - For E1, 1, 2, 3 and 4 pair modes (all ECH)
- Requires DSP for echo cancellation
- Mature DSL technology, now becoming obsolete

HDSL2

With the success of HDSL,
customers requested HDSL service that would :

- require only a single UTP HDSL
- attain at least full CSA reach
- be spectrally compatible w/ HDSL, T1, ADSL, etc.

The result, based on high order PAM, was called

- **HDSL2 (ANSI)**
- **SDSL Symmetric DSL (ETSI)**

and is now called

- **SHDSL Single pair HDSL (ITU)**

SHDSL

Uses Trellis Coded 16-PAM with various shaping options

Does not co-exist with POTS service on UTP

Can use regenerators for extended reach

single-pair operation

- 192 kbps to 2.312 Mbps in steps of 8 kbps
- 2.3 Mbps should be achieved for reaches up to 3.5 km

dual-pair operation (4-wire mode)

- 384 kbps to 4.608 Mbps in steps of 16 kbps
- line rate is the same on both pairs

Latest standard (G.shdsl.bis - G.991.2 2003 version)

- bonding up to 4 pairs
- rates up to 5696 kbps
- optional 32-PAM (instead of 16-PAM)
- dynamic rate repartitioning

ADSL

Asymmetric - high rate DS, lower rate US

Originally designed for video on demand

New modulation type - **Discrete MultiTone**

FDD and ECH modes

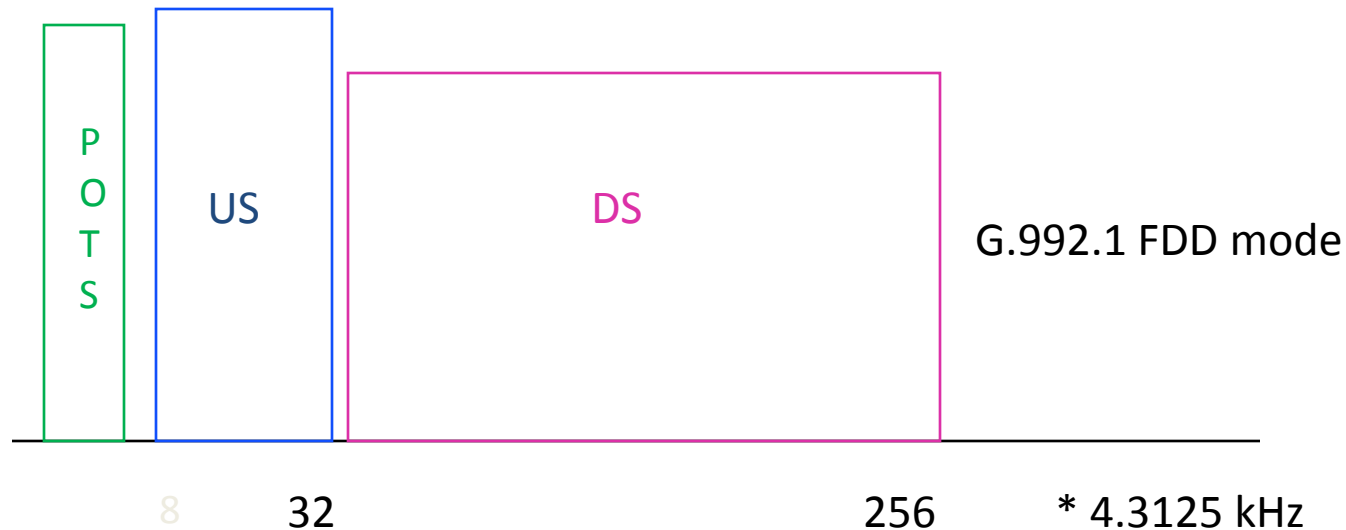
Almost retired due to lack of interest

...but then came the Internet

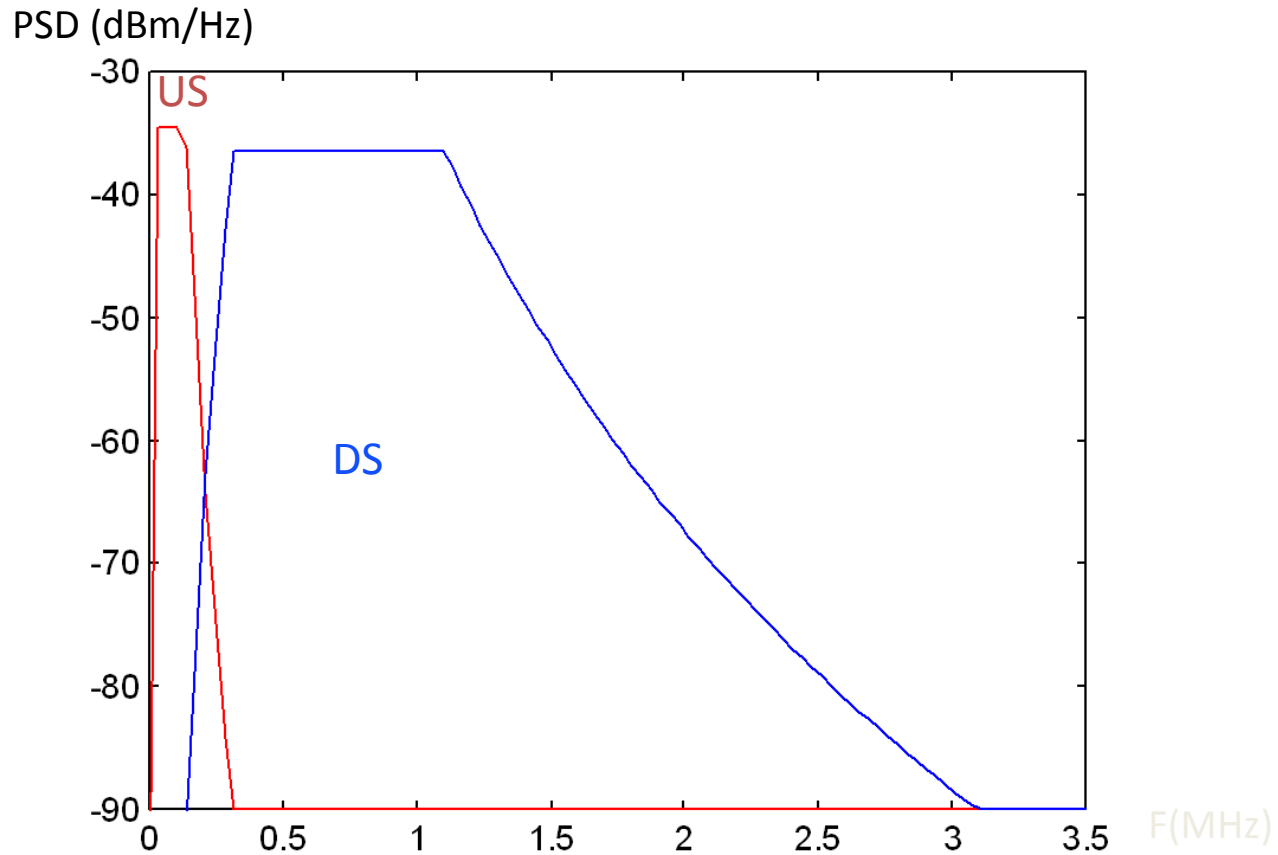
Studies - DS:US for both applications can be about 10:1

ADSL Duplexing

- US uses low DMT tones (e.g. 8 - 32)
- If over POTS / ISDN lowest frequencies reserved
- DS uses higher tones
 - If FDD no overlap
 - If ECH DS overlaps US



Why asymmetry?



ADSL standard

ITU (G.dmt) G.992.1, ANSI T1.413i2 standard

DS - 6.144 Mbps (minimum)

US- 640 kbps

First ADSL data implementations were CAP (QAM)

ITU/ANSI/ETSI standards are DMT with spacing of 4.3125 kHz

- DMT allows approaching water pouring capacity
- DMT is robust
- DMT requires more complex processing
- DMT may require more power

ADSL2

ADSL uses BW from 20 kHz to 1.1 MHz

ADSL2 Increases rate/reach of ADSL by using 20 kHz - 4.4 MHz

Also numerous efficiency improvements

- better modulation
- reduced framing overhead
- more flexible format
- stronger FEC
- reduced power mode
- misc. algorithmic improvements

for given rate, reach improved by 200 m

ADSL2+ dramatically increased rate at short distances

More ADSL2 features

Dynamic training features

- **Bit Swapping** (dynamic change of DMT bin bit/power allocations)
- **Seamless Rate Adaptation** (dynamic change of overall rate)

Frame bearers

- Multiple (up to 4) frame bearers (data flows)
- Multiple latencies for different frame bearers (FEC/interleave lengths)
- Dynamic rate repartitioning (between different latencies)

VDSL

Optical network expanding (getting closer to subscriber)

Optical Network Unit **ONU** at curb or basement cabinet
FTTC (curb), **FTTB** (building)

These scenarios usually dictates low power

Rates can be very high since required reach is minimal!

Proposed standard has multiple rates and reaches

VDSL - rate goals

Symmetric rates

6.5	4.5Kft	(1.4 Km)
13	3 Kft	(900 m)
26	1 Kft	(300 m)

Asymmetric rates (US/DS)

0.8 / 6.5	6 Kft	(1.8 Km)
1.6 / 13	4.5 Kft	(1.4Km)
3.2 / 26	3 Kft	(900 m)
6.4 / 52	1 Kft	(300 m)

Summary of xDSL Line Codes

PAM

- IDSL (2B1Q)
- HDSL
- SHDSL/HDSL2 (with TCM and optionally OPTIS)
- SDSL

QAM/CAP

- proprietary HDSL/ADSL/VDSL

DMT

- ADSL
- ADSL2, ADSL2+
- G.lite
- VDSL2

DMT processing

bit handling ((de)framer, CRC, (de)scrambler, RS, (de)interleaver)

tone handling (bit load, gain scaling, tone ordering, bit swapping)

QAM modem (symbolizer, slicer)

signal handling (cyclic prefix insertion/deletion, (I)FFT,
interpolation, PAR reduction)

synchronization (clock recovery)

channel handling (probing and training, echo cancelling, FEQ, TEQ)