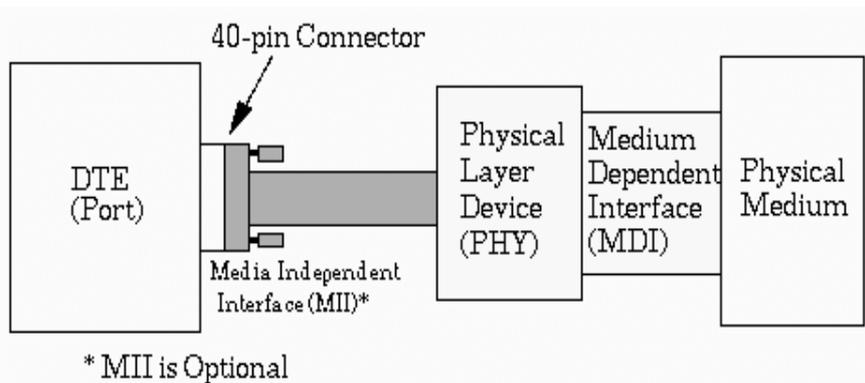


Ethernet rapide

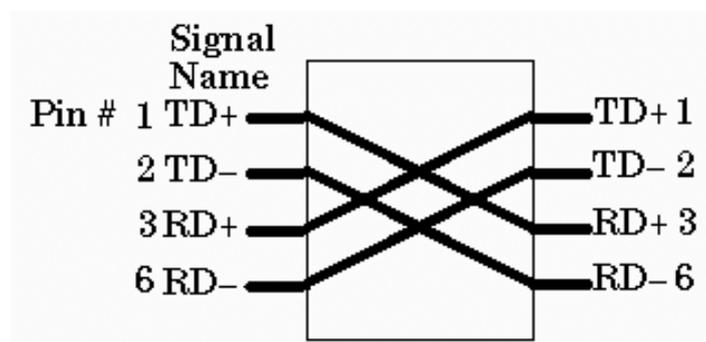
Ethernet 100 T

- Protocole identique à Ethernet 10bT
- Câblage de plusieurs types
 - 100 TX : 2 paires 100 m
 - 100 T4 : 4 paires
 - 100 FX
- Possibilité de mélange bassehaute vitesse
 - Sélection automatique

La connexion ethernet rapide



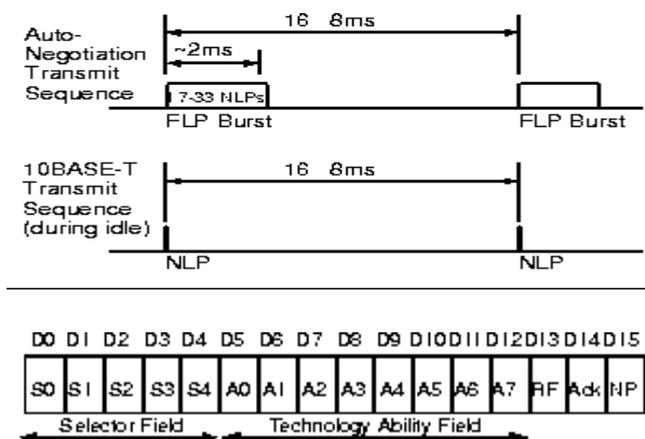
Câblage sur deux paires 100 T



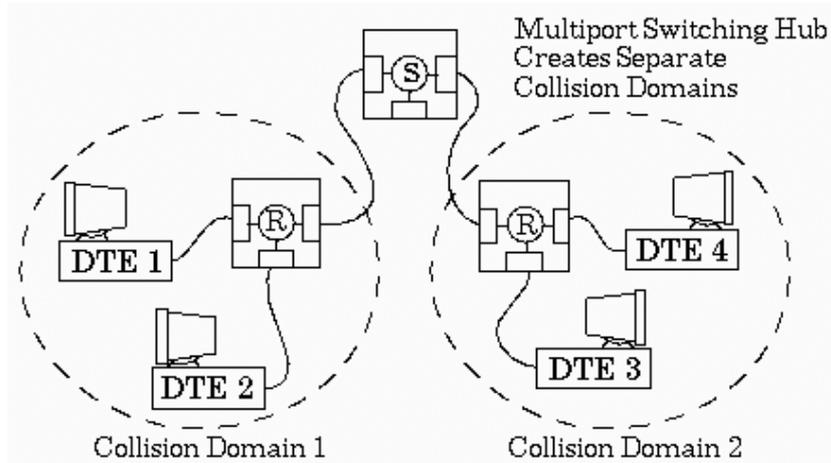
Les répéteurs

- Classe I
 - régénération analo-digital-analog
 - délais importants
 - possibilité de media différents
- Classe II
 - amplificateurs
 - délais courts
 - medium homogène

Négociation de performances



Planification : domaines de collision



Donnée de configuration typique Modèle 1

Model 1: Maximum collision domain in meters³

Repeater Type	Copper	Fiber	Copper and Fiber (T4 and FX)	Copper and Fiber (TX and FX)
DTE-DTE Single Segment	100	412	N/A	N/A
One Class I Repeater	200	272	231 ^b	260.8 ^b
One Class II Repeater	200	320	N/A ^c	308.8 ^b
Two Class II Repeaters	205	228	N/A ^c	216.2 ^d

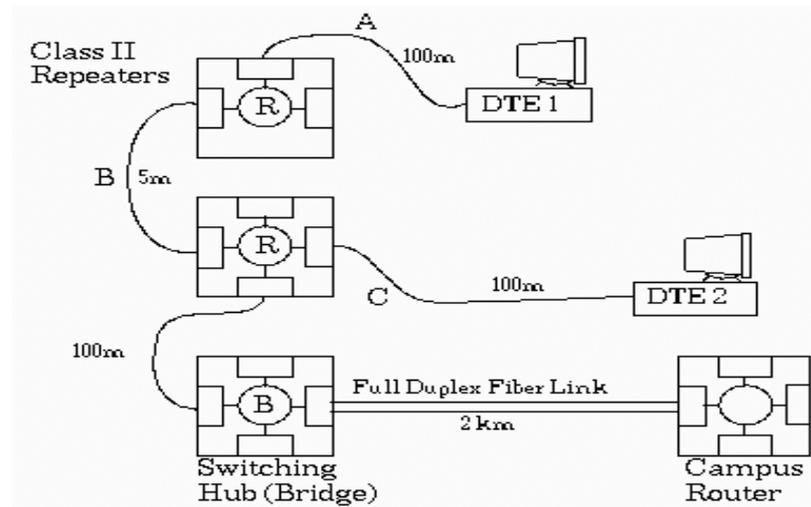
a. Segment lengths in meters, no timing margin.

b. Note: Assumes 100 meter copper link and one fiber link.

c. Not Applicable: T4 and FX cannot be linked with typical Class II repeater.

d. Note: Assumes 105 meters of copper link and one fiber link.

Exemple



Exemple de bilan

Two TX DTEs	100
100 m Cat 5 segment	111.2
100 m Cat 5 segment	111.2
5 m Cat 5 segment	5.56
Class II repeater ^a	92
Class II repeater ^a	92
Total Delay =	511.96

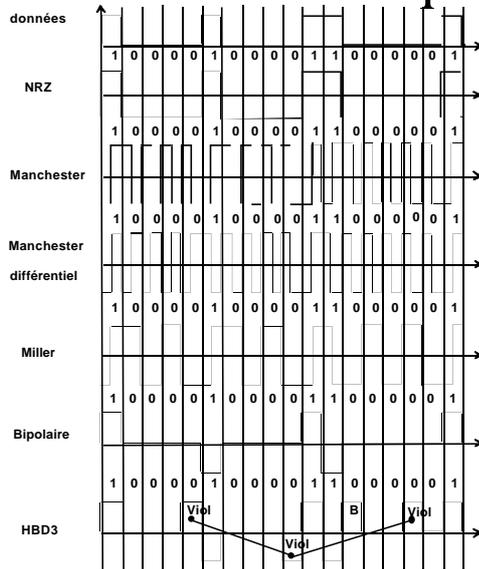
a. All ports TX/FX.

Le cablage

Transmission en bande de base

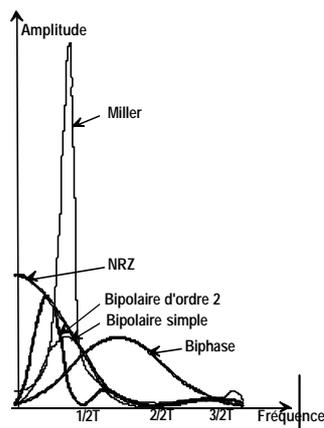
- Transmission du signal sans translation du spectre.
- Problèmes posés :
 - Composante continue
 - Synchronisation des horloges
 - Largeur du spectre
- Solution : le transcodage ou codage en ligne

Les techniques de codage

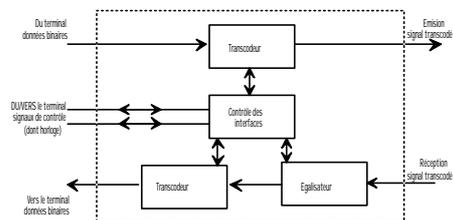


- **NRZ**
 - par rapport symétrise au 0
 - pas de transition sur une suite continue de bits à 1 ou 0
- **Manchester**
 - Transition à chaque temps bits
 - Sens significatif, largeur de spectre
- **Manchester différentiel**
- **Miller**
- **HDB3**
- **nBmB (4B5B dans FDDI)**

La transmission en bande de base

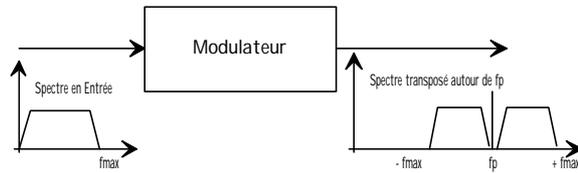


Spectres des différents codages



Principe d'un codeur ou ERBdB (Modem bande de base)

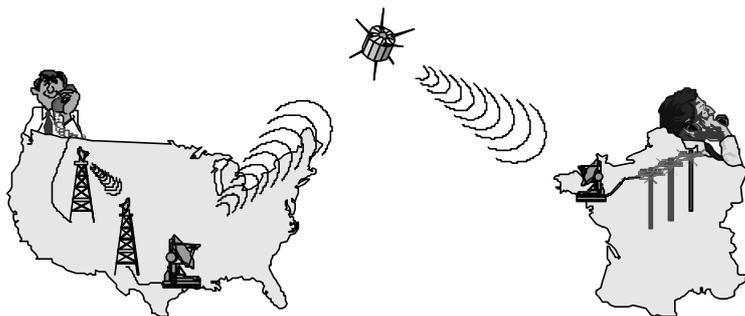
La transmission Large Bande Principe



En transmission Large Bande le spectre du signal est translaté autour d'une fréquence dite porteuse. La translation de fréquence ou modulation résout 2 problèmes :

- La dispersion du spectre (vitesse de groupe)
- La monopolisation du support

Les supports de transmissions



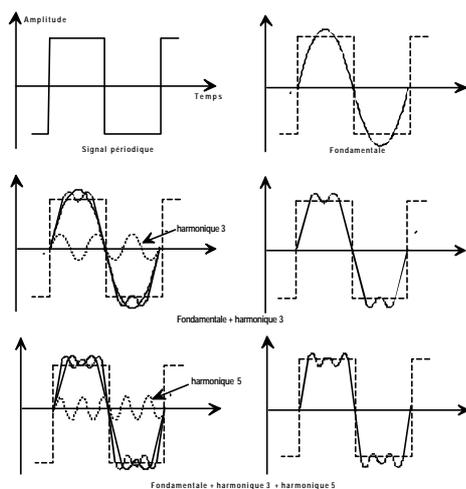
Une liaison peut mettre en jeu différents types de support

Caractéristiques des supports



- Un support dénature de signal
- Bande passante (BP)
- Diaphonie
- Atténuation (résistance)
- Impédance caractéristique

Bande Passante Analyse Harmonique



- **Théorème de Fourier**

- **Conséquence :**

- Toutes les harmoniques ne sont pas transmises identiquement, d'où une déformation du signal.

- **Attention :**

- Bande passante qualifie le système
- Largeur de bande qualifie le signal

Les différents supports

Supports cuivres

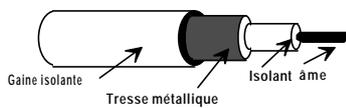
- **Paire torsadée**

- Impédance 100, 120, 150 ohms
- **AV** : coût,
- **INC** : sensibilité aux rayonnements



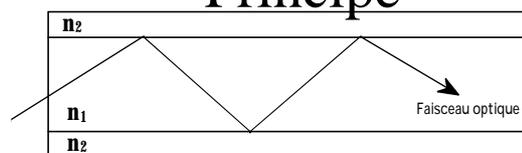
- **Coaxial**

- Impédance 50, 75 ohms
- **AV** : rayonnement
- **INC** : coût, installation



Fibre Optique

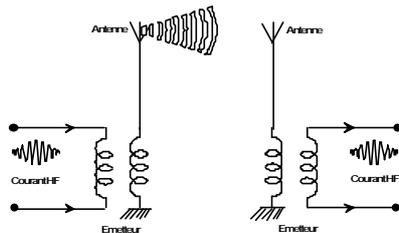
Principe



- **Loi de Descartes** : utilisation de la propriété de réflexion
- **Caractéristiques** :
 - Coeur : 10 à 50 micro mètre
 - Gaine : 125 micro mètre
- **Unidirectionnelle**, insensibilité aux rayonnements
- **Grande bande passante** (plusieurs Giga Hertz)

Les Ondes hertziennes

Principe

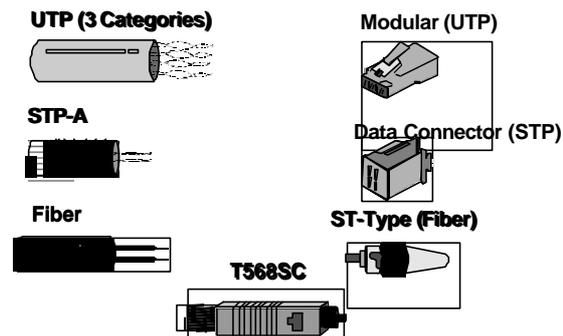


- Utilisées dans :
 - Les faisceaux hertziens
 - Les liaisons satellites

Caractéristiques de la couche physique

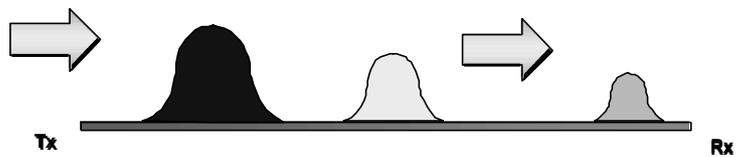
- Electronique
 - Niveau du signal
 - Codage
 - Conformité aux normes
 - Sensibilité au bruit
- Cablage
 - Interface physique (connecteur)
 - Budget atténuation
 - Marge signal à diaphonie

Les composants



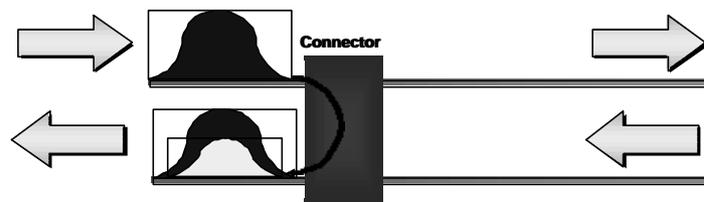
SWSA2006.013 6/28/94

Atténuation



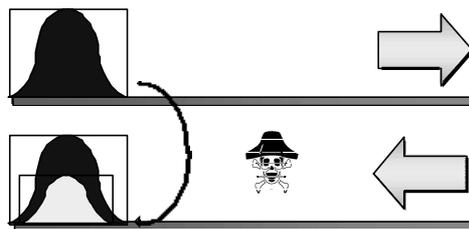
- Perte de puissance du signal
- S'exprime en dB
- L'atténuation augmente avec la distance
la fréquence

Paradiaphonie (NEXT)



- Couplage entrées/sortie
S'exprime en DB (on recherche des valeurs élevées)
- Augmente avec la fréquence
- Affectée par :
la construction du câble
la qualité de l'installation

Marge signal à NEXT



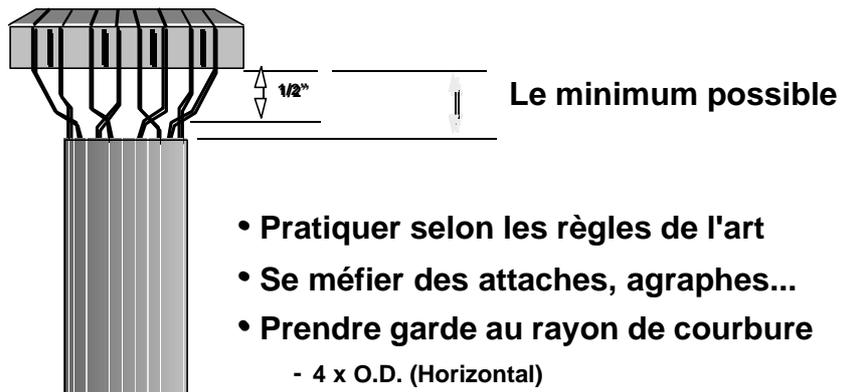
Signal désiré - bruit indésirable

UTP Performance du Cable

(@ 16 MHz)	Cat. 3 Up to 16 MHz	Cat. 4 Up to 20 MHz	Cat. 5 Up to 100 MHz	
ATTN. per 100 meters	13.1	8.9	8.2	TIA TR41.8.1 COMMITTEE: TSB-36
NEXT	23 dB	38 dB	44 dB	TIA TR41.8.1 Committee: TSB-40

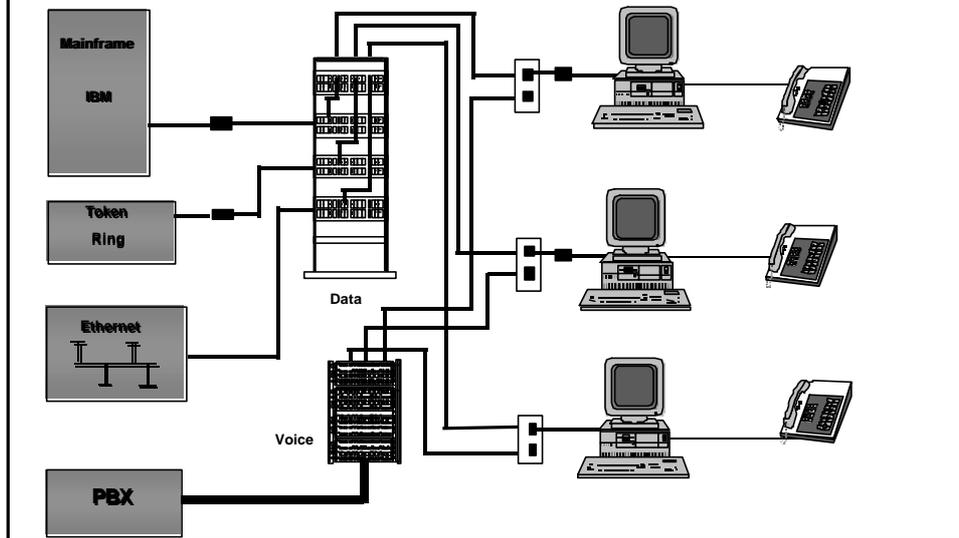
SWSA2006.029 6/28/94

Les règles d'installation



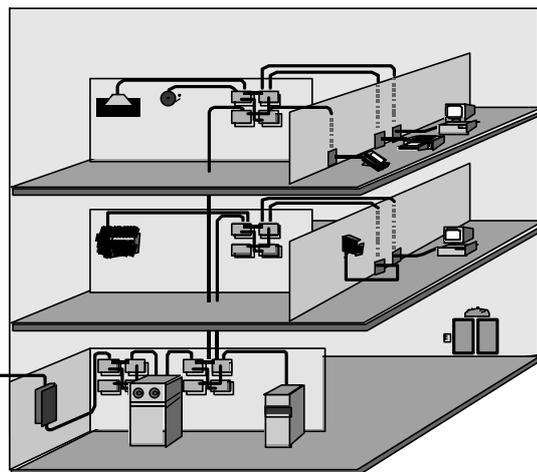
- Pratiquer selon les règles de l'art
- Se méfier des attaches, agrafes...
- Prendre garde au rayon de courbure
 - 4 x O.D. (Horizontal)
 - 10 x O.D. (Multipaire)
- Limiter la force de tirage

Cablage structuré



Infrastructure : impact architectural

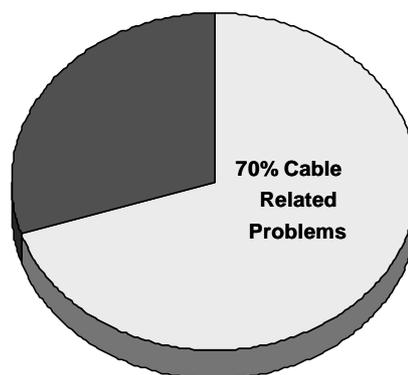
- Sous systèmes
- Campus Backbone
 - Horizontal
 - Intra-building Backbone
 - Poste de travail
 - Equipement
 - Administration



Les besoins en bande passante

	Débit	Codage	Fréquence max
Ethernet	10 Mbps	2 Level	10 MHz
Token Ring	16 Mbps	2 Level	16 MHz
TP-PMD	100 Mbps	Multi Level	31.25 MHz
ATM	155 Mbps	Multi Level	38.75 MHz

Les interruptions de service



Source: LAN Technology 1991

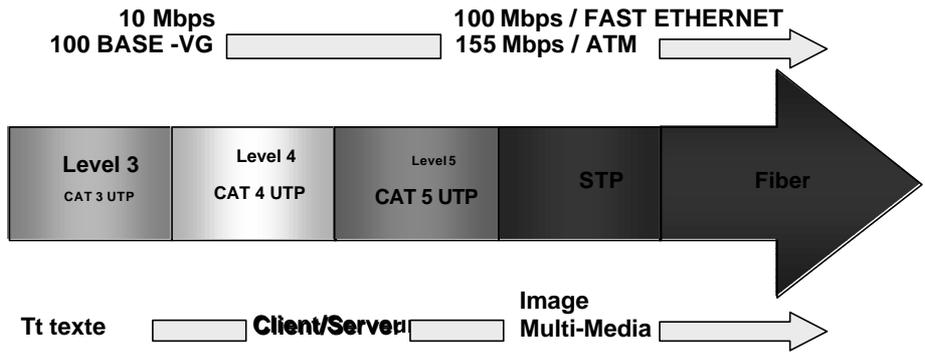
Standards de Câblage Générique

- ISO/CEI - DIS 11801 - Câblage Générique du Local Client
- EIA/TIA-568A - Câblage de Bâtiments Commerciaux
- CEN/CENELEC prEN50173 - Exigences sur les Performances des Modèles de Câblage Générique

ISO/CEI DIS 11801

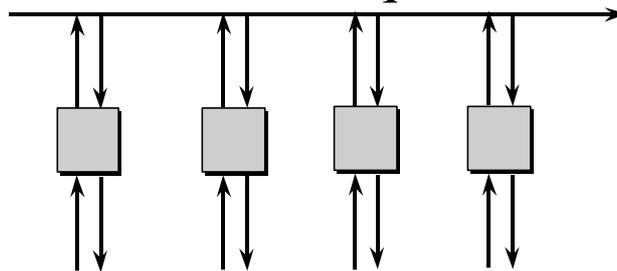
- Fin de la période d'approbation: 6-7-94
- Dernière réunion : Palo Alto, CA 3-10-94
- Texte Envoyé à Genève: 31-10-94
- En cours d'impression 28-4-95

La croissance des besoins



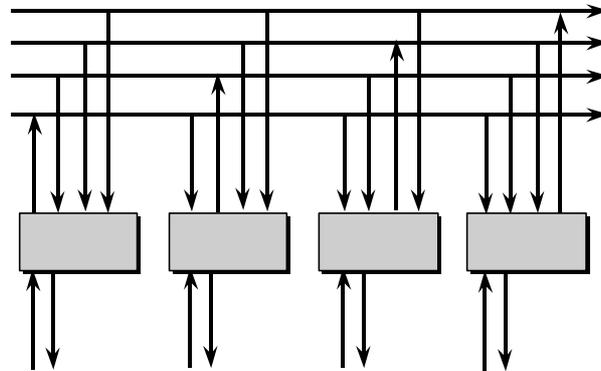
Commutation de réseau local

Bus Unique



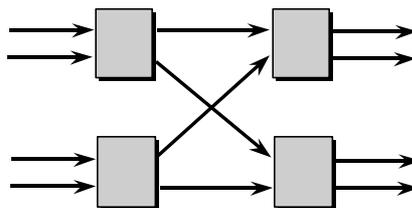
- Le plus simple
- 1–10 Gbps
- Multicast facile
- Blocage si over-subscription du bus

Bus Multiple



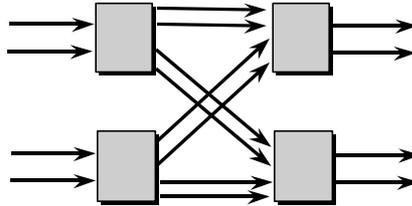
- Contrôle du blocage plus complexe
- Vitesse du Bus généralement supérieure au débit des portes
- Débit comparable au bus unique—10 Gbps
- Multicast facile

Commutation (Blocante)



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

Matrice non bloquante

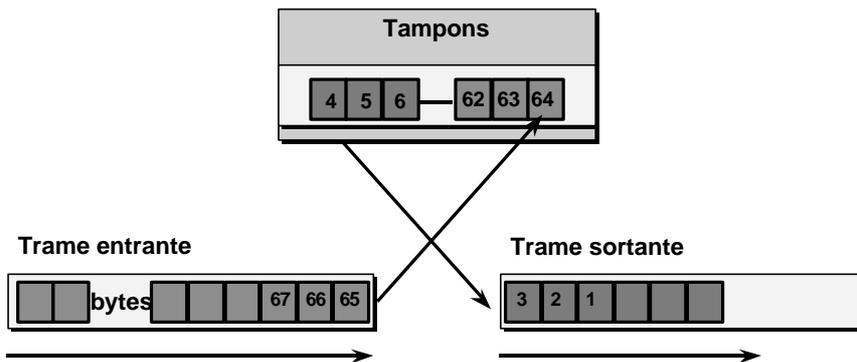


- Circuiterie plus complexe
- Généralement basé sur ASICs
- Multicasts par copie de trame
- La matrice interne fonctionne généralement à une vitesse supérieure à celle des entrées
- Faible probabilité de blocage
- Jusqu'à 200 Gbps

Technologie

- Cut-through
- Store-and-forward

Cut-Through



Cut-Through

- Très faible latence
- Transmission des fragments résultant de collisions
- Transmission des trames en erreur—runts, bad CRC, giants
- Excellent quand les contraintes temporelles sont plus importantes que le contrôle d'erreur

Cut-Through

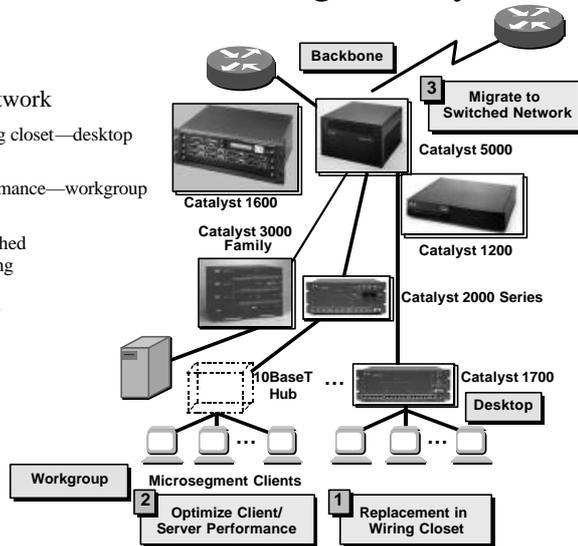
- Fragment free
 - contrôle des runts et des fragments
- Adaptive error free
 - Passage au store-and-forward sur dépassement d'un seuil d'erreur
 - Passage au cut-through quand le taux d'erreur passe au dessous du seuil d'erreur

Store-and-Forward

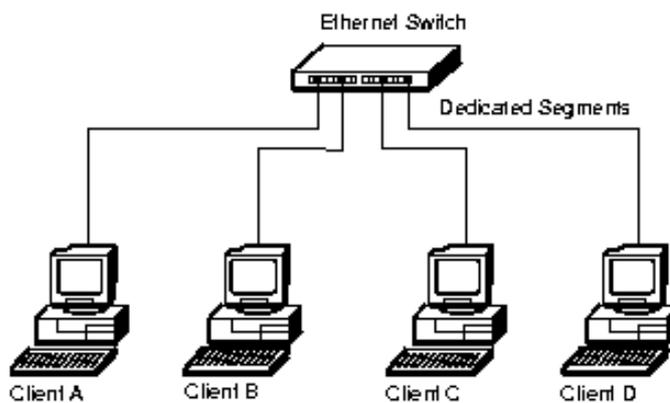
- Stockage de la trame entière avant commutation
- Latence augmentée (stockage à la vitesse du medium)
- Excellent si le stockage est nécessaire
 - Porte serveur oversubscribed
 - Backbone switch

Cisco LAN Switching Family

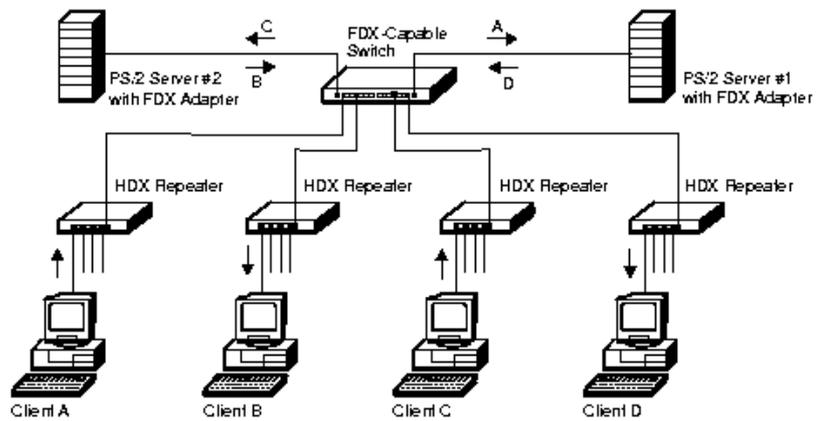
- Increase bandwidth and performance of existing network
 1. Switching
 - Replace shared hubs in wiring closet—desktop
 - Optimize client/server performance—workgroup
 2. Switching
 - Migrate from shared to switched backbone—backbone switching
 3. Switching
- Enable virtual LANs across switched network



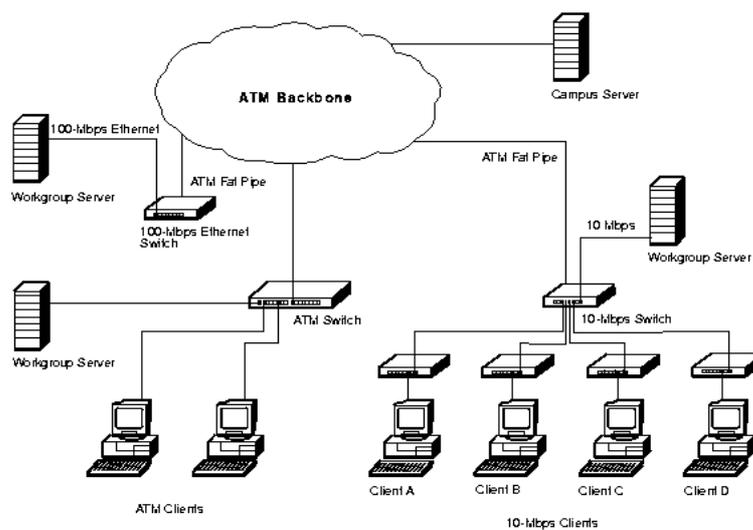
Commutation et microsegmentation



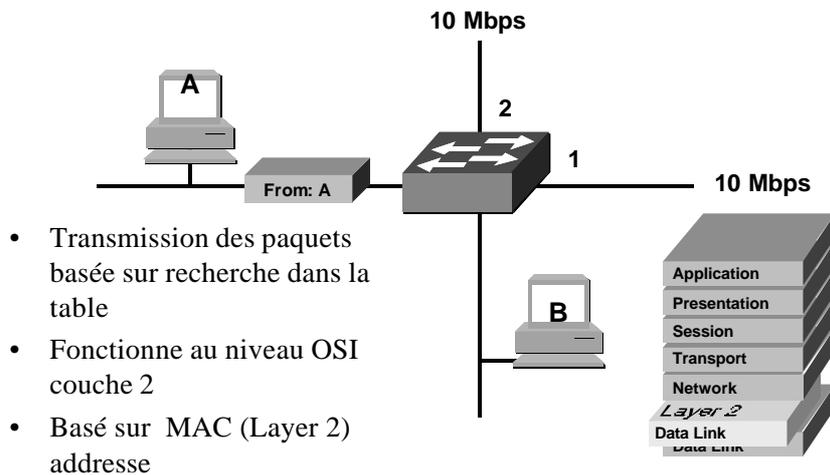
Disponibilité des serveurs attachement FDX



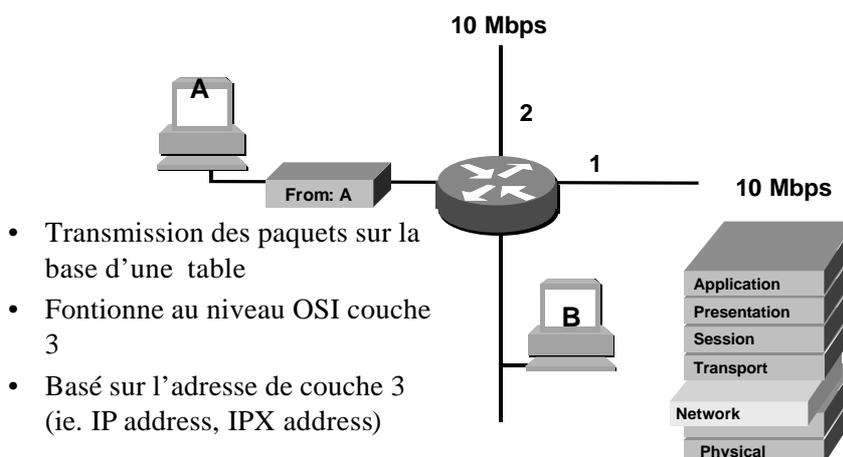
Evolution vers ATM



Fonctionnement d'un commutateur



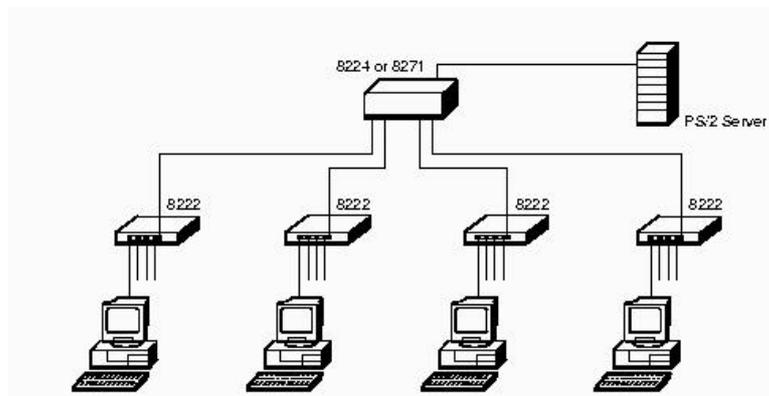
Fonctionnement d'un Routeur



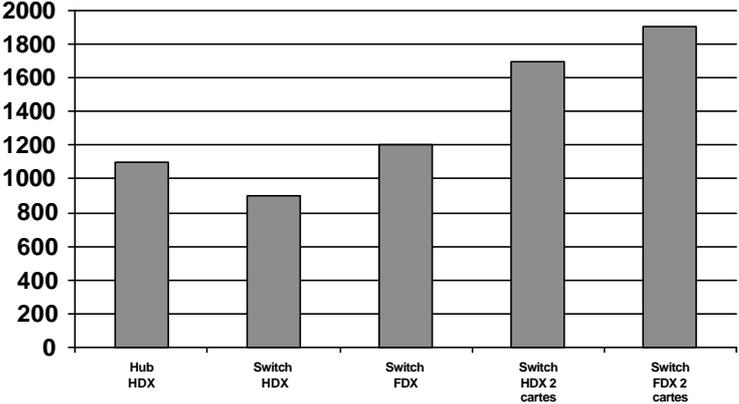
Comparaison

	Connectivité	Contrôle des Collisions	Contrôle des Broadcasts
 Hub	oui	non	non
 LAN Switch	oui	oui	non
 Routeur	oui	oui	oui

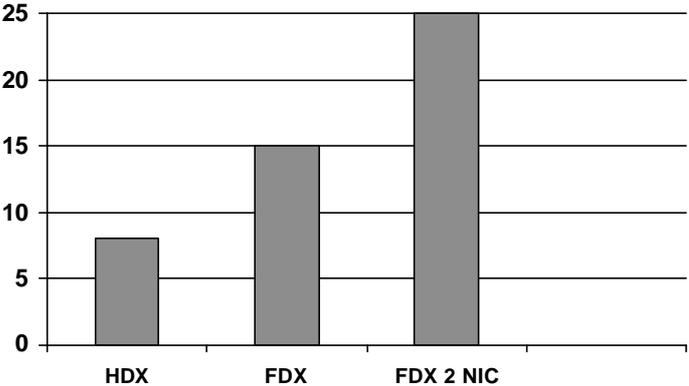
Configuration test



Performances (kbps)



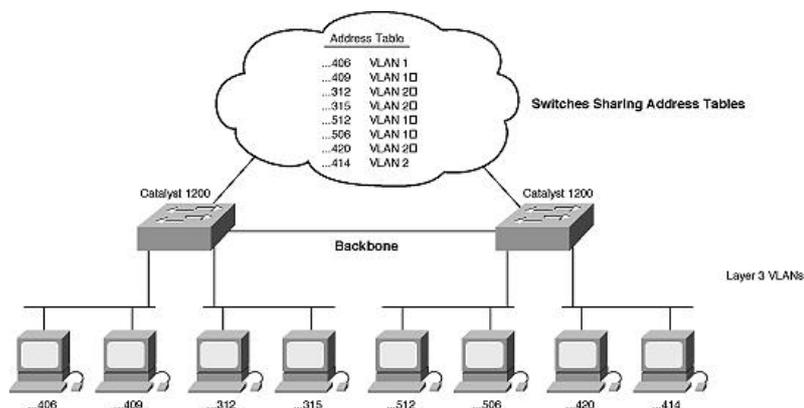
Trafic bidirectionnel (Mbps)



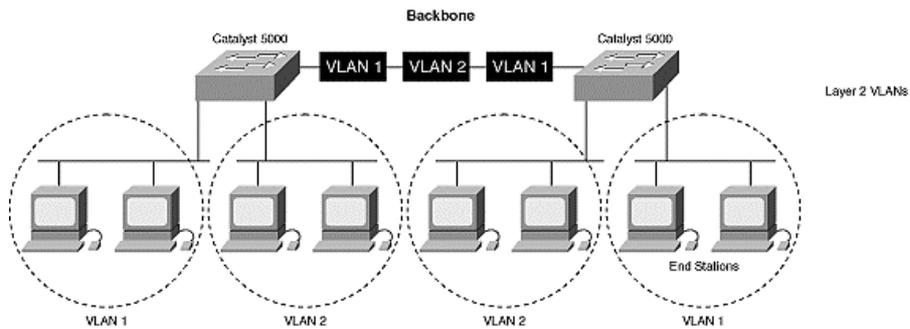
Les Vlan

- Administration
 - déplacement des stations
- Contrôle des broadcasts
- Sécurité
- Migration

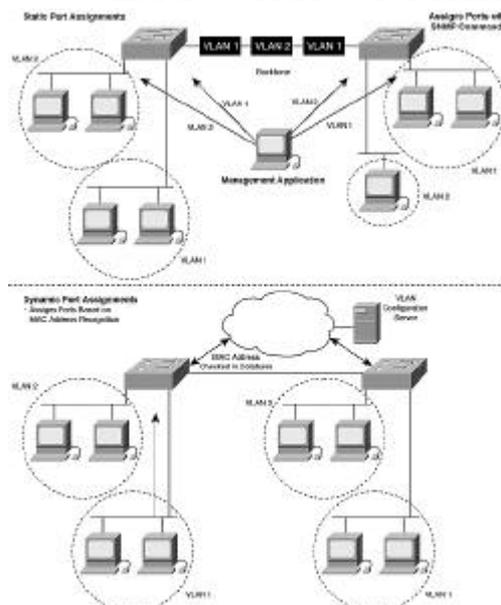
Les Vlan : niveau 3



Les Vlan : niveau 2



Les Vlan : administration



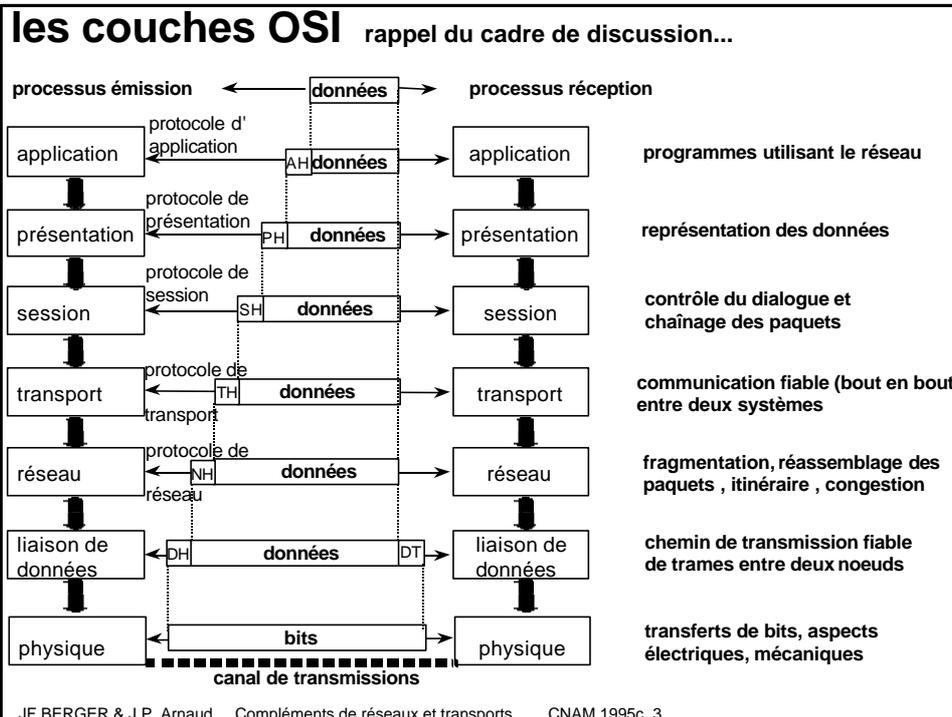
- Statique
 - simplicité
- Dynamique
 - adresse Mac
 - adresse logique
 - protocole

Typologie des équipements d' interconnexion

JF BERGER & J.P. Arnaud _ Compléments de réseaux et transports _ CNAM 1995c_1

I RAPPELS et INTRODUCTION

JF BERGER & J.P. Arnaud _ Compléments de réseaux et transports _ CNAM 1995c_2



Les Réseaux locaux d'entreprise(1)

- **le Comité 802 de l' IEEE**

- **couche physique et couche liaison de données**
- **décomposition de la couche liaison de données**
 - **sous couche MAC : Médium Access Control**
 - algorithmes de gestion de connexions (circulation de jetons, attente avant envoi après collision), priorités, détection d'erreurs, fractionnement en trames.
 - **sous couche LLC : Logical Link Control**
 - délimite les champs permettant à plusieurs protocoles des couches supérieures de partager l'utilisation de la liaison
 - trois types de contrôle de liaison:
 - **type 1: simple flux de données sans contrôle d'erreurs (orienté Donnéesgramme)**
 - **type 2: orienté connexion, donc avec des champs pour numérotter les messages, accusés de réception, champs différenciant les données des informations de contrôle**
 - **type 3: version simplifiée du type 2 (à moitié fiable, moins coûteux)**

Les Réseaux locaux d' entreprise(2)

- **les comités 802:**(normes ISO 8802.3, 8802.4, 8802.)
 - **802.1: problèmes communs** (adressage, gestion et ponts)
 - **802.2 : définit LLC**
 - **802.3 : réseau local à accès multiples** (méthode CSMA/CD) (dérivé d' éthernet de Xerox puis Intel,DEC et Xerox)
 - **802.4 : réseaux locaux à bus à jeton** (Token bus)
 - **802.5 : réseaux locaux à anneaux à jetons** (Token ring) (4Mb et 16 Mb)
- **FDDI : normalisé ANSI, anneau à jeton 100Mb, différent de 802.5**

JF BERGER & J.P. Arnaud Compléments de réseaux et transports CNAM 1995c 5

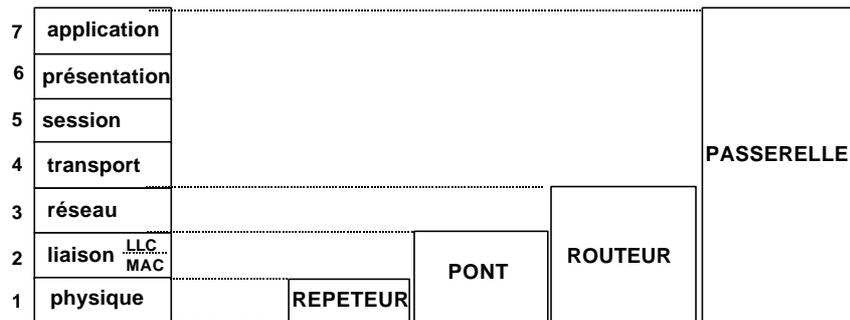
définitions de base

- **NOM : ce que c'est** (identificateur) indépendant de la localisation)
- **ADRESSE : où c' est** (valable quelle que soit la source, change si la destination se déplace)
- **ROUTE : comment s' y rendre** (dépend de la localisation de la source et de la localisation de la destination).
- **mais le 802 définit des adresses LAN de réseau local sur 48 bits attribuées de façon universelle==> ce sont des noms....qu' on appelle adresses.**
- **adresses de LAN : normalisées par le comité 802:**
 - **attribuées par l'IEEE : standard de fait : 48 bits**

JF BERGER & J.P. Arnaud Compléments de réseaux et transports CNAM 1995c 6

présentation générale

produits d' interconnexion et couches OSI



JF BERGER & J.P. Arnaud Compléments de réseaux et transports CNAM 1995c 9

les répéteurs

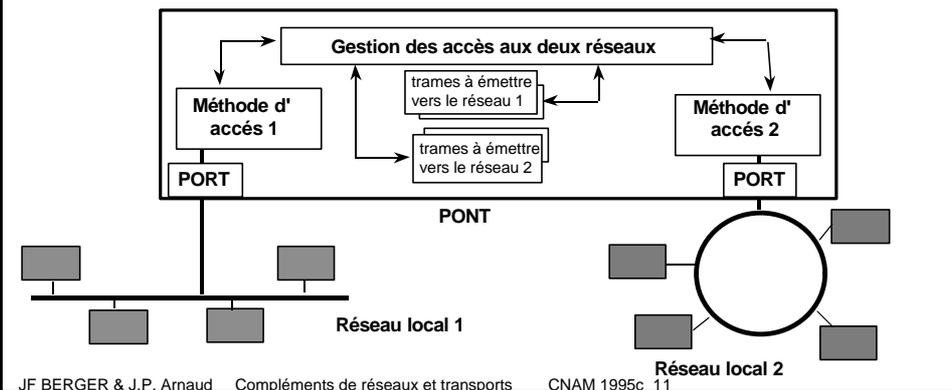
- agissant localement, au niveau couche physique
- réalisation de connexion physique entre deux médias identiques ou différents par régénération des signaux; (on assure la continuité physique: de l' amplification du signal (recopie des bits à mesure qu'ils arrivent)à la régénération et restitution d'horloge)
- les différents segments de câble constituent un seul réseau logique local (connexion transparente)

EX: les transceivers de 802.3 donnent une longueur maxi de segments de 500m.On relie les segments par des répéteurs pour atteindre les 2500m (4 répéteurs maxi en série)

JF BERGER & J.P. Arnaud Compléments de réseaux et transports CNAM 1995c 10

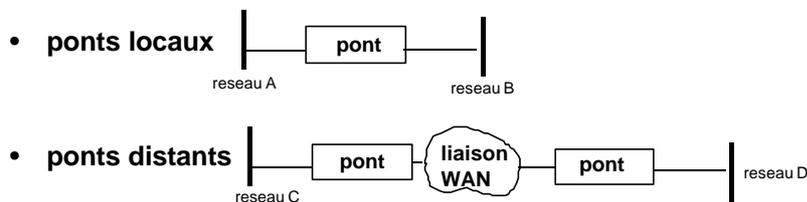
les ponts définitions appelés aussi répéteurs sélectifs

- permet d' interconnecter des réseaux ayant des couches physiques et sous-couche MAC différentes, donc transparents pour les niveaux supérieurs.
- Le pont reçoit des trames selon une technique d' accès (Réseau A) et les retransmet selon une autre vers le réseau B si leurs adresses de destination sont reconnues appartenir au réseau B:



les ponts suite

- permet de découpler deux (ou +) segments de réseau (aspect isolement de trafics)
- réunit deux ou plusieurs réseaux locaux physiques en un seul logique.
- peut être doté de fonctions de filtrage pour respecter des contraintes de temps ou de sûreté de fonctionnement
 - par exemple, bloquant les transmissions longues, ou assignant certains échanges à des parties bien précises du réseau.



ponts dynamiques: chaque pont gère dynamiquement une table des interlocuteurs locaux, ignore les trames de ceux-ci et ne transmet que celles destinées à un autre réseau local (ponts à apprentissage)

les ponts transparents (1)

- normalisé dans 802.1
- **apprentissage** : technique d'auto-apprentissage des adresses des noeuds situés sur chaque segment connecté au pont:

stratégie du pont:

- le pont écoute tous les paquets (mode promiscuous)
- pour chaque trame reçue sur un port du pont, le pont
 - enregistre l'adresse source et le port concerné (recevant) dans une mémoire cache stations
 - recherche dans cette mémoire cache stations l'adresse destination de la trame
 - si l'adresse destination ne figure pas, le pont réexpédie le paquet vers toutes les interfaces sauf celle de réception initiale du paquet (flooding)
 - si l'adresse destination est dans la mémoire cache stations, le pont se contente d'acheminer la trame vers l'interface spécifiée dans la table sauf si l'interface spécifiée est celui où il a été reçu (filtré)
- le pont date chaque entrée dans la mémoire cache-station et la détruit au bout d'un certain temps (aging time)

JF BERGER & J.P. Arnaud Compléments de réseaux et transports CNAM 1995c 13

les ponts transparents (2)

- le problème des boucles

- soit l'architecture suivante:

avec le seul pont P1:

pas de problèmes :(arbre)
 P1 sait juste qu'il a 3 ports
 à chaque transmission de trames,
 P1 va construire sa mémoire cache
 et accroître par auto-apprentissage
 ses connaissances

avec deux ponts P1 et P2:

problèmes de boucles:

l'auto-apprentissage ne fonctionne plus correctement:

Quand A transmet un paquet, Chaque pont:

-reçoit le paquet,

-note que A réside sur le LAN 2

-met le paquet en file pour le réexpédier aux LAN 2 et 3

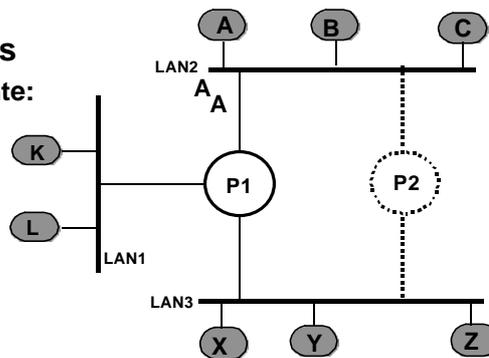
Or, un de ces deux ponts va réémettre le premier (par ex P2)

alors ce paquet va apparaître sur le réseau LAN3

donc P1 va recevoir le paquet depuis le lan 3 et donc

noter que A réside maintenant sur LAN3 et vouloir le réexpédier sur LAN1 et LAN2

Non seulement les paquets bouclent mais prolifèrent....



JF BERGER & J.P. Arnaud Compléments de réseaux et transports CNAM 1995c 14

les ponts transparents (3)

- d' où l' algorithme pour éliminer ces possibilités de bouclage:
algorithme de Spanning Tree : arbre recouvrant (appartient à 802.1)

Le but est de faire découvrir aux ponts de manière dynamique

- un sous-ensemble de la topologie du réseau qui soit sans boucle et
- de connectivité suffisante pour qu' il existe un chemin entre chaque paire de LAN

Pour cela, les ponts vont se transmettre des messages spéciaux : des messages de configuration (BDPU : Bridge Protocol Données Unit ou Unités de données de protocoles de ponts pour leur configuration) permettant de dérouler l' algorithme de l' arbre recouvrant:

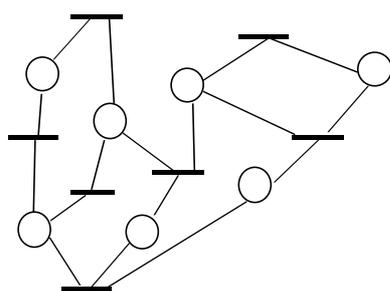
- choisir un pont racine parmi tous les ponts (en général, algorithme distribué)
- calculer la distance sur le plus court chemin entre les autres ponts et ce pont racine
- pour chaque LAN choisir un pont ,(pont désigné) le plus proche du pont racine
- pour chaque pont, choisir le port dit port racine qui donne l' accès au pont racine
- choisir les ports à inclure dans l' arbre. (ce sont les ports racines et les ports des ponts désignés)

le trafic est alors acheminé vers et en provenance des ports appartenant à l' arbre recouvrant, les autres ports n' étant pas utilisés

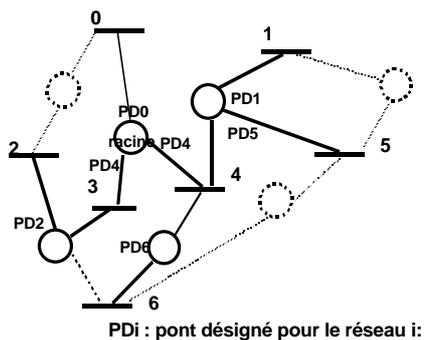
JF BERGER & J.P. Arnaud Compléments de réseaux et transports CNAM 1995c 15

les ponts transparents (4)

soit l'architecture de base:



exemple d' arbre recouvrant



PD_i : pont désigné pour le réseau i:

- les messages de configuration sont émis à intervalles réguliers (quelques secondes) pour permettre également la mise à jour de la topologie (et donc un nouveau calcul d' arbre recouvrant).
- le calcul du coût d' un chemin est fait à partir des BDPU (notamment des ID des ponts)

JF BERGER & J.P. Arnaud Compléments de réseaux et transports CNAM 1995c 16

les ponts transparents (fin)

- **quelques compléments:**

les messages de configuration émis par les ponts comportent

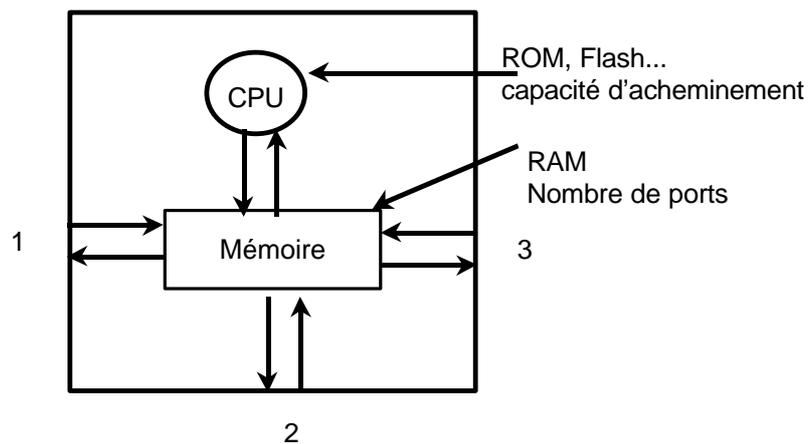
- l' identification du pont(+priorité) et du port utilisé, de la racine et du coût à celle-ci, des indications sur:
 - l'age du message (cad temps écoulé depuis que la racine a transmis son message de configuration), la durée de vie du message, le temps de prise de contact (temps qui s'écoule entre 2 messages de configuration émis par un pont qui se considère comme racine) ainsi que des délais liés à la durée d'apprentissage et d'écoute (pour réactiver un port)

- **avantages et problèmes:**

- autoconfiguration, détection des pannes de ponts, prise en compte des modifications de topologie.
- risque de sous-dimensionnement des ponts (car un non-traitement de BDPU engendre des boucles...)
- sous-utilisation de la topologie (cad de la capacité de transport installée)

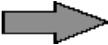
JF BERGER & J.P. Arnaud Compléments de réseaux et transports CNAM 1995c 17

Ponts : l'architecture



JF BERGER & J.P. Arnaud Compléments de réseaux et transports CNAM 1995c 18

Ponts : les performances

- **Maximum forwarding rate**
 - pps d'une porte vers une autre
 - **Aggregate forwarding rate**
 - capacité globale
 - **Exemple**
 - max forwarding : 14800 fps
 - agregate : 18000 fps
 - **Règle des 80/20**
-  oversubscribed

JF BERGER & J.P. Arnaud Compléments de réseaux et transports CNAM 1995c 19

Commutateurs

- **Interconnexion niveau 2**
- **Aggregate forwarding rate plus élevé**
 - nombre de portes plus élevé
- **Latence**
 - toujours plus élevée que pour un pont
 - pont : 40 à 60 temps bit, commutateur 120 temps bit
 - plus élevée en store et forward (décision)
 - jusqu'à 12 144 temps bit
- **Congestion**
 - manque de ressource (mémoire, bande passante, CPU...)
 - asymétrie de la charge (cas des serveurs)

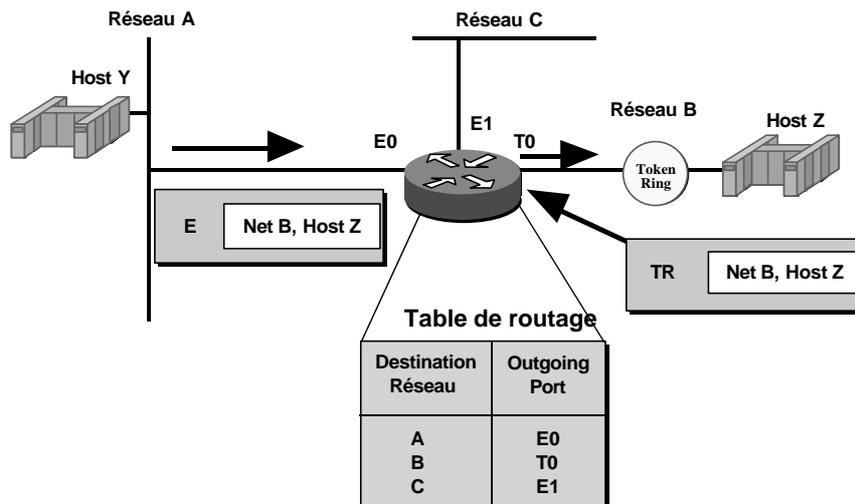
JF BERGER & J.P. Arnaud Compléments de réseaux et transports CNAM 1995c 20

les routeurs

- **Interconnexion de niveau 3 (adresse réseau)**
- **Non transparents**
 - dialogue station-routeur
- **Multiprotocole**
- **Posibilité de maillage**
- **Protocole de routage**
 - IP ou IPX
 - RIP, OSPF, EGP...
- **Latence plus élevée**
- **Grands réseaux**
 - broadcast
 - spanning tree : problème de la racine

JF BERGER & J.P. Arnaud Compléments de réseaux et transports CNAM 1995c 21

Le fonctionnement de niveau 3



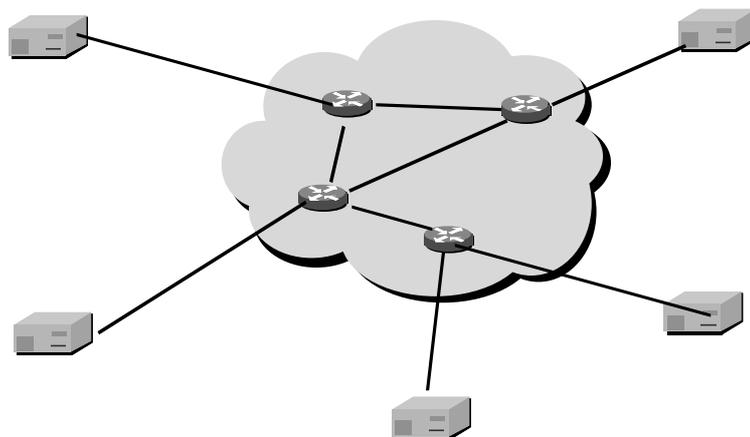
JF BERGER & J.P. Arnaud Compléments de réseaux et transports CNAM 1995c 22

TCP/IP et l'Internet

- **Un réseau de réseau**
 - Une interconnexion universelle
 - Des protocoles standardisés
- **Essentiellement du soft, pas de hard**
- **Des services**
 - Réseau
 - Application
- **Une percée technologique et commerciale**

JF BERGER & J.P. Arnaud - Compléments de réseaux et transports - CNAM 1995c - 23

Une vue conceptuelle



JF BERGER & J.P. Arnaud - Compléments de réseaux et transports - CNAM 1995c - 24

Le modèle d'adressage

- **Adresses IP affectées à toute machine du réseau**
- **Les logiciels applicatifs utilisent ces adresses pour envoyer les informations sur le réseau**
- **La conversion en adresse physique se fait automatiquement**

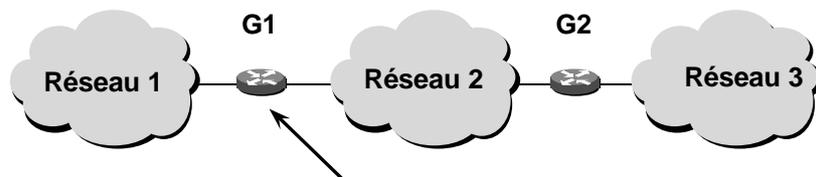
JF BERGER & J.P. Arnaud - Compléments de réseaux et transports - CNAM 1995c 25

Notion de routage

- **Si une machine peut atteindre son destinataire directement, elle envoie ses informations sur le réseau; sinon elle les envoie à une passerelle (le routeur)**
- **Si un routeur peut atteindre le destinataire directement, il envoie les informations sur le réseau; Sinon, il les envoie à un autre routeur.**

JF BERGER & J.P. Arnaud - Compléments de réseaux et transports - CNAM 1995c 26

Exemple : routage statique



Réseau 1	direct
Réseau 2	direct
Réseau 3	G2
autre	erreur

JF BERGER & J.P. Arnaud - Compléments de réseaux et transports - CNAM 1995c - 27

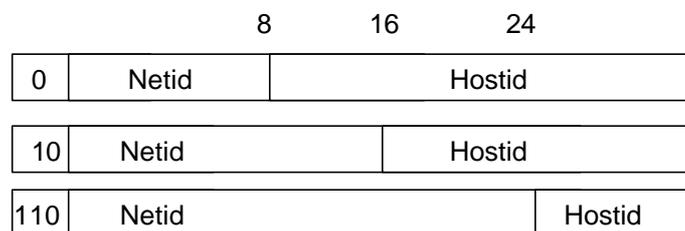
Qualités d'un plan d'adressage

- **Compacité**
- **universalité**
- **Utilisable sur tout type de matériel**
- **Efficace**
 - Test de la possibilité d'un chemin direct
 - Décision de choix d'une passerelle
 - Choix du routeur le plus proche
 - Détermination du chemin le plus court

JF BERGER & J.P. Arnaud - Compléments de réseaux et transports - CNAM 1995c - 28

L'adressage IP

- **Compact et universel**
- **32 bits pour tous**
- **Attribué par autorité centrale pour les préfixes**
- **Attribué par l'administrateur local pour les suffixes**



JF BERGER & J.P. Arnaud - Compléments de réseaux et transports - CNAM 1995c. 29

Caractéristiques de l'adressage TCP/IP

- **Adressage sur 32 bits**
- **Identification du réseau par préfixe attribué par une autorité centrale (IANA)**
- **Identification des machines par un suffixe attribué par l'administrateur local**

JF BERGER & J.P. Arnaud - Compléments de réseaux et transports - CNAM 1995c. 30

Protocoles de routage

d'après Jim Grubb , Cisco

2

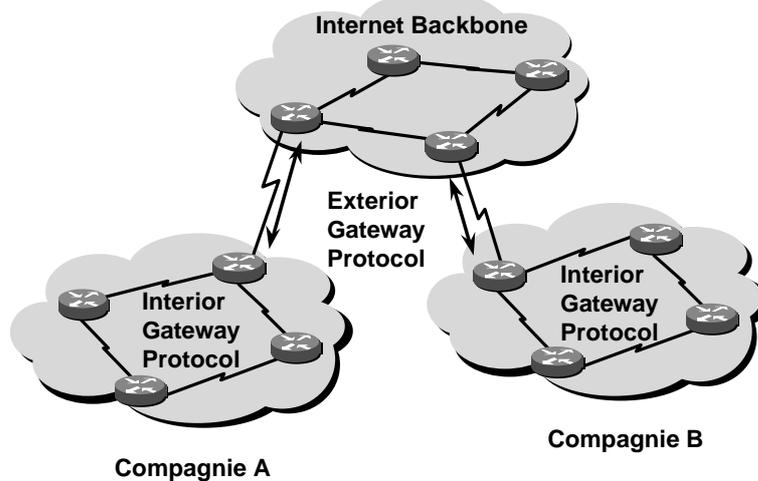
Agenda

- **Qu'est-ce que le routage?**
- **La Table de routage**
- **Types de protocoles**
- **Les protocoles TCP/IP**
- **Le routage multiprotocole**

► Routage et protocoles de routage

- **TCP/IP est routé par:**
 - RIP
 - IGRP®
 - OSPF
 - EIGRP
- **AppleTalk est routé par:**
 - RTMP
 - EIGRP
- **DECnet est routé par:**
 - DECnet
- **VINES est routé par:**
 - RTP

► Interieur/Exterieur



► Agenda

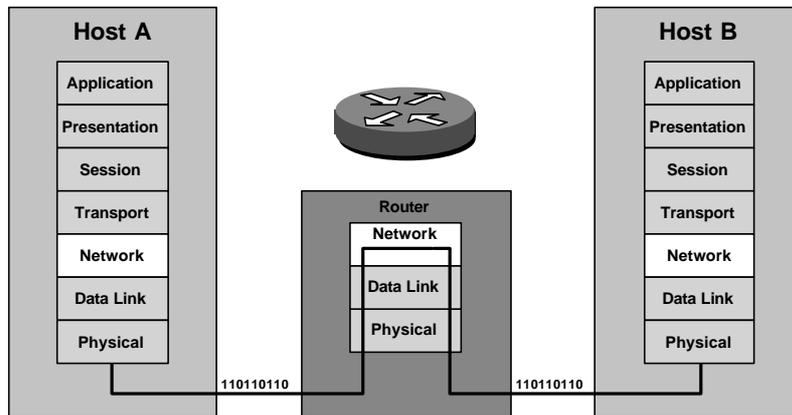
- Qu'est ce que le routage?
- La table de routage
- Types de protocoles
- Les protocoles TCP/IP
- Le routage multiprotocole

► Fonctions d'un routeur

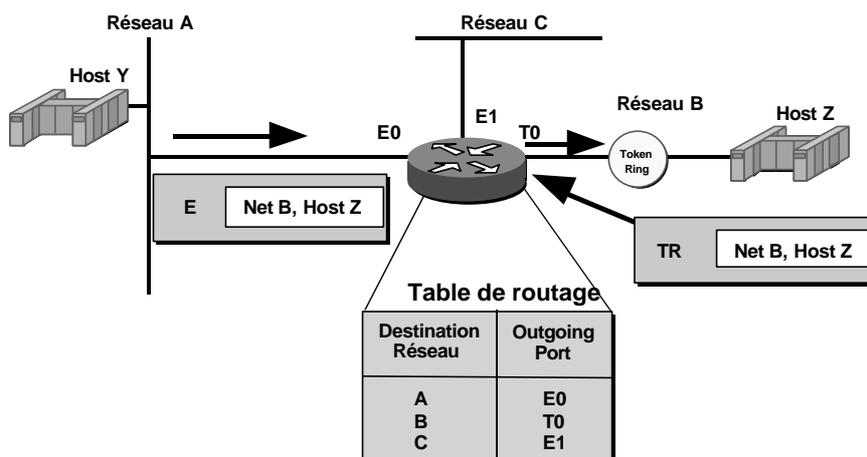
- Le routeur construit des cartes et donne les directions
- La commutation achemine les trames entre des interfaces



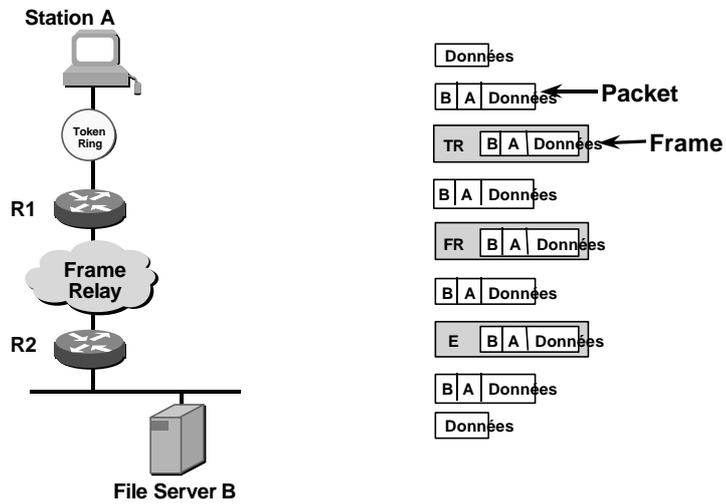
► Les routeurs opèrent au niveau 3



► Le fonctionnement de niveau 3



▶ Trames et Paquets



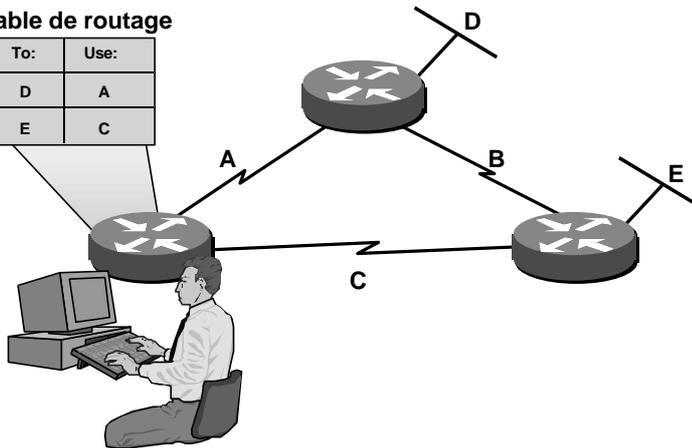
▶ Construction de la Table de routage

- statique
- dynamique

► Routage statique

Table de routage

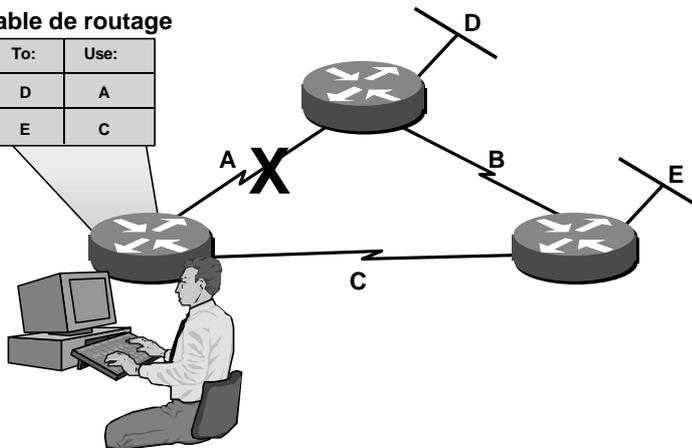
To:	Use:
D	A
E	C



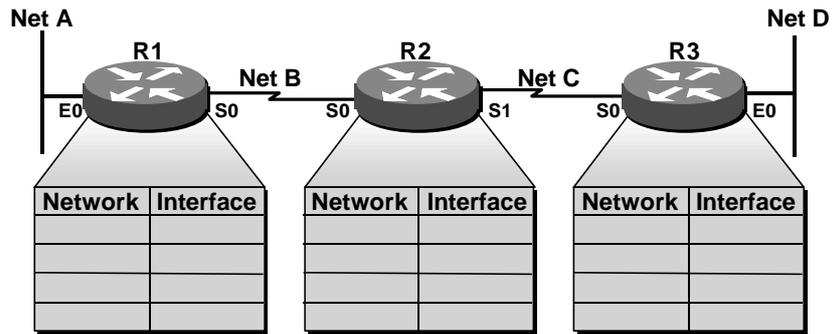
► Routage statique

Table de routage

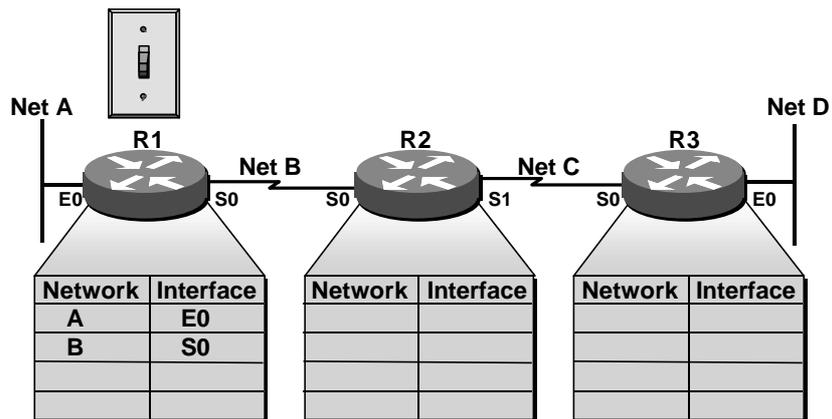
To:	Use:
D	A
E	C



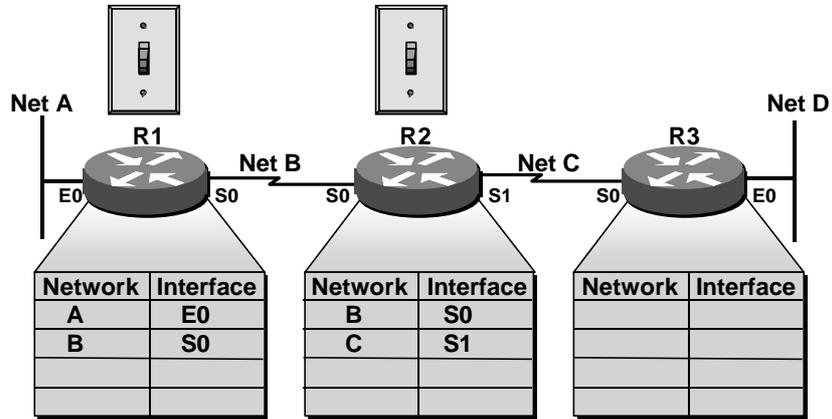
▶ Routage dynamique



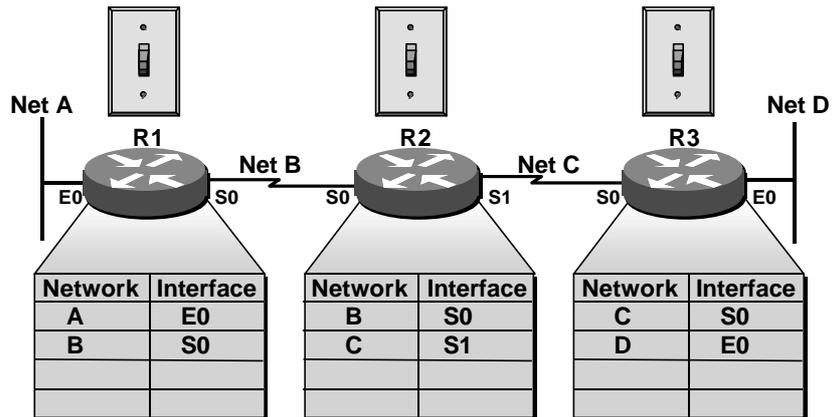
▶ Routage dynamique



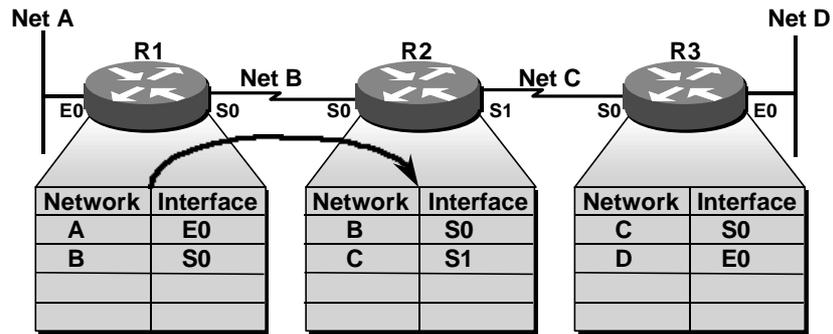
► Routage dynamique



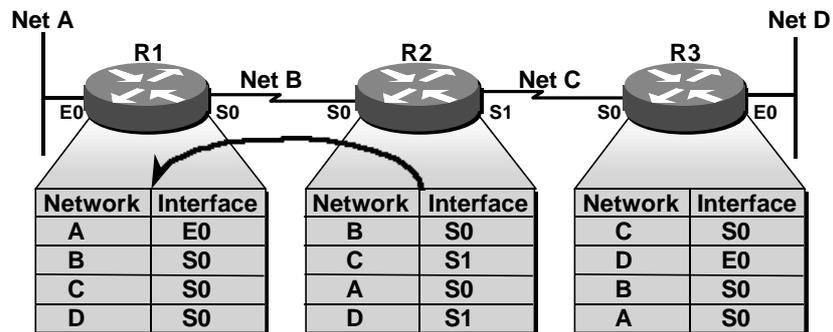
► Routage dynamique



► Routage dynamique



► Routage dynamique



Agenda

- Qu'est ce que le routage?
- La table de routage
- Types de protocoles
- Les protocoles TCP/IP
- Le routage multiprotocole

Table de routage

Network #	Interface	Next Saut	Metric	Age	Status
198.113.181.0	Ethernet0	192.150.42.177	[170/3047936]	02:03:50	D
198.113.178.0	Ethernet0	192.150.42.177	[170/3047936]	02:03:50	D
192.168.96.0	Ethernet0	192.150.42.177	[170/324608]	03:36:50	D
192.168.97.0	Ethernet0				C

► N° de réseau

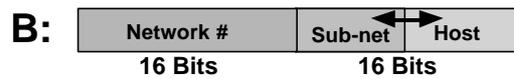
- Attribué par l'administrateur du réseau
- Enregistré par le NIC

► N° de réseau

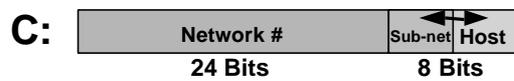
- 32 Bit Address

A:	<table border="1"><tr><td>Network #</td><td>Host #</td></tr><tr><td>8 Bits</td><td>24 Bits</td></tr></table>	Network #	Host #	8 Bits	24 Bits	23.0.0.0
Network #	Host #					
8 Bits	24 Bits					
B:	<table border="1"><tr><td>Network #</td><td>Host #</td></tr><tr><td>16 Bits</td><td>16 Bits</td></tr></table>	Network #	Host #	16 Bits	16 Bits	144.254.0.0 (>128)
Network #	Host #					
16 Bits	16 Bits					
C:	<table border="1"><tr><td>Network #</td><td>Host #</td></tr><tr><td>24 Bits</td><td>8 Bits</td></tr></table>	Network #	Host #	24 Bits	8 Bits	202.148.104.0 (>192)
Network #	Host #					
24 Bits	8 Bits					
D:	<table border="1"><tr><td>Multicast</td></tr></table>	Multicast	223.103.96.154 (>224)			
Multicast						

► N° de sous-réseau

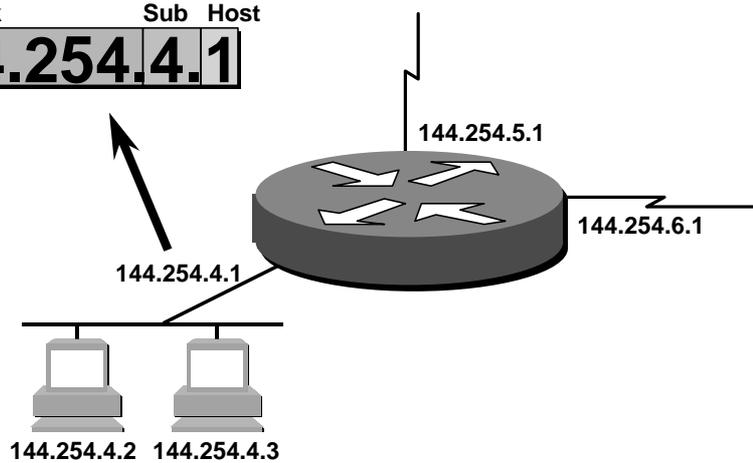


144.254.4.1



► Network/Subnet Number

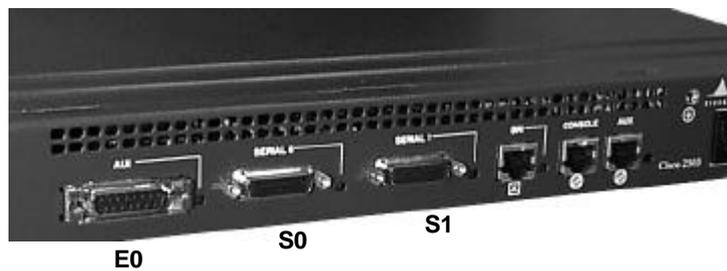
Network	Sub	Host
144	254	4.1



► Table de routage

Network	Interface	Next Saut	Metric	Age	Status
198.113.181.0	Ethernet0	192.150.42.177	[170/3047936]	02:03:50	D
198.113.178.0	Ethernet0	192.150.42.177	[170/3047936]	02:03:50	D
192.168.96.0	Ethernet0	192.150.42.177	[170/324608]	03:36:50	D
192.168.97.0	Ethernet0				C

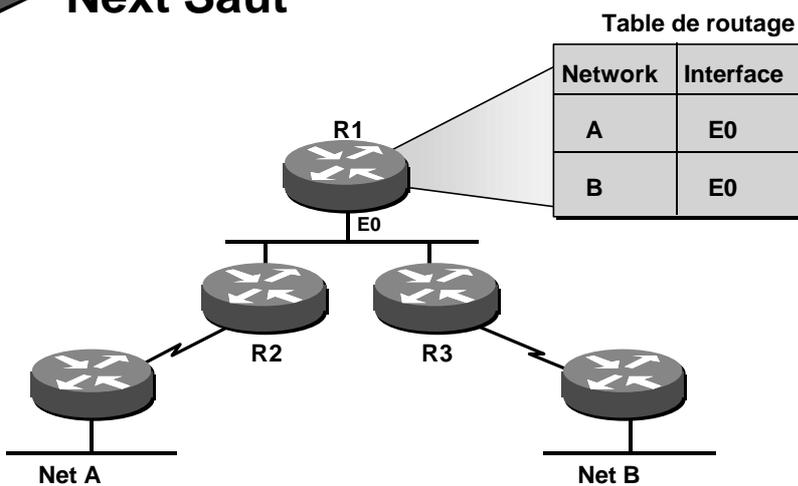
► Router Interfaces



► Table de routage

Network	Interface	Next Saut	Metric	Age	Status
198.113.181.0	Ethernet0	192.150.42.177	[170/3047936]	02:03:50	D
198.113.178.0	Ethernet0	192.150.42.177	[170/3047936]	02:03:50	D
192.168.96.0	Ethernet0	192.150.42.177	[170/324608]	03:36:50	D
192.168.97.0	Ethernet0				C

► Next Saut



Next Saut

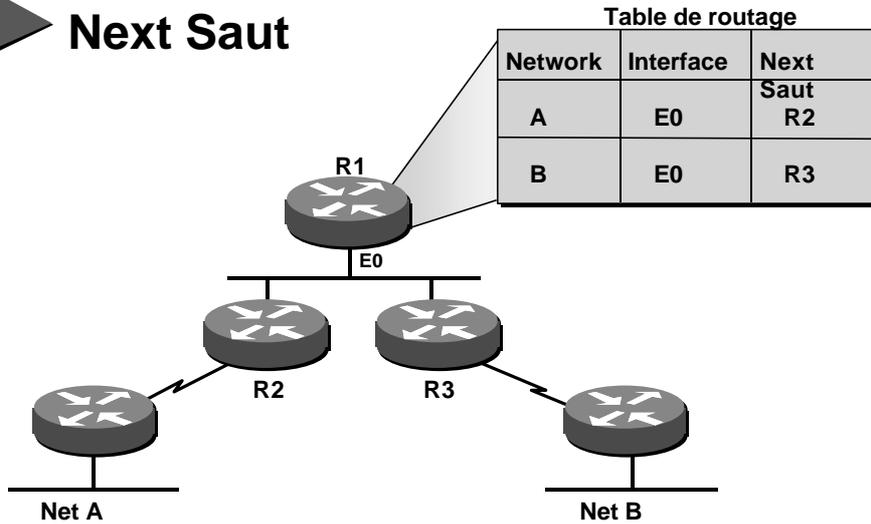
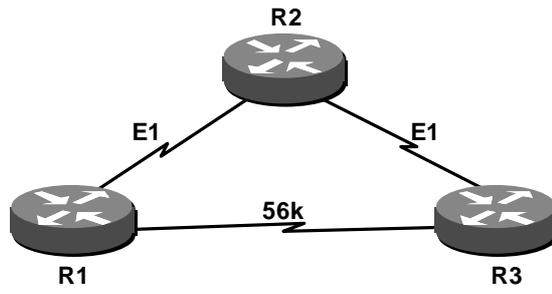


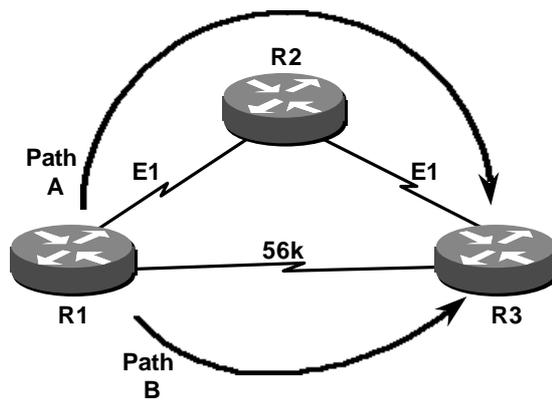
Table de routage

Network	Interface	Next Saut	Metric	Age	Status
198.113.181.0	Ethernet0	192.150.42.177	[170/3047936]	02:03:50	D
198.113.178.0	Ethernet0	192.150.42.177	[170/3047936]	02:03:50	D
192.168.96.0	Ethernet0	192.150.42.177	[170/324608]	03:36:50	D
192.168.97.0	Ethernet0				C

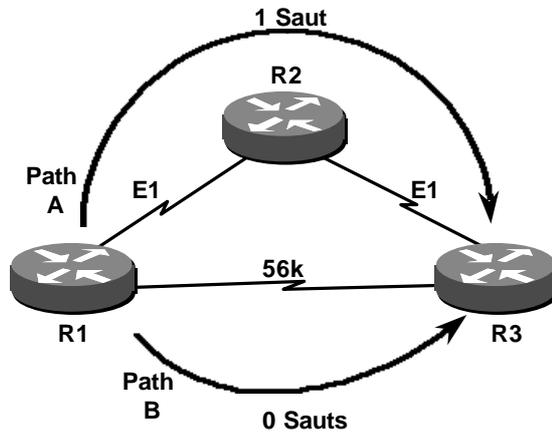
► Métrique



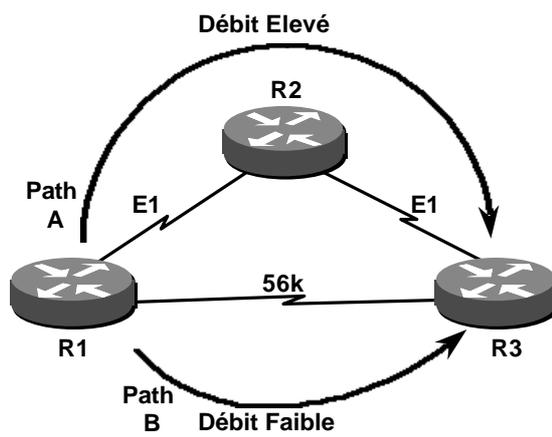
► Métrique



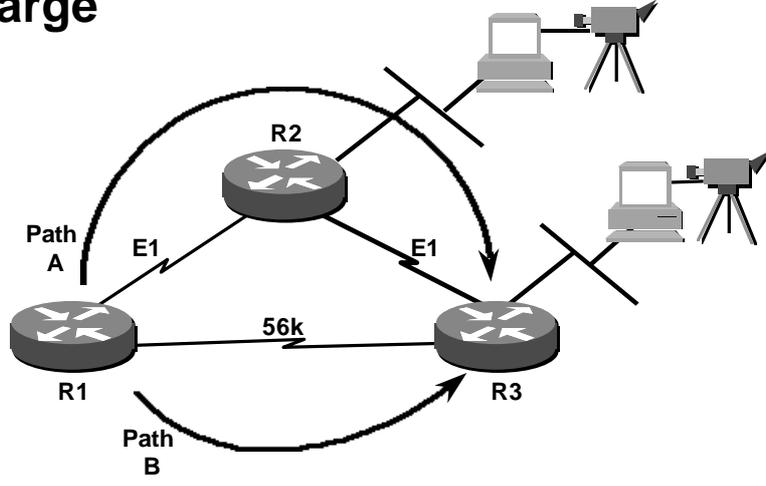
► Sauts



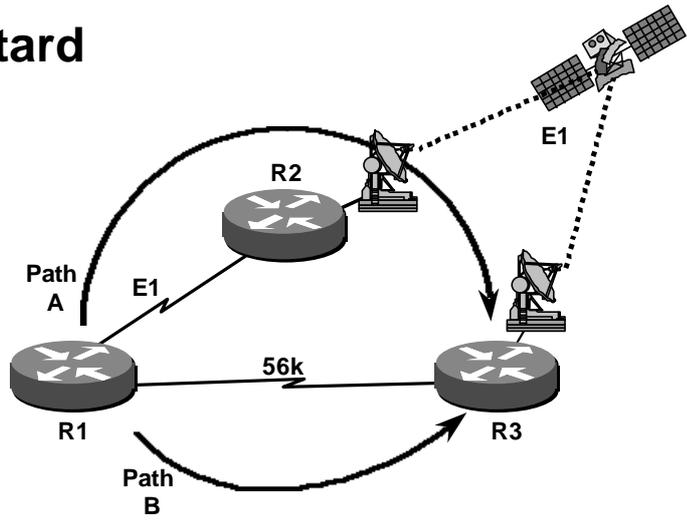
► Débit



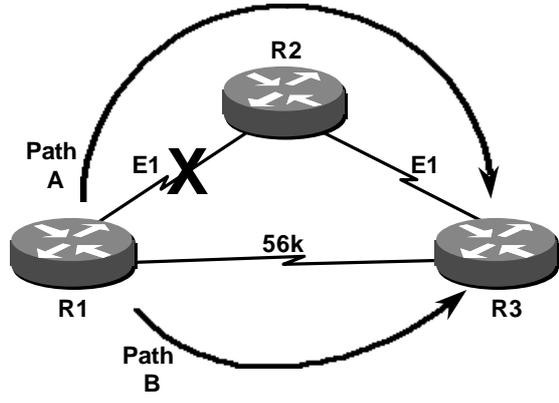
Charge



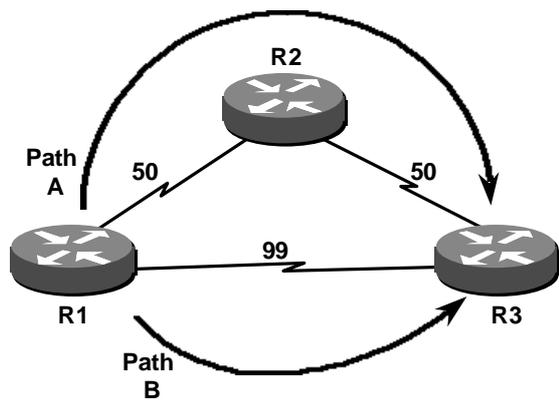
Retard



► Fiabilité



► Coût



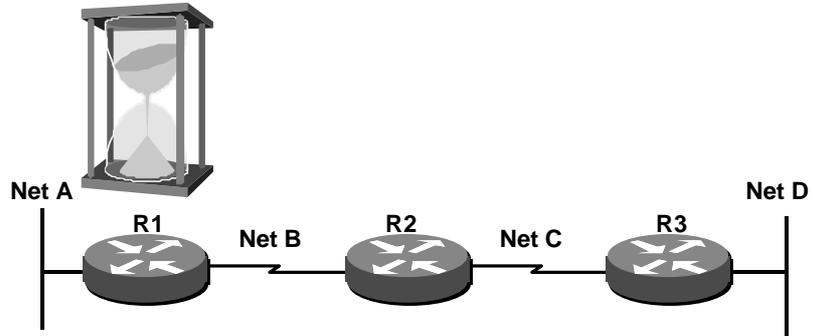
Métrique

- Sauts
- Débit
- Charge
- Retard
- Fiabilité
- Coût

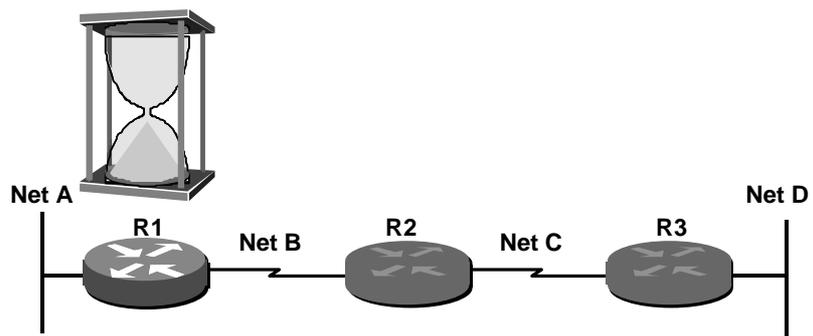
Table de routage

Network	Interface	Next Saut	Metric	Age	Status
198.113.181.0	Ethernet0	192.150.42.177	[170/3047936]	02:03:50	D
198.113.178.0	Ethernet0	192.150.42.177	[170/3047936]	02:03:50	D
192.168.96.0	Ethernet0	192.150.42.177	[170/324608]	03:36:50	D
192.168.97.0	Ethernet0				C

► Age/mise à jour périodique



► Age/mise à jour périodique



► Table de routage

Network	Interface	Next Saut	Metric	Age	Status
198.113.181.0	Ethernet0	192.150.42.177	[170/3047936]	02:03:50	D
198.113.178.0	Ethernet0	192.150.42.177	[170/3047936]	02:03:50	D
192.168.96.0	Ethernet0	192.150.42.177	[170/324608]	03:36:50	D
192.168.97.0	Ethernet0				C

► Etat/protocole

- C—connecté
- S—statique
- I—IGRP
- R—RIP
- D—EIGRP
- O—OSPF

Le processus d'acheminement

- **Destination de type unicast**
Choix de l'interface, envoi à l'adresse IP (routeur) ou ARP (station), décrémentation du TTL
- **Destination de type broadcast**
limited (255.255.255.255) : traitement
directed (subnet.255) : choix de l'interface, envoi à l'adresse IP (routeur) ou broadcast, décrémentation du TTL

Sélection de la route (1)

- **Règle 1 : concordance de base**
Appliquer le masque à chaque entrée de la table et à la destination
Conserver les entrées pour lesquelles il y a concordance et la route par défaut
- **Règle 2 : concordance maximum**
sélection de la route de masque le plus long
- **Règle 3 : Type de service**
- **Règle 4 : métrique**

Agenda

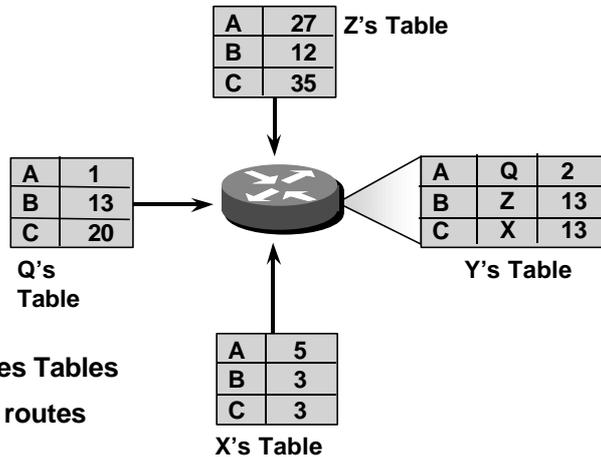
- **Qu'est ce que le routage?**
- **La table de routage**
- **Types de protocoles**
- **Les protocoles TCP/IP**
- **Le routage multiprotocole**

Protocoles de routage dynamique

- **Distance vector**
- **Link state**
- **Distance vector amélioré**

▶ Traditional Distance Vector

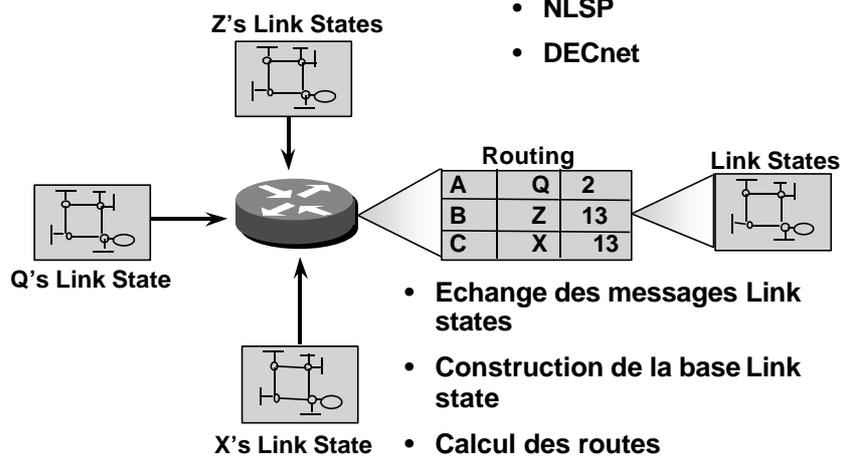
- RIP
- IGRP
- RTMP
- Novell RIP



- Echange des Tables
- Calcul des routes

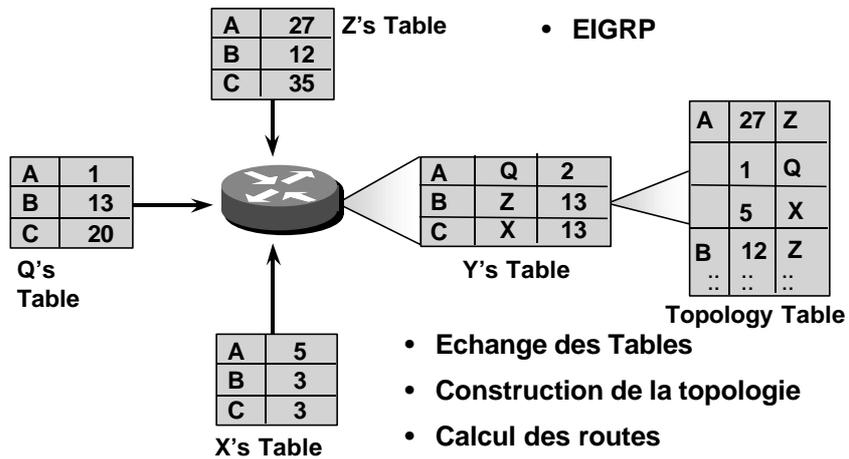
▶ Link State

- OSPF
- NLSP
- DECnet



- Echange des messages Link states
- Construction de la base Link state
- Calcul des routes

► Advanced Distance Vector



► Objectifs d'un protocole de routage

- Sélection d'un chemin optimal
- Routage sans boucle
- Convergence rapide
- Réseau de toute taille
- Limitation des tâches d'administration

► Agenda

- Qu'est ce que le routage?
- La table de routage
- Types de protocoles
- Les protocoles TCP/IP
- Le routage multiprotocole

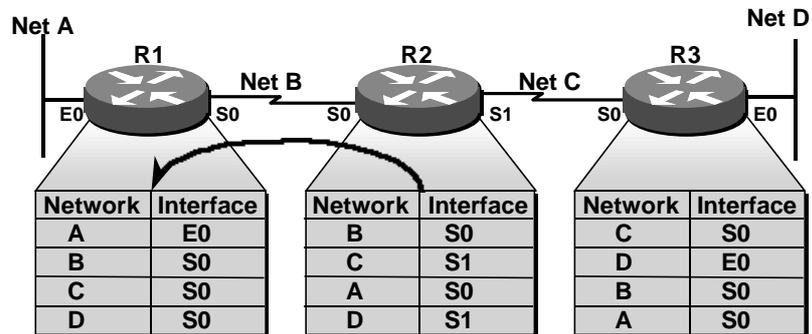
► Les protocoles TCP/IP

Distance Vector	Link-State	Distance Vector Amélioré
RIP IGRP	OSPF	EIGRP

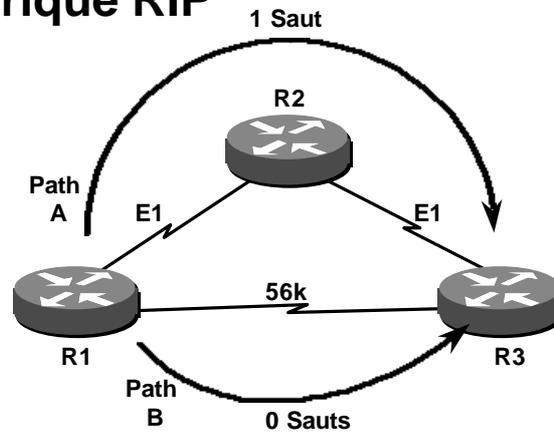
► RIP

Distance Vector	Link-State	Distance Vector Amélioré
RIP IGRP	OSPF	EIGRP

► RIP—Distance Vector



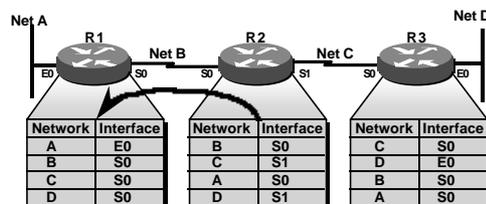
► Métrique RIP



- Sauts

► RIP Timers

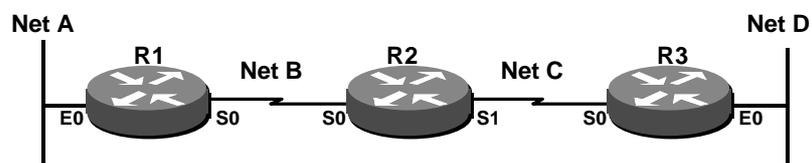
- Update = 1x 30 Sec
- Invalid = 3x 90 Sec
- Hold Down = 3x 90 Sec
- Flush = 7x 210 Sec



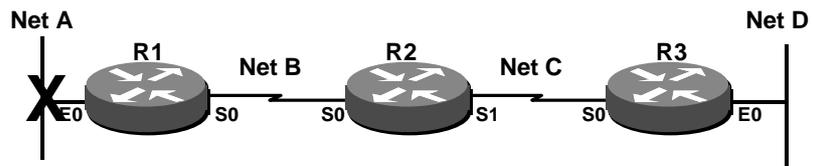
► RIP—Simple = Limitations

- Comptage à l'infini
- Boucles de routage
- Métrique limitée

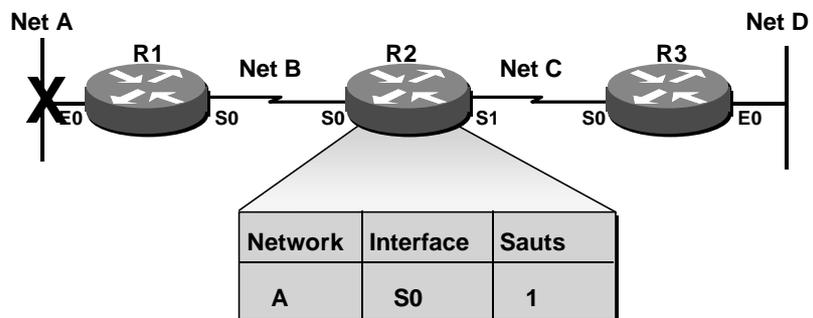
► Comptage à l'infini



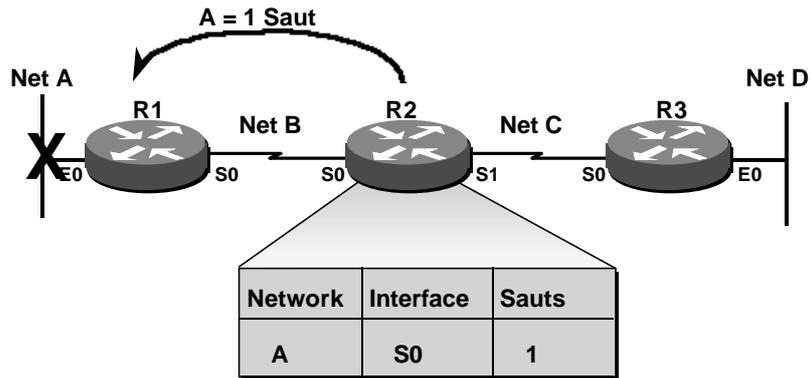
► Comptage à l'infini



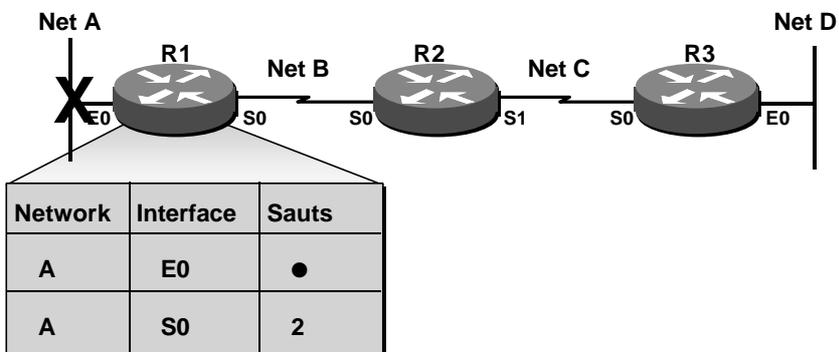
► Comptage à l'infini



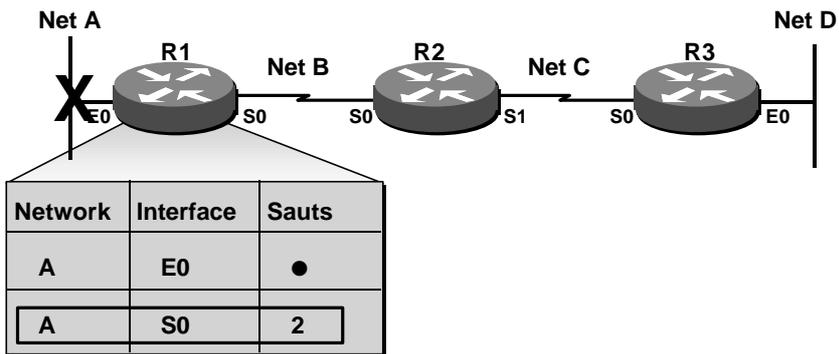
► Comptage à l'infini



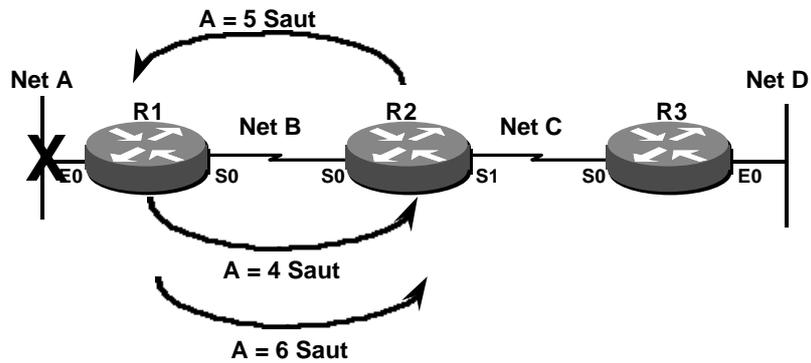
► Comptage à l'infini



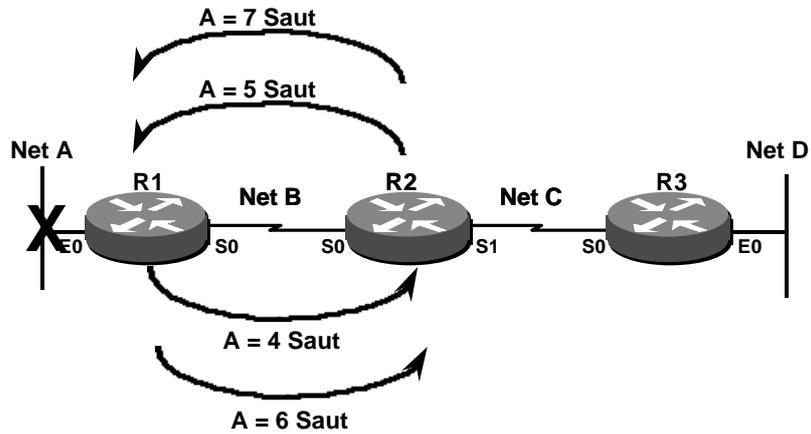
► Comptage à l'infini



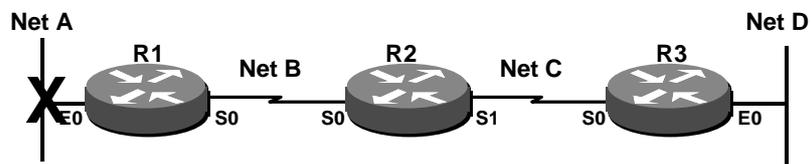
► Comptage à l'infini



► Comptage à l'infini

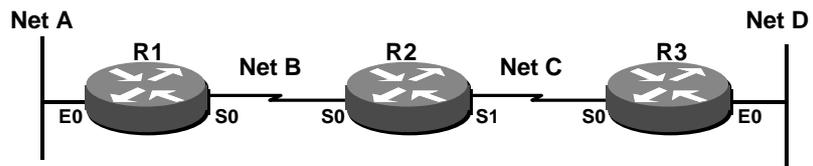


► Comptage à l'infini

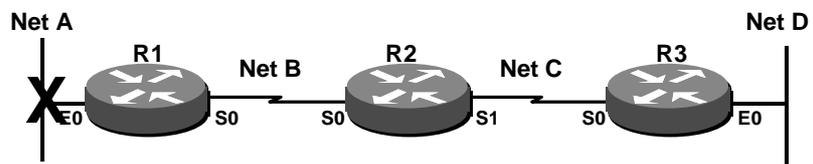


- Nombre maximum de sauts = 15
- 16 = •

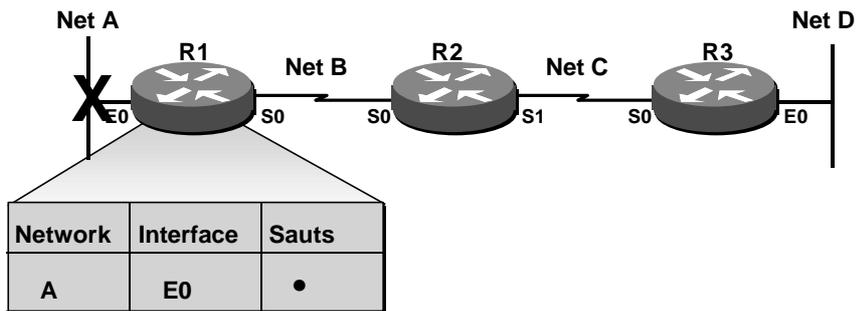
► Hold Down



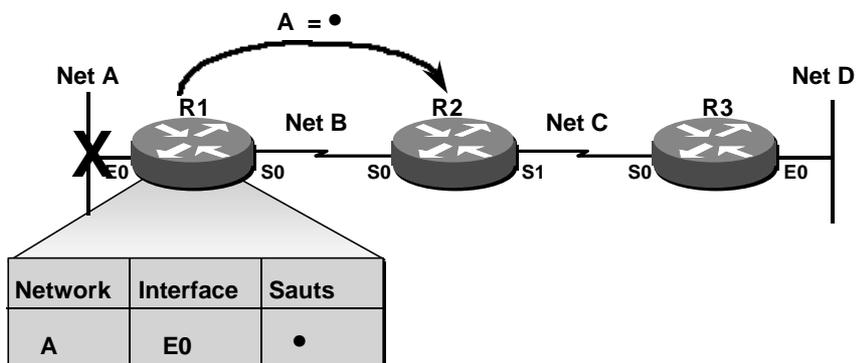
► Hold Down



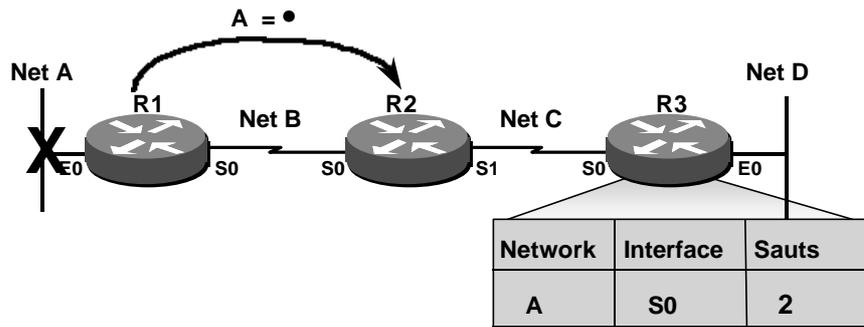
► Hold Down



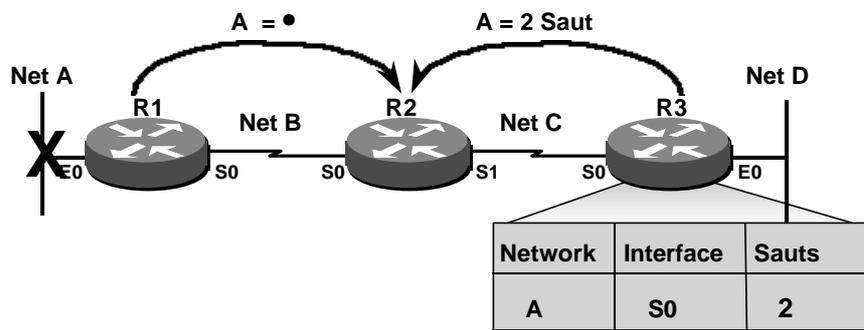
► Hold Down



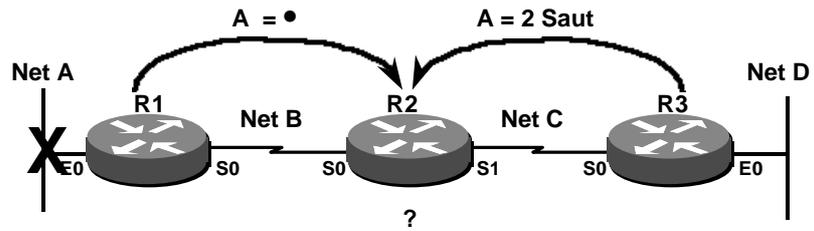
► Hold Down



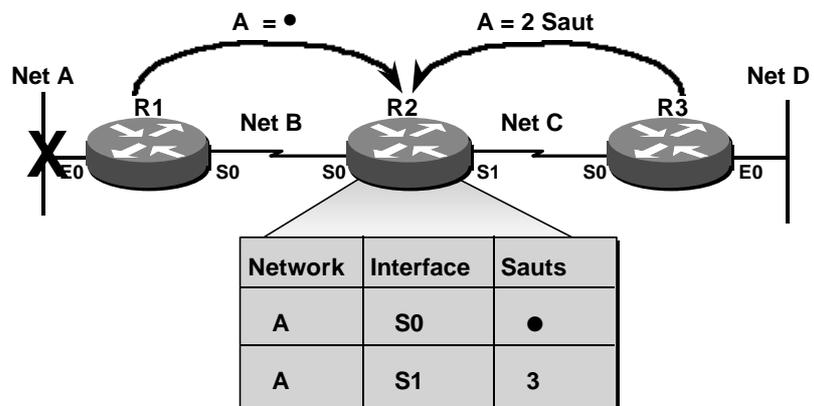
► Hold Down



► Hold Down

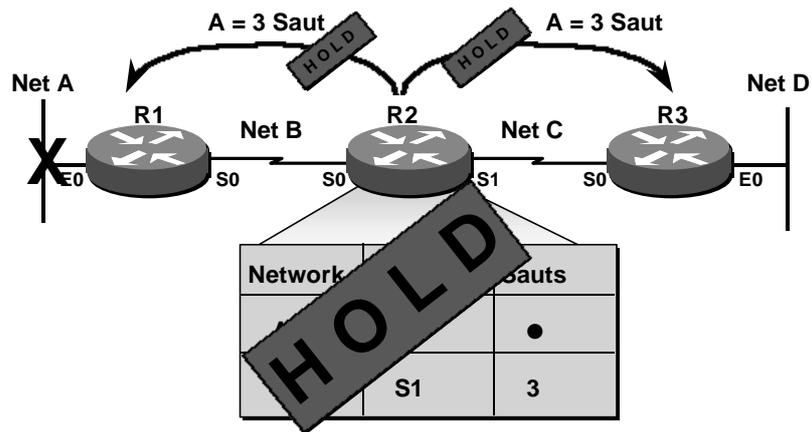


► Hold Down



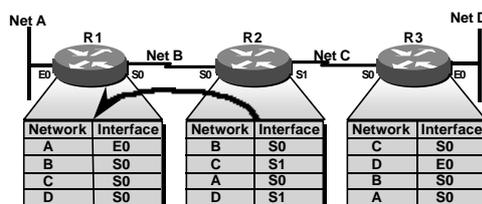
► Hold Down

- Quarantine period



► RIP Timers

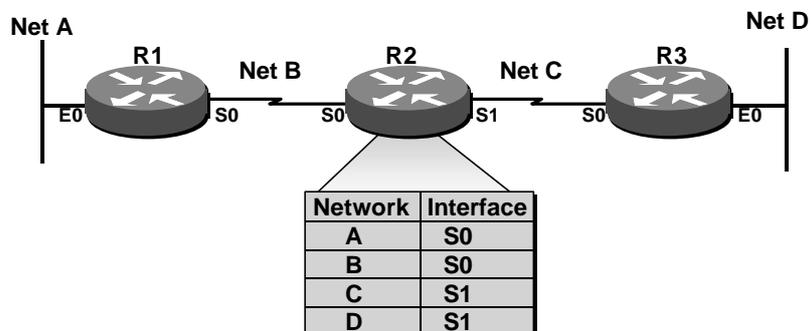
- Update = 1x 30 Sec
- Invalid = 3x 90 Sec
- Hold Down = 3x 90 Sec
- Flush = 7x 210 Sec



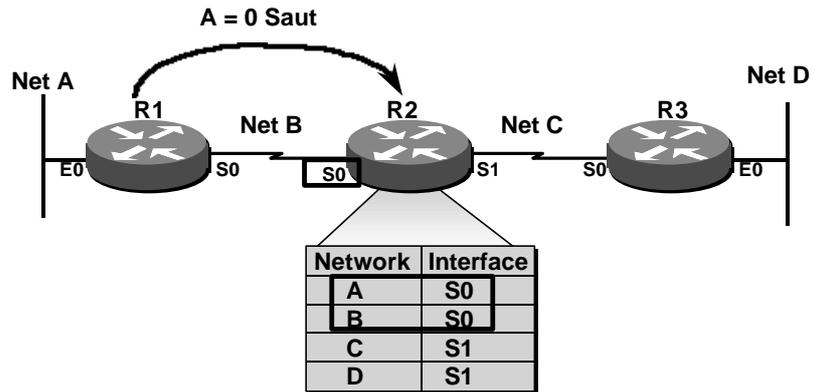
► Clivage d'Horizon

Il n'est jamais utile de renvoyer une information de routage dans la direction d'où elle provient

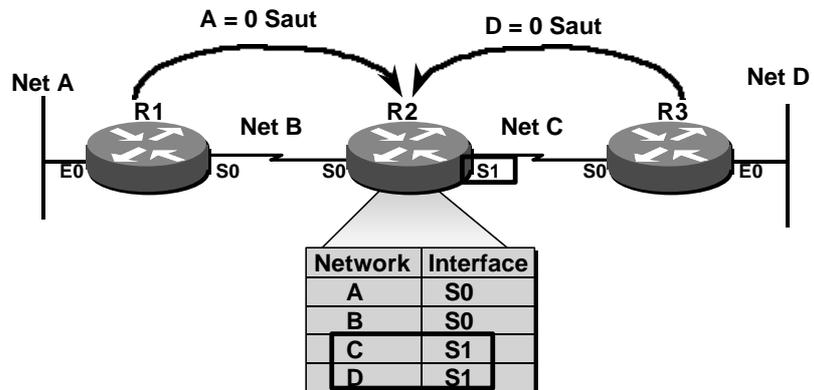
► Clivage d'Horizon



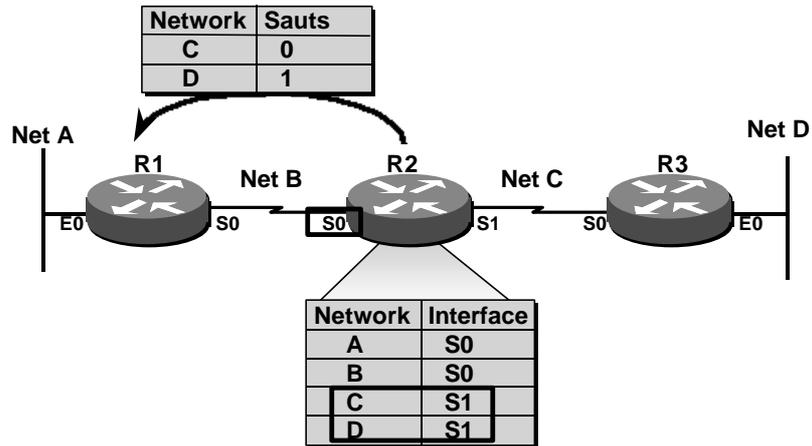
► Clivage d'Horizon



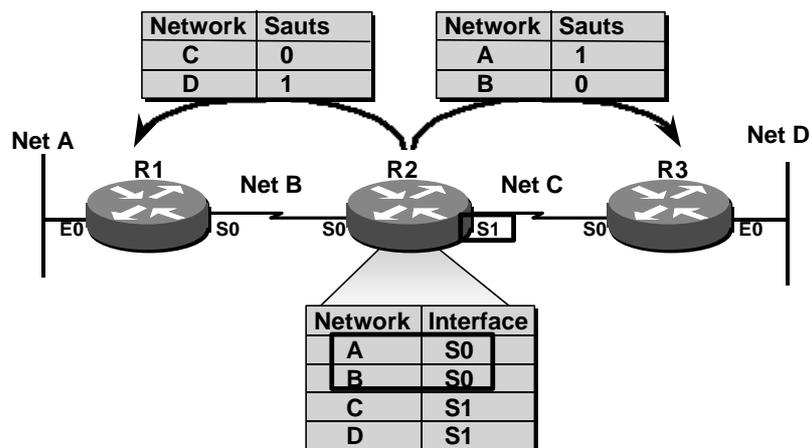
► Clivage d'Horizon



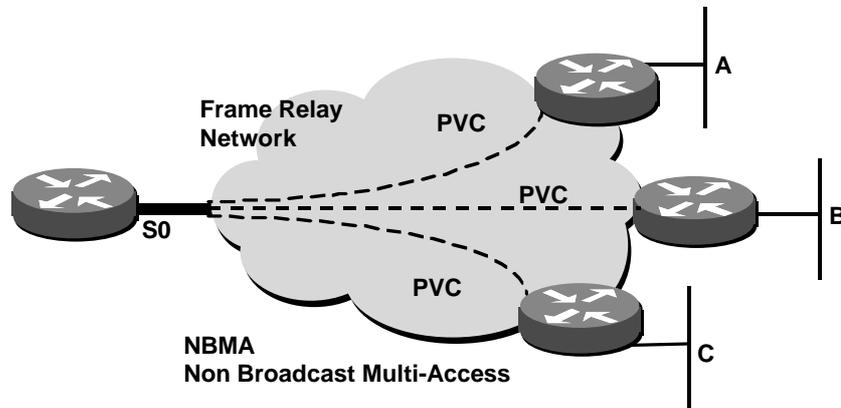
► Clivage d'Horizon



► Clivage d'Horizon



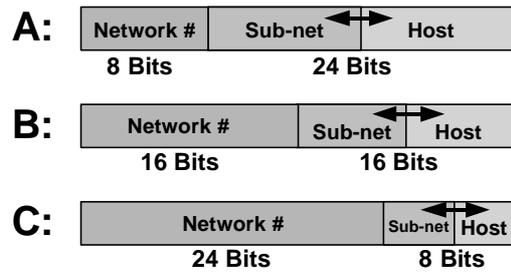
► Désactivation du Clivage d'Horizon



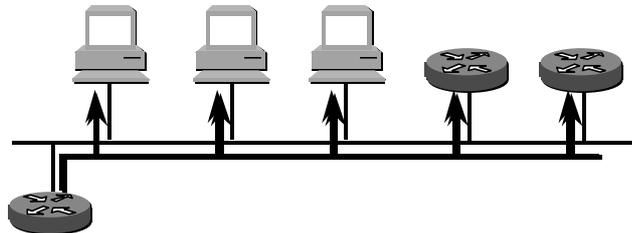
► RIP V2

- Support des masques de sousréseau
- Mise à jour du routage en multicast
- Métrique additionnelle (Débit)

► Masques de sous réseau

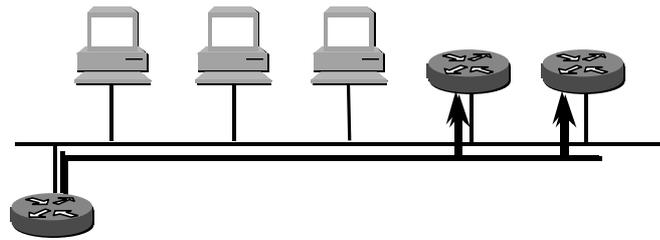


► Mise à jour par Broadcast



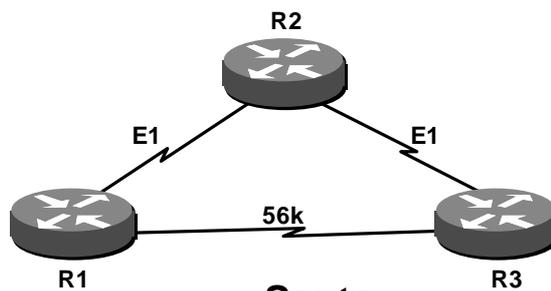
• RIP V1

► Mise à jour en Multicast



- RIP V2

► Métrique additionnelle



- Sauts
- Débit

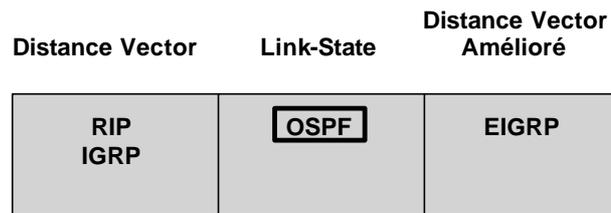
Evaluation de RIP

- **Sélection d'un chemin optimal** **D**
- **Routage sans boucle** **B**
- **Convergence rapide** **C**
- **Réseau de toute taille** **D**
- **Limitation des tâches d'administration** **A**

Quand utiliser RIP?

- **Implementation rapide**
- **Bon pour des liaisons stables**
- **Bon pour les petits réseaux**
- **Environment UNIX et multiconstructeur**

▶ OSPF



▶ OSPF

- **Link state**
- **Normalisé (RFC 1247)**
- **Plus récent que IGRP**
- **Algorithme SPF**

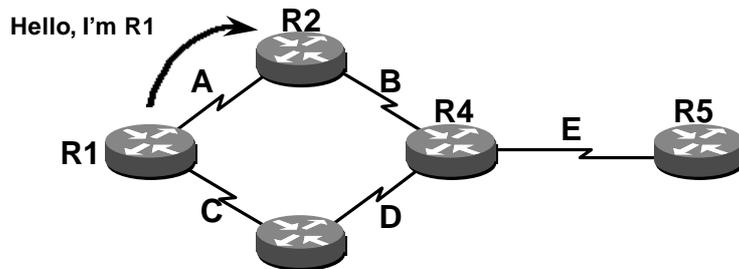
Métrieque OSPF

- **Evaluation des interfaces selon une métrieque par défaut**
 - Au démarrage : Débit
- **configuration**

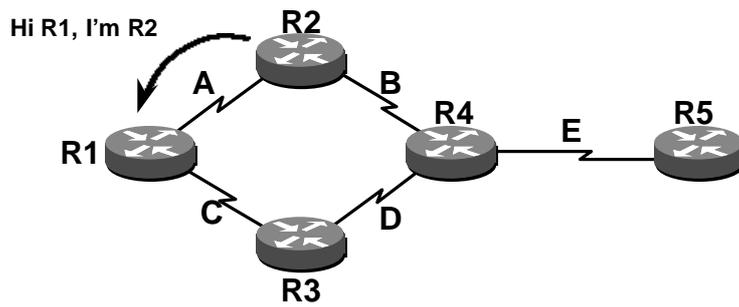
Routage Link State

- **Découverte des voisins**
- **Construction du LSP**
- **Distribution du LSP**
- **Calcul des routes**

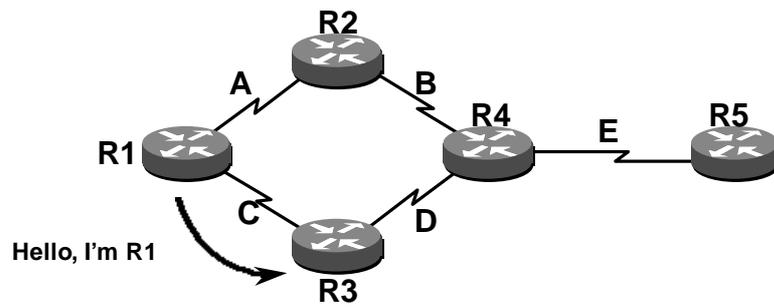
► Découverte du voisin



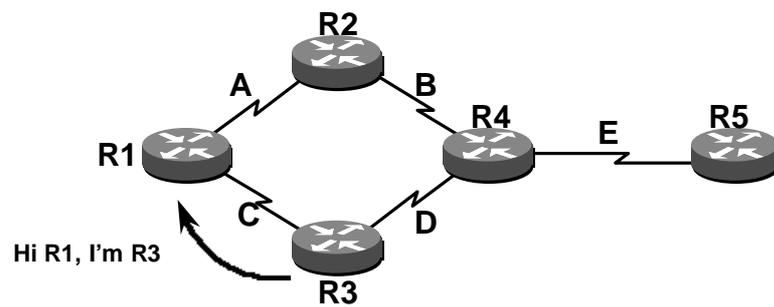
► Découverte du voisin



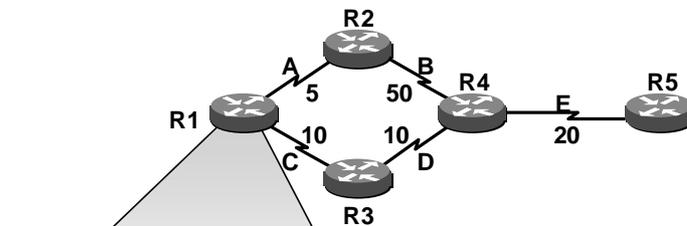
► Découverte du voisin



► Découverte du voisin



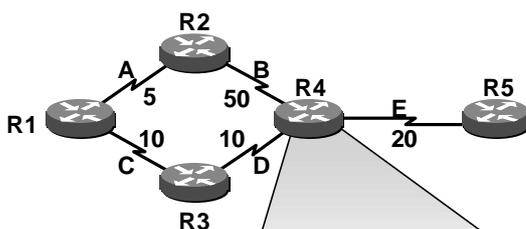
► Construction d'un LSP



From	To	Link	Cost
R1	R2	A	5
R1	R3	C	10

Link State Packet

► Construction d'un LSP



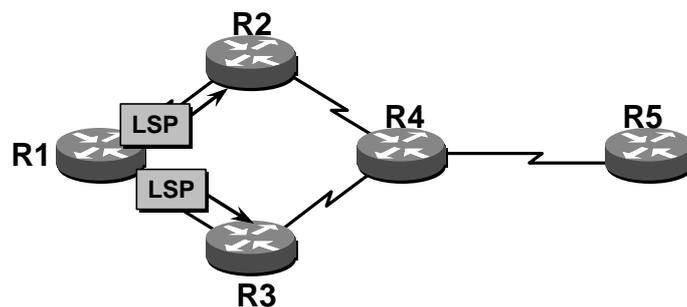
From	To	Link	Cost
R4	R2	B	50
R4	R3	D	10
R4	R5	E	20

Link State Packet

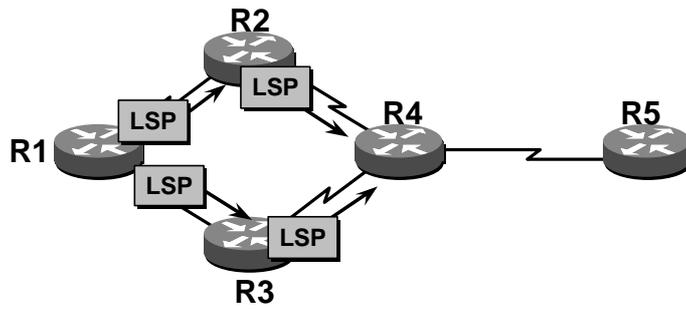
► Distribution du LSP

- Tâche critique et complexe
- Cohérence
- Rapidité
- Ne doit pas surcharger le réseau

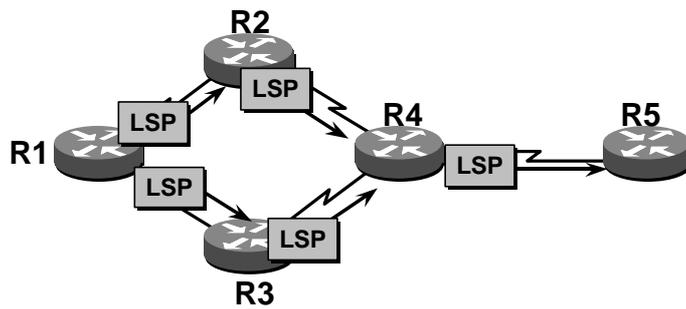
► Distribution du LSP



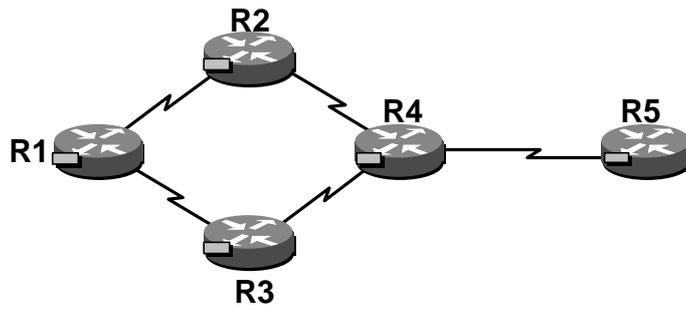
► Distribution du LSP



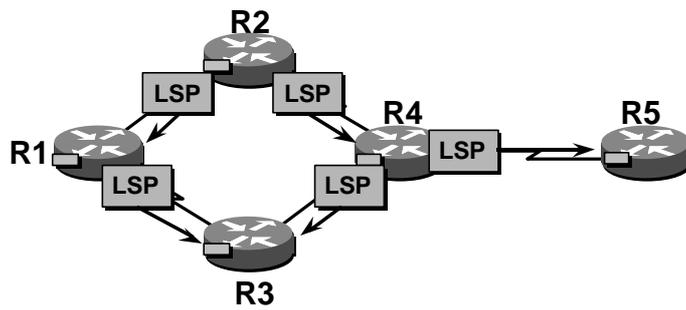
► Distribution du LSP



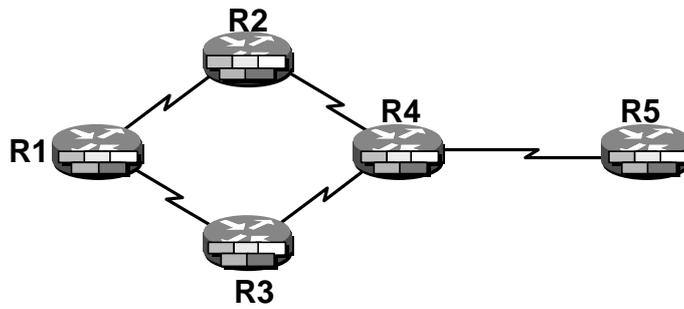
► Distribution du LSP



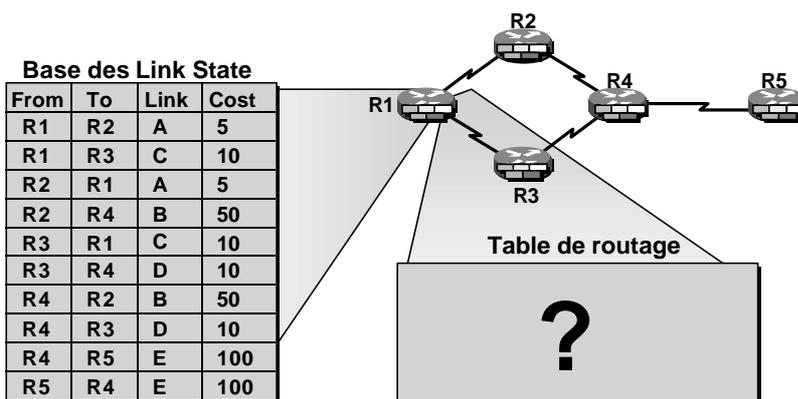
► Distribution du LSP



► Distribution du LSP

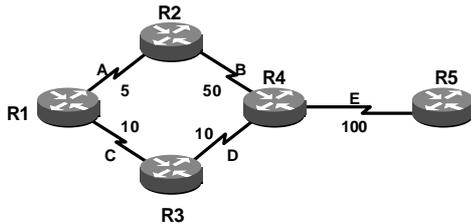


► Calcul des routes



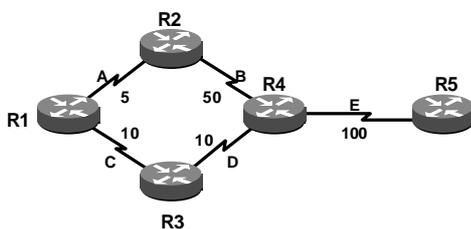
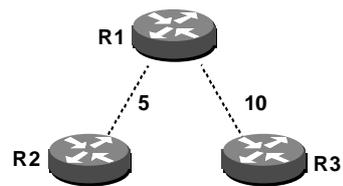
► Calcul des routes

- Chaque routeur commence avec soi-même à la racine



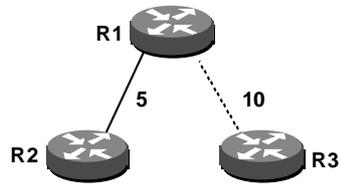
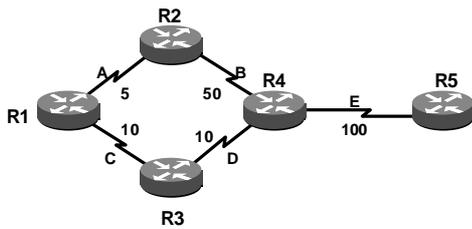
► Calcul des routes

- Ajouter R2 et R3 à l'arbre



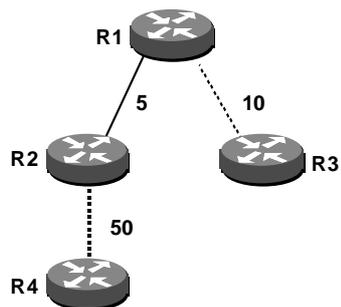
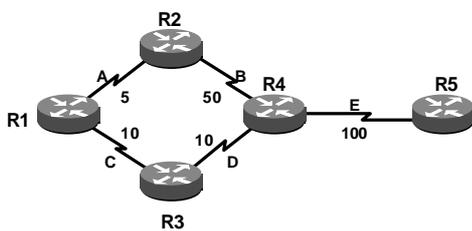
► Calcul des routes

- Examiner R2'



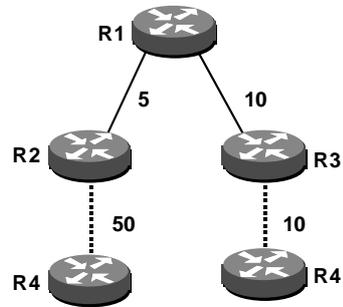
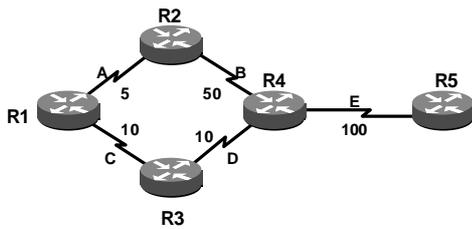
► Calcul des routes

- Ajouter R4



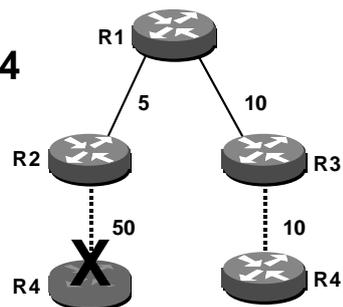
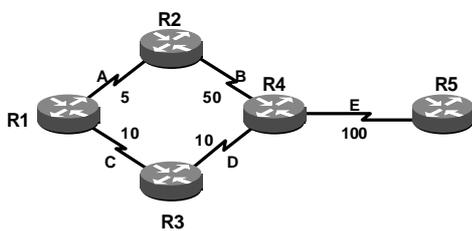
► Calcul des routes

- Examiner R3



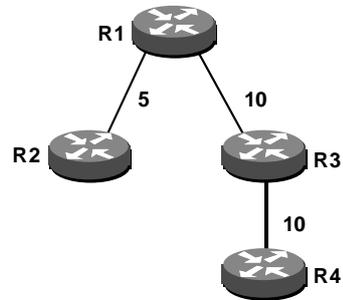
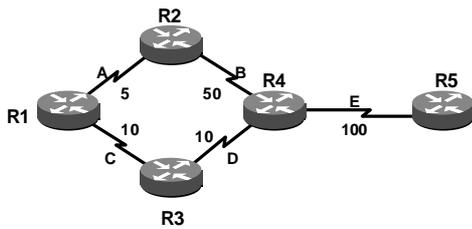
► Calcul des routes

- Meilleure route vers R4



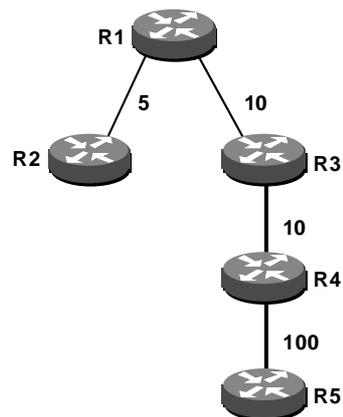
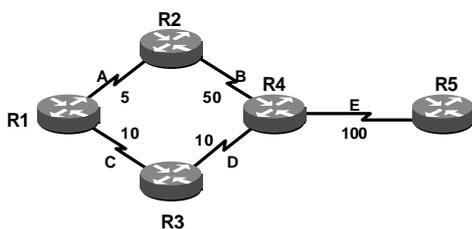
► Calcul des routes

- Examiner R4



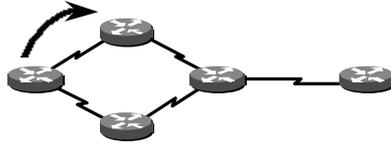
► Calcul des routes

- Ajouter R5

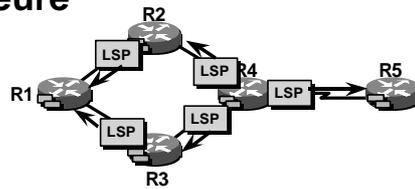


► Timers OSPF

- Hello = 10 Sec



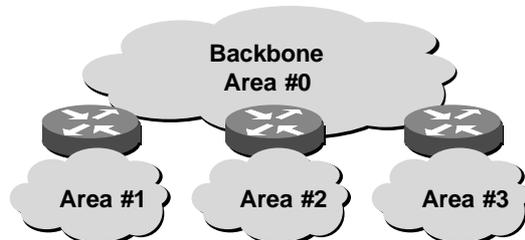
- LSP Updates = 1 Heure



► En cas d'incident

- Inondation de nouveaux LSP
- Tous les routeurs recalculent leurs tables de routages

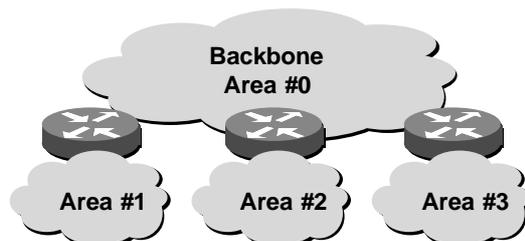
► Zones OSPF (areas)



- **Règles**

Toutes les zones ont une connexion au backbone
Le backbone doit être connexe

► Pourquoi des zones?



- La topologie d'une zone est invisible en dehors de la zone
- Reduction du trafic de routage

OSPF Report Card

- **Sélection d'un chemin optimal** **B**
- **Routage sans boucle** **A**
- **Convergence rapide** **A**
- **Réseau de toute taille** **A**
- **Limitation des tâches d'administration** **D**

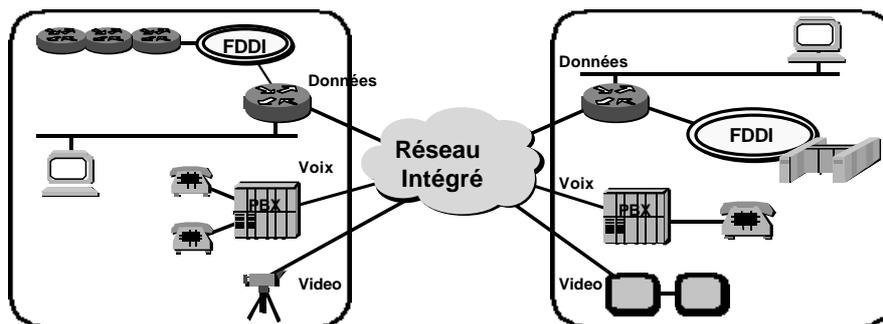
Quand utiliser OSPF

- **Réseaux Complexes**
 - Topology restrictive
 - Additional network design
- **VLSM**
- **Besoin de convergence rapide**
- **Multiconstructeur**

ATM

1

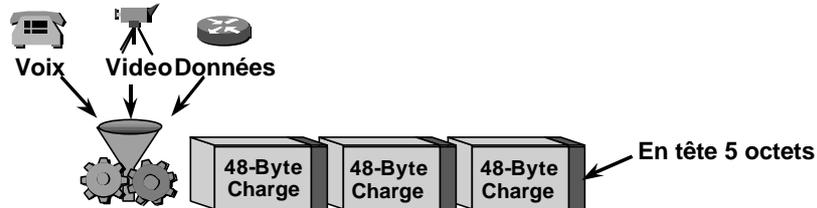
Intégration de services



- Voix, Données, video
- RNIS
- RNIS Large bande

2

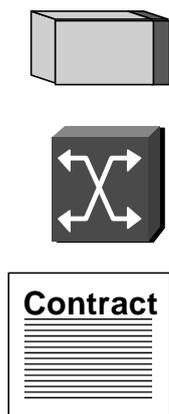
Caractéristiques de l'ATM



- Applicable aux réseaux à grande distance et LAN
- Débits allant de quelques Mbps à plusieurs Gbps
- Intégration Voix, vidéo, et Données
- Retards déterministes

3

ATM : les bases

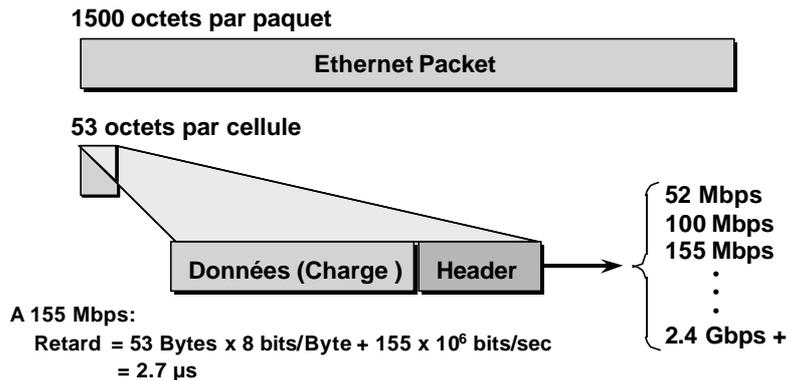


- Cellules de taille fixe
- fragmentation et réassemblage au niveau terminal
- Réalisation matérielle
- Routage fixe après connexion de bout en bout
- Orienté Connection
- Qualité de Service (QoS) contractuelle : négociation à la connexion

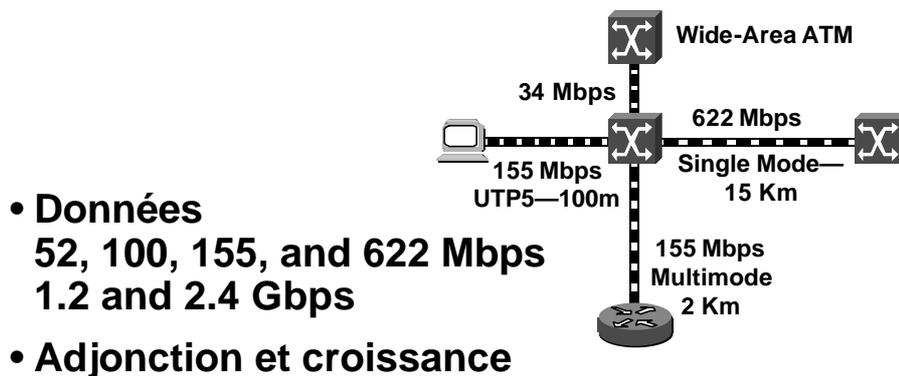
4

ATM : performances temporelles

- Supports des transferts isochrones et asynchrones



Une même technologie de commutation pour différents débits

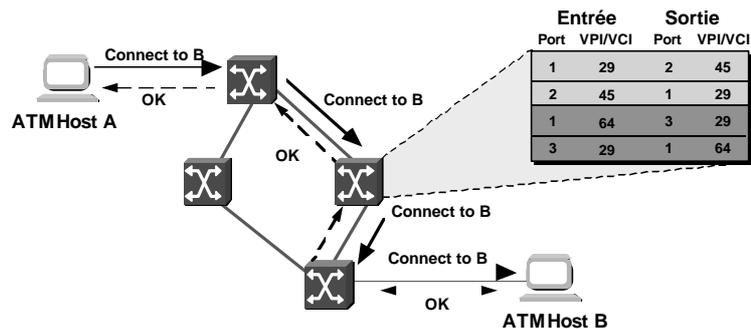


ATM : Etablissement de la Connection

- **Commutation de circuit virtuel (SVCs)**
Signalisation et adressage ATM
- **Connection Permanente (PVCs)**
application network management
- **Routage par les identifiieurs de connexion contenus dans l'en-tête de cellule**
Virtual Channel Identifier (VCI)
Virtual Path Identifier (VPI)

7

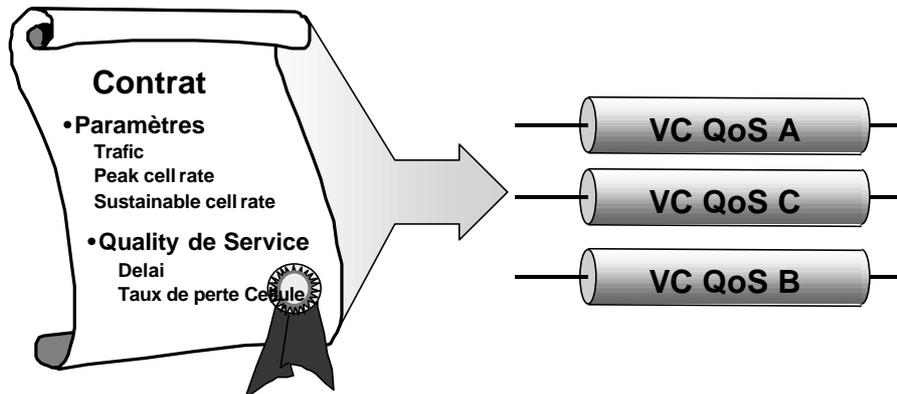
Etablissement d'une connexion SVC



- **Routage de la signalisation : établissement du chemin**
- **Connexion acceptée/rejetée**
- **Mise à jour de la table de traduction dans chaque commutateur**
- **Les données suivent le chemin établi**

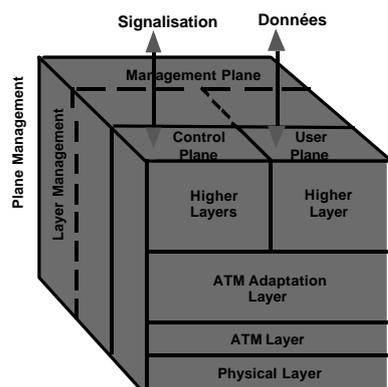
8

Contrats de QoS



9

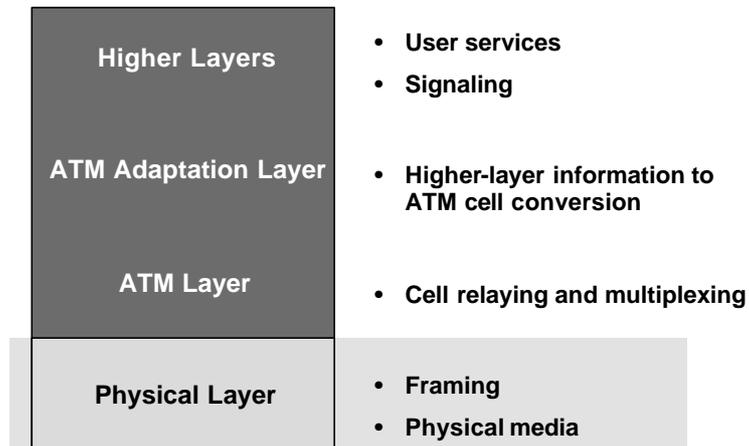
ATM : le Modèle de Référence



- Données, Voix, video
- Signalisation
- information des couches hautes pour la conversion en cellules
- relayage and multiplexage des cellules
- Tramage
- Adaptation au medium Physique

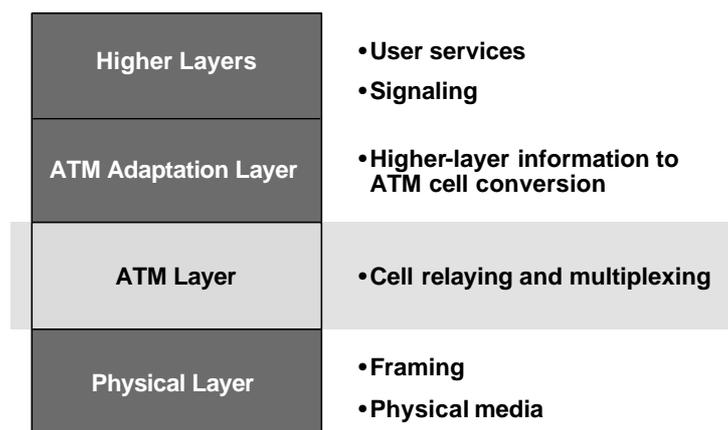
10

Technologie: Architecture des Protocoles



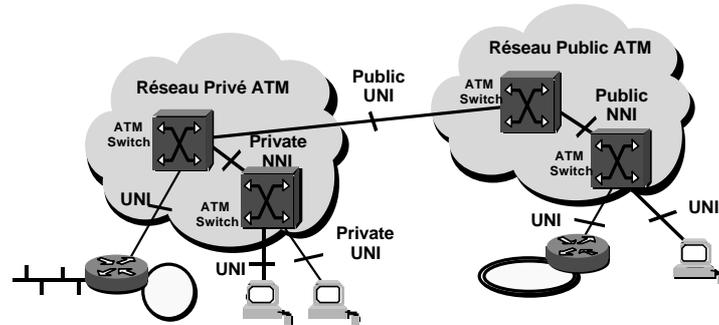
11

Technologie: Architecture des Protocoles



12

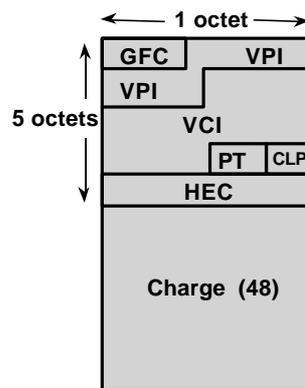
La couche ATM : Interfaces Réseau



- User-Network Interface (UNI)
- Network-Network Interface (NNI)

13

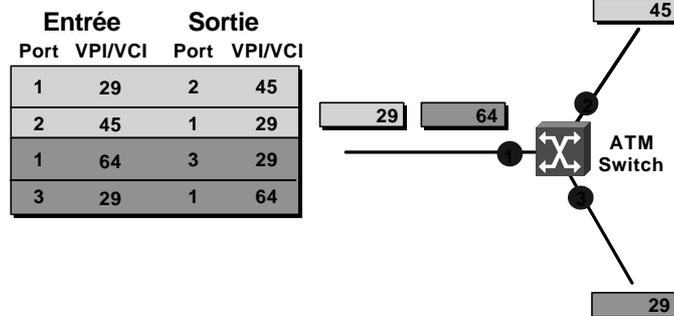
Couche ATM : Format Cellule



- UNI
 - Generic Flow Control (GFC)
 - Virtual Path/Channel Identifier (VPI/VCI)
 - Charge Type (PT)
 - Données utilisateur ou flux maintenance
 - Congestion rencontrée
 - End of message (AAL 5)
 - Cell Loss Priority (CLP)
 - Header Error Control (HEC)
- NNI
 - Pas de champ GFC
 - Champ VPI plus large (trunking)

14

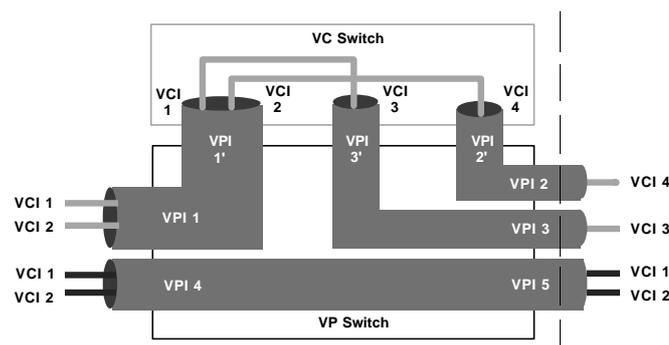
Couche ATM : Relayage de Cellule



- **Connections Virtuelles VPI/VCIs sur les differents ports**
- **Chaque commutateur change la valeur des VPI/VCI**
- **la valeur des VPI/VCI est unique sur chaque interface**

15

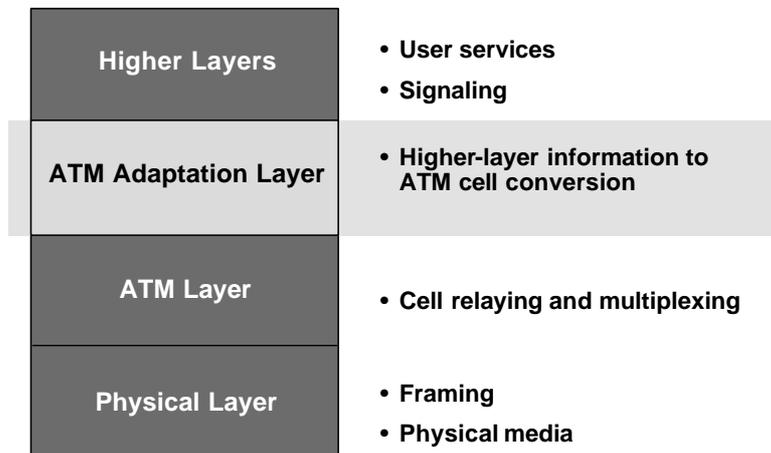
Virtual Paths et Virtual Channels



- **Les conduits virtuels (Virtual paths) regroupent plusieurs circuits virtuels (virtual channels)**
- **Les cellules vides sont marquées par VPI/VCI=0**

16

ATM Protocol Architecture



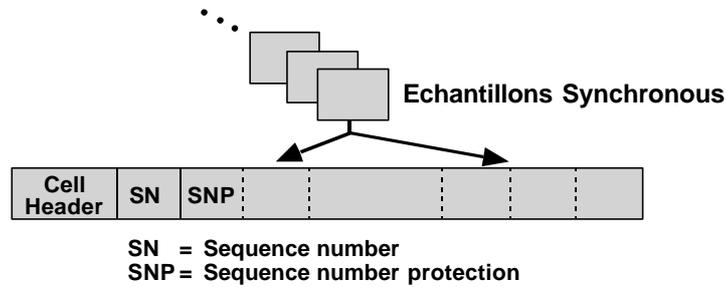
17

ATM Adaptation Layer (AAL) B-ISDN Classes of Services

Class:	A	B	C	D
Exemples	Voix / Video	Paquet Video	Données IP, X.25	Données SMDS
Connection Mode	Connection-Oriented			Connectionless
Débit	Constant	Variable		
ATM Adaptation Layer	AAL 1	AAL 2	AAL 3/4 AAL 5	AAL 3/4

18

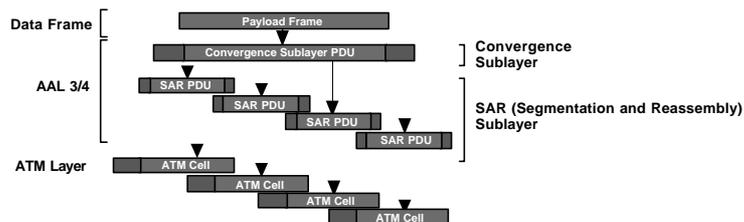
AAL 1



- Cellules envoyées à intervalles réguliers
- Données synchrones
délai de paquetisation
- Normalisation de récupération d'horloge nécessaire

19

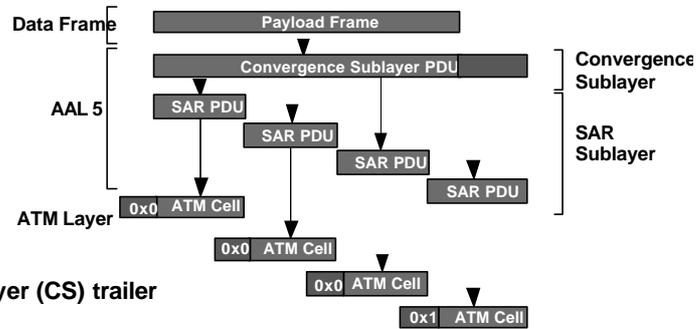
AAL 3/4



- **Convergence Sublayer (CS) header/trailer**
Marquage de début/fin
Longueur
- **Segmentation And Reassembly (SAR) header/trailer**
Type: BOM, COM, EOM, SSM
Sequence number
Message Identifier (MID)
CRC-10
- Charge : 44 octets
- Used for SMDS/CBDS services

20

AAL 5



- **Convergence Sublayer (CS) trailer**
Longueur, CRC-32
- **En tête de Cellule**
Type: empty, not EOM, EOM
- **Charge : 48 bytes**
- **AAL la plus courante pour les Données (IRLE)**

21

Le Relais de trames

Position du problème

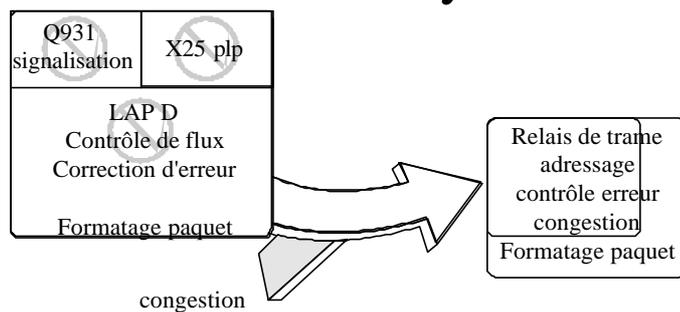
- Autrefois les lignes étaient non fiables
- **X.25**: Une technique destinée à travailler sur les lignes de manière efficace
- Mais
 - overhead de traitement
- "Aujourd'hui": Amélioration des techniques de transmission (fibre, numérisation...)
- Amélioration de la commutation de paquet :
 - Réduction des fonctionnalités offertes
 - 2 couches au lieu de 3
 - Routage dans la couche 2
 - Contrôle de bout en bout

FRAME RELAY

La nouvelle génération des protocoles de liaison

- Robustesse ou simplicité
- La robustesse garantit la fiabilité de bout en bout
 - utilisation sur les lignes analogiques bruitées
- La simplicité sera visée sur les lignes numériques fiables
- La fiabilité sera obtenue par les protocoles de niveau supérieur

Frame Relay

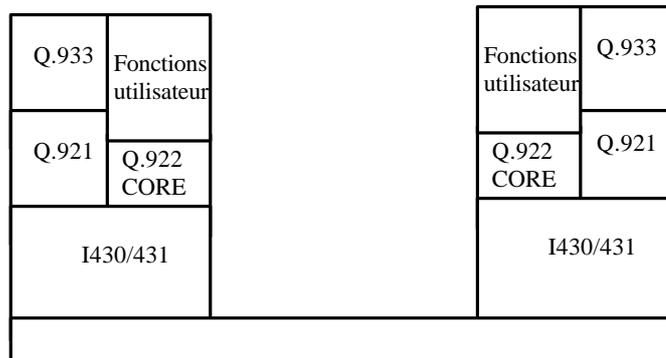


- Diminution des coûts d'accès
- Augmentation de l'efficacité
- Accroissement des performances vues des applications

Relais de trames : principes

- Réseau de niveau 2
 - ajout de fonctions de niveau 3 : adressage, routage, contrôle de flux
- Norme Q922
 - Délimitation, alignement et transparence
 - Multiplexage et démultiplexage
 - Vérifications de vraisemblance (longueur, erreurs...)
 - Contrôle de flux de bout en bout

Environnement du FR

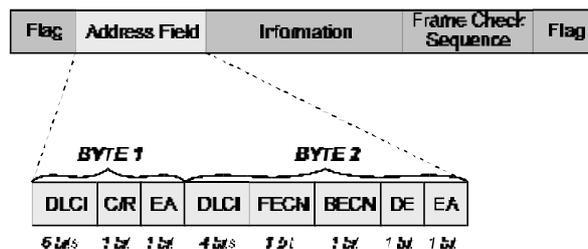


Implantations industrielles sur ISDN ou T1/E1

Les normes

- ANSI
 - T1.606: Architecture and service
 - T1.606A: Congestion management
 - T1.617: Signalling specification
 - T1.618: Core aspects of protocol
- CCITT:
 - 1.122: Framework for frame relay
 - 1.233: Frame relay bearer service
 - Q.922: Core protocol
 - Q.933: Access signalling

Les PDU



FLAG packet delimiter

Address Field adressage et contrôle de la congestion

EA Extension d'Adresse

C/R Command/Response (non normalisé)

DLCI Data Link Connection Identifier

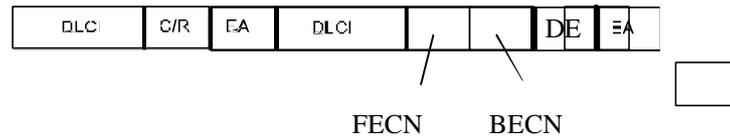
DE Discard Eligibility

BECN Backward Explicit Congestion Notification

FECN Forward Explicit Congestion Notification

Information longueur variable, < 4000 octets, FCS 16 bit CRC

Frame Relay (I.122)



FECN: Forward explicit congestion notification bit positionné par le réseau pour indiquer la congestion du réseau au dispositif appelé

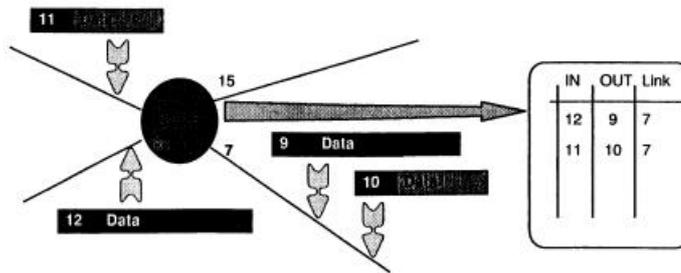
BECN: Backward explicit congestion notification bit positionné par le réseau pour indiquer la congestion du réseau au dispositif appelant

DE: Discard Eligibility bit
Positionné par le dispositif connecté au réseau pour indiquer au réseau les trames à purger en cas de congestion

Format de la trame FR

0	1	1	1	1	1	1	1	0
DLCI (msb)						CR	EA	
DLCI (lsb)				FECN	BECN	DE	EA	
Données utilisateur								
FCS								
0	1	1	1	1	1	1	1	0

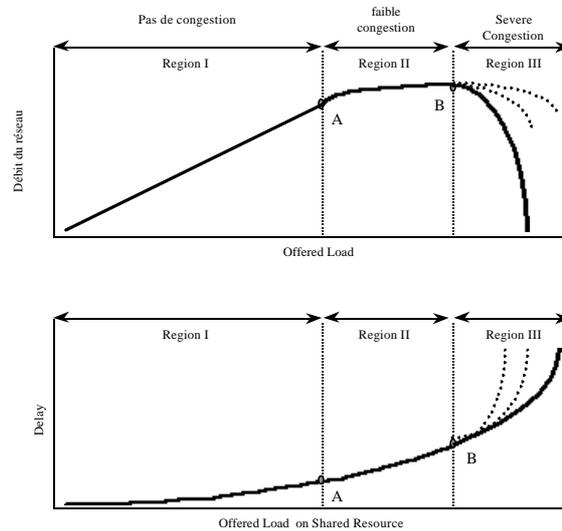
Le routage dans frame relay



Contrôle d'erreur

- Principe de base : en cas de problème avec une trame, la détruire!
- Les protocoles de bout en bout au niveau supérieur sont responsables de la détection des trames manquantes et demandent leur réémission
- La détection d'erreur étant effectuée de bout en bout et non de noeud à noeud une erreur bit peut causer un retard important
 - acceptable uniquement sur un réseau fiable
- Causes de rejet:
 - Erreurs bit : Relativement rare
 - Encombrement réseau : Plus vraisemblable (bouffées de trafic)

Relation entre retard et charge réseau

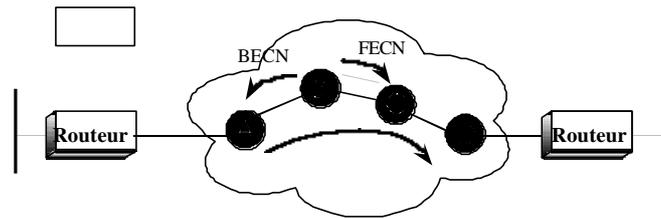


Congestion

- La congestion survient quand le réseau ne peut plus acheminer le trafic offert
- Pendant les périodes non congestionnées le réseau achemine un trafic égal à la charge offerte
- En A, "congestion faible" ; seules quelques trames sont rejetées (congestion locale)
- En B, "congestion sévère" ; les demandes de retransmission s'ajoutent au trafic offert
- La stratégie : Une fois en A, ralentir le trafic et ne jamais arriver en B

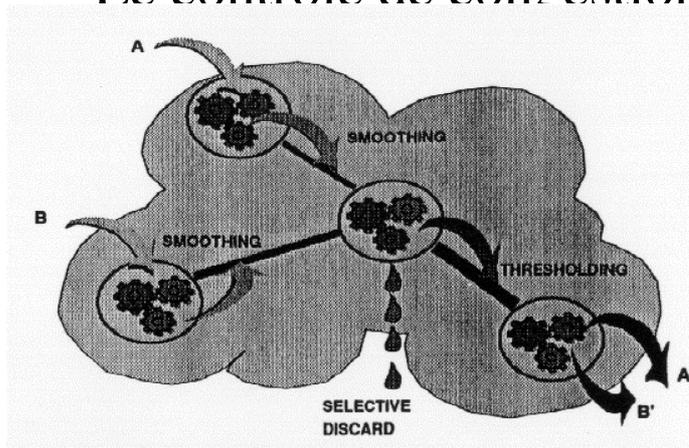
La notification explicite de Congestion

- Les bits de congestion sont positionnés par le réseau
 - Les spécifications donnent des suggestions de réponse aux bits ECN mais aucune action spécifique n'est exigée ...

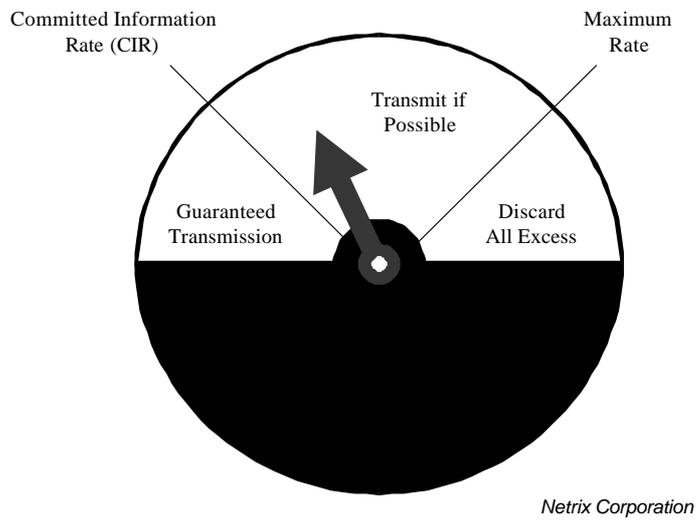


Risque d'incohérence : destinataire niv 3 essaie de ralentir le réseau
émetteur niv 4 continue à émettre : augmentation congestion
Appletalk vs dectnet

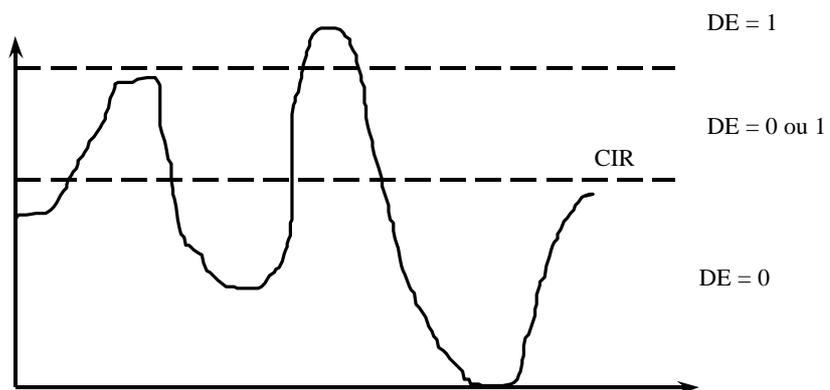
Le contrôle de congestion



Frame Relay CIR



FR : le contrôle de congestion



Le DE-bit

- Discard Eligibility bit : il assure l'équité d'accès au réseau
- Les terminaux demandent des bouffées de bande passante qui varient en durée et en fréquence (terminal point de vente vs. CAD/CAM workstation). Le réseau doit assurer que les utilisateurs qui ont des besoins importants en débits ne bloquent pas les autres.
- L'équipement utilisateur ou le réseau peuvent positionner le DE-bit:
 - 1: priorité basse, détruire si nécessaire
 - 0: haute priorité
- Le réseau peut changer le DE et le mettre à 1 en fonction du CIR
 - le CIR est Défini à l'abonnement (PVC) ou à l'établissement (SVC)

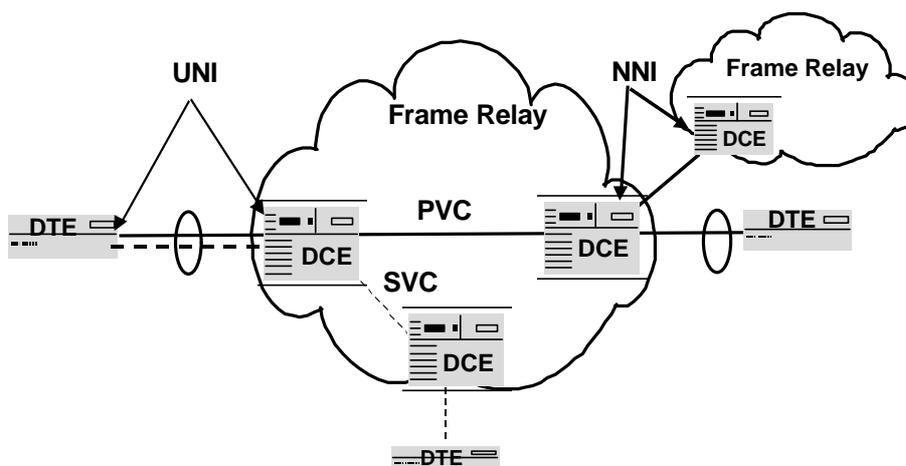
CLLM

- Consolidated Link Layer Management
- Le problème
 - liaisons unidirectionnelles donc risque de retard dans la transmission du BECN
- Signalisation entre noeuds
 - DLCI = 1023
 - envoi à tous les voisins des DLCI congestionnés

L'architecture

- Réseaux privés
- Réseaux publics
- Mélange réseaux privés/publics
- Interface
 - UNI
 - NNI
- Nécessité d'une signalisation
 - mécanisme minimal : LMI

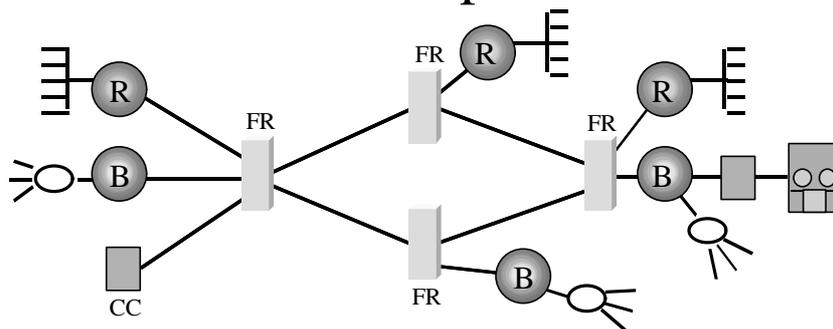
Architecture et normes



Les questions à évaluer

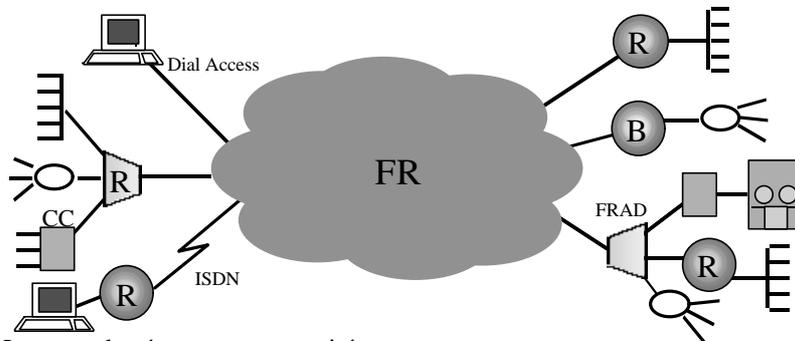
- Le contrôle de congestion et de débit
- Les connexions : permanentes vs commutées
- Tarifs et facturation
- La continuité de services entre les réseaux
- Les fournisseurs
- Les opérateurs de réseau
- La disponibilité internationale
- Les compromis publics/privés
- Les coûts

Réseau privé



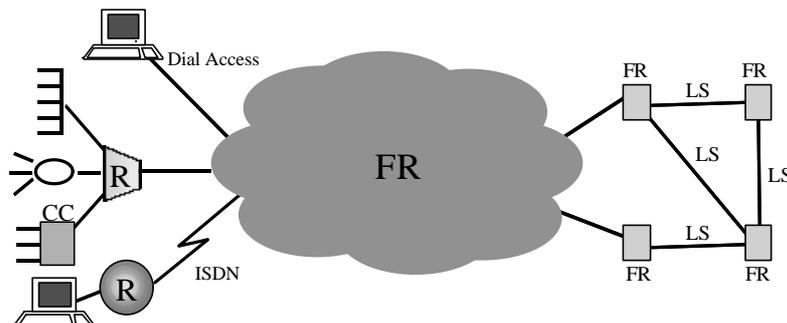
- Améliore l'utilisation des moyens télécom
- Récupération de l'existant
- Sécurité (et coût) d'exploitation du réseau

Réseau public (opérateur)



- Le cœur du réseau est sous-traité
 - Gestion par l'opérateur
 - Diminution des coûts de possession (Management and Equipment)
- Un seul accès au réseau (multiplexage)
- Le maintien du mode connecté protège la confidentialité et la sécurité

Réseau Hybride



- Contrôle des liens critiques
- Analyse site par site

Comparaison avec LS (PDH)

LS

Frame Relay

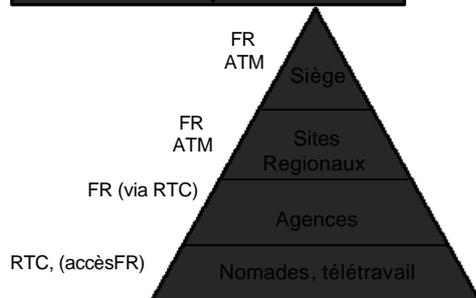
Dimensionnement au trafic de pointe
Un point d'accès par ligne et par site
TDM
Redondance des liens à construire

Dimensionnement au trafic moyen
Un point d'accès par porte
Multiplexage statistique et
Redondance des liens interne au réseau

Positionnement

Application	Technologie
LAN	FR, ATM
LAN & SNA	FR, ATM
VDI	FR, ATM

Vitesse	Technologie
< 1.5 MBPS	FR
1.5 - 45 MBPS	FR, ATM
>45 MBPS	ATM



Interfonctionnement	Agreement
FR - ATM	FRF.5 and FRF.8
FR - SMDS	SIP

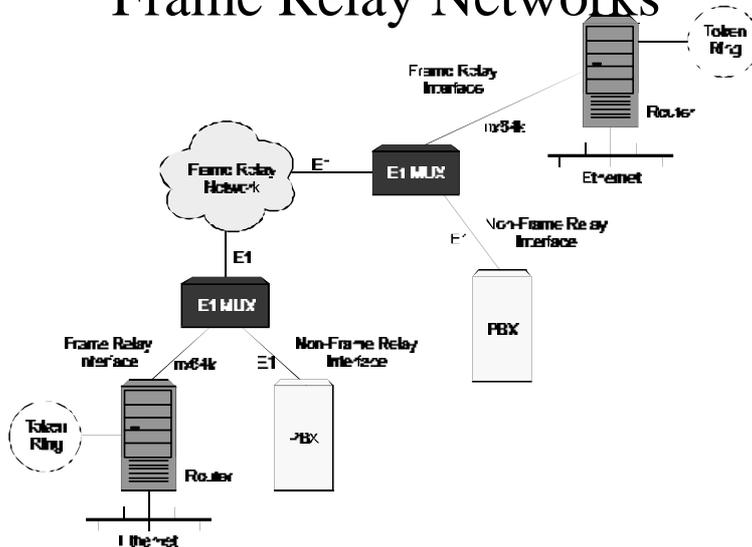
Local Management Interface

- DLCI = 0
- Informations sur l'état des CVP
 - ajout, disparition ou présence d'un CVP
 - Notification de la disponibilité d'un CVP préconfiguré
 - Scrutation de la continuité de service

Mécanisme du LMI

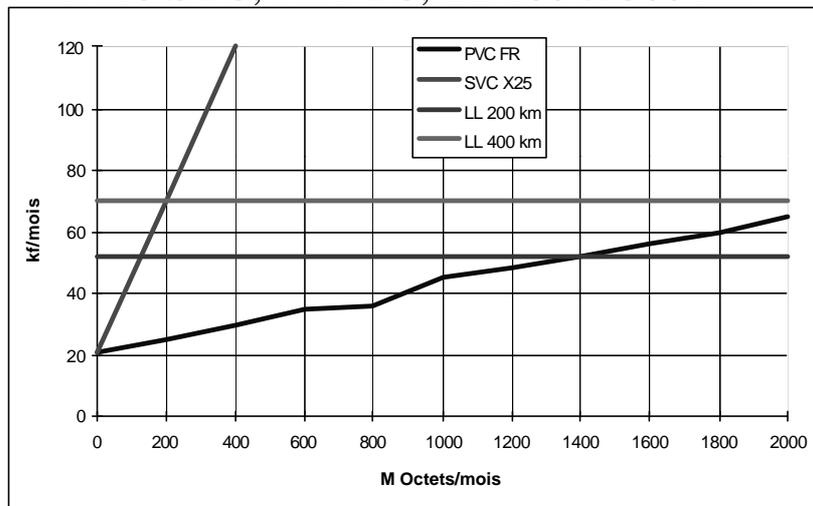
- Périodiquement
 - demande de statut (tous les CVP, un seul CVP)
 - réponse du réseau
- Sur dépassement d'un compteur
 - demande sur tous les CVP

Frame Relay Networks



Comparaison tarifaire

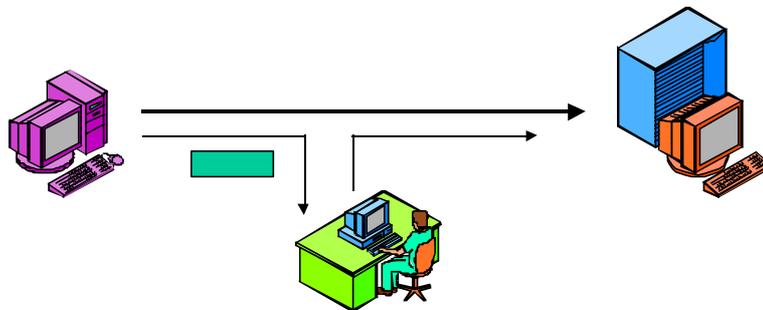
- XPAC SVC, FR PVC, LL 200 et 300 km



Sécurité

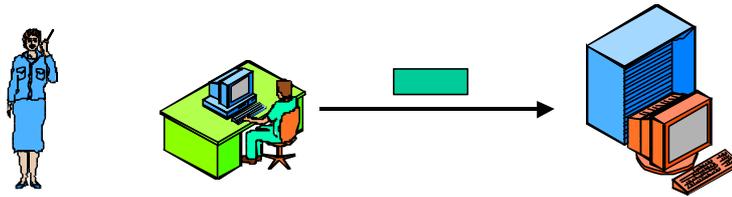
Menace : interception

- confidentialité : l'intercepteur ne peut lire les données
- intégrité : les données ne peuvent être modifiées sans que cela ne soit détecté



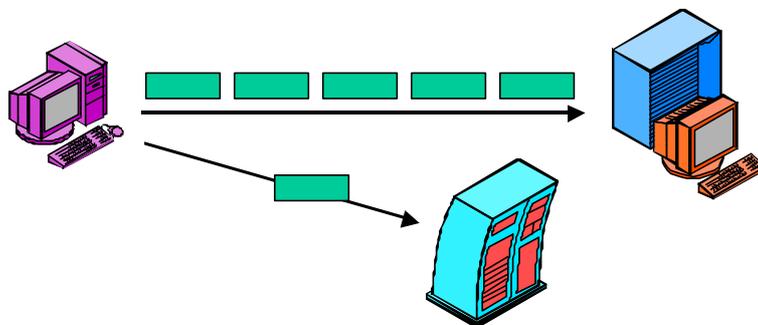
Menace : imposture

- L'imposteur prétend être une personne autorisée
- réponse : authentification



Menace : déni de service

- Surcharge du système par une inondation de message
- Envoi d'un message qui paralyse la machine



Menace : les applicatifs

- Problèmes liés aux applicatifs
 - Virus
 - Ce sont aujourd'hui les plus dangereux
- Accès à une application non protégée, puis envoi de messages à des applications non autorisées
- Nécessite un examen de la PDU application

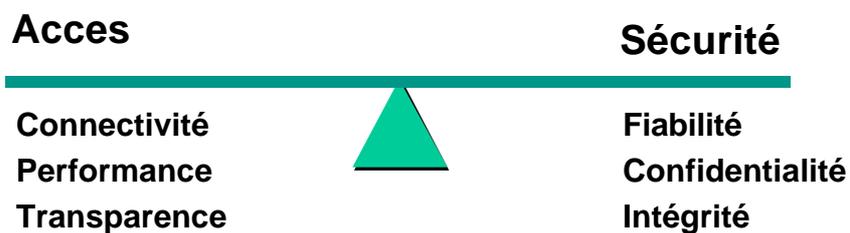
La politique de sécurité

Acces

Connectivité
Performance
Transparence

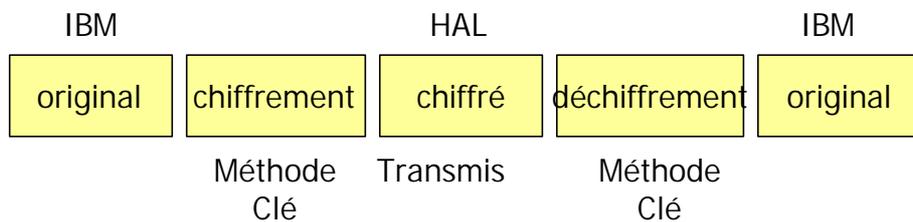
Sécurité

Fiabilité
Confidentialité
Intégrité



Chiffrement

- Chiffrement : brouillage du message le rendant illisible lorsqu'il est intercepté
 - Méthode : algorithme ne peut être tenu secret
 - la clé doit être tenue secrète



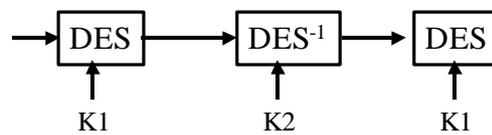
Méthodes à clé secrète

- La même clé est utilisée des deux côtés pour le chiffrement et le déchiffrement
- La clé unique doit être secrète
 - Toute personne connaissant la clé peut lire le message
- La protection est proportionnelle à la longueur de la clé
 - n bits peuvent être découverts en 2^n essais
 - sécurité faible 40 bits, forte 128 bits



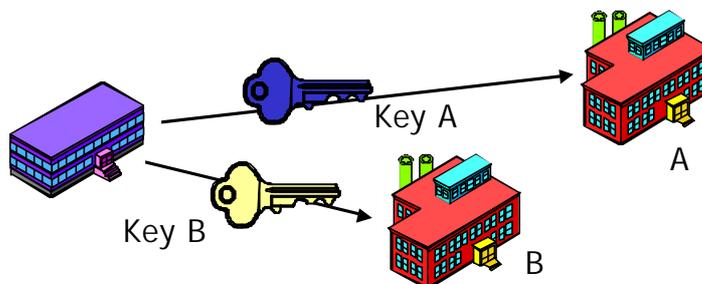
DES

- Norme la plus utilisée (origine IBM)
 - devenue norme ANSI X3.92 (DEA)
- Clés de 56 bits
 - Peuvent être cassées par des ordinateurs puissants (objectif du gouvernement US)
- Utilisation du tripe DES
 - 2 clés, trois chiffrement



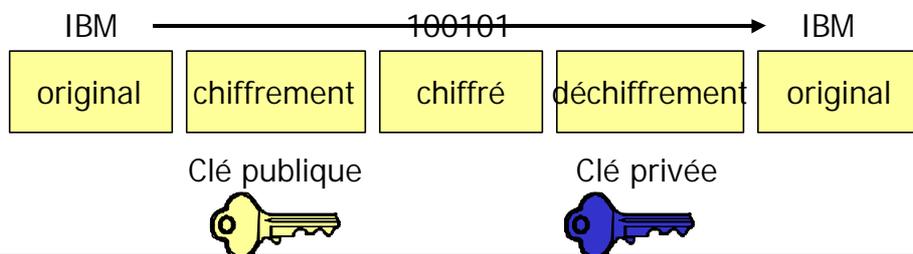
Le problème de la distribution

- La distribution des clés doit être secrète
- Les clés doivent être différentes pour chaque partenaire



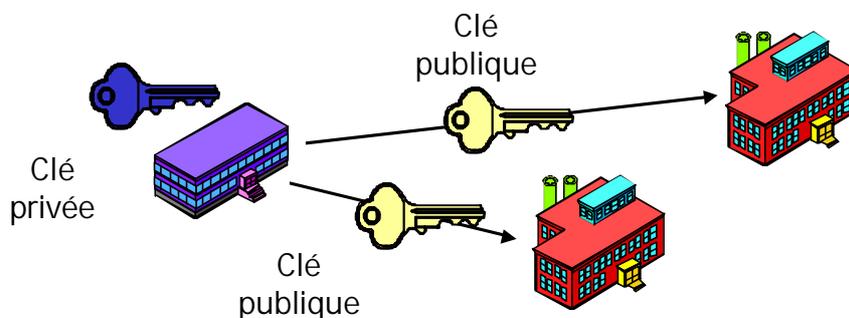
Méthodes à clés publiques

- Des clés différentes sont utilisées pour le chiffrement et le déchiffrement
 - Chiffrement par la clé publique du récepteur
 - Déchiffrement par la clé privée du récepteur
 - Seule la clé publique (res : privée) peut décrypter un message crypté avec la clé privée (publique) correspondante



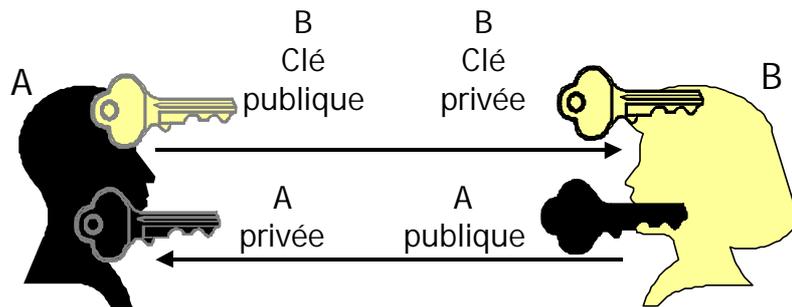
Distribution des clés asymétriques

- Chacun possède deux clés
 - la clé privée est gardée secrète
 - Les clés publiques peuvent être distribuées librement



Usage des clés

- Le système complet nécessite quatre clés
 - Chiffrement avec la clé publique du destinataire
 - Déchiffrement avec la clé privée par le destinataire



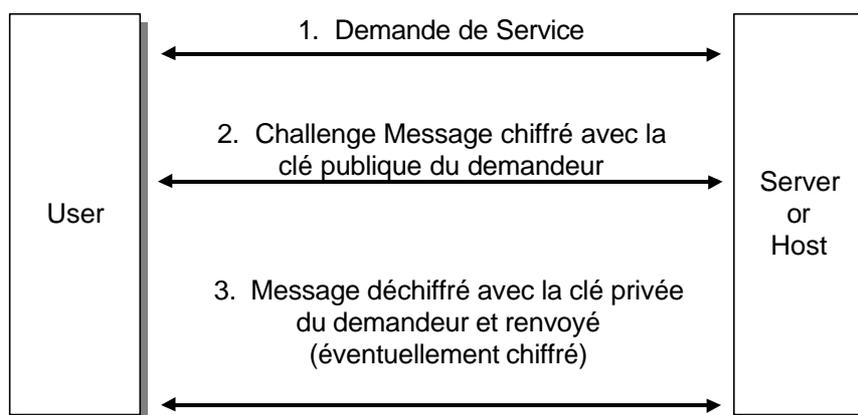
Clé publique ou clé privée?

- Clé privée
 - Calcul rapide, distribution complexe
- Clé publique
 - calculs complexes, distribution simple
- Fréquemment utilisées conjointement
 - début avec clé publique (authentification)
 - un côté génère une clé privée aléatoire
 - chiffrée avec la clé publique et envoyée au destinataire
 - La communication continue avec la clé privée
 - utilisée pour une seule session (clé de session)

Authentification

- Objectif : prouver l'identité de l'émetteur
- Méthodes
 - Mot de passe: faible
 - Biométrie
 - Emprunte digitale, analyse de l'iris : contraignant
 - *Clé publique*
 - L'émetteur prouve qu'il détient sa clé privée : seule la clé publique permet le décodage
- Permet la non-répudiation
 - l'émetteur ne peut nier avoir émis le message

Authentification par Challenge et Réponse



Authentication

- Digital Certificate
 - Trusted third party gives you a digital certificate, saying you are who you say you are.
 - You append this digital certificate to your messages



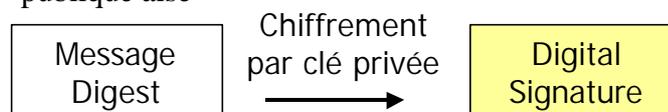
41

Authentification à clé publique (1)

- Envoi d'une signature numérique sur chaque paquet
 - Création d'un "digest" du message (MD)
 - message raccourci calculé par fonction de hachage

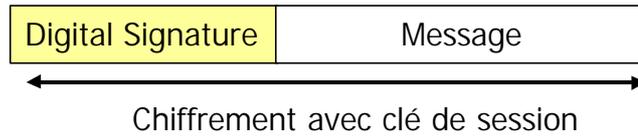


- Création de la signature
 - Chiffrement du digest avec la clé privée de l'émetteur
 - Le message est court et le déchiffrement par la clé publique aisé



Authentification à clé publique (2)

- Envoi de l'ensemble signature+message crypté avec une clé unique de session

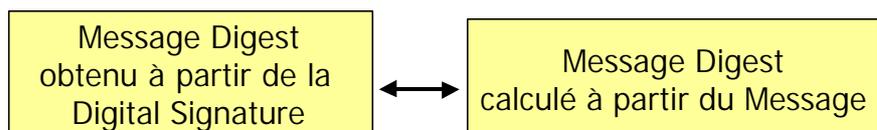


- Le récepteur déchiffre le message avec la clé unique de session et la signature avec la clé publique de l'émetteur de façon à obtenir le digest.



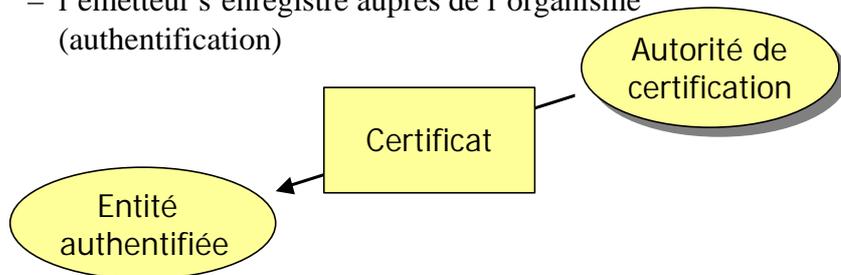
Authentification à clé publique (3)

- Le récepteur recalcule le digest.
- Si concordance :
 - l'émetteur est authentifié
 - le message est bien celui qu'a envoyé l'émetteur

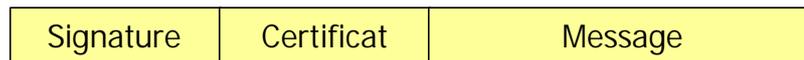


Les certificats

- Créés et gérés par une organisation indépendante
 - l'émetteur s'enregistre auprès de l'organisme (authentification)

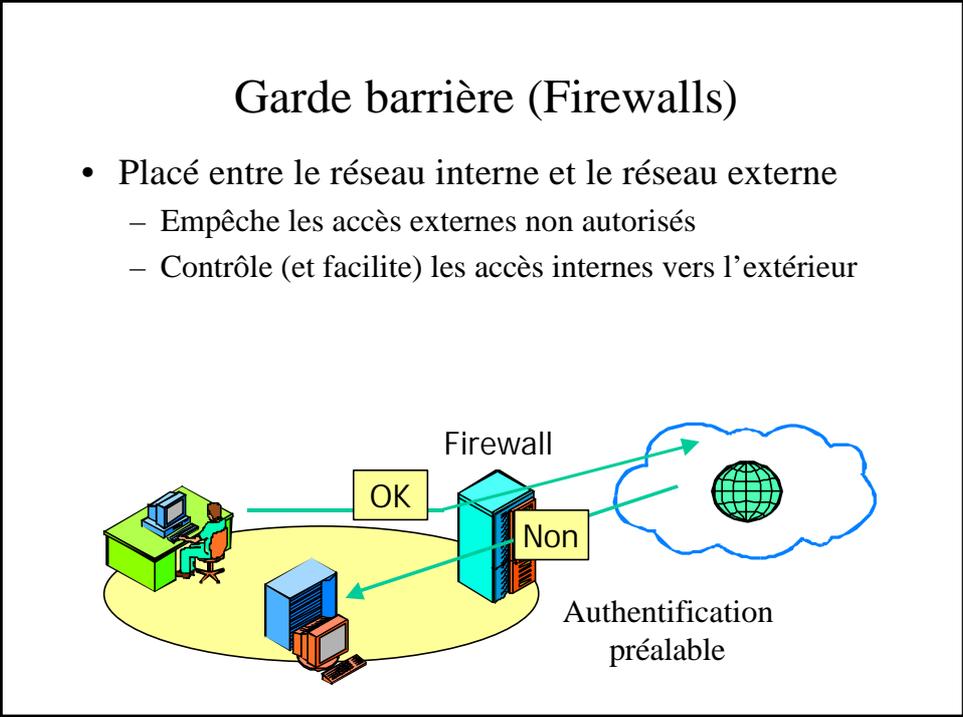
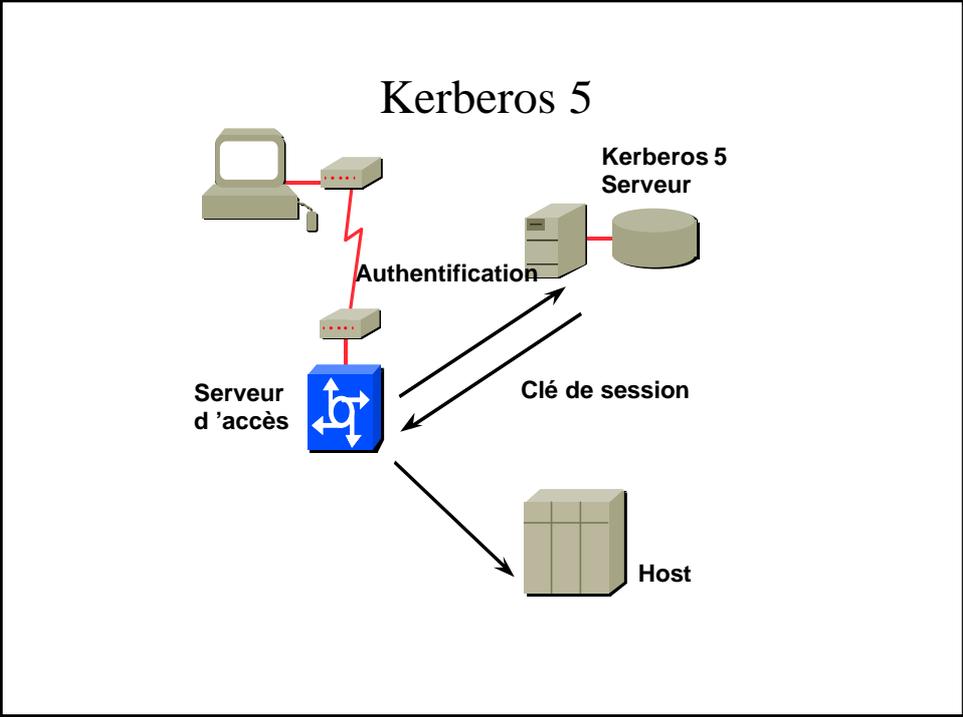


- Le certificat est ajouté à l'ensemble message+signature



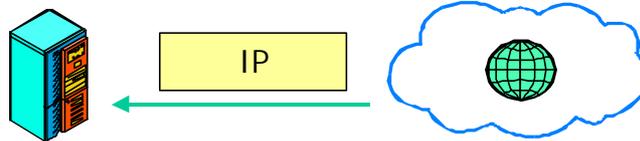
Un processus sécurité

- Mise en communication ...
 - géré par les pilotes de communication
 - Négociation des méthodes employées
 - Authentification
 - Chifrement
 - Authentification mutuelle
 - Echange des clés de session
 - Mise en relation



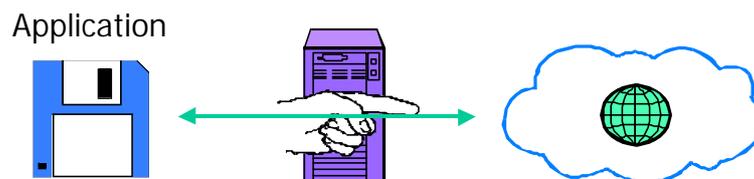
Firewalls

- Filtrage de paquets
 - Examine les adresses IP des paquets entrants
 - Autorise les paquets provenant des machines autorisées
 - Peuvent être contournés en modifiant le champ adresse du paquet IP (spoofing)



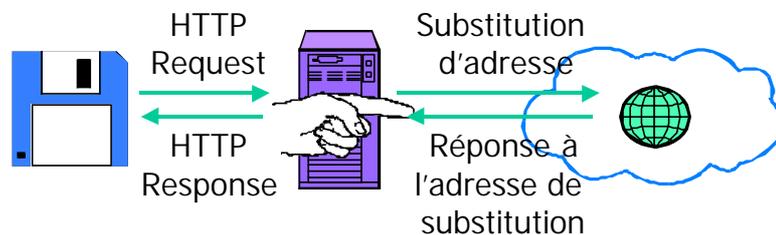
Firewalls

- Garde barrière applicatif (proxy)
 - Basé sur le comportement de l'application
 - exemple HTTP : on refuse une réponse sauf si une requête a été émise vers le serveur



Masquage des adresses internes

- Proxy
 - Le client envoie une requête HTTP
 - Le proxy remplace l'adresse du client par une adresse conventionnelle
 - La réponse est envoyée à l'adresse de remplacement et transmise par le garde barrière au client
 - Le proxy remplace le client pour les échanges externes



Bastion et zone démilitarisée

