

Routage et commutation de base

Pr Cheikh Ahmadou Bamba GUEYE

<http://edmi.ucad.sn/~gueye>

Plan du cours

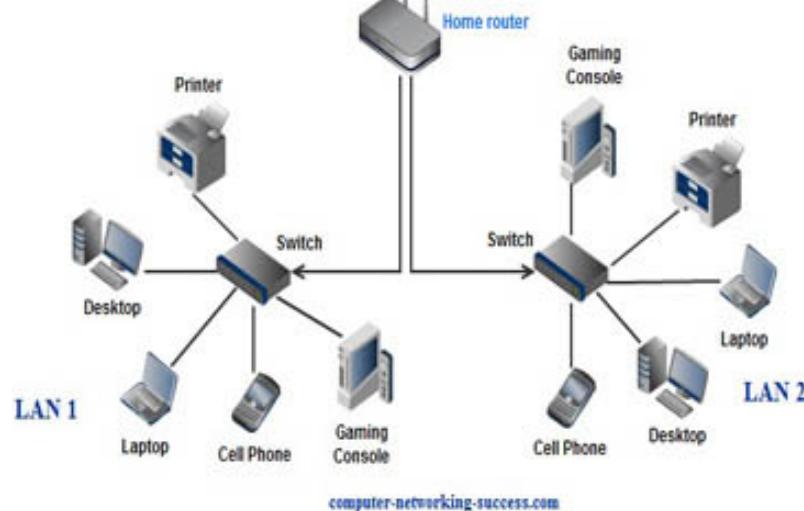
- Introduction
- Adressage IP
- Création de sous-réseaux
- VLSM
- Commutation vs routage
- Types de Routage
 - Vecteur de distance et ++
 - Etats de liens
 - Vecteur de chemin
- Notions de Systèmes Autonomes

Bibliographie

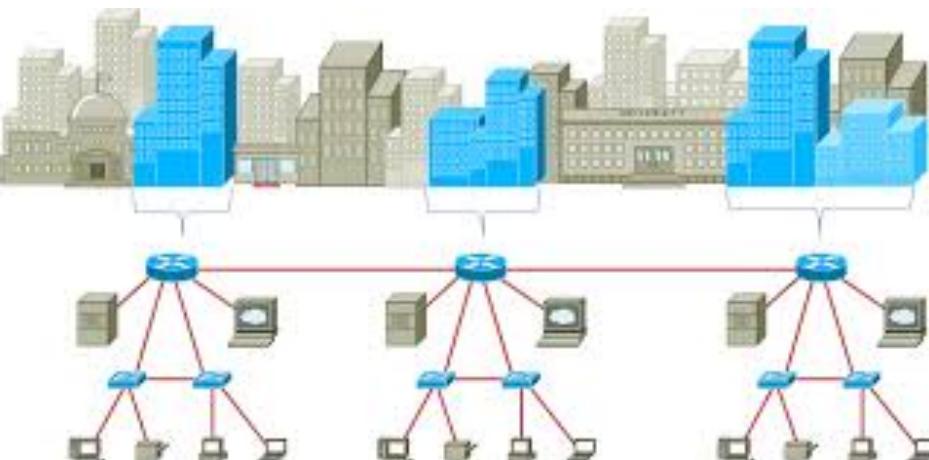
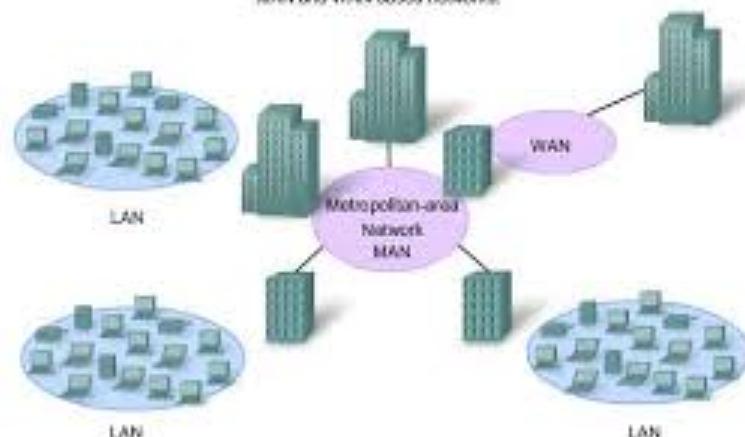
- **Réseaux et Télécom: cours avec 129 exercices corrigés**, Claude Servin (Auteur), Editeur : Dunod; DUNOD edition
- **Computer Networking : A Top-Down Approach Featuring the Internet**, James F. Kurose (Auteur), Keith W. Ross (Auteur), Pearson; 6th edition (March 5, 2012)
- **Réseaux d'entreprises par la pratique**, Jean Luc Montagnier (Auteur), Eyrolles
- **Cisco CCNA Exploration 2**

Rappel (1)

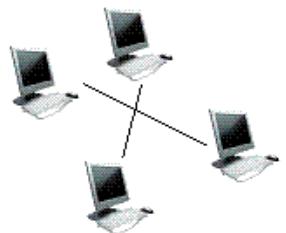
Local Area Network



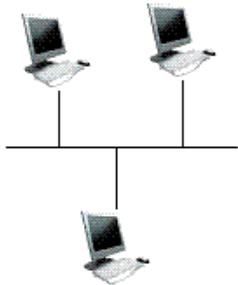
Gigabit Ethernet
Gigabit Ethernet technology is applied beyond the enterprise LAN to MAN and WAN-based networks.



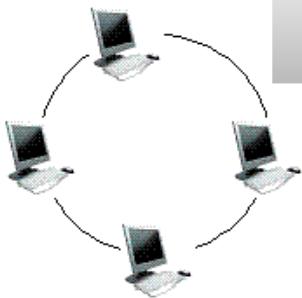
Rappel (2)



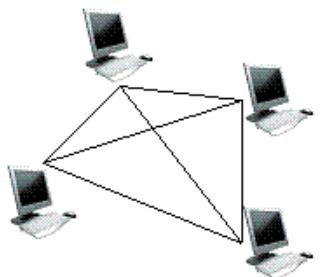
Etoile



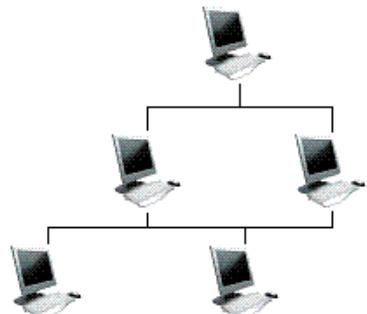
Bus



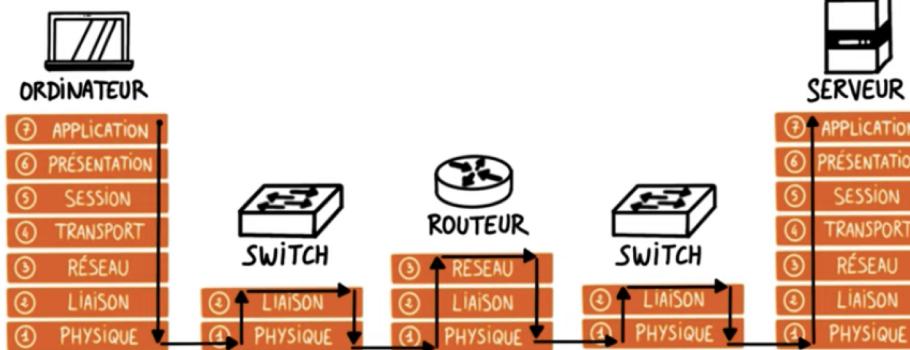
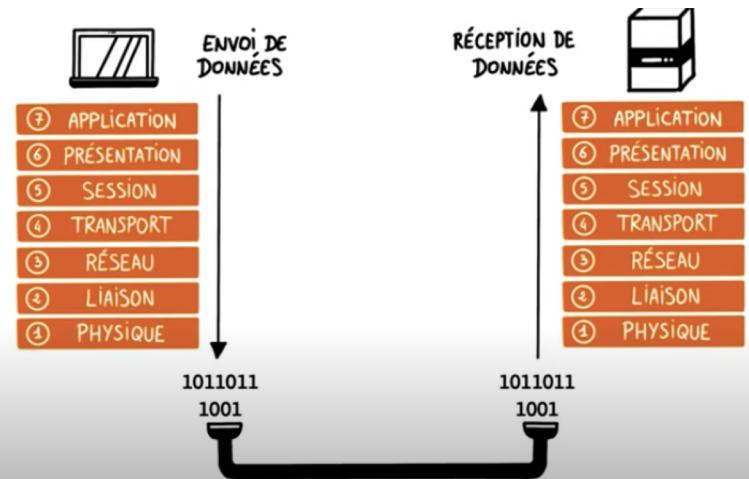
Anneau



Maillée



Hiérarchisée ou arbre



Introduction

- La communication numérique à base de données, de son audio et de vidéo est essentielle pour les PME
- Un réseau local correctement conçu est aujourd’hui fondamental pour mener une activité
- Un modèle de conception hiérarchique est plus idoine pour réussir votre projet

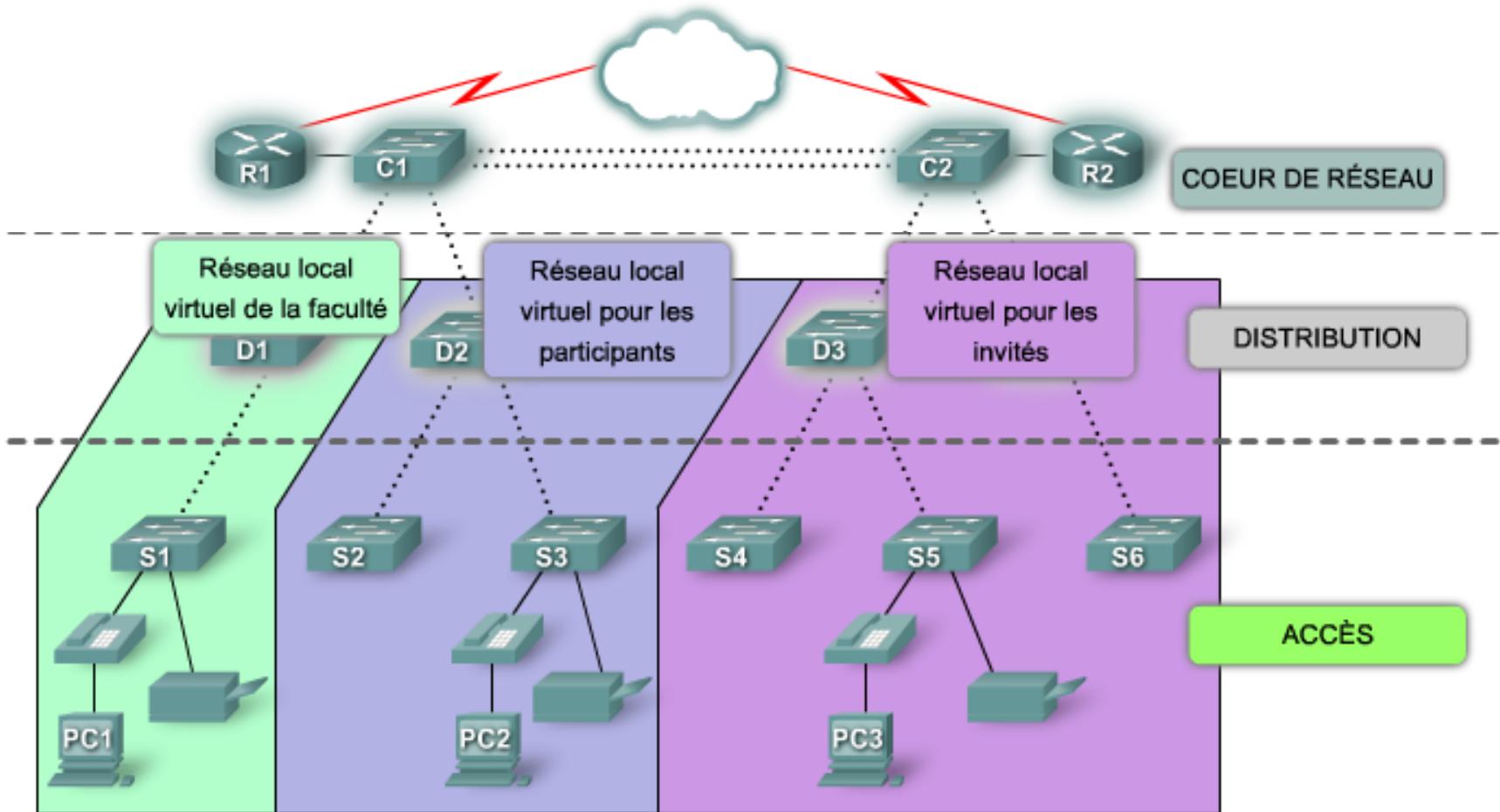
Réseau hiérarchique

- Comparé à d'autres conceptions de réseau, un réseau hiérarchique est plus simple à gérer et à développer, tandis que les problèmes sont résolus plus rapidement
- Chaque couche fournit des fonctions spécifiques qui définissent son rôle dans le réseau global
- En séparant les différentes fonctions existantes sur un réseau, la conception de réseau devient modulaire, ce qui facilite l'évolutivité et les performances
- Le modèle de conception hiérarchique classique se divise en trois couches : la couche d'accès, la couche de distribution et la couche cœur de réseau

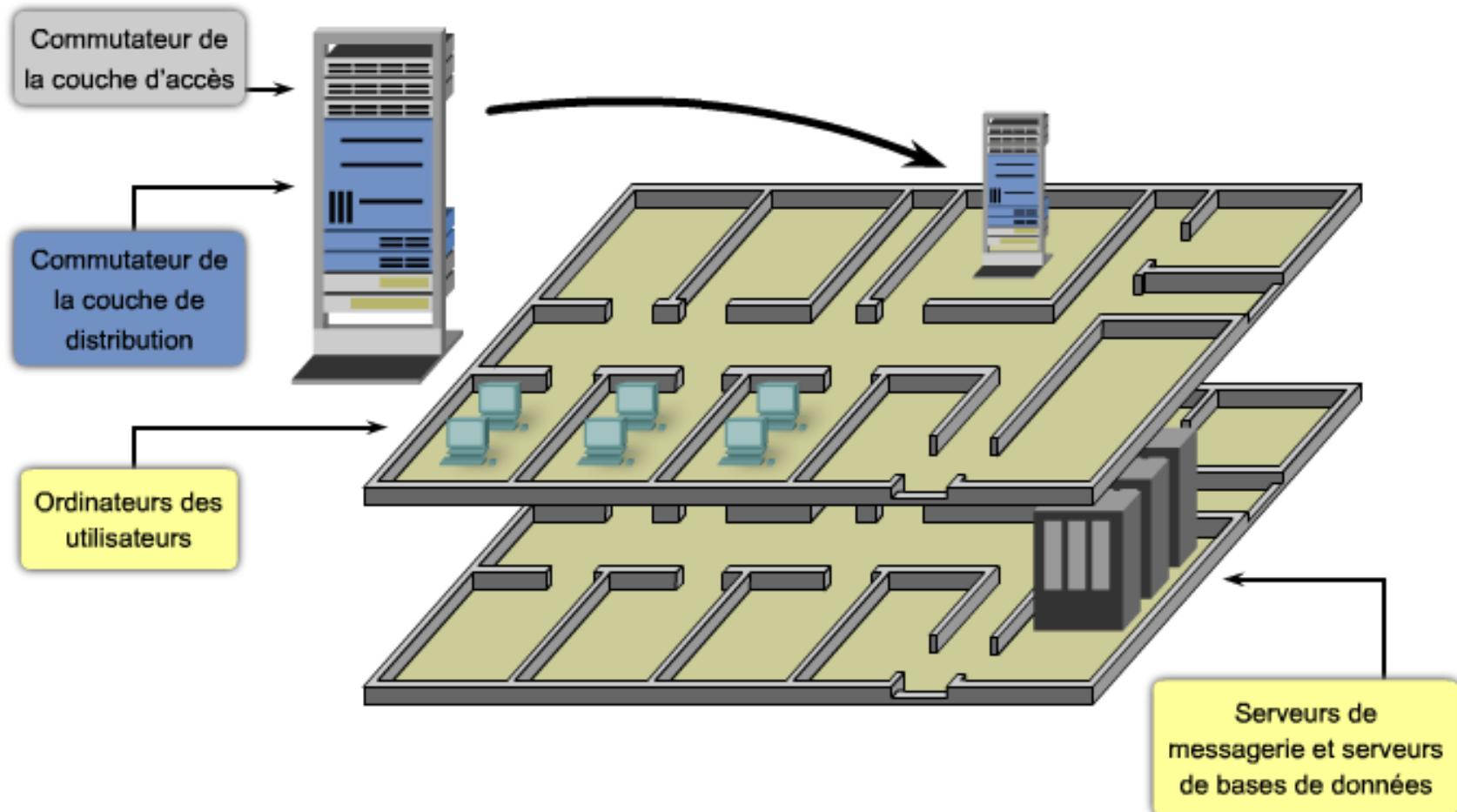
Modèle de réseau hiérarchique

- **Couche d'accès** : elle sert d'interface avec des périphériques, tels que des ordinateurs, des imprimantes et des téléphones sur IP, afin de fournir un accès au reste du réseau
 - Elle peut inclure des routeurs, des commutateurs, des ponts, des concentrateurs et des points d'accès sans fil
- **Couche de distribution** : elle regroupe les données reçues à partir des commutateurs de la couche d'accès, avant leur transmission vers la couche cœur de réseau, en vue du routage vers leur destination finale
 - La couche de distribution gère le flux du trafic réseau à l'aide de stratégies, et délimite les domaines de diffusion via des fonctions de routage entre des réseaux locaux virtuels (VLAN) définis au niveau de la couche d'accès
- **Couche cœur de réseau** : elle constitue le réseau fédérateur à haut débit de l'interréseau et est essentielle à l'interconnectivité entre les périphériques de la couche de distribution
 - Par conséquent, il est important qu'elle bénéficie d'une disponibilité et d'une redondance élevées
 - La zone principale peut également se connecter à des ressources Internet

Modèle de réseau hiérarchique



Réseau hiérarchique d'une entreprise moyenne



Avantage d'un réseau hiérarchique

Évolutivité

- Les réseaux hiérarchiques peuvent être aisément étendus.

Redondance

- La redondance au niveau des couches principale et de distribution garantit la disponibilité de chemins d'accès.

Performances

- L'agrégation de liaisons entre les niveaux et les commutateurs des couches principale et de distribution très performants permettent de bénéficier d'une vitesse proche de celle du câble à travers le réseau.

Sécurité

- La sécurité de port au niveau de l'accès et les stratégies au niveau de la distribution renforcent la sécurité du réseau.

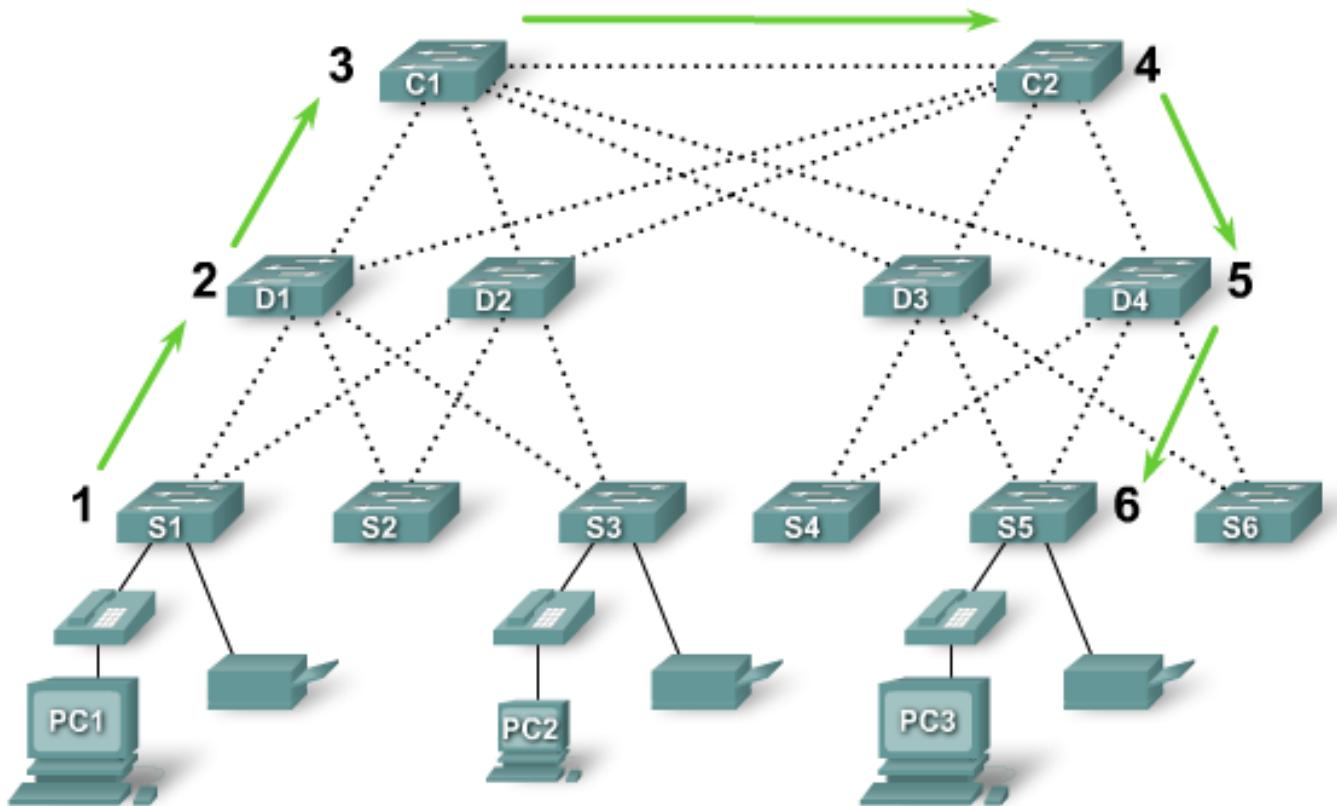
Facilité de gestion

- La cohérence entre les commutateurs à chaque niveau simplifie davantage la gestion.

Maintenance

- La modularité de la conception hiérarchique permet une mise à l'échelle du réseau sans trop de complexité.

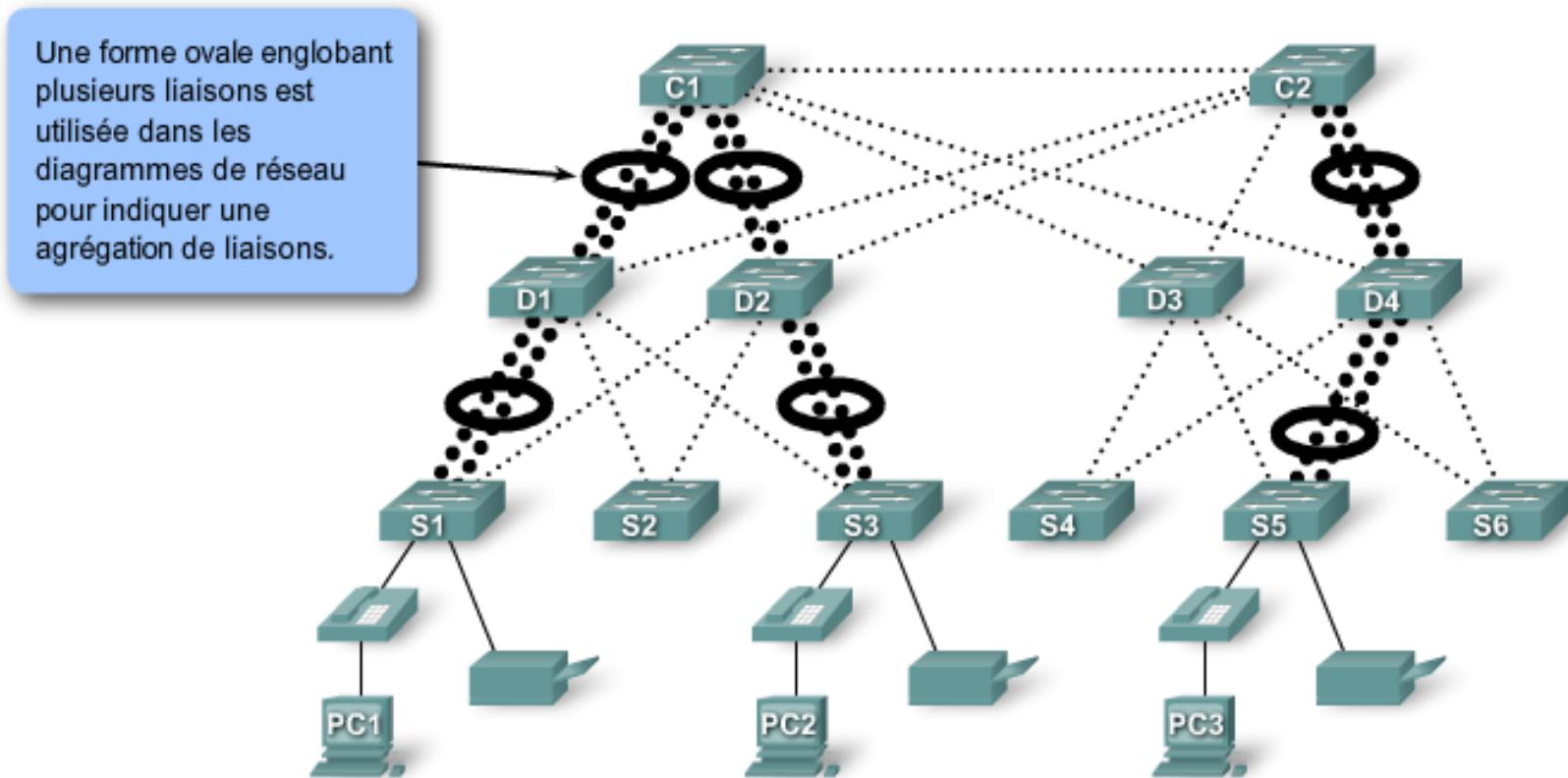
Principes du modèle de réseau hiérarchique : diamètre du réseau



- Le diamètre de réseau correspond au nombre de périphériques que doit traverser un paquet avant d'atteindre sa destination
- Lorsque vous maintenez un **faible diamètre de réseau**, cela garantit une **latence faible** et prévisible entre les périphériques

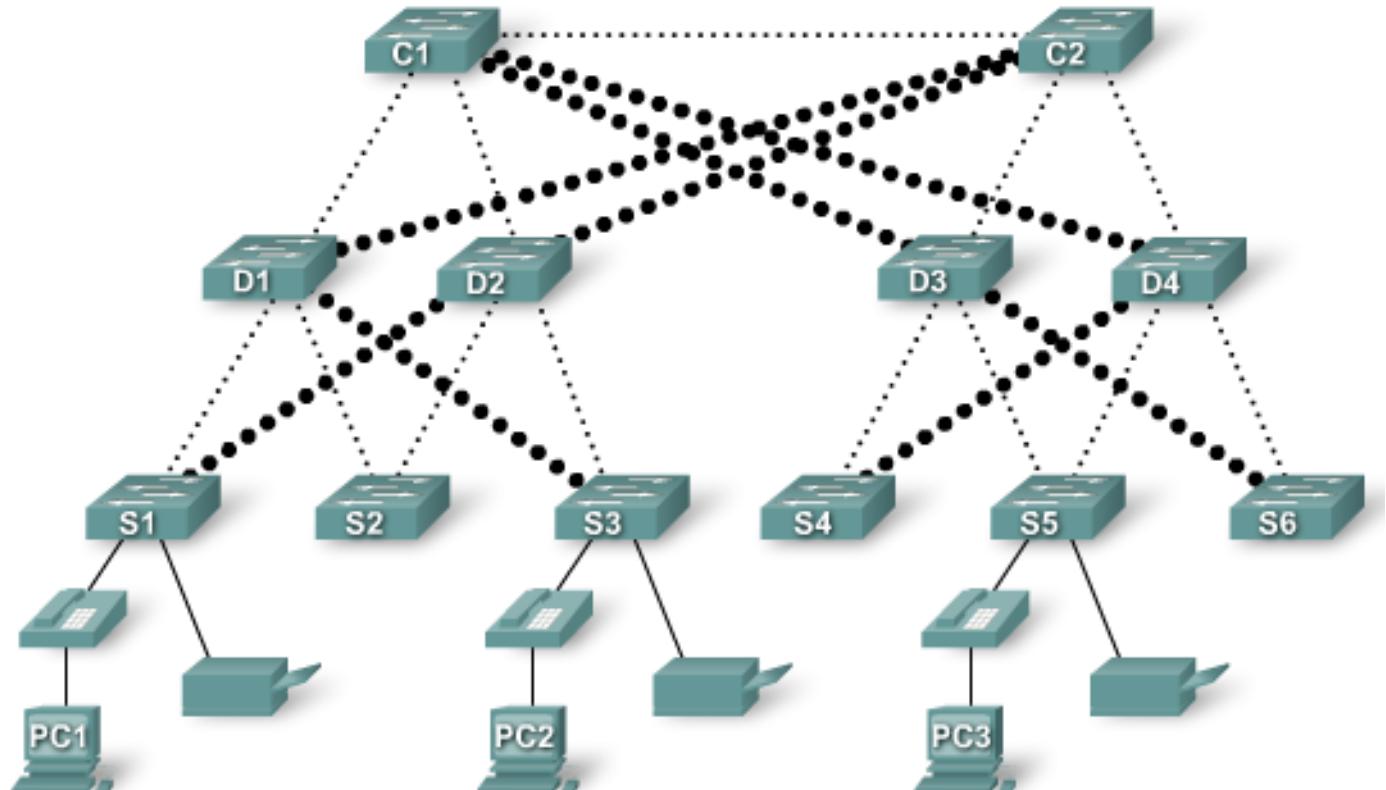
Agrégation de bande passante

L'agrégation de bande passante est normalement implémentée en combinant plusieurs liaisons parallèles entre deux commutateurs au sein d'une liaison logique.



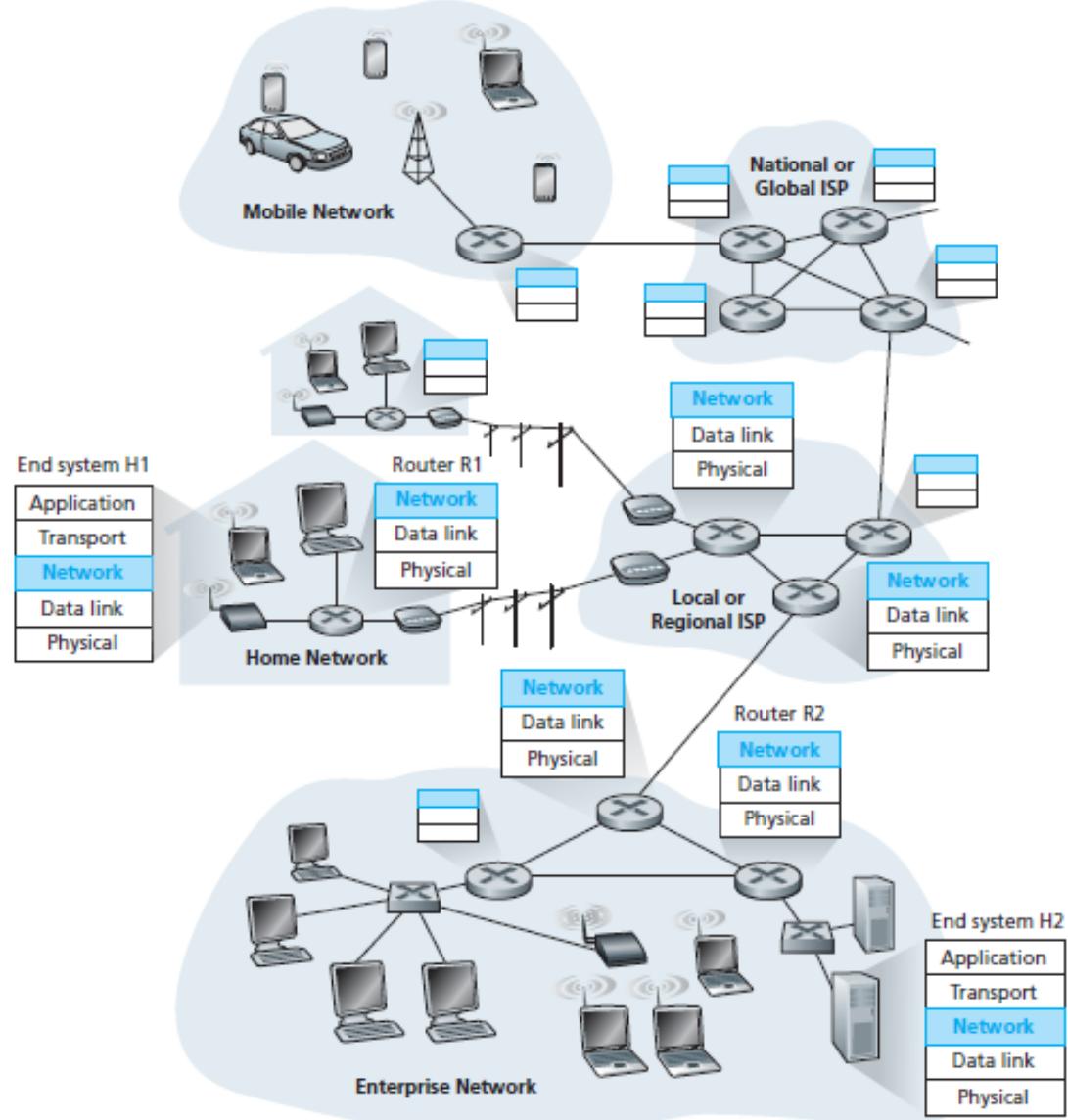
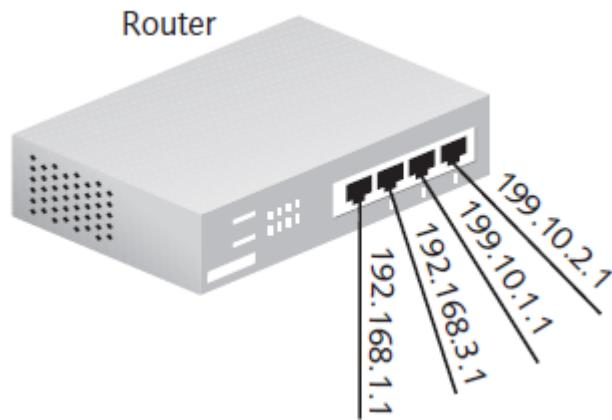
Liaisons redondantes

Des réseaux modernes utilisent des liaisons redondantes entre des couches de réseau hiérarchique afin de garantir la disponibilité du réseau.



ADRESSAGE IP

La couche réseau



Adresse IP (Internet Protocol)

Les sites Web ceux sont les boutiques et magasins ...

②

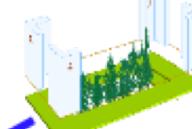


Site Web
Amazon
@IP: 84.201.66.25



Site Web
Bibliothèque Nationale de France
L'adresse IP : 194.199.8.10
c'est l'adresse postale

③



Mon ordina

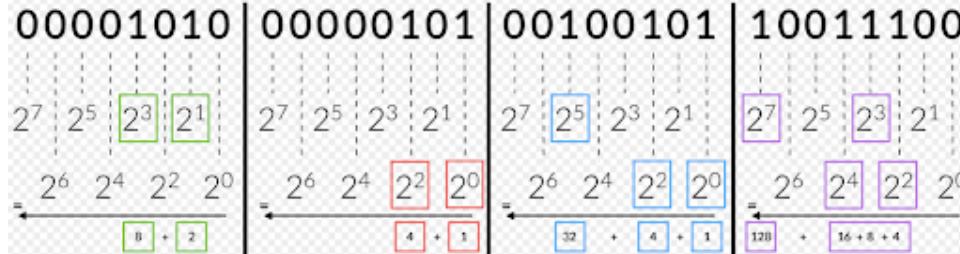
① Internet c'est le réseau routier



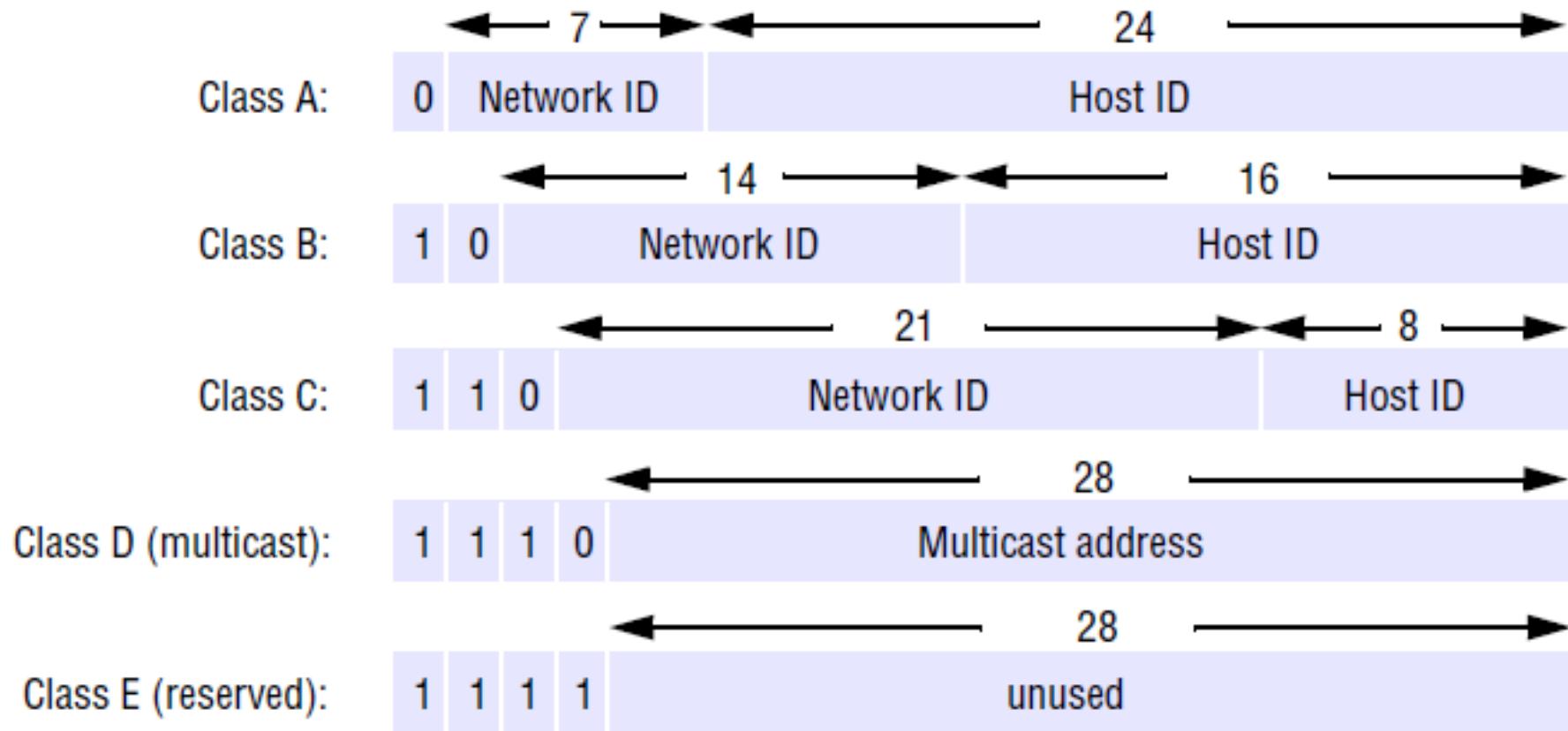
Site Web
www.coursinfo.fr
@ip: 213.186.33.16

IPv4 Address (4 Octets)

10.5.37.156



Structure de l'adresse IP



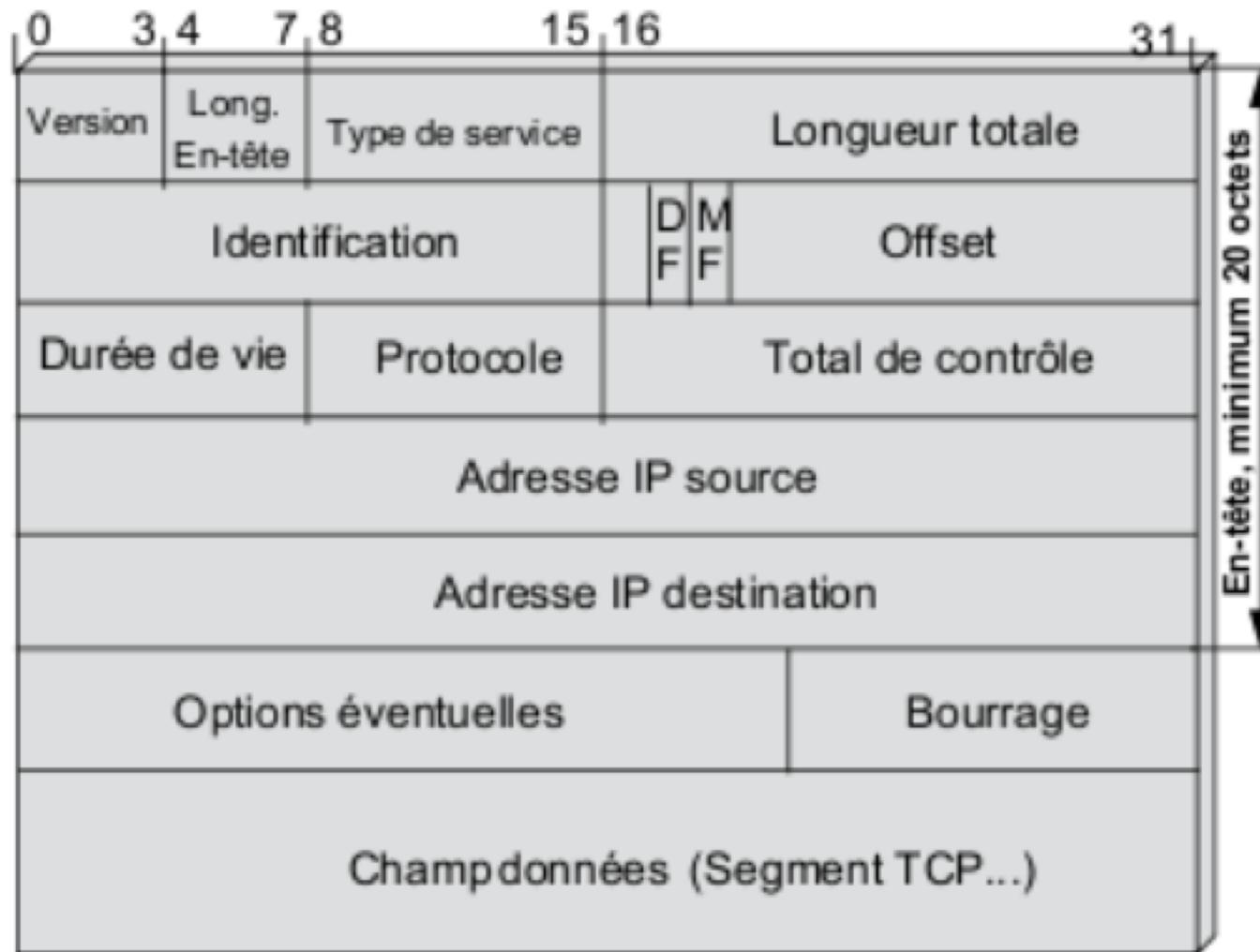
Représentation décimale des adresses IP

	<i>octet 1</i>	<i>octet 2</i>	<i>octet 3</i>	<i>Range of addresses</i>
Class A:	<i>Network ID</i> 1 to 127	0 to 255	0 to 255	0 to 255 1.0.0.0 to 127.255.255.255
Class B:	<i>Network ID</i> 128 to 191	0 to 255	0 to 255	0 to 255 128.0.0.0 to 191.255.255.255
Class C:	<i>Network ID</i> 192 to 223	0 to 255	0 to 255	1 to 254 192.0.0.0 to 223.255.255.255
Class D (multicast):	<i>Multicast address</i>			
Class E (reserved):	224 to 239	0 to 255	0 to 255	1 to 254 224.0.0.0 to 239.255.255.255
	240 to 255	0 to 255	0 to 255	1 to 254 240.0.0.0 to 255.255.255.255

Adresses IP privées

- Elles sont utilisables localement dans un réseau mais ne doivent pas circuler sur Internet et sont rejetées par les routeurs
- Elles ne sont donc attribuables à aucun réseau ni aucune station pour se relier à Internet
 - 10.0.0.0 à 10.255.255.255
 - 172.16.0.0 à 172.31.255.255
 - 192.168.0.0 à 192.168.255.255
 - 169.254.0.0 à 169.254.255.255

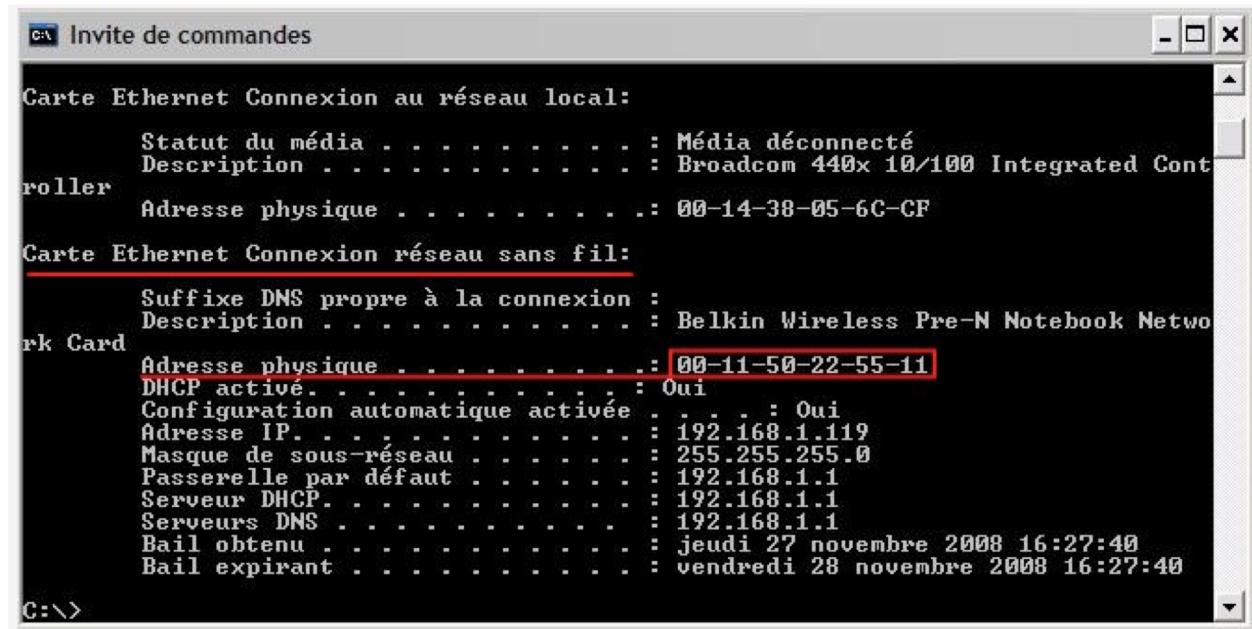
Structure du datagramme IP



Trouver l'adresse MAC et IP de sa carte réseau

- Sous windows :

- Fenêtre cmd
- Tapez ipconfig /all



```
c:\> ipconfig /all

Carte Ethernet Connexion au réseau local:
    Statut du média . . . . . : Média déconnecté
    Description . . . . . : Broadcom 440x 10/100 Integrated Cont
    roller
    Adresse physique . . . . . : 00-14-38-05-6C-CF

Carte Ethernet Connexion réseau sans fil:
    Suffixe DNS propre à la connexion :
    Description . . . . . : Belkin Wireless Pre-N Notebook Netwo
    rk Card
    Adresse physique . . . . . : 00-11-50-22-55-11
    DHCP activé . . . . . : Oui
    Configuration automatique activée . . . . . : Oui
    Adresse IP . . . . . : 192.168.1.119
    Masque de sous-réseau . . . . . : 255.255.255.0
    Passerelle par défaut . . . . . : 192.168.1.1
    Serveur DHCP . . . . . : 192.168.1.1
    Serveurs DNS . . . . . : 192.168.1.1
    Bail obtenu . . . . . : jeudi 27 novembre 2008 16:27:40
    Bail expirant . . . . . : vendredi 28 novembre 2008 16:27:40
```

- Sous Linux

- Fenêtre terminal
- Tapez /sbin/ifconfig -a



```
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
      options=400<CHANNEL_IO>
      ether 98:e0:d9:79:18:53  l'adresse MAC de sa carte réseau
      inet6 fe80::1ccc:63f2:47f2:a3b4%en0 prefixlen 64 secured scopeid 0x4
      inet 192.168.1.37 netmask 0xffffffff broadcast 192.168.1.255
        nd6 options=201<PERFORMNUD,DAD>
        media: autoselect
        status: active
```

Packet Internet Gropher « PING »



La commande PING permet de tester une liaison TCP/IP de bout en bout :

- ▶ PING sur l'adresse 127.0.0.1 teste l'installation de la pile TCP/IP sur la machine source ;
- ▶ Sur l'adresse IP de la machine source, elle vérifie que cette station est correctement configurée ;
- ▶ Sur l'adresse de la passerelle par défaut, elle contrôle la validité du masque de sous-réseau et la configuration de la passerelle par défaut ;
- ▶ PING sur l'adresse de l'interface de sortie (LS locale) valide la configuration de cette interface ;
- ▶ Sur l'adresse de LS distante, elle s'assure que le lien WAN est établi et que les routeurs local et distant sont correctement configurés vis-à-vis du réseau source ;
- ▶ Sur l'adresse de station distante, elle valide la configuration de bout en bout.

Exemple de commande PING

```
C:> Ping 195.221.126.186
```

Envoi d'une requête 'ping' sur 195.221.126.186 avec 32 octets de données :

Réponse de 195.221.126.186 : octets=32 temps=135 ms TTL=53

Réponse de 195.221.126.186 : octets=32 temps=140 ms TTL=53

Réponse de 195.221.126.186 : octets=32 temps=156 ms TTL=53

Réponse de 195.221.126.186 : octets=32 temps=156 ms TTL=53

Statistiques Ping pour 195.221.126.186:

Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),

Durée approximative des boucles en millisecondes :

Minimum = 135 ms, Maximum = 156 ms, Moyenne = 146 ms

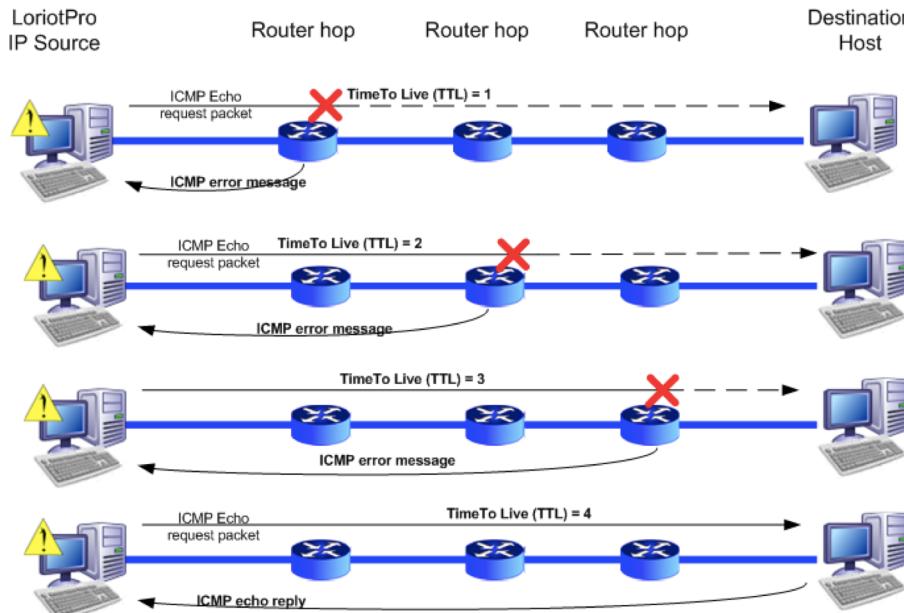
Outils « Traceroute ou tracert »

C:> Tracert 195.221.126.186

Détermination de l'itinéraire vers cnam-st-martin.rap.prd.fr [195.221.126.186]

avec un maximum de 30 sauts :

```
1 237 ms 156 ms 140 ms nssta107.francetelecom.net [193.252.253.123]
2 156 ms 156 ms 156 ms GE2-201.ncidf103.Puteaux.francetelecom.net
3 156 ms 156 ms 156 ms pos6-0.nraub103.Aubervilliers.francetelecom.net [193.252.159.42]
4 140 ms 156 ms 140 ms pos13-3.ntaub201.Aubervilliers.francetelecom.net [193.252.103.18]
5 156 ms 156 ms 156 ms 193.251.126.54
6 140 ms 156 ms 140 ms P14-0.PASCR2.Pastourelle.opentransit.net [193.251.128.105]
7 156 ms 156 ms 155 ms 193.51.185.2
8 140 ms 156 ms 140 ms nri-b-pos11-0.cssi.renater.fr [193.51.179.10]
9 156 ms 156 ms 156 ms jussieu-pos4-0.cssi.renater.fr [193.51.180.157]
10 140 ms 156 ms 140 ms 193.50.20.73
11 156 ms 156 ms 155 ms cr-cnam.rap.prd.fr [195.221.125.205]
12 140 ms 156 ms 156 ms cnam-st-martin.rap.prd.fr [195.221.126.186]
```

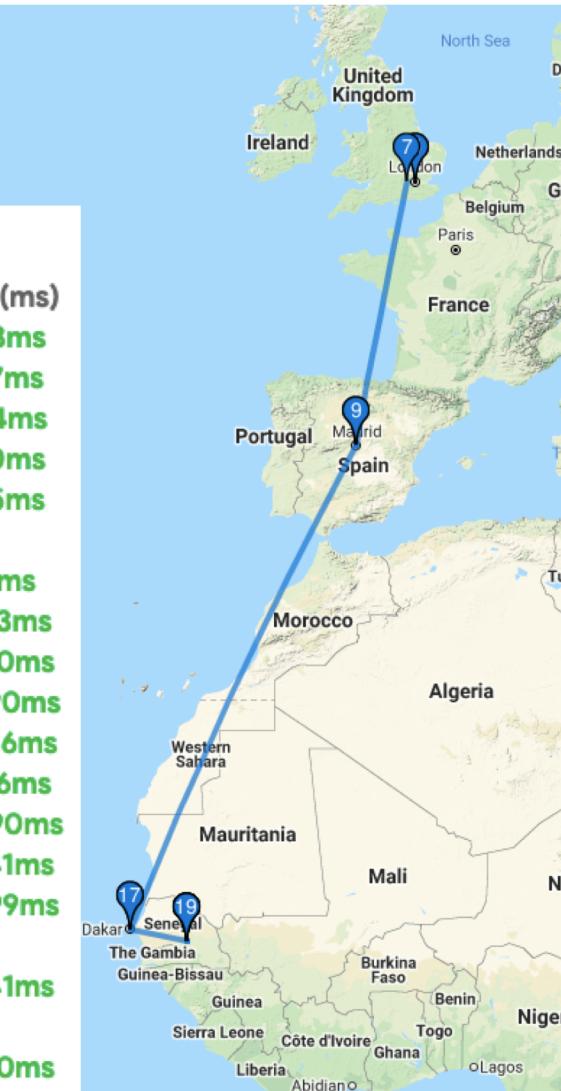


Traceroute visuel sur internet

- <https://gsuite.tools/fr/traceroute>

traceroute to www.ucad.sn (196.1.97.203), 30 hops max

Hop	Host	IP	Time (ms)
1	dgw1-wan-uk-lon1.ipv4.upcloud.com	83.136.248.1	0.093ms
2	100.69.2.209	100.69.2.209	0.247ms
3	172.17.255.241	172.17.255.241	0.304ms
4	172.17.255.253	172.17.255.253	0.320ms
5	5-1-33.ear2.London1.Level3.net	212.187.165.105	0.435ms
6	*	*	*
7	Telefonica-level3-100G.London1.Level3.net	195.50.116.90	1.286ms
8	5.53.4.102	5.53.4.102	31.823ms
9	sonatel-te0-1-0-7-2-grtmadte2.net.telefonicaglobalsolutions.com	213.140.50.31	77.780ms
10	196.207.219.180	196.207.219.180	85.590ms
11	196.207.249.108	196.207.249.108	83.586ms
12	196.207.250.176	196.207.250.176	83.136ms
13	rc-medina2-bis.sonatel.sn	196.207.224.97	84.490ms
14	196.207.255.180	196.207.255.180	83.641ms
15	196.207.255.59	196.207.255.59	84.699ms
16	*	*	*
17	41.214.73.42	41.214.73.42	86.341ms
18	*	*	*
19	196.1.97.203	196.1.97.203	83.160ms



Exercice depuis votre machine perso

- Faites un PING vers les adresses ci-dessous :
 - www.google.com
 - www.youtube.com
 - www.sonatel.sn
 - www.ucad.sn
 - Commentez les résultats
- Faites un traceroute vers les adresses ci-dessous :
 - www.google.com
 - www.youtube.com
 - www.sonatel.sn
 - www.orange.sn
 - www.ucad.sn
 - Commenter les résultats

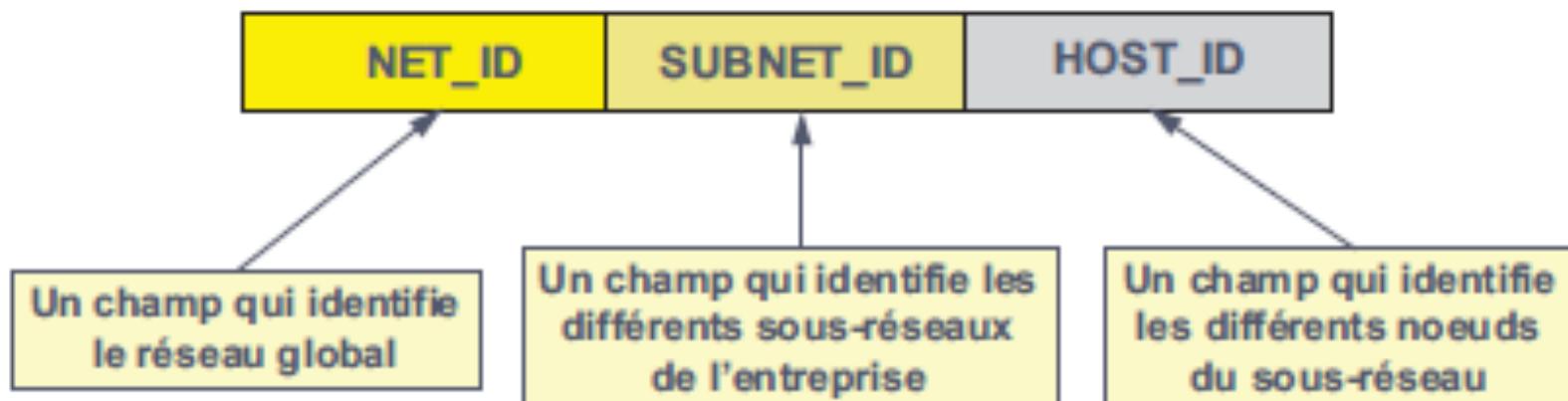
TP depuis <https://gsuite.tools/fr/traceroute>

- Faites un traceroute vers les adresses ci-dessous
 - www.google.com
 - www.youtube.com
 - www.sonatel.sn
 - www.orange.sn
 - www.free.sn
 - www.ucad.sn
 - www.adie.sn

Sous-réseaux (subnetting)

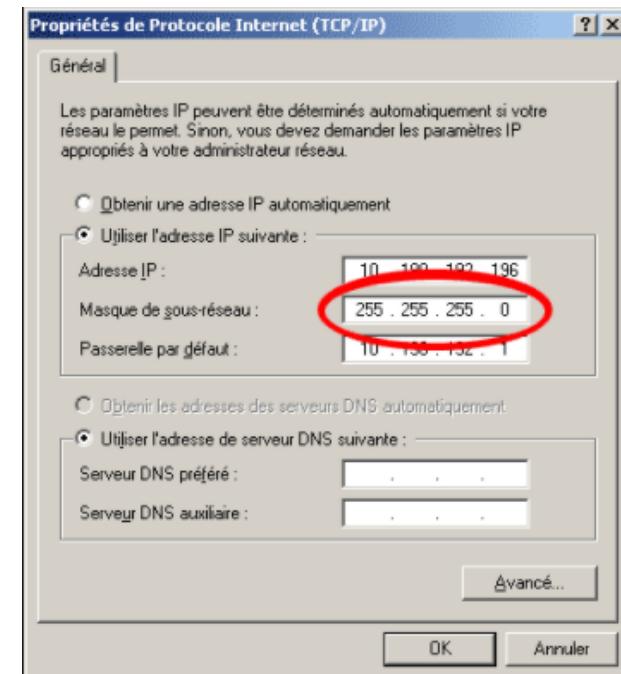
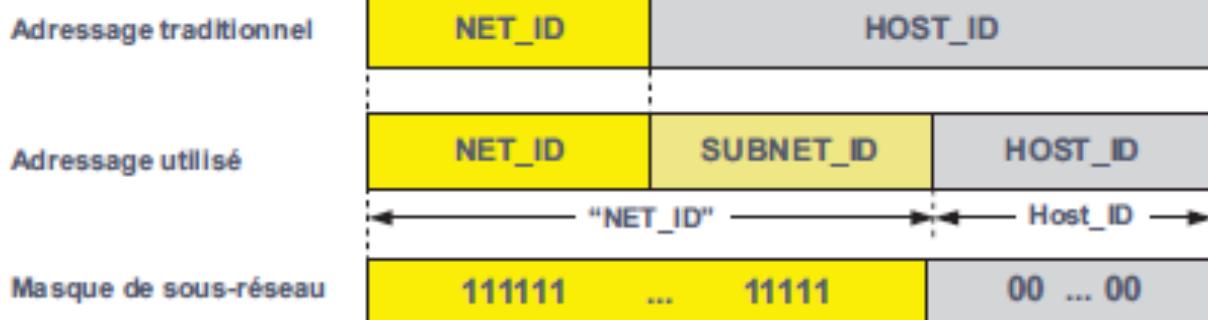
Objectif

- Subdiviser un réseau en sous-réseaux
- Permettre de constituer des réseaux internes au sein d'un réseau **a.b.c.d/x**
 - « x » est appelé le préfixe du réseau (nombre de bits réservés à la partie réseau)



Exemple

- On utilise alors un masque de sous-réseau



Réseau	Masque de sous-réseau	Sous-réseau
172.16.0.0/23	255.255.254.0	172.16.2.0
		172.16.4.0
		172.16.6.0
		...

Formules pour trouver le nombre de sous-réseaux et le nombre d'hôtes

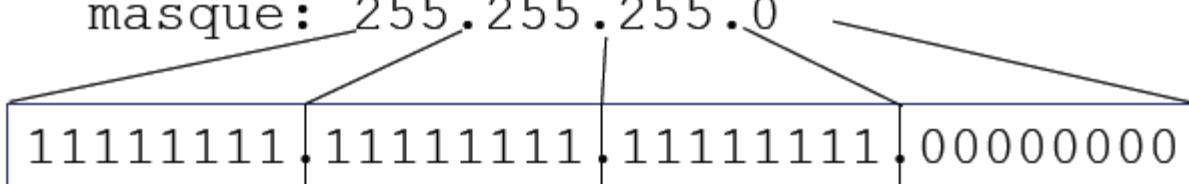
- Nombre de sous-réseaux
 - $2^n - 1$ = nombre de sous-réseaux réels et utilisables
 - **Attention:** le premier réseau est actuellement utilisable avec les nouveaux protocoles de routage
- Nombre d'hôtes par sous-réseaux
 - $2^z - 2$ = nombre d'hôtes réels et utilisables par sous-réseau
- n représente le nombre de bits empruntés aux octets hôtes
- z représente le nombre de bits restants aux octets hôtes

Est-on sur le même réseau ?

Adr IP1: 192.168.1.102

Adr IP2: 192.168.1.36

masque: 255.255.255.0

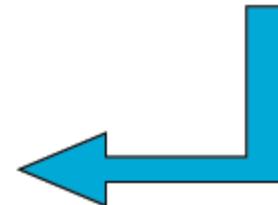


Donc adresse de réseau=192.168.1.0

Adr IP1: 11000000.10101000.00000001.01100110

et

11111111.11111111.11111111.00000000



réseau: 11000000.10101000.00000001.00000000

Adr IP2: 11000000.10101000.00000001.01100110

11111111.11111111.11111111.00000000

réseau: 11000000.10101000.00000001.00000000

Même adresse de réseau = même réseau logique

VLSM

CIDR et IPv4

- **CIDR alloue efficace des adresses v4**
 - CIDR permet de coller assez finement aux demandes
 - Récupération d'anciennes adresses A, B ou C
 - Un prestataire Internet .ISP. attribue librement ses adresses
 - La découpe peut opérer à tous les niveaux
- **CIDR permet d'agréger les routes à tous les niveaux**
 - Contrôle de la taille des tables de routage
 - Facilite l'administration des routeurs
- **CIDR présente les inconvénients de la hiérarchisation:**
 - Si une organisation souhaite changer de prestataire sans changer d'adresse on doit créer une route d'exception ce qui est coûteux (autre solution voir plus loin NAT)

VLSM

- (**V**ariable **L**ength **S**ubnet **M**ask) permet à un réseau classless d'utiliser différents masques de sous-réseaux au sein d'une organisation
- Avoir sous-réseaux plus appropriés aux besoins

Masques de longueur variable

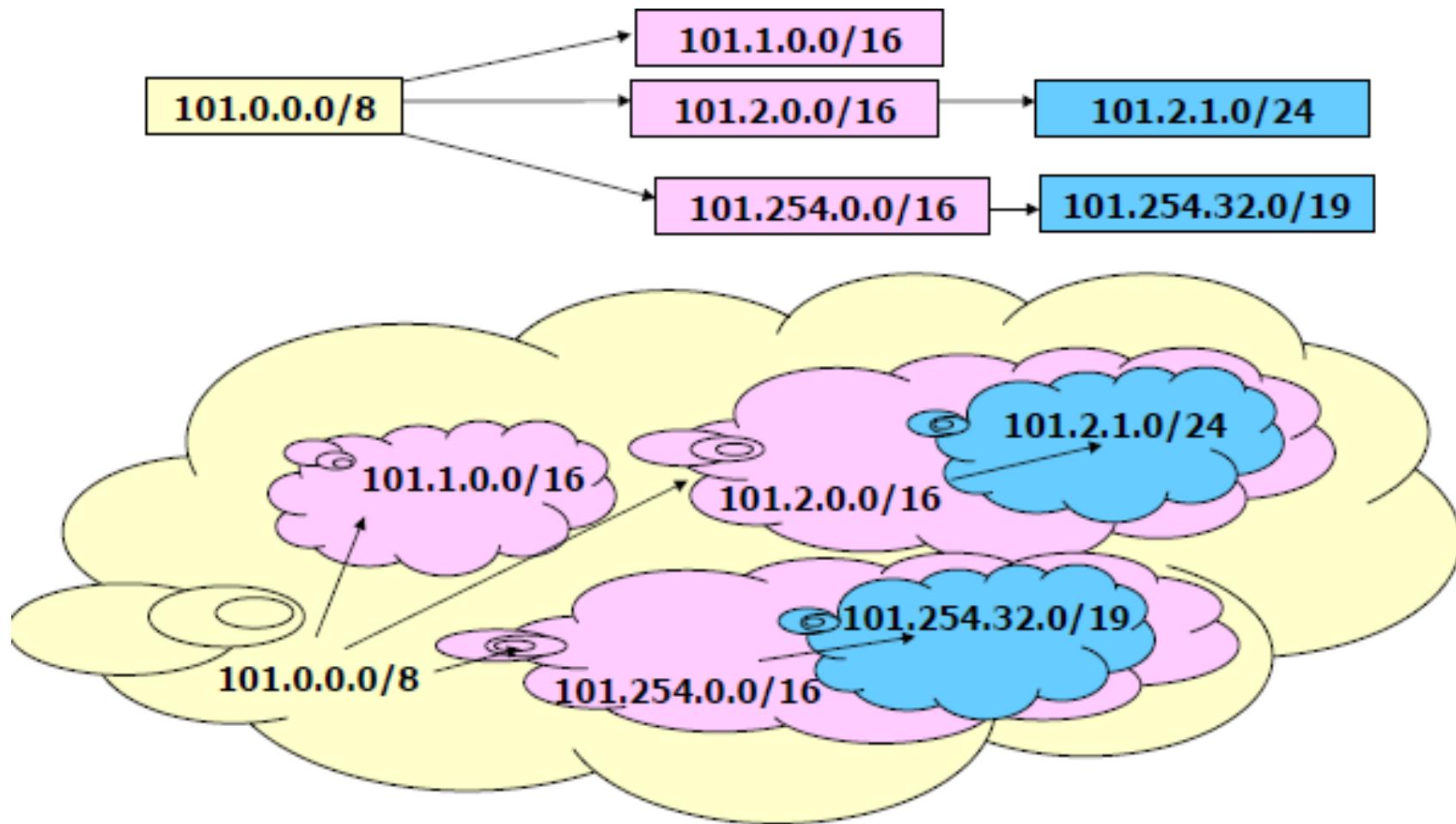
VLSM Variable Length Subnet Mask

- Besoin: créer des sous réseaux de taille différente
- Exemple : Classe B 135.8.0.0/16 découpé par le masque 255.255.254.0 ou /23 (soit $2^7 = 128$ sous-réseaux de $2^9 - 2 = 510$)
- Il se crée un nouveau sous-réseau de 15 hôtes (extension prévisible à 50)
 - Si on lui attribue une adresse de sous-réseau /23 on va perdre environ 500 adresses
 - Il serait par contre très intéressant de lui attribuer une adresse /26 d'un sous réseau de $64 - 2 = 62$ hôtes
- La solution : VLSM Variable Length Subnet Mask (RFC 1009 en 1987) : masques de taille variable

Problèmes posés par VLSPM : Gestion des masques

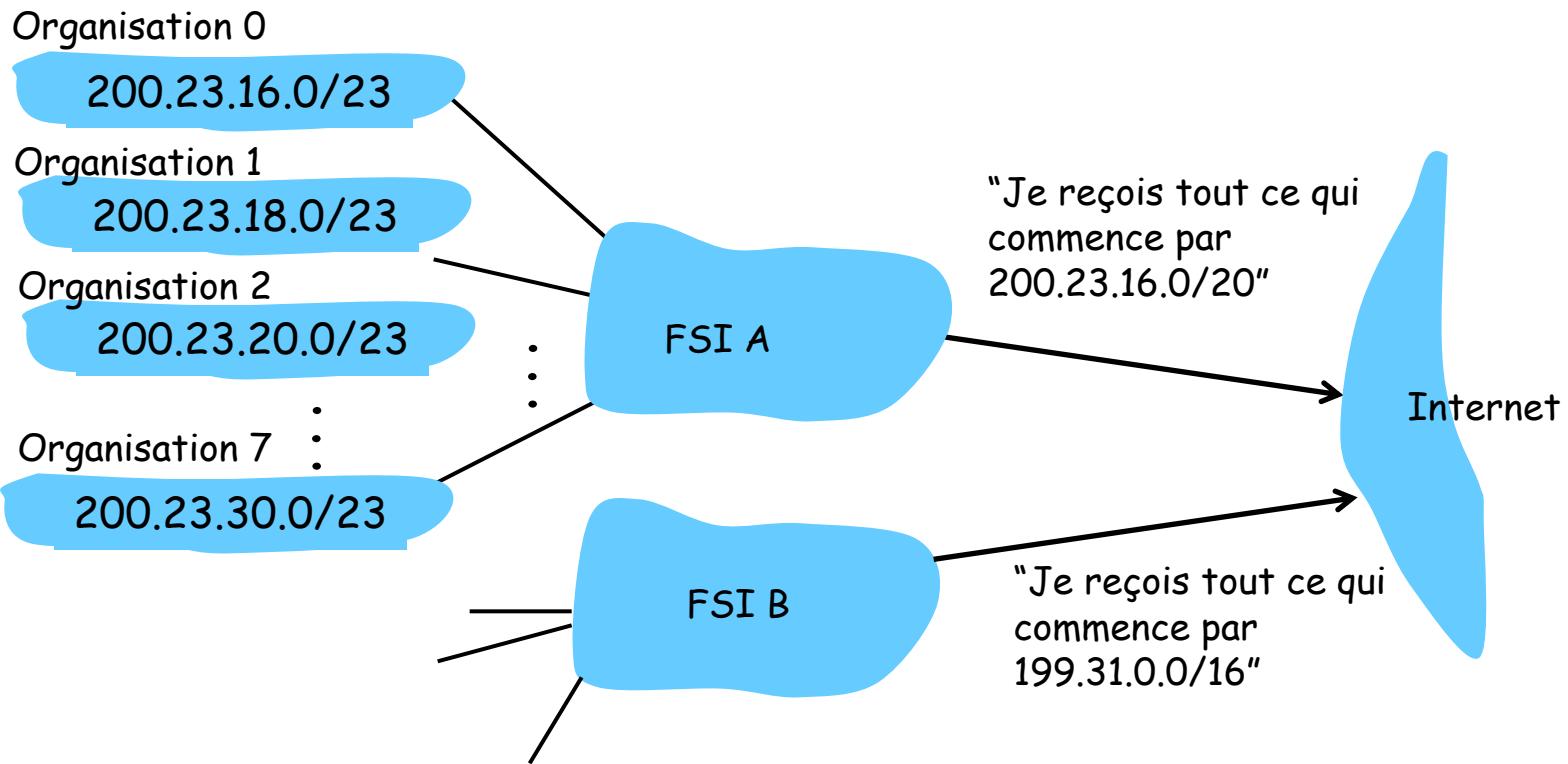
- Chaque sous-réseau possède sa propre taille
 - Pour déterminer correctement le numéro de réseau quelque soit sa taille
 - Le protocole de routage interne doit utiliser un masque (un préfixe étendu) différent pour chaque sous réseau
 - Il doit transférer ces masques dans chaque route
- => Modifier les protocoles de routage
- RIP V2 ('Routing Information Protocol' RFC1388)
 - La version 2 permet de déployer VLSPM.
 - OSPF ('Open Shortest Path First')

Exemple de gestion d'adresse avec agrégation 'topologique' en VLSM

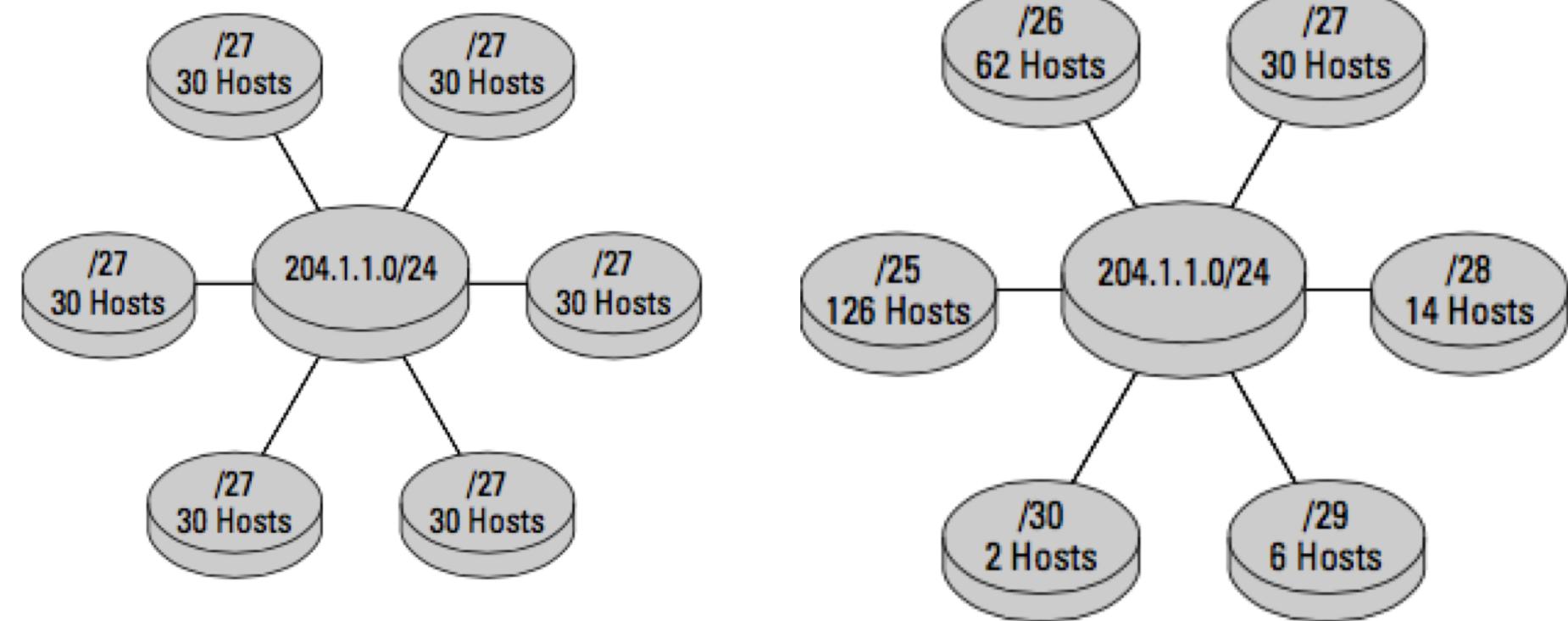


Adressage hiérarchique: agrégation de routes

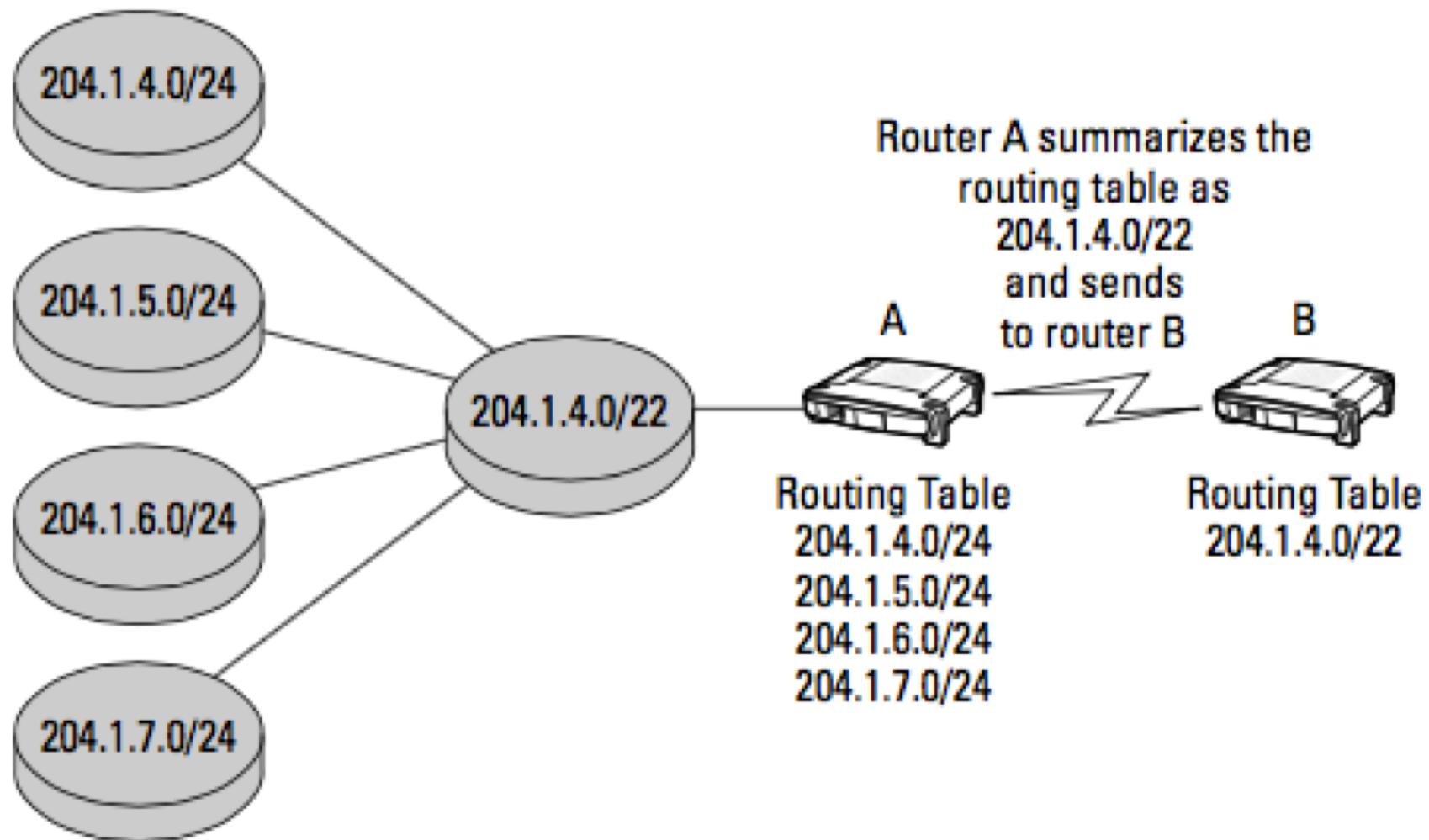
Le routage hiérarchique permet une annonce efficace des informations de routage



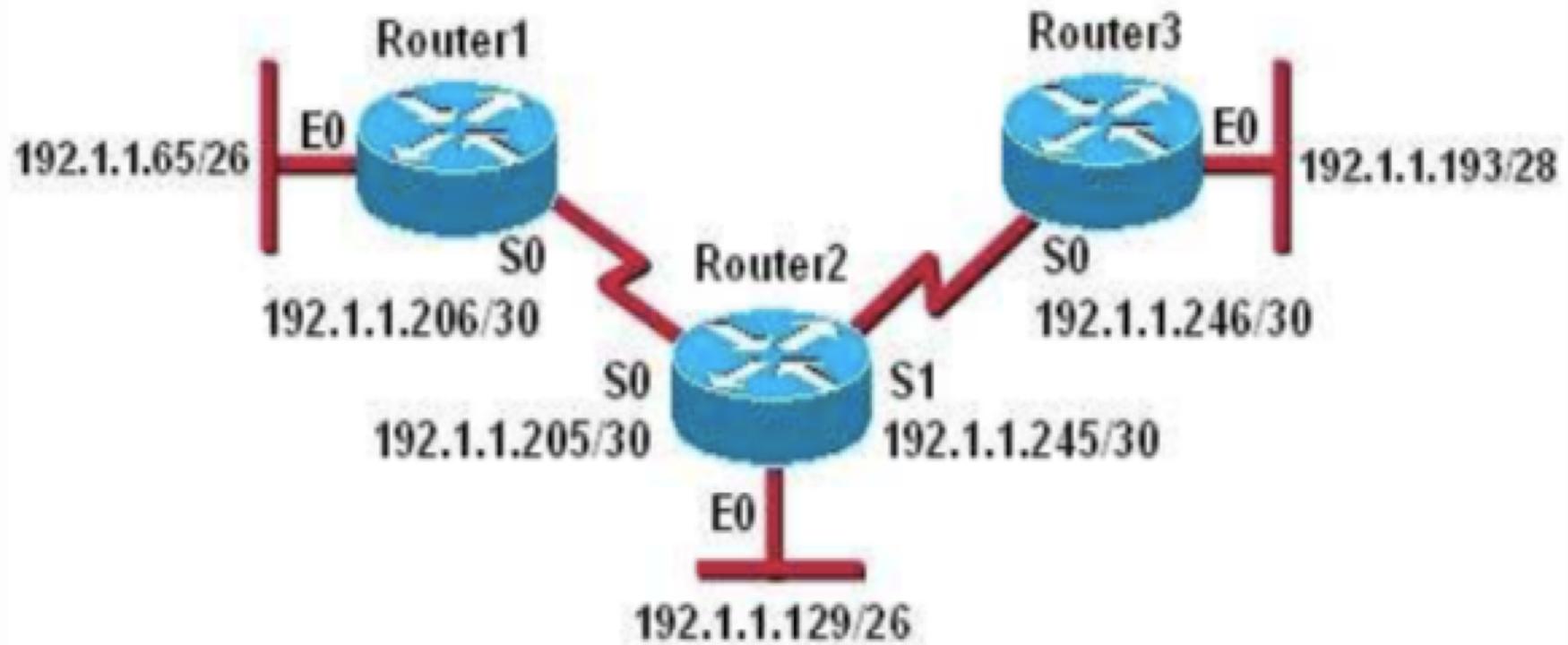
Etudier les pertes



Résumé de route

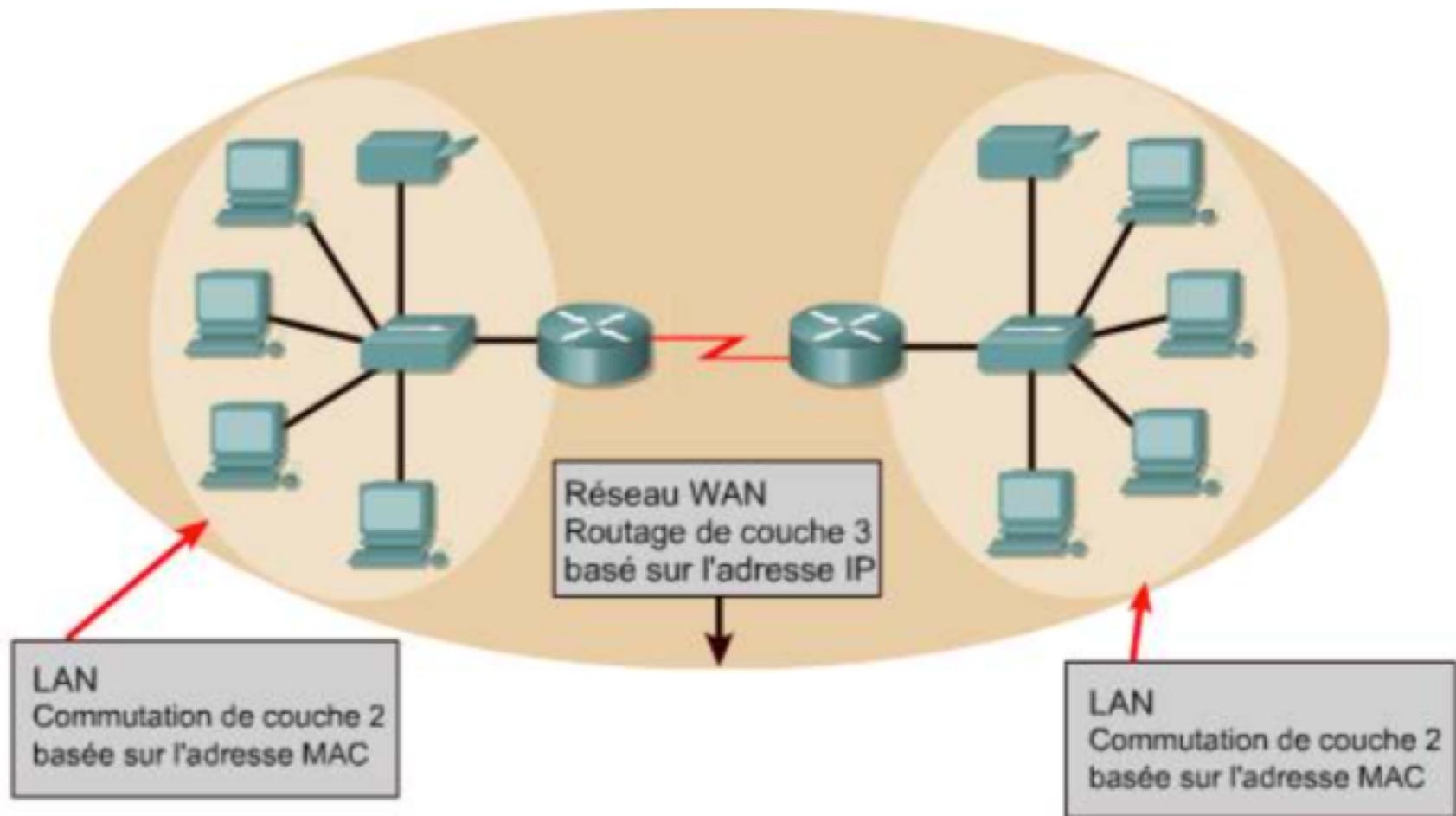


Trouver l'incohérence !



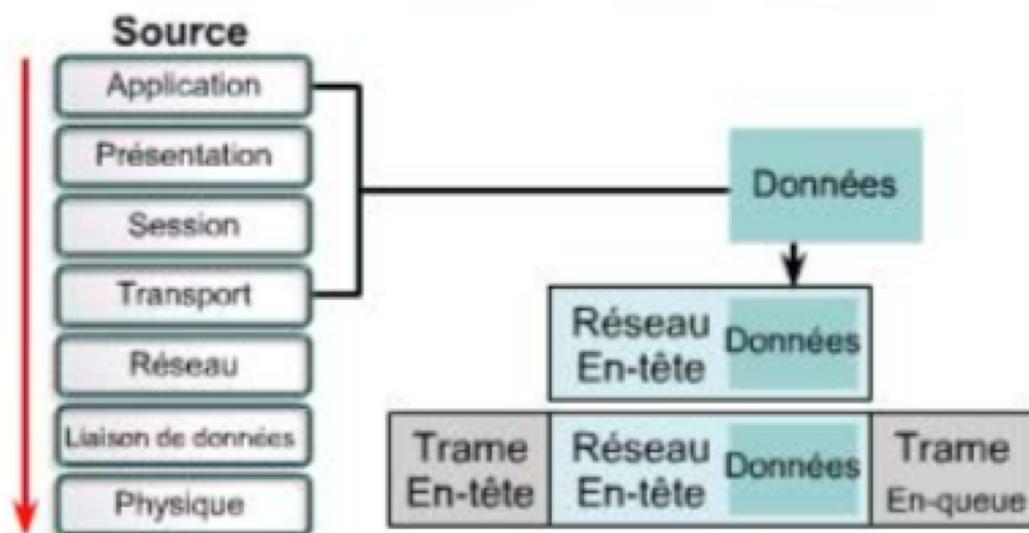
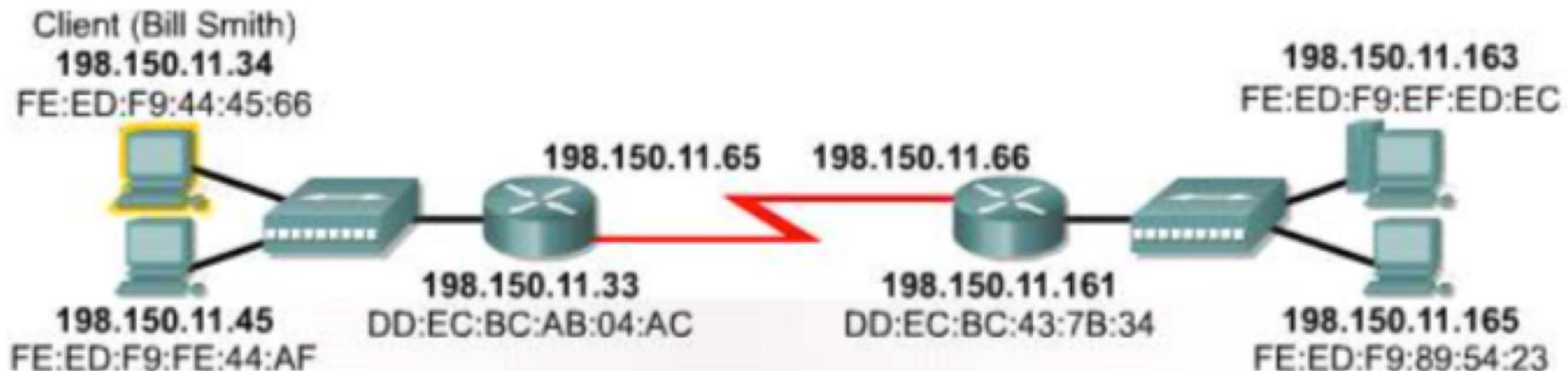
COMMUTATION VS ROUTAGE

Commutation et routage

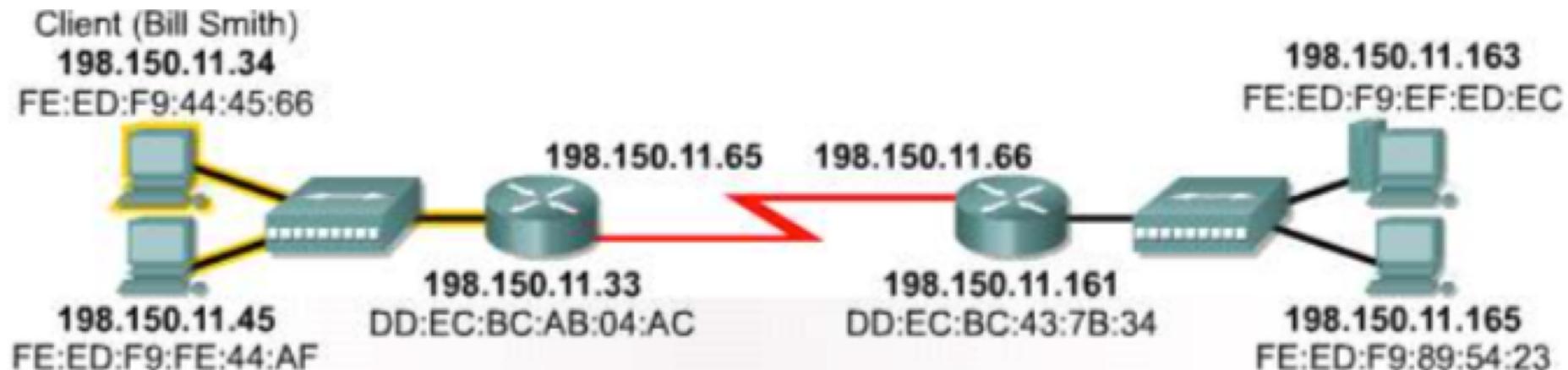


La commutation de couche 2 s'effectue au sein du réseau LAN. Le routage de couche 3 achemine le trafic entre les domaines de broadcast. Cela nécessite le format d'adressage hiérarchique d'un système d'adressage de couche 3, tel que IP.

Commutation vs routage

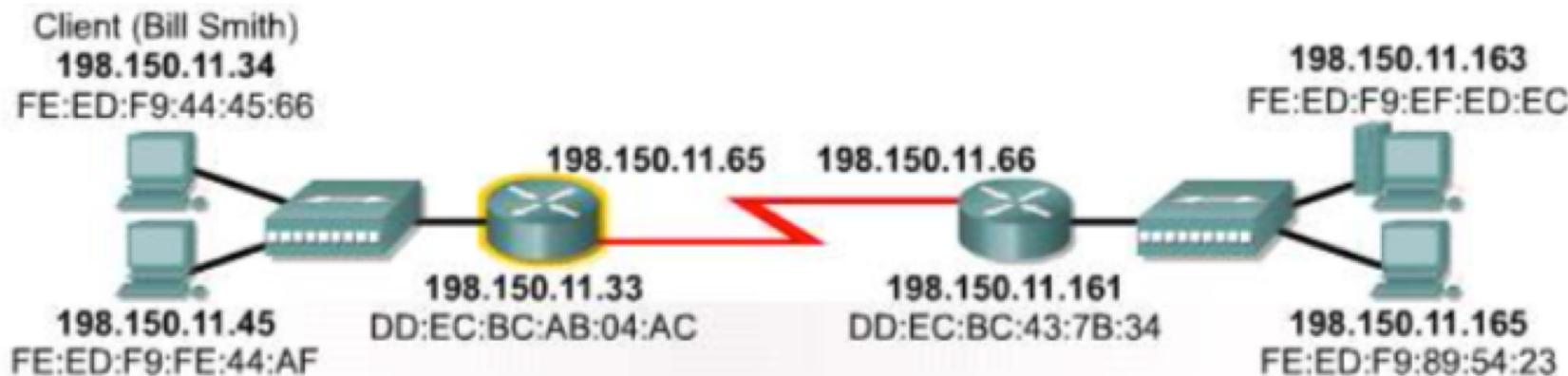


Commutation vs routage (suite)



Trame En-tête		Réseau En-tête		Données		Trame En-queue
Destination	Source	Source	Destination			
DD:EC:BC:AB:04:AC	FE:ED:F9:44:45:66	198.150.11.34	198.150.11.163	Courrier électronique	Données	CRC-32

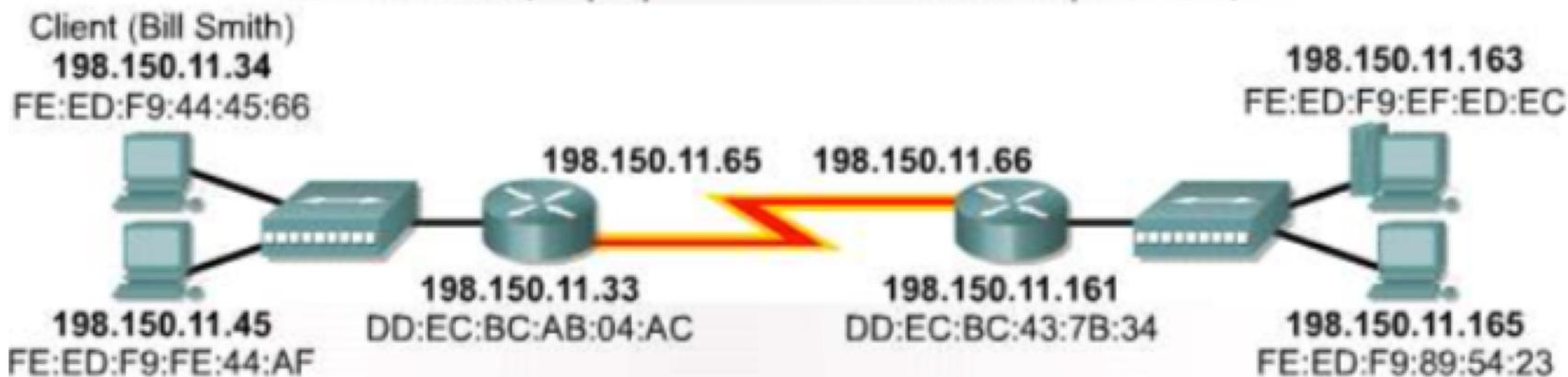
Commutation vs routage (suite)



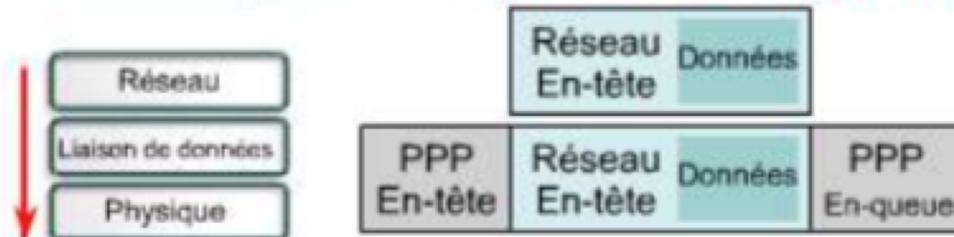
198.150. 11.163	Adresse IP
255.255.255.224	Masque de sous-réseau
198.150. 11.160	Résultat

Le routeur applique le masque de sous-réseau à l'adresse de destination. Il compare ensuite le résultat avec sa table de routage. La table indique que pour accéder au réseau 198.150.11.160, le paquet doit être transmis au port série,

Le routeur applique le masque de sous-réseau à l'adresse de destination. Il compare ensuite le résultat avec sa table de routage. La table indique que pour accéder au réseau 198.150.11.160, le paquet doit être transmis au port série,

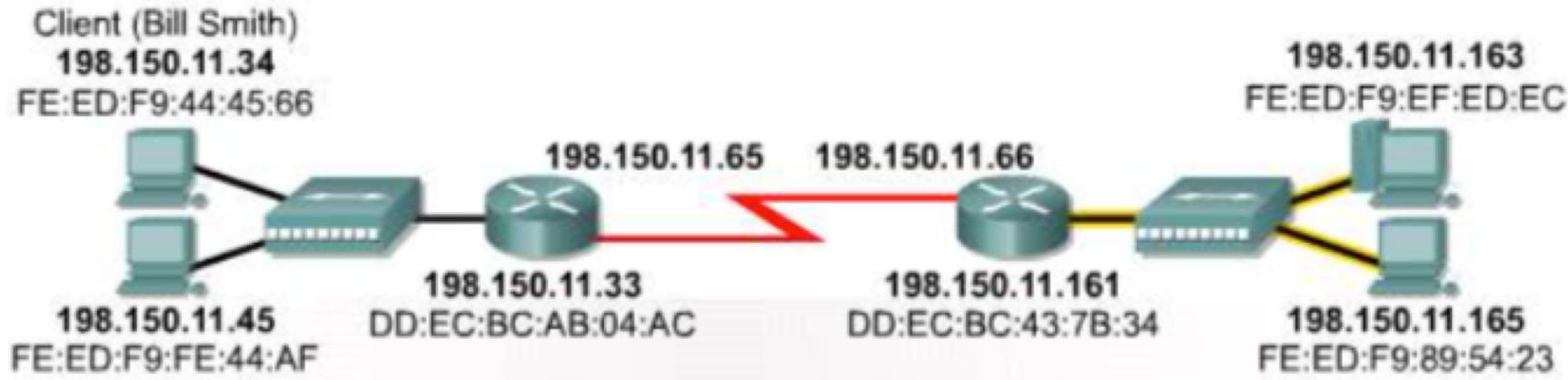


Trame En-tête		Réseau En-tête		Données	Trame En-queue
Destination	Source	Source	Destination		
PPP	PPP	198.150.11.34	198.150.11.163	Courrier électronique	CRC-32

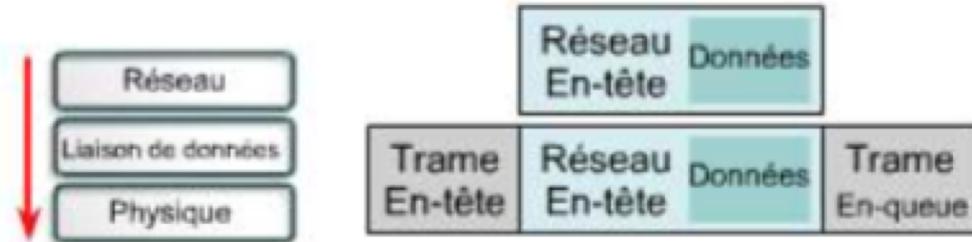


La demande est encapsulée pour une transmission série, puis envoyée au routeur

A l'arrivée de l'information

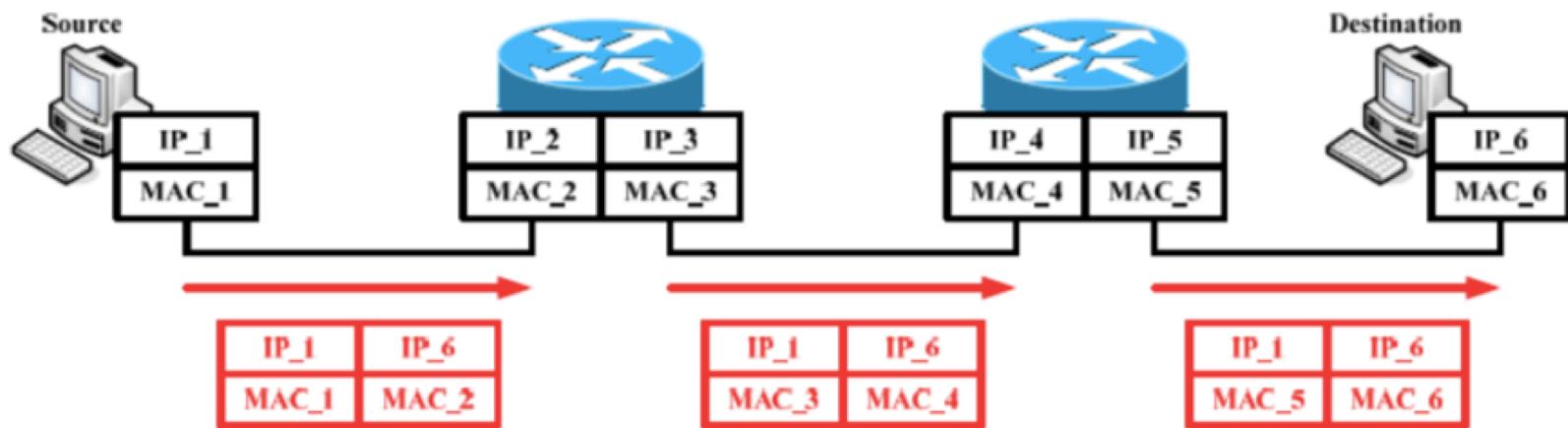
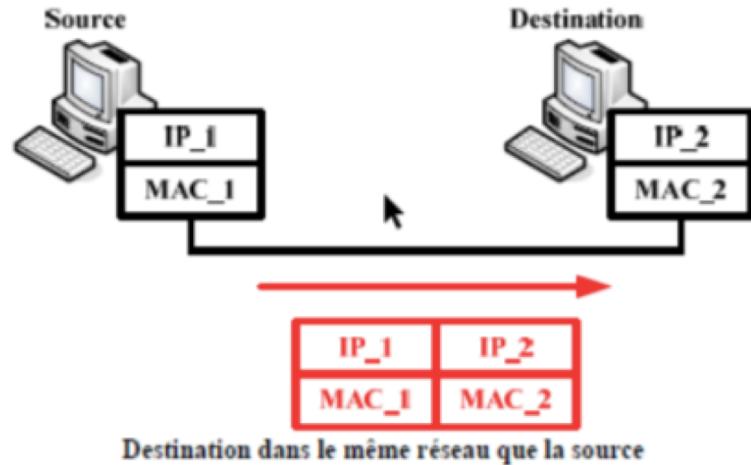


Trame En-tête		Réseau En-tête		Données	Trame En-queue
Destination	Source	Source	Destination		
FE:ED:F9:EF:ED:EC	DD:EC:BC:43:7B:34	198.150.11.34	198.150.11.163	Courrier électronique	CRC-32



La demande est encapsulée pour la transmission Ethernet et envoyée sur le segment Ethernet. Toutes les stations de travail prennent la trame et vérifient si elle leur est destinée. Toutes les unités, à l'exception de l'ordinateur doté

Résumé



ROUTAGE

Le routage à travers le réseau



Routage statique vs dynamique

- **Statique** : Tout est géré manuellement par un administrateur réseau qui enregistre toutes les informations dans la configuration d'un routeur
 - Il doit mettre à jour manuellement les entrées de route statique chaque fois qu'une modification de la topologie le nécessite.
- **Dynamique** : Une fois qu'un administrateur réseau a entré les commandes de configuration pour lancer le routage dynamique, les informations relatives aux routes sont mises à jour automatiquement, par un processus de routage

Métriques utilisées

- **Bandé passante** : Le débit d'une liaison, mesuré en bits par seconde
- **Délai** : Le temps requis pour acheminer un paquet, de la source à la destination
- **Charge** : La quantité de trafic sur une ressource réseau telle qu'un routeur ou une liaison
- **Fiabilité** : Cette notion indique généralement le taux d'erreurs sur chaque liaison du réseau
- **Nombre de sauts** : Le nombre de routeurs par lesquels un paquet doit passer avant d'arriver à destination
- **Tics** : L'intervalle de temps entre 2 trames pour une liaison de donnée précise (environ 55 millisecondes)
- **Coût** : Généralement basée sur une dépense monétaire attribuée à un lien par un administrateur réseau

Convergence d'un protocole de routage

- La convergence est le fait que tous les dispositifs réseau ont la même vue de la topologie du réseau
- Le temps de convergence est donc le temps pendant lequel les dispositifs réseaux n'ont pas la même vue de celui-ci
- Lorsque tous les routeurs d'un réseau utilisent les mêmes informations, le réseau est convergent
- Une convergence rapide est recommandée pour un réseau, car elle réduit la période au cours de laquelle les routeurs prennent des décisions de routage incorrectes ou inefficaces

Boucles de routage

- Des boucles de routage peuvent se produire si la convergence lente d'un réseau avec une nouvelle configuration entraîne des entrées de routage incohérentes
- Les paquets tournent sans cesse sur une boucle bien que le réseau de destination soit en panne
- Pour tenter de contrer les boucles de routages, il existe :
 - Métrique de mesure infinie (Finite State Metric)
 - Split Horizon
 - Route Poisoning
 - Mises à jour déclenchées (Triggered Updates)
 - Compteurs de retenue (Hold-down Timers)

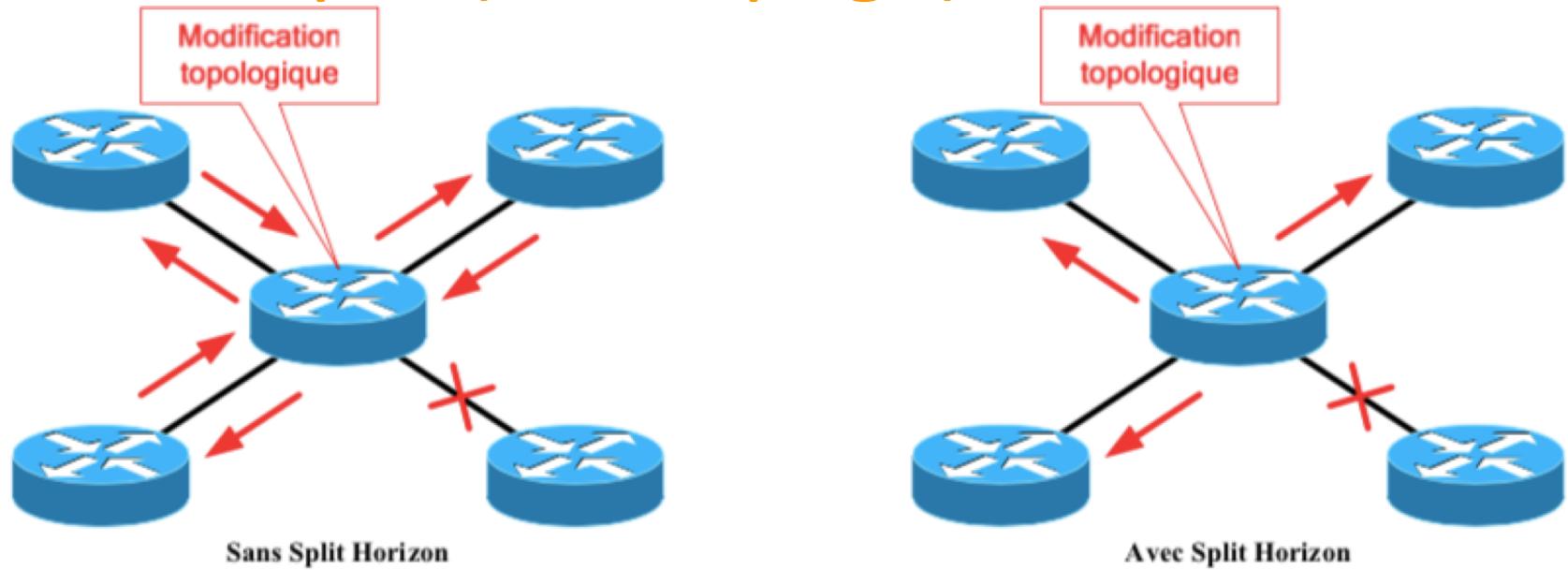
Boucles de routage (suite)

- Ces cinq méthodes sont uniquement utilisées par les protocoles de routage à vecteur de distance, afin d'essayer de contrer les plausibles boucles de routage
- On ne se préoccupe que de la table de routage avec ces cinq solutions, car le problème des paquets en eux-mêmes est réglé automatiquement grâce au principe de TTL (Time To Live)

Contrer les boucles de routage : Métrique de mesure infinie

- Le principe est de définir l'infini en tant que nombre maximum spécifique
- Ce nombre se réfère à une métrique de routage. Grâce à cette méthode, le protocole de routage permet à la boucle de routage d'exister jusqu'à ce que la métrique dépasse la valeur maximale autorisée
- Le réseau en panne est considéré comme inaccessible lorsque la valeur métrique atteint la valeur maximale

Contrer les boucles de routage : Split (découpage) Horizon

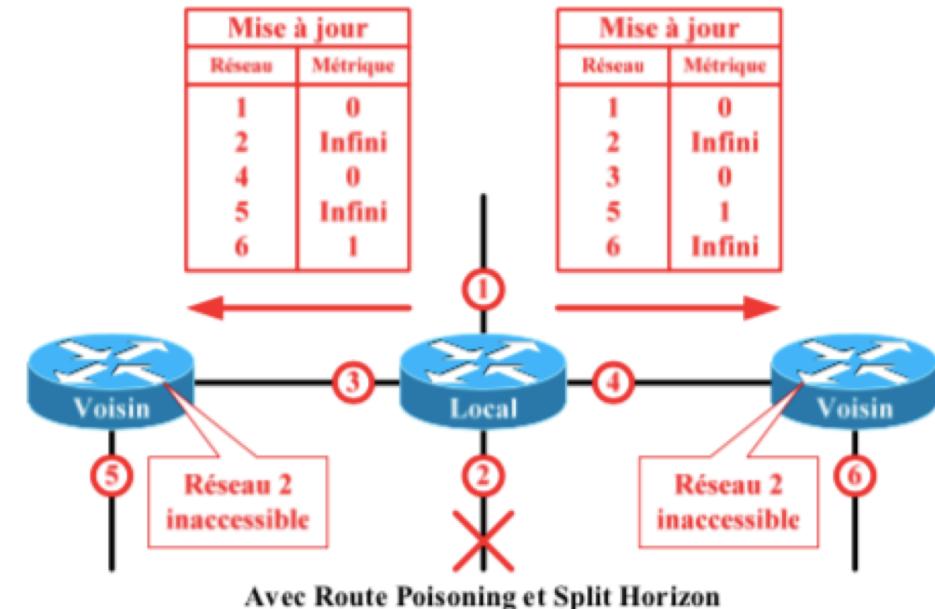
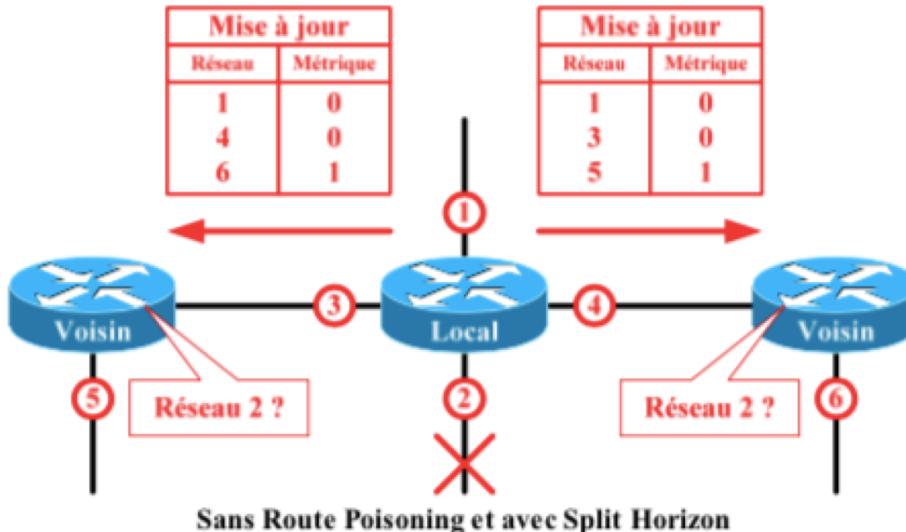


- Aucune information de mise à jour ne sera renvoyée par le chemin par lequel on a appris la modification de topologie
 - Permet d'éviter de renvoyer à la source des informations erronées
- L'information se propage toujours du plus près du réseau de destination au plus éloigné, sans jamais revenir en arrière

Contrer les boucles de routage : Route Poisoning

- Le Route Poisoning, aussi appelé Poison Reverse, est utilisé lorsqu'un réseau devient inaccessible
- Au lieu de n'avertir que les routes existantes dans la table de routage aux voisins, le Route Poisoning inclut aussi les routes devenues inaccessibles en leur octroyant une métrique infinie
 - Permet d'informer directement les voisins qu'un réseau est devenu inaccessible au lieu d'attendre l'expiration de leur compteur d'invalidité (Invalid Timer).

Route Poisoning (suite)



- Combiné au Split Horizon, le Route Poisoning n'exclut pas les routes concernées par la règle du Split Horizon mais leur attribue une métrique infinie

Contrer les boucles de routage : Mises à jour déclenchées

- Les mises à jour déclenchées servent à informer les voisins d'une modification topologique au moment où elle survient
- Permettent de réduire le temps de convergence en n'attendant pas l'expiration de l'intervalle de temps de transmission des mises à jour périodique

Contrer les boucles de routage : Compteurs de retenue

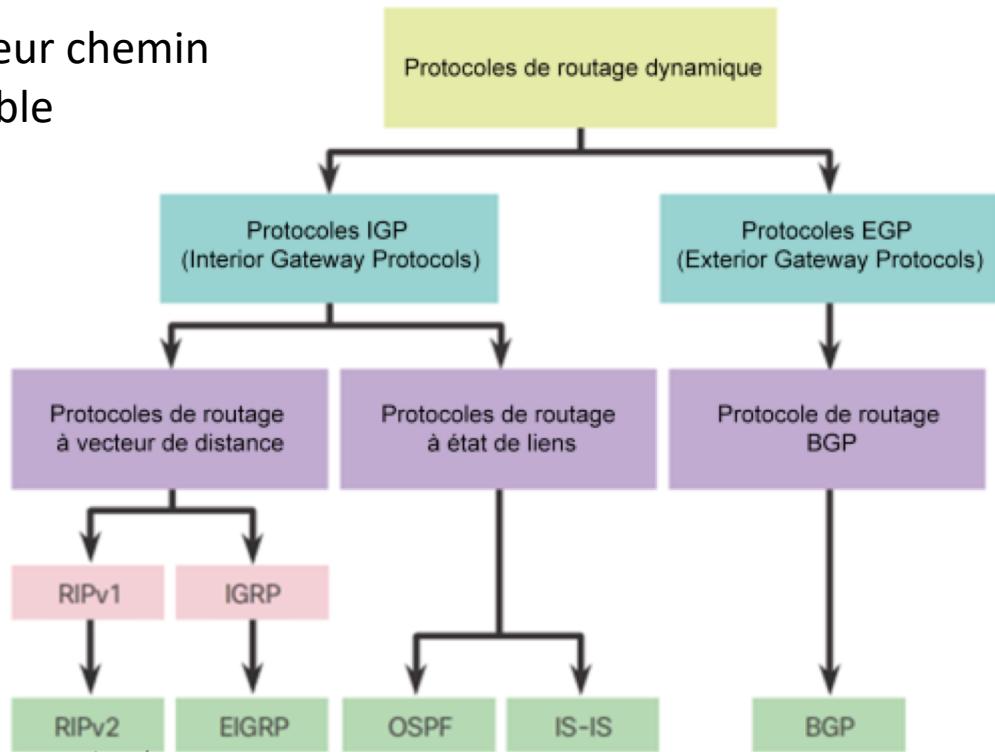
- Permettent d'éviter de changer l'état d'une entrée dans la table de routage impunément
- Ils ont pour but de laisser le temps à l'information d'atteindre l'intégralité du réseau avant de modifier de nouveau la même entrée
- Ils fonctionnent de la façon suivante :
 - Lorsqu'une modification est effectuée sur une entrée de la table de routage, on lance un compteur de retenue pour cette entrée
 - Si une mise à jour contenant une modification pour cette entrée a eu lieu alors que le temps du compteur de retenue est dépassé, alors la modification est appliquée
 - Si une mise à jour contenant une modification pour cette entrée pendant le temps du compteur de retenue, alors le protocole suivra les règles imposées par le principe des compteurs de retenue
-

Compteurs de retenue (suite)

- Les règles imposées par le principe des compteurs de retenue sont les suivantes :
 - On autorise l'activation ou l'amélioration de qualité (métrique) pour une entrée
 - On refuse la désactivation ou la dégradation de qualité pour l'entrée concernée
- Pour calculer le temps à utiliser pour la configuration des compteurs de retenue, il faut multiplier le plus petit nombre de sauts à effectuer pour atteindre le routeur le plus éloigné par l'intervalle de temps entre les mises à jour

Les types de protocoles de routage

- La fonction des protocoles de routage dynamique
 - Découverte des réseaux distants
 - Actualisation des informations de routage
 - Choix du meilleur chemin vers des réseaux de destination
 - Capacité à trouver un nouveau meilleur chemin si le chemin actuel n'est plus disponible
- Les types de protocoles de routage
 - État de liens
 - Vecteur de distance
 - Vecteur de chemin
 - **Hybride (uniquement EIGRP)**

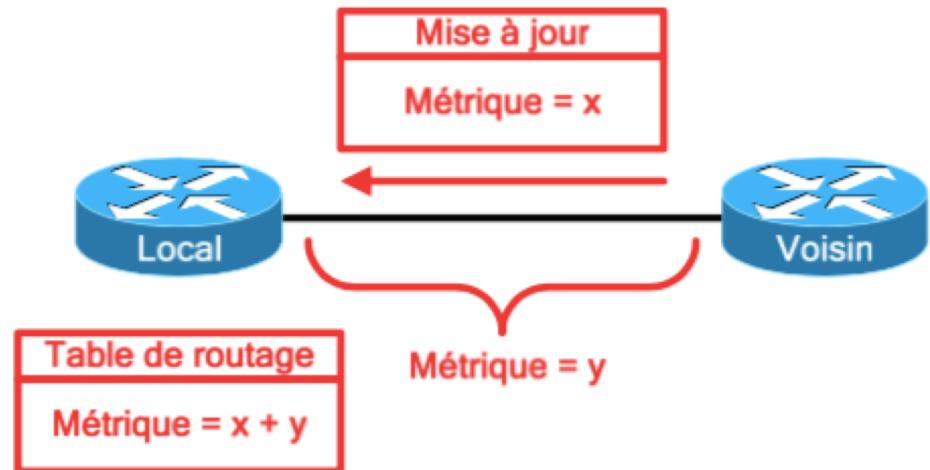


Quelles autres améliorations ont été introduites dans les protocoles RIPv2 et EIGRP ?

Caractéristiques et fonctions	RIPv1	RIPv2	IGRP	EIGRP
Métrique	Les deux technologies utilisent le nombre de sauts comme simple métrique. Le nombre maximal de sauts correspond à 15.		Utilisez à la fois une métrique composée consistant en la bande passante et le délai. La fiabilité et la charge peuvent également être incluses dans le calcul de la métrique.	
Mises à jour transmises à l'adresse	255.255.255.255	224.0.0.9	255.255.255.255	224.0.0.10
Prise en charge de VLSM	✗	✓	✗	✓
Prise en charge de CIDR	✗	✓	✗	✓
Prise en charge de la récapitulation	✗	✓	✗	✓
Prise en charge de l'authentification	✗	✓	✗	✓

Routage à vecteur de distance

- L'algorithme de routage à vecteur de distance possède une vision de la topologie du réseau qui est basée sur celle de ses voisins
- les mises à jour de routage envoyées par les protocoles de routage à vecteur de distance contiennent directement la table de routage du routeur émetteur



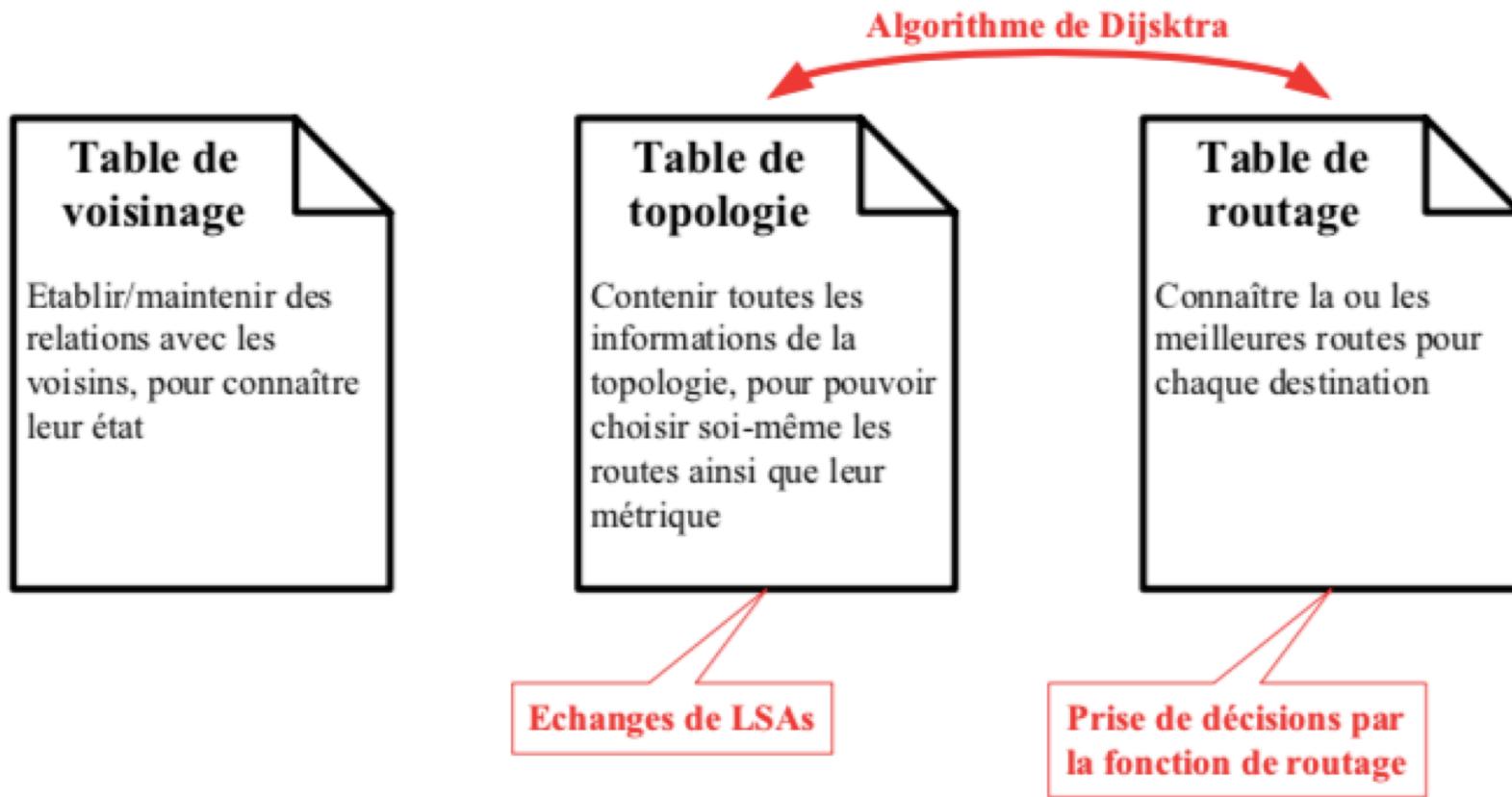
Routage à vecteur de distance (suite)

- Les mises à jour possèdent des caractéristiques précises :
 - Elles sont envoyées périodiquement
 - Elles contiennent directement toutes les entrées de la table de routage de l'émetteur (sauf les entrées supprimées par Split Horizon)
 - Elles sont émises en broadcast (sauf exceptions telles qu'avec RIPv2 et EIGRP)
- La sélection du meilleur chemin, qui sera inclus dans la table de routage, se fait en utilisant **l'algorithme de Bellman Ford**
- Ce dernier se base sur le nombre de sauts pour calculer les métriques
- Une exception existe pour les protocoles de routage à vecteur de distance propriétaires, tels que IGRP et EIGRP de Cisco

Routage à état de liens

- Le principe du plus court chemin d'abord (Shortest Path First) est utilisé. Ce principe est basé sur l'utilisation de :
 - Une table de données topologiques
 - L'**algorithme de Dijkstra**
 - Un arbre du plus court chemin d'abord (SPF Tree)
- Les mises à jour de routage des protocoles à état des liens possèdent de grandes différences comparées à celles des protocoles à vecteur de distance :
 - Elles sont uniquement envoyées lors de modifications topologiques (Triggered Updates)
 - Elles contiennent des informations topologiques (Link State Advertisements)
 - Elles sont incrémentielles
 - Elles sont émises en multicast sur des adresses spécifiques

Routage à états de liens



Tables utilisées par un protocole de routage à état de liens

- Le routage à état de liens se base sur l'utilisation de trois tables distinctes (au contraire des protocoles à vecteur de distance qui ne gèrent que la table de routage)

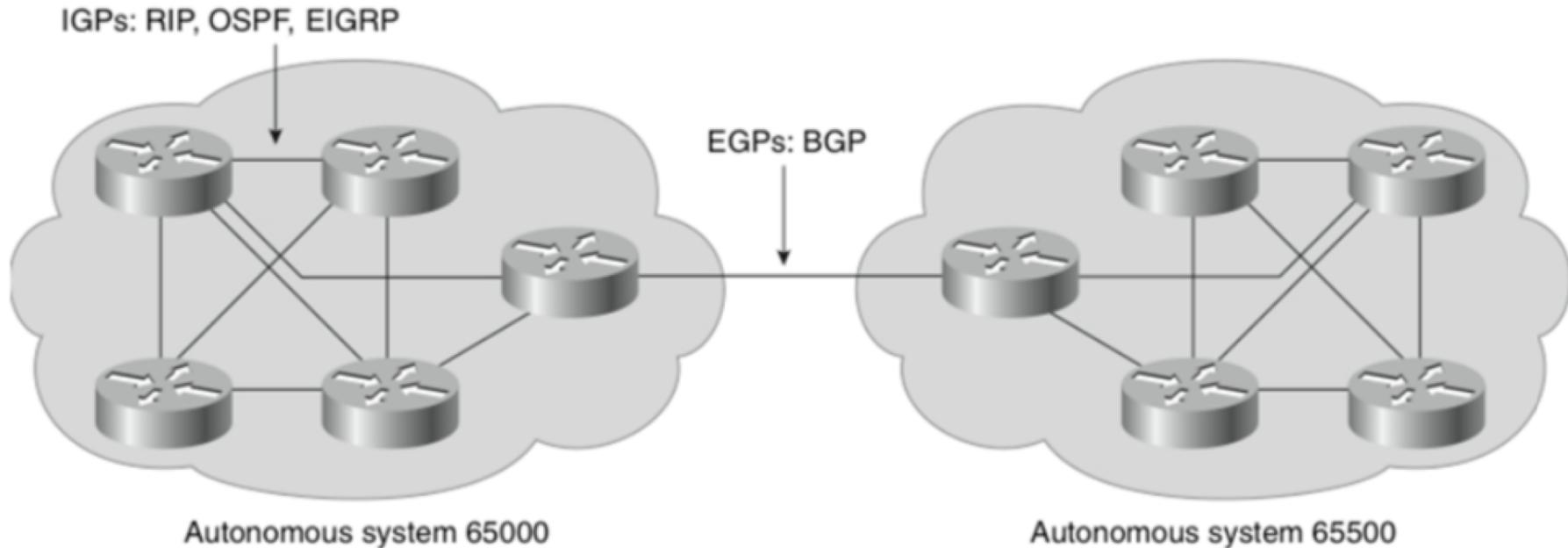
Les bénéfices des protocoles de routage à état de liens

- Avantages
 - Crée une carte topologique complète du réseau pour déterminer le chemin le plus court
 - Diffuse immédiatement le paquet LSP pour atteindre une convergence plus rapide
 - Envoie uniquement le paquet LSP avec de nouvelles informations en cas de modification de la topologie
 - Utilise le concept de zones et prend en charge la récapitulation
- Inconvénients
 - Nécessite de la mémoire supplémentaire pour assurer la maintenance de la base de données et de l'arborescence SPF
 - Requiert davantage de ressources de traitement du CPU pour calculer l'algorithme SPF et créer une carte topologique complète
 - Exige davantage de bande passante lors du démarrage initial des routeurs, ce qui peut poser problème sur les réseaux instables

Systèmes autonomes

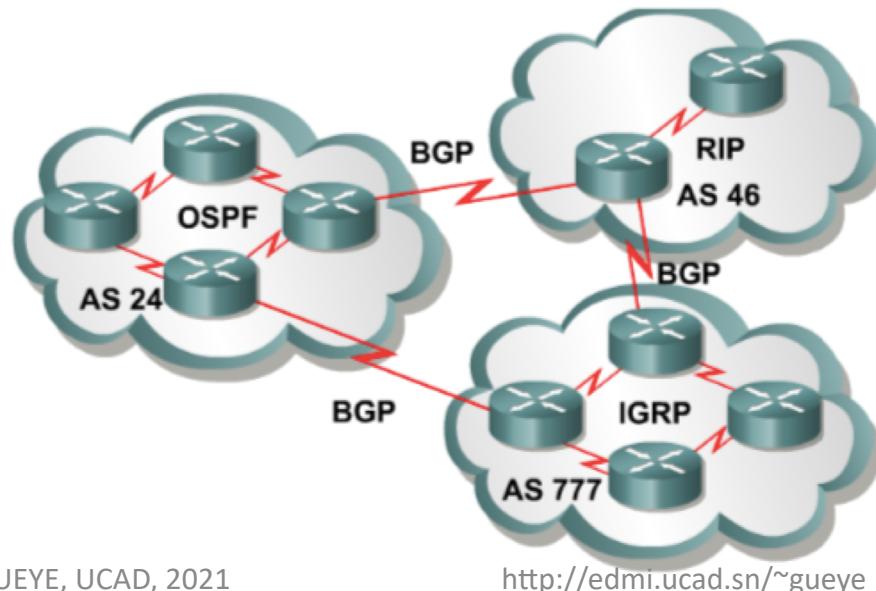
- Un système autonome (AS) défini par le RFC 1772 est, par définition, l'ensemble des dispositifs interconnectés régis par la même administration
- Permet de délimiter la responsabilité du routage à un ensemble défini
- Les numéros des AS sont uniques dans le monde et permettent d'identifier une organisation aux yeux du reste du monde informatique
 - Attribués par une entité (IANA)
 - Entre 1 et 65535
 - Les adresses de 64512 à 65535 sont réservées pour un usage privée
 - Les RFCs 4893 et 5398 proposent l'extension à 4.294.967.296 AS
 - Utilisation de 4 octets au lieu de 2
- Cette notion de système autonome crée donc une nouvelle distinction entre les protocoles de routage

Notions d'AS



Autonomous system 65000

Autonomous system 65500



Protocoles de routage intérieurs et extérieurs

- **Protocoles de routage intérieurs (IGP)** : Protocoles ayant pour mission principale le routage à l'intérieur d'un système autonome
- **Protocoles de routage extérieurs (EGP)** : Protocoles permettant le routage entre les systèmes autonomes
- Les protocoles de routage intérieurs voient un système autonome comme un seul et unique protocole de routage
- De ce point de vue, si plusieurs protocoles de routage existent dans un même système autonome, chaque protocole considérera le protocole adjacent comme externe
- La convergence d'un réseau est restreinte au système autonome et le temps de convergence dépend donc du protocole utilisé dans le système autonome

COMMUTATION

Introduction à la commutation

- En mode point à point, avec N clients on a :

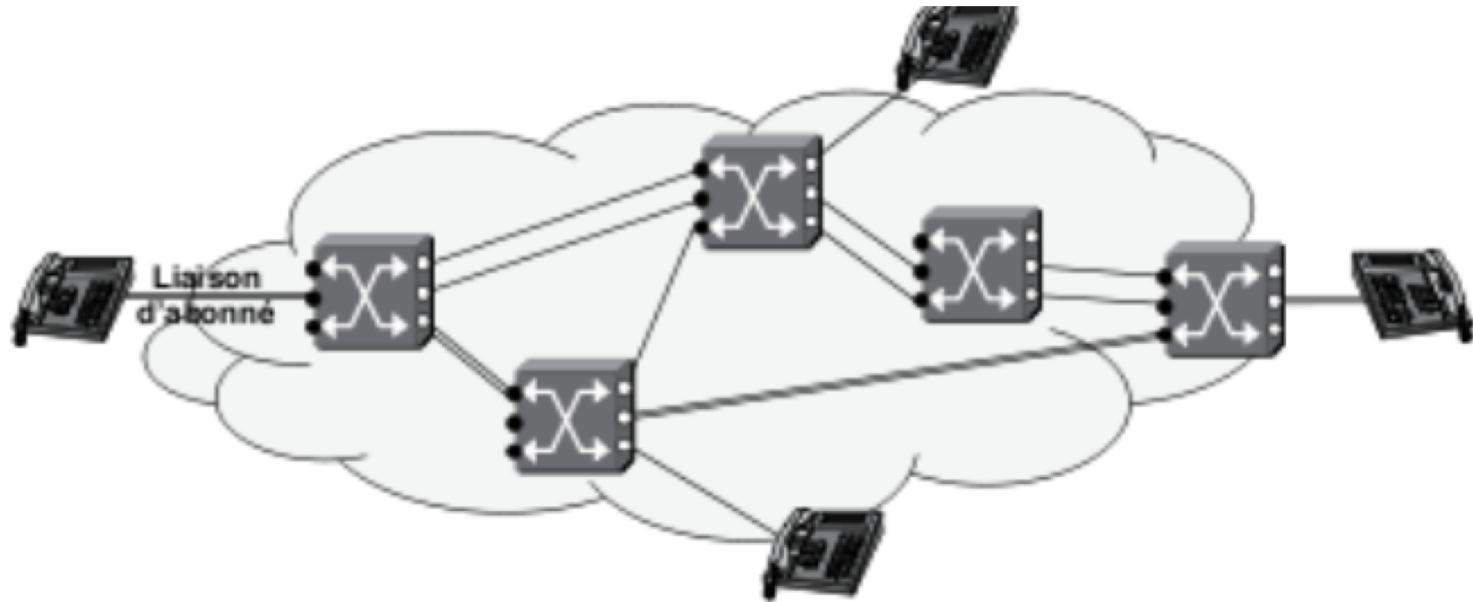
$$\text{Nombre de liens} = \frac{N(N-1)}{2}$$

- Il faut optimiser le partage de ressources, c'est l'objectif des techniques de commutation



Le réseau à commutation de circuit

- La mise en relation physique est réalisé par les commutateurs avant tout échange de données
- Elle est maintenue tant que les entités communicantes ne la libèrent pas expressément



La commutation temporelle

- La commutation de circuits ou commutation spatiale est remplacée par une commutation par intervalle de temps (IT) entre des appels multiplex entrants et des multiplex sortants (commutation temporelle)



Principe commutation de paquets

- Optimiser au maximum l'utilisation du lien, chaque paquet est acheminé indépendamment du précédent
- Les paquets de différentes sources sont multiplexés sur un même circuit cependant chaque paquet contient les informations nécessaires à son acheminement (adresse ou label)



Le multiplexage des sources dans le réseau

- La ressource est banalisée et non attribuée à une communication particulière comme dans la commutation de circuit

