OFPPT

ISTA HAY HASSANI

CISCO

CCNA 3

Switching Basics & Intermediate Routing

Résumé

Réalisé par : **BOUTAHIR Mounir**

Keep Connection to Share Information ★ NAMIRO ★ Keep Connection to Share Information

SOMMAIRE

Module 1

Introduction au routage sans classe (routage CIDR)

VLSM :

Qu'est-ce que la technique VLSM et à quoi sert-elle ?

Avec **VLSM** (Variable-Length Subnet Masks), un administrateur réseau peut utiliser un masque long sur les réseaux qui ne comportent pas beaucoup d'hôtes et un masque court sur les sous-réseaux qui comportent beaucoup d'hôtes.

Qu'est-ce que la technique VLSM et à quoi sert-elle ?

- Crise d'adressage
- L'IETF (Internet Engineering Task Force) a identifié deux problèmes en 1992
- Pénurie d'adresses réseau IPv4 non affectées, en particulier pour la classe B
- Augmentation rapide de la taille des tables de routage de l'Internet

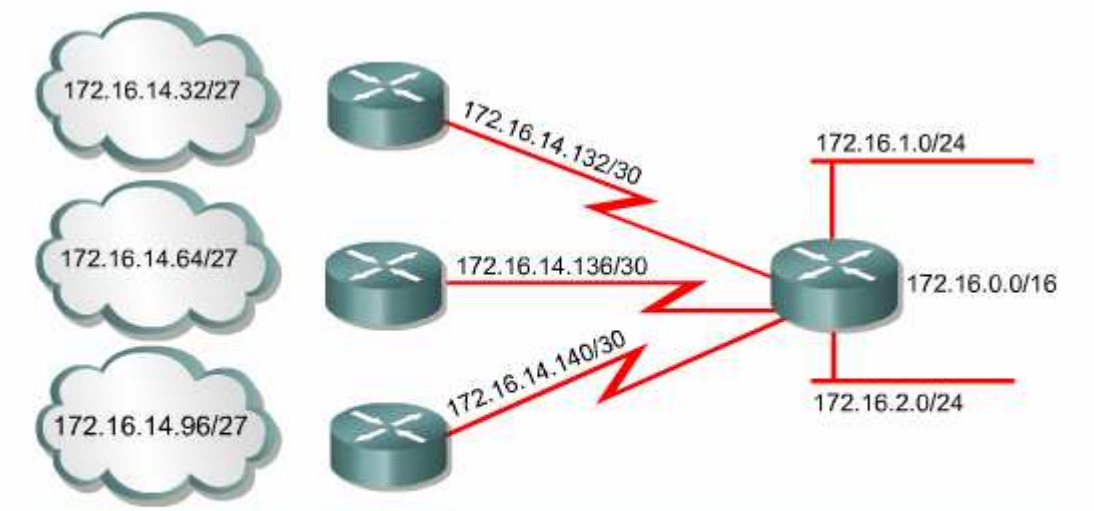
Voici quelques solutions à court terme quant à la pénurie d'adresse IPv4:

Extensions à court terme à IPv4
- Sous-réseaux 1985
- Sous-réseaux de longueur variable 1987
- Routage CIDR 1993
- Adresses IP privées

Pour pouvoir utiliser VLSM, un administrateur réseau doit utiliser un protocole de routage compatible avec cette technique.

→ Les routeurs Cisco sont compatibles avec VLSM grâce aux solutions OSPF Integrated IS-IS, EIGRP, RIP v2 et au routage statique.

La technique VLSM permet à une entreprise d'utiliser plusieurs sous-masques dans le même espace d'adressage réseau → améliorer l'efficacité de l'adressage.



Le sous-réseau 172.16.14.0/24 est divisé en sous-réseaux plus petits

- Découpage en sous-réseaux avec un masque (/27)
- Puis découpage de l'un des sous-réseaux /27 inutilisés en plusieurs sous-réseaux /30

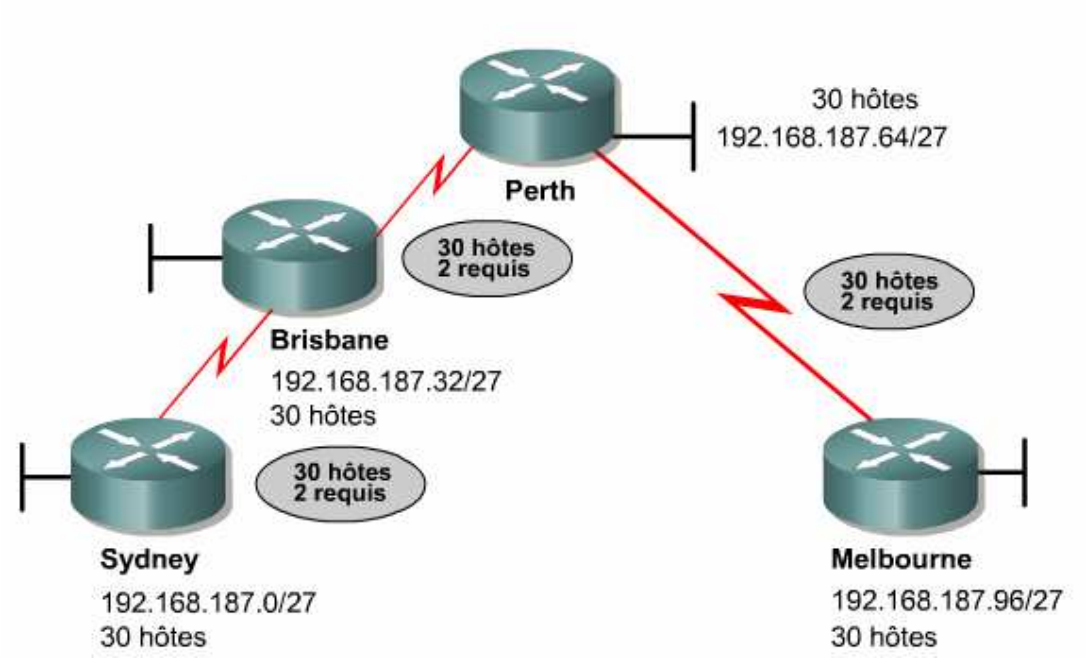
Gaspillage de l'espace

Avec l'évolution des technologies de réseau et la pénurie anticipée d'adresses IP, il est devenu acceptable d'utiliser le premier et le dernier sous-réseau dans un réseau subdivisé en sous réseaux, en association avec la technique VLSM.

No ip subnet-zero → pour ne pas utiliser le premier sous-réseau.

Remarque : à partir de la version 12.0 de Cisco IOS, les routeurs Cisco utilisent le sous-réseau zéro par défaut.

Supposons que nous utiliserons 30 adresses par sous réseau, lors de l'utilisation des connexions point à point, on va gaspiller 28 adresses hôte sur chaque sous-réseau.

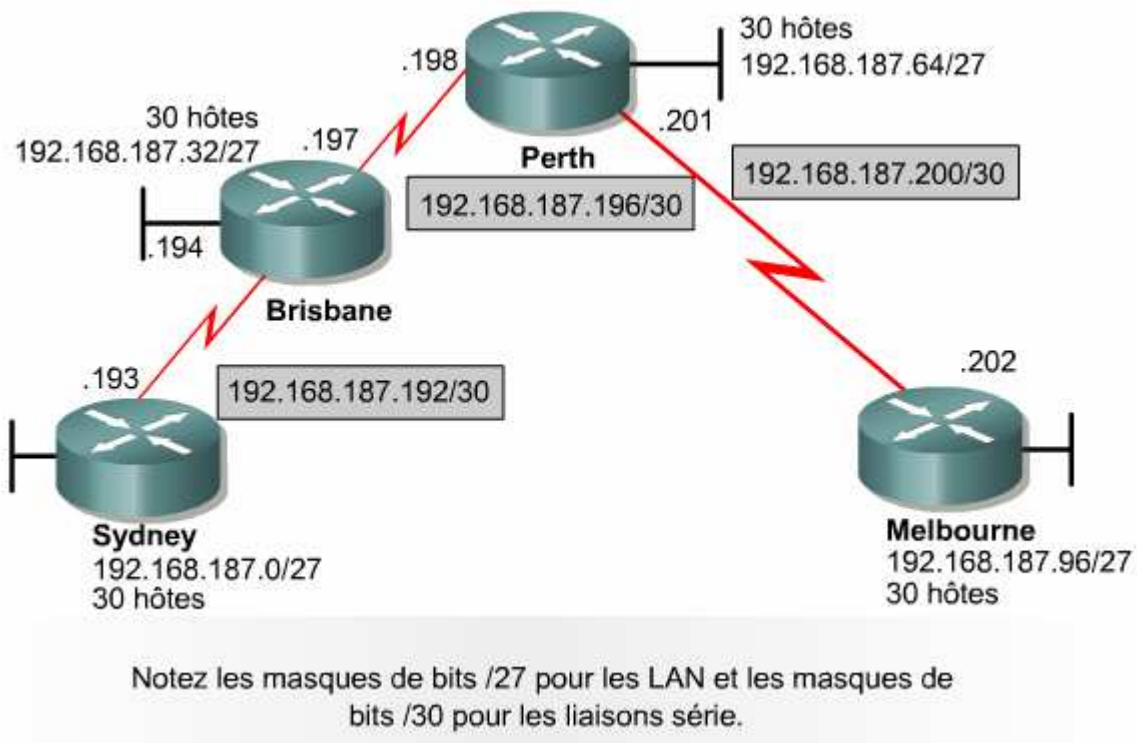


Quand utiliser VLSM ?

VLSM autorise la subdivision en sous-réseaux d'une adresse déjà divisée.

Pour appliquer la technique VLSM au problème d'adressage, l'équipe va décomposer l'adresse de classe C en plusieurs sous-réseaux de tailles variables.

→ De grands sous-réseaux sont créés pour l'adressage des LAN.
→ De très petits sous-réseaux sont créés pour les liaisons WAN.



Dans cet exemple, l'équipe a récupéré un des trois derniers sous-réseaux, le sous-réseau 6, et l'a encore subdivisé en sous-réseaux. Cette fois-ci, l'équipe utilise un masque de 30 bits.

Calcul des sous-réseaux avec VLSM

Adresse de réseau subdivisé : 172.16.32.0/20
Format binaire : 10101100.00010000.00100000.00000000
Adresse VLSM : 172.16.32.0/26
Format binaire : 10101100.00010000. 0010 0000.00 000000

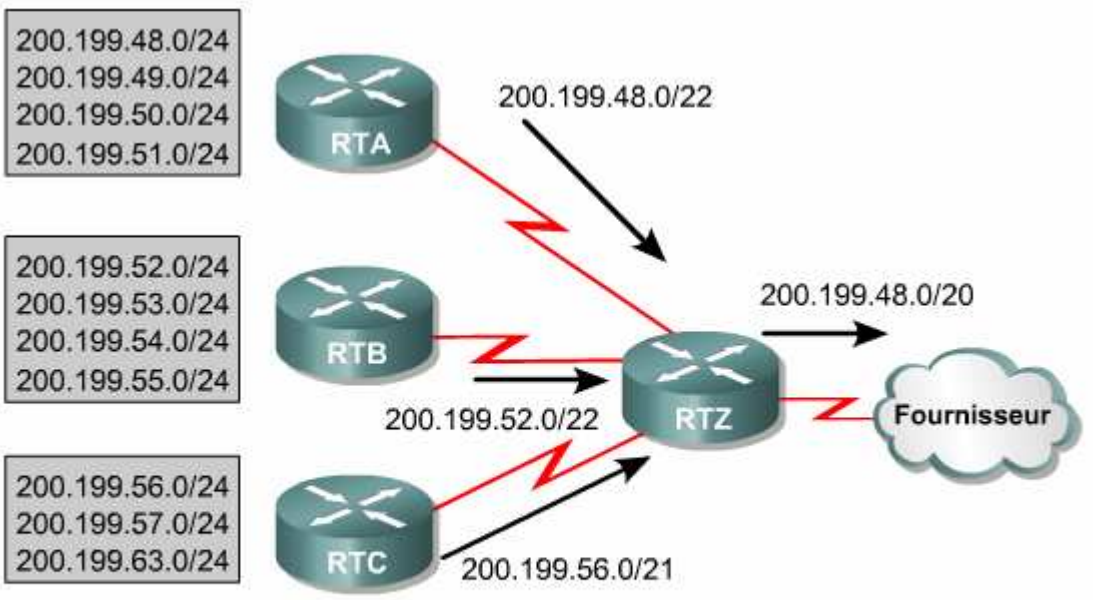
	Réseau			Sous-réseau	Sous-réseau VLSM	Hôte	
1er sous-réseau :	172	•	16	.0010	0000.00	000000	= 172.16.32.0/26
2e sous-réseau :	172	•	16	.0010	0000.01	000000	= 172.16.32.64/26
3e sous-réseau :	172	•	16	.0010	0000.10	000000	= 172.16.32.128/26
4e sous-réseau :	172	•	16	.0010	0000.11	000000	= 172.16.32.192/26
5e sous-réseau :	172	•	16	.0010	0001.00	000000	= 172.16.33.0/26

Remarque : seuls les sous-réseaux inutilisés peuvent être subdivisés. Si une des adresses d'un sous-réseau est utilisée, ce sous-réseau ne peut plus être subdivisé.

Regroupement de routes avec VLSM

Lorsque vous utilisez VLSM, essayez de grouper les numéros des sous-réseaux du réseau pour pouvoir utiliser le regroupement.

Par exemple : les réseaux 172.16.14.0 et 172.16.15.0 doivent être proches l'un de l'autre pour que les routeurs n'aient qu'une route à gérer pour 172.16.14.0/23.



Le résumé de routes réduit la taille de la table de routage en regroupant les routes vers plusieurs réseaux en une même route SUPERNET.

- Un routeur doit parfaitement connaître les numéros des sous-réseaux qui lui sont connectés.
- Un routeur n'a pas besoin de signaler individuellement chaque sous-réseau aux autres routeurs s'il peut se contenter d'envoyer une route globale.
- Un routeur qui utilise des routes globales peut réduire le nombre d'entrées de sa table de routage.

VLSM permet le résumé de routes et améliore la flexibilité en basant entièrement le mécanisme de résumé sur le *partage des bits de valeur supérieure situés à gauche*, même si les réseaux ne sont pas contigus.

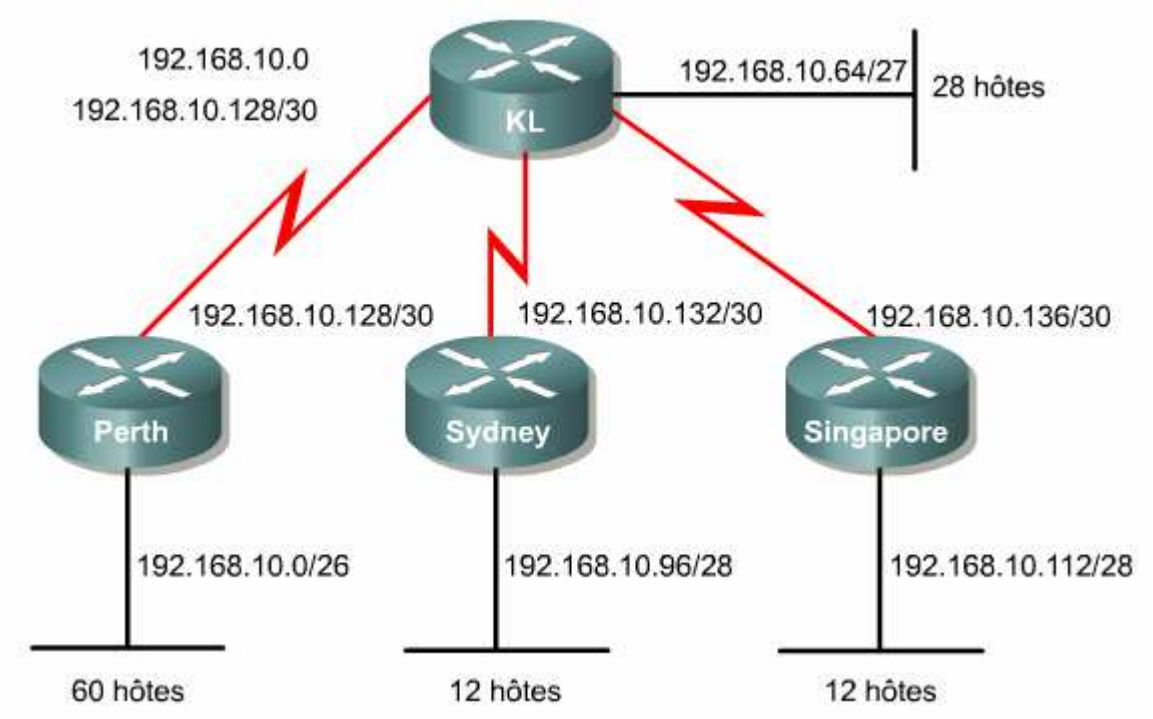
Remarque : Le résumé de routes, aussi appelé « supernetting », ne peut être utilisé que si les routeurs d'un réseau exécutent un protocole de routage CIDR

Exemple :

Adresses	Premier Octet	Second Octet	Troisième Octet	Quatrième Octet
192.168.98.0	11000000	10101000	01100010	00000000
192.168.99.0	11000000	10101000	01100011	00000000
192.168.100.0	11000000	10101000	01100100	00000000
192.168.101.0	11000000	10101000	01100101	00000000
192.168.102.0	11000000	10101000	01100110	00000000
192.168.105.0	11000000	10101000	01101001	00000000
La route sommaire est 192.168.96.0/20				
192.168.96.0	11000000	10101000	01100000	00000000

Le tableau montre que les adresses, ou les routes, partagent les 20 premiers bits, 20ème inclus. Ces bits apparaissent en rouge. Le 21ème bit peut varier d'une route à l'autre. Par conséquent, la longueur du préfixe de la route sommaire sera de 20 bits. Ce préfixe est utilisé pour calculer le numéro de réseau de *la route sommaire*.

Exemple de Configuration de VLSM



Adresse réseau: 192.168.10.0

Le routeur Perth doit accueillir 60 hôtes. Dans ce cas, il faut au moins six bits dans la portion hôte de l'adresse. Six bits permettent de générer 62 adresses hôte, $2^6 = 64 - 2 = 62$, la division donne donc **192.168.10.0/26**.

Les routeurs Sydney et Singapore doivent gérer 12 hôtes chacun. Dans ce cas, il faut au moins quatre bits dans la portion hôte de l'adresse. Quatre bits permettent de générer 14 adresses hôte, $2^4 = 16 – 2 = 14$, la division donne donc **192.168.10.96/28** pour Sydney et **192.168.10.112/28** pour Singapore.

Le routeur Kuala Lumpur doit gérer 28 hôtes. Dans ce cas, il faut au moins cinq bits dans la portion hôte de l'adresse. Cinq bits permettent de générer 30 adresses hôte, $2^5 = 32 – 2 = 30$, la division donne donc ici **192.168.10.64/27.**

Les connexions suivantes sont des connexions point à point :

- *Perth vers Kuala Lumpur 192.168.10.128/30* – Comme il ne faut que deux adresses, la portion hôte de l'adresse doit contenir au moins deux bits. Deux bits permettent de générer 2 adresses hôte ($2^2 = 4 – 2 = 2$), la division donne donc ici **192.168.10.128/30**.
- *Sydney vers Kuala Lumpur 192.168.10.132/30* – Comme il ne faut que deux adresses, la portion hôte de l'adresse doit contenir au moins deux bits. Deux bits permettent de générer 2 adresses hôte ($2^2 = 4 – 2 = 2$), la division donne donc ici **192.168.10.132/30**.
- *Singapore vers Kuala Lumpur 192.168.10.136/30* – Comme il ne faut que deux adresses, la portion hôte de l'adresse doit contenir au moins deux bits. Deux bits permettent de générer 2 adresses hôte ($2^2 = 4 – 2 = 2$), la division donne donc ici **192.168.10.136/30.**

RIP Version 2

Historique du protocole RIP

RIP v1 est considéré comme un protocole IGP par classes (classful) + Un protocole à vecteur de distance qui diffuse intégralement sa table de routage à chaque routeur voisin, à intervalles prédéfinis. L'intervalle par défaut est de 30 secondes. RIP utilise le nombre de sauts comme métrique, avec une limite de 15 sauts maximum + capable de gérer l'équilibrage de charge sur au plus de six chemins de coût égal, avec quatre chemins par défaut.

Si le routeur reçoit des informations concernant un réseau et que l'interface de réception appartient au même réseau mais se trouve sur un sous-réseau différent, le routeur applique le masque de sous-réseau configuré sur l'interface de réception.

RIP v1 comporte les ***limitations*** suivantes:

- Il n'envoie pas d'informations sur les masques de sous-réseau dans ses mises à jour.
- Il envoie des mises à jour sous forme de broadcasts sur 255.255.255.255.
- Il ne prend pas l'authentification en charge.
- Il ne prend en charge ni VLSM, ni le routage CIDR (Classless Interdomain Routing).

Caractéristiques de RIP v2

RIP v2 présente une fonctionnalité de routage CIDR lui permettant d'envoyer des informations sur les masques de sous-réseau avec la mise à jour des routes.

RIP v2 permet l'authentification dans ses mises à jour. Il est possible d'utiliser une combinaison de clés sur une interface comme vérification d'authentification. RIP v2 permet de choisir le type d'authentification à utiliser dans les paquets RIP v2. Il peut s'agir de texte en clair ou d'un cryptage basé sur l'algorithme d'authentification MD5. Le type d'authentification par défaut est le texte en clair. L'algorithme.

Pour une meilleure efficacité, RIP v2 utilise l'adresse de classe D 224.0.0.9 pour envoyer les mises à jour de routage en multicast.

Comparaison des versions 1 et 2 de RIP :

RIP v1	RIP v2
Facile à configurer	Facile à configurer
Prend en charge uniquement un protocole de routage par classes (classful).	Prend en charge l'utilisation du routage CIDR (Classless).
La mise à jour de routage ne contient aucune information de sous-réseau.	Envoie des informations sur les masques de sous-réseau avec les mises à jour des routes.
Ne supporte pas le routage CIDR ce qui oblige tous les équipements d'un même réseau à utiliser le même masque de sous-réseau	Supporte le routage CIDR ce qui permet à des équipements d'un même réseau d'utiliser différents masques de sous-réseau
Aucune authentification dans les mises à jour	Permet l'authentification dans ses mises à jour de routage
Envoie les broadcasts sur 255.255.255.255.	Envoie les mises à jour de routage en multicast sur 224.0.0.9 ce qui est plus efficace.

Configuration de RIP v2 :

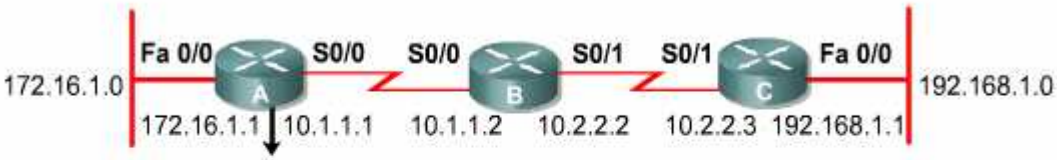
Router(config)#**router rip** ← activer RIP
Router(config-router)#**version 2** ← la version de RIP
Router(config-router)#**network {adresse réseau}** ← les réseau directement connectés

La commande **network** entraîne la mise en œuvre des fonctions suivantes:

- Diffusion multicast des mises à jour de routage en sortie d'une interface.
- Traitement des mises à jour de routage en entrée de cette même interface.
- Annonce du sous-réseau directement connecté à cette interface.

Vérification de RIP v2

Show ip protocols → affiche les valeurs des protocoles de routage et les informations relatives aux compteurs de routage associées à ce routeur.




```
RouterA#show ip protocols
Routing Protocol is "rip"
  Sending updates every 30 seconds, next due in 12 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Redistributing rip
  Default version control: send version 1, receive any version
    Interface         send   Recv  Triggered  RIP  Keychain
    Ethernet          1      1 2
    Serial2           1      1 2
Routing for Networks:
    10.0.0.0
    172.16.0.0
Routing Information Sources:
    Gateway         Distance      Last Update
    (this router)   120             0:2:12:15
    10.1.1.2        120             0:1:09:01
Distance: (default is 120)
```

Si un routeur RIP ne reçoit pas de mise à jour d'un autre routeur pendant au moins 180 secondes, le premier routeur déclare non valides les routes desservies par le routeur qui n'envoie pas de mise à jour. Par conséquent, la mise à jour d'une route qui, après avoir été indisponible redevient disponible, pourrait rester gelée pendant 180 secondes.

Si aucune mise à jour n'a eu lieu après un délai de 240 secondes, le routeur supprime les entrées correspondantes dans la table de routage. Le routeur insère des routes pour les réseaux répertoriés sous la ligne Routing for Networks.

Le routeur reçoit des routes des routeurs RIP voisins, répertoriés sous la ligne Routing Information Sources. La distance par défaut de 120 correspond à la distance administrative d'une route RIP.

Show ip interface brief → pour obtenir un résumé des informations relatives à une interface et à son état.

Show ip route → affiche le contenu de la table de routage IP.

Dépannage de RIP v2

Debug ip rip → afficher les mises à jour de routage RIP lors de leur envoi et de leur réception.

No debug all ou undebug all → désactiver toutes les opérations de débogage.


```
RouterA#debug ip rip

RIP protocol debugging is on
RouterA#
00:32:56.656: RIP: received v2 update from 10.1.1.2 on Serial0/0
00:32:56.656:      10.2.2.0/24 via 0.0.0.0 in 1 hops
00:32:56.660:      192.168.1.0/24 via 0.0.0.0 in 2 hops

00:33:07.557: RIP: sending v2 update to 224.0.0.9 via FastEthernet0/0
                   (172.16.1.1)
00:33:07.557: RIP: build update entries
00:33:07.557:      10.0.0.0/8 via 0.0.0.0, metric 1, tag 0

00:33:07.557:      192.168.1.0/24 via 0.0.0.0, metric 3, tag 0

00:33:07.557: RIP: sending v2 update to 224.0.0.9 via Serial0/0 (10.1.1.1)

00:33:07.557: RIP: build update entries

00:33:07.557:      172.16.0.0/16 via 0.0.0.0, metric 1, tag 0

00:33:25.006: RIP: received v2 update from 10.1.1.2 on Serial0/0
```

Ces messages apparaissent au démarrage ou lorsqu'un événement survient tel qu'une transition d'interface ou la réinitialisation de la table de routage par un utilisateur.

```
RIP: broadcasting general request on Ethernet0
RIP: broadcasting general request on Ethernet1
```

Si vous obtenez le message suivant, il est probable que l'émetteur a envoyé un paquet mal formé :

```
RIP: bad version 128 from 160.89.80.43
```

Affichage	Signification possible
RIP: broadcasting general request on Ethernet0	Interface effacée manuellement par un utilisateur
RIP: bad version 128 from 160.89.80.43	Paquet incorrect de l'émetteur
RIP: received v2 update from 150.100.2.3 on Serial0	Indique que RIP Version 2 est en mode réception
RIP: sending v1 update to 255.255.255 via Serial0 (150.100.2.2)	Indique que RIP Version 1 est en service
RIP: ignored v1 packet from 150.100.2.2 (illegal version)	Indique que le routeur ne peut pas prendre en charge un paquet RIP v1
RIP: sending v2 update to 224.0.0.9 via FastEthernet0 (150.100.3.1)	Indique que RIP Version 2 est en mode envoi
RIP: build update entries 150.100.2.0/24 via 0.0.0.0 metric 1, tag	Indique l'utilisation de la route par défaut et de l'étiquetage

Module 2

OSPF Zone unique

Protocoles de routage à état de liens :

Comparaison entre les protocoles à vecteur de distance et état de liens :

Vecteur de distance	État de lien
• Visualise la topologie du réseau du point de vue de leurs voisins • Ajoute des vecteurs de distance d'un routeur à l'autre • Mises à jour périodiques fréquentes et convergence lente • Passe des copies des tables de routage aux routeurs voisins	• Dispose d'une vue commune de la topologie • Calcule le plus court chemin vers les autres routeurs • Mises à jour déclenchées par événement et convergence plus rapide • Passe les mises à jour du routage à état de liens aux autres routeurs

Fonctions du protocole de routage à état de liens :

Les protocoles de routage à état de liens ***assurent les fonctions*** *suivantes* :

- ils réagissent rapidement aux changements qui interviennent sur le réseau
- ils envoient des mises à jour déclenchées lorsqu'un changement se produit sur le réseau.
- ils envoient des mises à jour périodiques appelées rafraîchissements d'état de liens.
- ils utilisent un mécanisme HELLO pour déterminer l'accessibilité de leurs voisins.

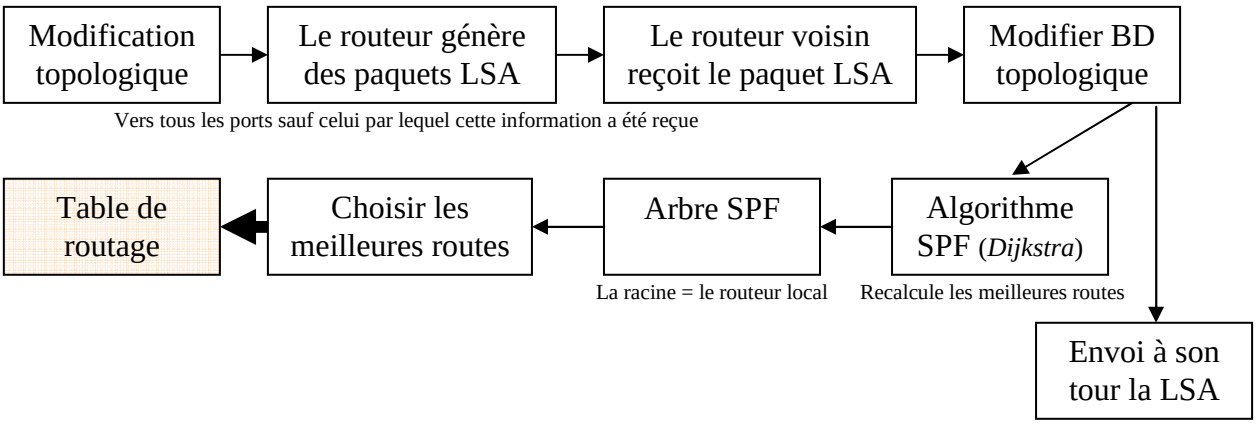
Comment les informations de routage sont mises à jour ?

Le routage à état de liens utilise les fonctions suivantes:

- des *mises à jour* de routage à état de liens (*LSA*).
- une *base de données topologique*.
- *l'algorithme* du plus court chemin d'abord (*SPF*).
- *l'arbre SPF* résultant.
- une *table de routage* afin de déterminer les meilleurs chemins pour les paquets.

Remarque : Si un changement se produit sur le réseau, une mise à jour partielle est immédiatement envoyée. Cette dernière contient uniquement des informations sur les liens qui ont changé, et non pas une table de routage complète.

Un lien joue le même rôle qu'une interface sur un routeur. L'état d'un lien correspond à la description d'une interface et de la relation avec les routeurs voisins (l'adresse IP de l'interface, le masque de sous-réseau, le type de réseau auquel elle est connectée, les routeurs connectés à ce réseau ...).



Avantages et inconvénients du protocole à état de liens

Avantages	Inconvénients
• Convergence rapide: modifications signalées immédiatement par les sources affectées • Robustesse face aux boucles de routage • Les routeurs connaissent la topologie • Les paquets à état de liens sont séquencés et horodatés • La taille des bases de données d'état de liens peut être réduite avec une conception réseau soignée	• Demandes significatives sur la mémoire et la puissance de traitement • Nécessite une conception de réseau rigoureuse • Nécessite un administrateur réseau ayant des compétences en routage à état de liens • Le flux initial peut ralentir les performances

Concepts de zone unique OSPF

Vue d'ensemble de l'OSPF :

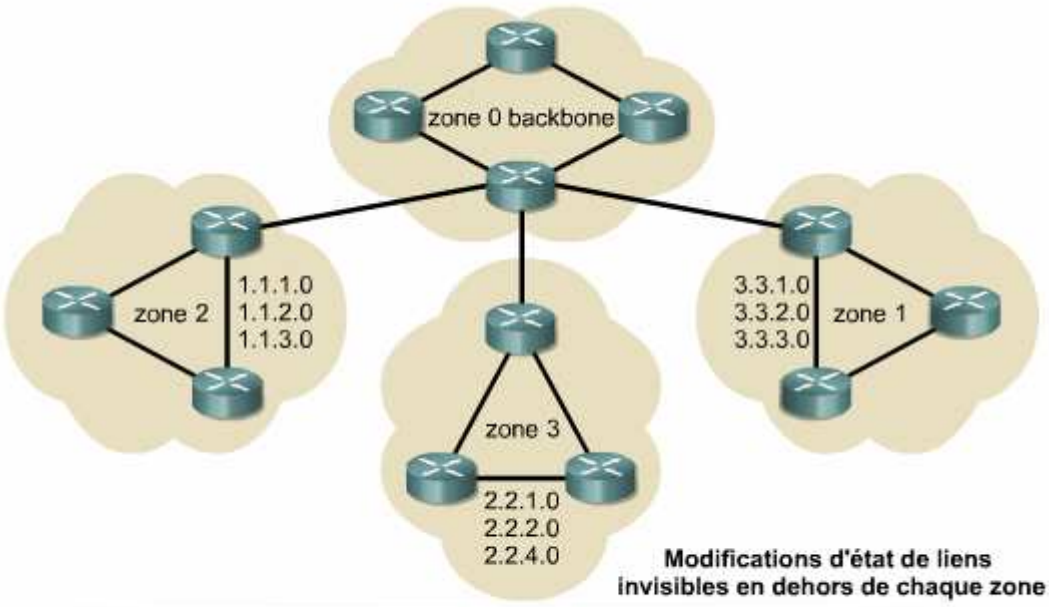
→ OSPF est un protocole IGP ouverte.

→ Un désavantage d'OSPF est qu'il ne supporte que la pile de protocoles TCP/IP.

→ L'OSPF peut être utilisé et configuré en tant que zone unique pour les petits réseaux.
→ Le routage OSPF peut évoluer vers les grands réseaux si les principes de conception de réseau hiérarchique sont appliqués.

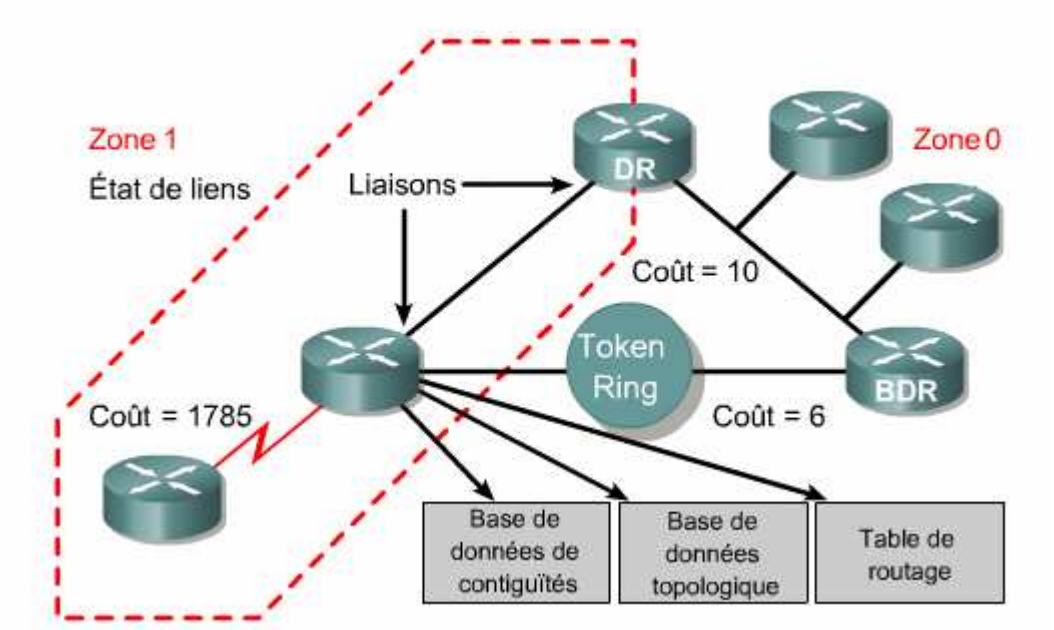
Les grands réseaux OSPF utilisent une ***conception hiérarchique***. Plusieurs zones se connectent à une zone de distribution, *la zone 0*, également appelée backbone.

Avantages : réduit la charge de routage, accélère la convergence, isole l'instabilité du réseau à zone unique et améliore les performances



Les grands réseaux OSPF sont hiérarchiques et divisés en plusieurs zones.

Terminologie OSPF :



→ Les routeurs traitent les informations sur les états de liens et construisent *une base de données d'état de liens*. Chaque routeur de la zone OSPF dispose de la même base de données de liens.

→ Les routeurs utilisent *L'algorithme SPF* « cumule le coût, qui est la valeur habituellement basée sur la bande passante ».

→ Le chemin de moindre coût est ajouté à la *table de routage*, également appelée base de données d'acheminement.

→ *La base de données d'adjacence* est une liste de tous les routeurs voisins avec lesquels le routeur a établi des communications bidirectionnelles « de contigüité »

→ Les routeurs OSPF choisissent un *routeur désigné* (DR) et un *routeur désigné de secours* (BDR) qui servent de points focaux pour l'échange des informations de routage.

Avantages de l'OSPF :

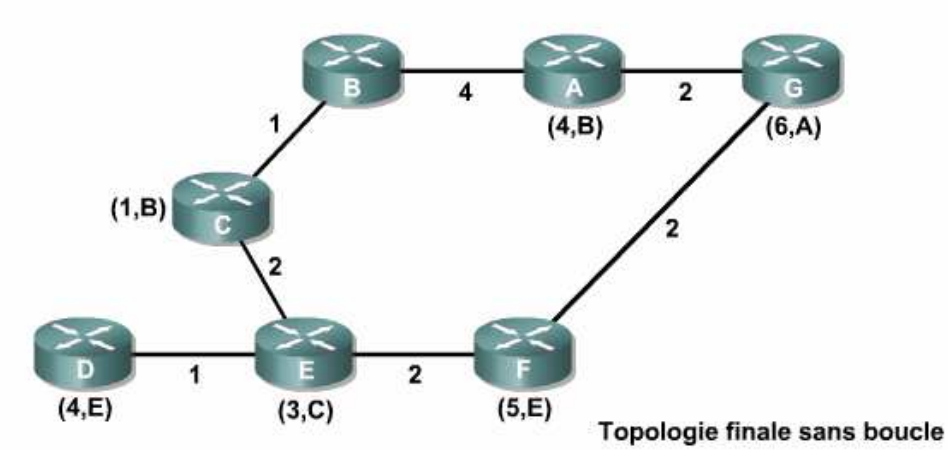
L'OSPF présente tous les avantages des protocoles à état de lien + résout les problèmes suivants:

- vitesse de convergence.
- prise en charge de masque de sous-réseau de longueur variable (VLSM)
- taille du réseau.
- sélection du chemin.
- regroupement des membres

Si des liens sont instables, la diffusion des informations sur l'état des liens peut désynchroniser les annonces d'état de liens et rendre les décisions incohérentes.

Algorithme du plus court chemin d'abord :

Selon cet algorithme, un réseau est un ensemble de nœuds connectés par des liaisons point-à-point. Chaque lien a un coût. Chaque nœud a un nom. Chaque nœud dispose d'une base de données complète de tous les liens.

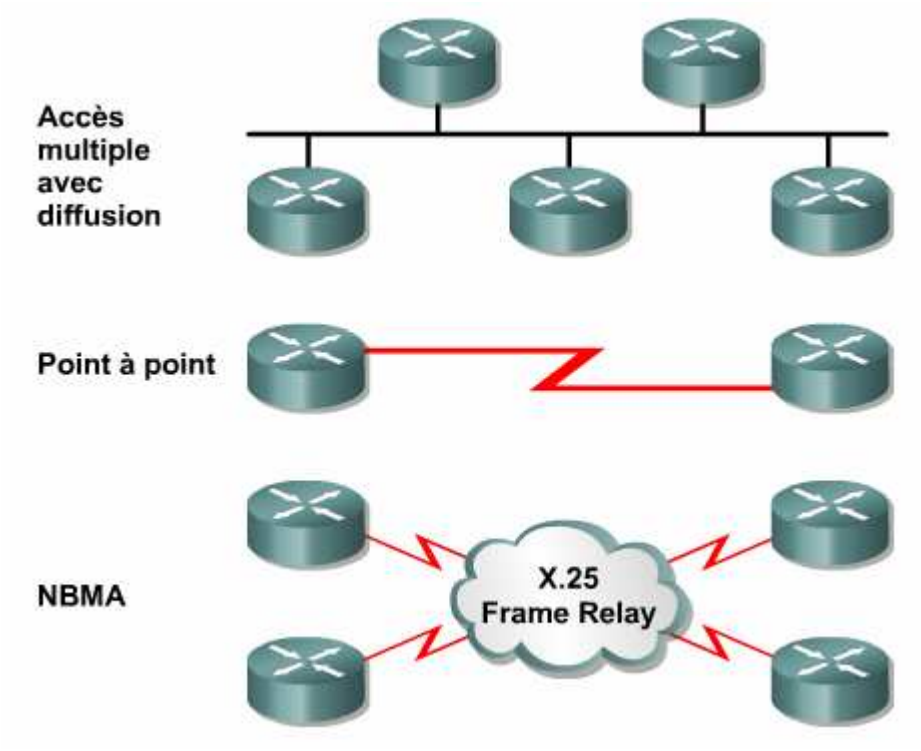


Topologie finale sans boucle

A	B	C	D	E	F	G
B/4	A/4	B/1	C/4	C/2	E/2	A/2
G/2	C/1	D/4	E/1	D/1	G/2	F/2
		E/2		F/2		

Types de réseau OSPF

Les routeurs OSPF déterminent avec quel routeur ils doivent devenir adjacents en fonction du type de réseau auquel ils sont connectés.



Les interfaces OSPF reconnaissent automatiquement trois types de réseaux :

- les réseaux *à accès multiple avec diffusion*, comme Ethernet.
- les réseaux *point à point*.
- les réseaux *à accès multiple sans diffusion* (Nonbroadcast multi-access - NBMA).
- *point à multipoint*, peut être configuré manuellement sur une interface par un administrateur

Type de réseau	Caractéristiques	Sélection DR ?
Accès multiple avec diffusion	Ethernet, Token Ring ou FDDI	Oui
Accès multiple sans diffusion	Frame Relay, X.25, SMDS	Oui
Point à point	PPP, HDLC	Non
Point-à-multipoint	Configuré par un administrateur	Non

Dans un réseau broadcast à accès multiple avec diffusion, pour n routeurs, **n*(n-1)/2** contiguïtés devraient être formées.

La solution à cette surcharge consiste à opérer une sélection de routeur désigné (DR). Ce routeur devient adjacent à tous les autres routeurs du segment de broadcast. Tous les autres routeurs sur le segment envoient leurs informations d'état de liens au routeur désigné.

Le routeur désigné envoie des informations d'état de liens à tous les autres routeurs sur le segment en utilisant l'adresse multicast 224.0.0.5 pour tous les routeurs OSPF.

Un deuxième routeur est sélectionné comme routeur désigné de secours (BDR) pour prendre le relais du routeur désigné au cas où ce dernier tomberait en panne.

Protocole HELLO de l'OSPF

Au niveau de la couche 3 du modèle OSI, des paquets HELLO sont adressés à l'adresse multicast 224.0.0.5.

Les routeurs OSPF utilisent des paquets HELLO pour initier de nouvelles contiguïtés et pour s'assurer que les routeurs voisins fonctionnent encore.

- Des HELLO sont envoyés toutes les 10 secondes par défaut sur les réseaux broadcast à accès multiple et sur les réseaux point-à-point.
- Sur les interfaces qui se connectent aux réseaux NBMA, telles que le Frame Relay, le délai par défaut est de 30 secondes.

Bien que le paquet hello soit de petite taille, il est constitué de l'en-tête de paquet OSPF. Le champ **type** est défini à **1** pour le **paquet hello**.

Entête de paquet ospf :

Version	Type	Longueur du paquet
ID du routeur		
ID de zone		
Somme de contrôle		Type d'authentification
Données d'authentification		

Entête de paquet Hello ospf :

Masque de réseau		
Intervalle HELLO	Options	Priorité du routeur
Intervalle d'arrêt		
Routeur désigné		
Routeur désigné de secours		
ID du routeur voisin		
ID du routeur voisin		
(Des champs ID du routeur voisin peuvent être ajoutés à la fin de l'en-tête, si nécessaire.)		

Configuration OSPF :

Configuration du protocole de routage OSPF

→ Pour activer le routage OSPF

```
Router(config)#router ospf {id-processus}
```

→ Pour indiquer les réseaux IP :

```
Router(config-router)#network {adresse} {masque-générique} area {id-zone}
```

NB : → ID de zone entre 0 et 4294967295.
→ ID de processus entre 1 et 65535.
→ Dans les réseaux OSPF à zones multiples, toutes les zones doivent se connecter à la zone 0.

Configuration d'une @ d'essai en mode bouclé OSPF

Lorsque le processus OSPF démarre, la plate-forme logicielle Cisco IOS utilise l'adresse IP active locale la plus élevée comme ID de routeur OSPF. En l'absence d'interface active, le processus OSPF ne démarre pas.

Pour *garantir la stabilité de l'OSPF*, une interface doit être active en permanence pour le processus. Vous pouvez configurer à cet effet une interface en mode bouclé (c'est-à-dire une interface logique).
→ L'OSPF utilise alors cette adresse comme ID de routeur, quelle que soit sa valeur.

Sur un routeur possédant plusieurs interfaces en mode bouclé, l'OSPF choisit l'adresse IP en mode bouclé la plus élevée comme ID de routeur.

→ Pour créer et affecter une adresse IP à une interface en mode bouclé :

```
Router(config)#interface loopback {numéro}
Router(config-if)#ip address {adresse-ip} {masque-sous-réseau}
```

Cette interface doit être configurée avec une adresse utilisant un masque de sous réseau 32 bits de 255.255.255.255 (masque d'hôte).

La priorité des routeurs

Si le type de réseau d'une interface est broadcast, *la priorité par défaut* de l'OSPF est ***1***. Lorsque des priorités OSPF sont identiques, la sélection du routeur désigné par l'OSPF se fait sur la base de l'ID du routeur. L'ID de routeur la plus élevée est sélectionnée comme DR. Le routeur dont la priorité est immédiatement inférieure sera le BDR.

L'interface qui signale la priorité la plus élevée (au niveau des paquets Hello) pour un routeur s'assure que ce dernier devienne le routeur désigné.

```
Router(config-if)#ip ospf priority {numéro}
```
→ Modifiez la priorité OSPF

→ Les priorités sont comprises entre 0 et 255
Show ip ospf interface {id interface} → Permet d'afficher la valeur de priorité d'interface

NB : Une valeur égale à 0 empêche la sélection du routeur.

Modification de la métrique de coût OSPF :

OSPF utilise *le coût* comme la mesure de détermination de la meilleure route.

En général, le coût d'un chemin est calculé d'après la formule 10^8/bande passante, où la bande passante est exprimée en bits/s

→ Plus le coût est faible, plus le chemin est meilleure.

Type de lien et bande passante	Coût
Liaison série - 56 kbits/s	1785
Liaison série T1 - 1,544 Mbits/s	64
Liaison série E1 - 2,048 Mbits/s	48
Token Ring - 4 Mbits/s	25
Ethernet - 10 Mbits/s	10
Token Ring - 16 Mbits/s	6
Fast Ethernet / FDDI - 100 Mbits/s	1

`Router(config-if)#`**bandwidth {numéro}** → définir la bande passante d'interface correcte
`Router(config-if)#`**ip ospf cost {numéro}** → définir le coût de la liaison

Configuration de l'authentification OSPF

Chaque interface OSPF peut présenter une clé d'authentification à l'usage des routeurs qui envoient des informations OSPF aux autres routeurs du segment. La clé d'authentification, ou mot de passe, est un secret partagé entre les routeurs.

→ Pour *configurer l'authentification* OSPF.
`Router(config-if)#`**ip ospf authentication-key {mot de passe}** -8 caractères maximum-

→ Une fois le mot de passe configuré, l'authentification doit être *activée*:
`Router(config-router)#`**area {id-de-zone} authentication**

→ Pour une authentification *cryptées* et pour renforcer la sécurité : l'algorithme MD5 :
`Router(config-if)#`**ip ospf message-digest-key {id-de-clé} {type-d-encryption} md5 {clé}**
`Router(config-router)#`**area {id-de-zone} authentication message-digest**

- L'id-de-clé est un identifiant entre 1 et 255.
- La clé est un mot de passe alphanumérique qui comporte jusqu'à 16 caractères.
- Le champ de type de cryptage (0 signifie aucun et où 7 signifie propriétaire).

- L'authentification MD5 crée un condensé de message (pour détermine que la source et le contenu du paquet n'ont pas été altérés).
- Dans le cas de l'authentification par algorithme MD5, le champ de données d'authentification contient l'id de clé et la longueur du condensé de message.

Configuration des compteurs OSPF

Les routeurs OSPF *doivent disposer des mêmes intervalles HELLO et des mêmes intervalles d'arrêt (dead)* pour échanger des informations.

→ Par défaut, l'intervalle d'arrêt est quatre fois plus long que l'intervalle HELLO.

- Sur les réseaux OSPF *avec diffusion*, l'intervalle HELLO par défaut est de 10 secondes et l'intervalle d'arrêt par défaut de 40 secondes.
- Sur les réseaux *sans diffusion*, l'intervalle HELLO par défaut est de 30 secondes et l'intervalle d'arrêt par défaut de 120 secondes.

Ces valeurs par défaut garantissent un bon fonctionnement de l'OSPF et ont rarement besoin d'être modifiées.

```
Router(config-if)#ip ospf hello-interval {secondes}
```
→ configurer les intervalles HELLO

```
Router(config-if)#ip ospf dead-interval {secondes}
```
→ configurer les intervalles d'arrêt

OSPF, propagation d'une route par défaut :

Il suffit de définir une route par défaut sur un routeur et la diffuser vers les autres routeurs du même zone par la commande :

```
Router(config-router)#default-information originate
```

Problèmes de configuration OSPF fréquents :

L'incapacité à établir une relation de voisinage peut être due à l'une des raisons suivantes:

- Les HELLO ne sont pas envoyés par les deux voisins.
- Les compteurs d'intervalles HELLO et d'intervalles d'arrêt ne sont synchronisés.
- Les interfaces se trouvent sur des types de réseau différents.
- Les mots de passe ou les clés d'authentification sont différents.

Dans le routage OSPF, il est également important de *vérifier les points suivants*:

- Toutes les interfaces ont une adresse et un masque de sous réseau corrects.
- Les instructions **network area** ont des masques génériques appropriés.
- Les instructions **network area** placent les interfaces dans la zone correcte.

Vérification de la configuration OSPF :

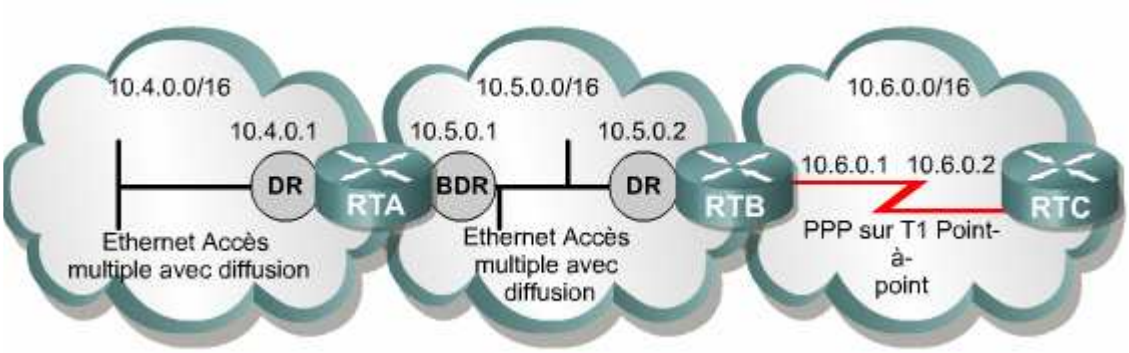
Commande de vérification :

Commande	Description
`show ip protocol`	Affiche des paramètres sur les compteurs, les filtres, les métriques, les réseaux et d'autres informations sur le routeur dans sa globalité.
`show ip route`	Affiche les routes connues du routeur et la manière dont elles ont été apprises. Il s'agit d'une des meilleures méthodes de détermination de la connectivité entre le routeur local et le reste de l'interréseau.
`show ip ospf interface`	Vérifie que les interfaces ont été configurées dans les zones appropriées. Si aucune adresse d'essai en mode bouclé n'est spécifiée, l'interface dont l'adresse est la première dans la hiérarchie est utilisée comme ID de routeur. Indique également les intervalles de compteur, y compris l'intervalle HELLO, et précise les contiguïtés.
`show ip ospf`	Indique le nombre d'exécutions de l'algorithme du plus court chemin d'abord (SPF). Indique également l'intervalle de mise à jour des états de liens, en supposant qu'aucun changement de topologie ne survienne.
`show ip ospf neighbor detail`	Affiche la liste détaillée des équipements voisins, leur priorité et leur état (par exemple : init, exstart ou full).
`show ip ospf database`	Affiche le contenu de la base de données topologique mise à jour par le routeur. Cette commande indique également l'ID du routeur et l'ID du processus OSPF. Un certain nombre de

Commandes de dépannage :

Commande	Description
`clear ip route *`	Efface toutes les routes de la table de routage
`clear ip route a.b.c.d`	Efface toutes les routes vers a.b.c.d dans la table de routage
`debug ip ospf events`	Signale tous les événements OSPF
`debug ip ospf adj`	Signale tous les événements de contiguïté OSPF

Exemple de choix des DR et BDR :



Module 3

Protocole EIGRP

Protocole EIGRP :

Comparaison entre les protocoles EIGRP et IGRP :

→ En 1994, Cisco a lancé l'EIGRP, une version évolutive de l'IGRP.

→ La comparaison des protocoles EIGRP et IGRP se fonde sur les catégories majeures :

- le mode de compatibilité.
- le calcul de métrique.
- le nombre de sauts.
- la redistribution automatique de protocole.
- l'étiquetage de route.

→ L'IGRP et l'EIGRP sont compatibles entre eux.
→ À la différence de l'IGRP, L'EIGRP offre la prise en charge multi protocoles.

→ Les deux protocoles utilisent des calculs de métrique différents. Du fait qu'il utilise une métrique de 32 bits de longueur, et non de 24 bits comme l'IGRP, L'EIGRP multiplie la valeur de la métrique de l'IGRP par 256. En multipliant ou en divisant par 256, l'EIGRP peut facilement échanger des informations avec l'IGRP.

Les protocoles EIGRP et IGRP utilisent la formule de calcul de métrique suivante :
- métrique = [K1 * bande passante + (K2 * bande passante) / 256 - charge) + (K3 * délai)] * [K5/(fiabilité + K4)]

Les valeurs constantes par défaut sont les suivantes :
- K1 = 1, K2 = 0, K3 = 1, K4 = 0, K5 = 0
- métrique = bande passante + délai

Lorsque K4 et K5 = 0, la partie [K5/(fiabilité+ K4)] de l'équation n'est pas prise en compte dans la métrique. Ainsi, avec les valeurs constantes par défaut, l'équation de la métrique est : Bande passante + Délai.

IGRP et EIGRP utilisent les équations suivantes pour déterminer les valeurs utilisées dans le calcul de la métrique (notez que pour EIGRP, la valeur est multipliée par 256) :
- bande passante pour IGRP = (10000000/bande passante)
- bande passante pour EIGRP = (10000000/bande passante) * 256
- délai pour IGRP = délai/10
- délai pour EIGRP = (délai/10) * 256

→ L'IGRP prend en charge un nombre maximum de sauts de 255. L'EIGRP se limite à 224 sauts.
→ Des fonctions telles que la redistribution et le partage des routes, s'effectuent automatiquement entre l'IGRP et l'EIGRP tant que les deux processus utilisent le même numéro de système autonome (AS).

→ L'EIGRP étiquettera comme externes les routes acquises auprès d'IGRP ou d'une autre source extérieure, car elles ne proviennent pas de routeurs EIGRP. L'IGRP ne peut faire la différence entre les routes internes et les routes externes. L'étiquette peut être configurée avec un numéro compris entre 0 et 255.

→ Les routes EIGRP sont étiquetées «**D**», et les routes externes «**EX**».

```
RTA#show ip route
<Affichage tronqué>
C    10.1.1.0 is directly connected, Serial0
D    172.16.1.0 [90/2681856] via 10.1.1.1, Serial0
D EX 192.168.1.0 [170/2681856] via 10.1.1.1,
00:00:04, Serial0
```

Concepts et terminologie de l'EIGRP

→ Les routeurs EIGRP stockent les informations de topologie et de route en mémoire RAM
** Pour réagir rapidement aux changements

→ À l'instar de l'OSPF, l'EIGRP enregistre ces informations dans diverses tables et bases de données.

→ L'EIGRP met à jour trois tables:

- la table de voisinage
- la table topologique
- la table de routage

→ Chaque routeur EIGRP tient à jour une table de voisinage qui répertorie les routeurs adjacents. Il y a une table de voisinage pour chaque protocole pris en charge par l'EIGRP.

La table de voisinage comporte les champs suivants:

- **Adresse du voisin –** Il s'agit de l'adresse de couche réseau du routeur voisin.
- **Délai de conservation** – Intervalle à l'issue duquel la liaison est considérée comme indisponible si aucun signal n'a été reçu du voisin.
- **Smooth Round-Trip Timer (SRTT)** – C'est le temps moyen nécessaire pour envoyer et recevoir des paquets d'un voisin.
- **Queue count (Q Cnt)** – Il s'agit du nombre de paquets en attente d'envoi dans une file d'attente.
- **Sequence Number (Seq No)** – C'est le numéro du dernier paquet reçu de ce voisin. L'EIGRP utilise ce champ pour accuser réception de la transmission d'un voisin et pour identifier les paquets hors séquence.

Lorsque des voisins nouvellement découverts sont acquis, l'adresse et l'interface du voisin sont enregistrées dans la structure de données de voisinage.

Lorsqu'un voisin envoie un paquet *HELLO*, il annonce un délai de conservation. Si un paquet HELLO n'est pas détecté pendant le délai de conservation, celui-ci expire. Au moment de l'expiration, le *DUAL* (Diffusing Update Algorithm), algorithme à vecteur de distance de l'EIGRP, est informé du changement de topologie et doit recalculer la nouvelle topologie.

```
Router#show ip eigrp neighbors
IP-EIGRP neighbors for process 100
M   Address         Interface Hold Uptime SRTT RTO  Q  SEQ
                              (sec)       (ms)     CNT NUM
2   200.10.10.10    Se1       13 00:19:09  26  200  0  10
1   200.10.10.5     Se0       12 03:31:36  50  300  0  39
0   199.55.32.10    Et0       11 03:31:40  10  200  0  40
```

→ La table topologique est constituée de toutes les tables de routage EIGRP du système autonome. Toutes les routes apprises jusqu'à une destination sont conservées dans cette table.

L'algorithme DUAL extrait les informations fournies dans la table de voisinage et dans la table topologique et calcule les routes de moindre coût vers chaque destination.

```
Router#show ip eigrp topology
IP-EIGRP Topology Table for process 100

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply
       r - Reply status

P 32.0.0.0/8, 1 successors, FD is 2195456
         via 200.10.10.10 (2195456/281600), Serial1
P 170.32.0.0/16, 1 successors, FD is 2195456
         via 199.55.32.10 (2195456/2169856), Ethernet0
         via 200.10.10.5 (2681856/2169856), Serial0
```

La table topologique inclut les champs suivants:

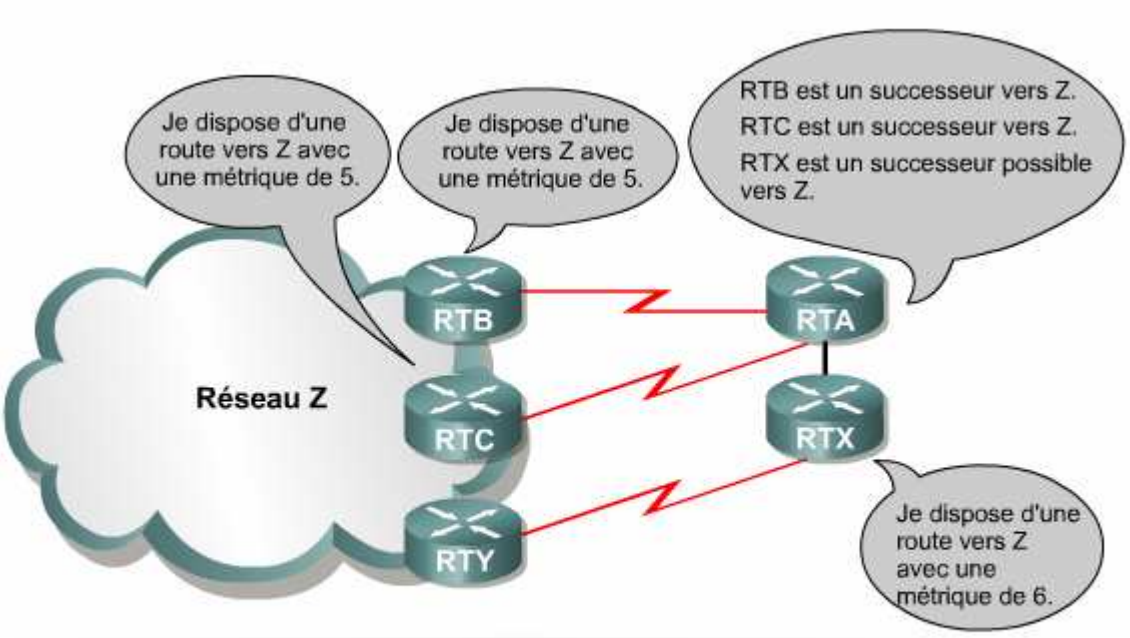
- **Distance possible (FD) –** La distance possible (FD, acronyme de Feasible Distance) est la métrique calculée la plus faible vers chaque destination. Par exemple, la distance possible jusqu'à 32.0.0.0 est 2195456**.**
- **Source de la route (via 200.10.10.10) –** La source de la route est le numéro d'identification du routeur qui a initialement annoncé cette route (Ce champ est uniquement renseigné pour les routes apprises en externe auprès du réseau EIGRP). Par exemple la source de la route qui mène à 32.0.0.0 est 200.10.10.10 via 200.10.10.10.
- **Distance annoncée (RD) –** La distance annoncée (RD, acronyme de Reported Distance) du chemin est celle annoncée par un voisin adjacent jusqu'à une destination spécifique. Par exemple, la distance annoncée jusqu'à 32.0.0.0 est /281600 comme l'indique (2195456/281600).
- **Informations d'interface –** L'interface permettant d'atteindre la destination
- **État de la route –** Une route est identifiée comme étant soit passive (P), c'est-à-dire stables et prêtes à l'utilisation, soit active (A), ce qui signifie qu'elle va être recalculée par l'algorithme DUAL.

→ La table de routage EIGRP contient les meilleures routes vers une destination donnée. Chaque routeur EIGRP tient à jour une table de routage pour chaque protocole de réseau.

Une route successeur est une route sélectionnée comme route principale à utiliser pour atteindre une destination.

Il peut y avoir jusqu'à *quatre* routes successeur pour une route particulière. Ces routes peuvent être de coût égal ou différent et elles sont identifiées comme les meilleurs chemins exempts de boucles vers une destination donnée.

Une route *successeur possible* (FS) est une route de secours. Ces routes sont identifiées en même temps que les routes successeur, mais elles ne sont conservées que dans la table topologique.



En identifiant des successeurs possibles, les routeurs EIGRP peuvent installer immédiatement d'autres routes en cas d'échec d'un successeur.

! *Si une route successeur est interrompue !!!* Le routeur cherchera une route successeur possible identifiée. Cette route sera promue à l'état de successeur. S'il n'est pas possible d'identifier une route successeur possible avec les informations existantes, le routeur place un état *Actif* sur une route et envoie des *paquets de requête* à tous les voisins afin de recalculer la topologie actuelle. Le routeur peut identifier alors toute route successeur ou route successeur possible à l'aide des nouvelles données reçues. Le routeur place alors un état Passif sur la route.

Caractéristiques de conception du protocole EIGRP

L'EIGRP est un protocole de routage à vecteur de distance avancé qui joue le rôle d'un protocole à état de liens lors de la mise à jour des voisins et de la gestion des informations de routage.

- Convergence rapide
- Utilisation efficace de la bande passante
- Compatibilité avec VLSM et CIDR
- Prise en charge de couches réseau multiples
- Indépendance par rapport aux protocoles routés

L'EIGRP utilise la bande passante de façon rationnelle en envoyant des mises à jour partielles et limitées, et sa consommation est minime lorsque le réseau est stable. Les routeurs

EIGRP effectuent des mises à jour partielles et incrémentielles, plutôt que d'envoyer leurs tables en entier.

Contrairement aux routeurs OSPF, les routeurs EIGRP envoient ces mises à jour partielles uniquement aux routeurs qui ont besoin de l'information, et pas à tous les routeurs d'une zone.

→ L'EIGRP prend en charge IP, IPX et AppleTalk à travers des modules dépendant des protocoles (PDM). L'EIGRP peut redistribuer les informations IPX, Novell RIP et SAP pour améliorer les performances globales.

→ L'EIGRP peut également remplacer le protocole RTMP (AppleTalk Routing Table Maintenance Protocol).

Technologies EIGRP

Ces nouvelles technologies peuvent être classées dans l'une des catégories suivantes:

- Découverte et récupération de voisinage
- Protocole de transport fiable
- Algorithme de machine à états finis DUAL
- Modules dépendant du protocole

Les routeurs EIGRP établissent de façon active des relations avec leurs voisins, d'une façon très similaire aux routeurs OSPF (par contre les autres protocoles n'établissent aucune relation avec les voisins).

Pour former des contiguïtés, les routeurs EIGRP procèdent comme suit (Paquet Hello ! par défaut toutes les cinq secondes) :

- Ils prennent connaissance de façon dynamique des nouvelles routes.
- Ils identifient les routeurs qui deviennent inaccessibles ou inutilisables.
- Ils redécouvrent les routeurs qui étaient précédemment inaccessibles.

Le *RTP* (Reliable Transport Protocol) est un protocole de la couche transport qui peut garantir la livraison ordonnée des paquets EIGRP à tous les voisins → l'EIGRP est indépendant des protocoles. Cela signifie qu'il ne dépend pas du TCP/IP pour échanger des informations de routage comme le font les protocoles RIP, IGRP et OSPP.

L'EIGRP peut faire appel à RTP pour fournir un service fiable ou non fiable selon la situation. Par exemple, les paquets HELLO ne nécessitent pas la surcharge de la livraison fiable car ils sont envoyés fréquemment et sont de taille limitée. Toutefois, la livraison fiable des autres informations de routage peut accélérer la convergence, parce que les routeurs EIGRP n'attendent pas l'expiration d'un compteur pour retransmettre.

L'algorithme DUAL (Diffusing Update Algorithm) :

Le nom entier de cette technologie est «DUAL finite-state machine» (FSM).

Un FSM est un système algorithmique non lié au matériel. Les FSM définissent un ensemble d'états possibles que peut prendre un objet, les événements à l'origine de ces états et les événements résultant de ces états. Le système DUAL FSM contient toute la logique permettant de calculer et comparer des routes dans un réseau EIGRP.

* L'algorithme DUAL analyse toutes les routes annoncées par les voisins. Les métriques composées de chaque route sont utilisées pour les comparer.

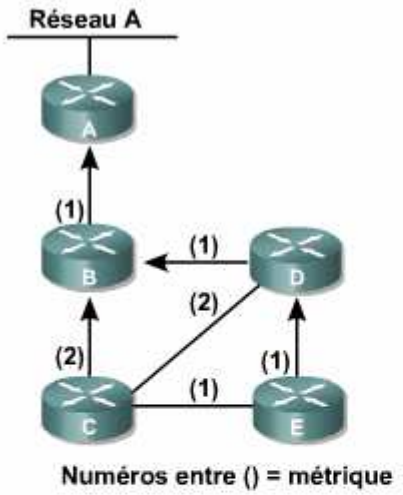
* Il garantit également que chaque chemin est exempt de boucles. Il insère des chemins de moindre coût dans la table de routage.

Conception de l'EIGRP :

L'une des caractéristiques de l'EIGRP est sa conception modulaire. Ce type de conception en couches s'avère être des plus évolutives et des plus adaptables. Grâce aux PDM, la prise en charge des protocoles routés, comme IP, IPX et AppleTalk est incluse dans l'EIGRP. Théoriquement, l'EIGRP peut s'adapter facilement aux protocoles routés nouveaux ou révisés, tels que IPv6, par simple ajout de modules dépendant des protocoles.

Le module IP-EIGRP assure les fonctions suivantes:

- Envoi et réception des paquets EIGRP qui transportent les données IP
- Notification à l'algorithme DUAL des nouvelles informations de routage IP reçues
- Actualisation des résultats des décisions de routage DUAL dans la table de routage IP
- Redistribution des informations de routage qui ont été apprises par d'autres protocoles de routage compatibles IP



Numéros entre () = métrique

C EIGRP Réseau A	FD	RD	Topologie
	3		(FD)
via B	3	1	(Successor)
via D	4	2	(FS)
via E	4	3	

D EIGRP Réseau A	FD	RD	Topologie
	2		(FD)
via B	2	1	(Successor)
via C	5	3	

E EIGRP Réseau A	FD	RD	Topologie
	3		(FD)
via D	3	2	(Successor)
via C	4	3	

Légende	
EIGRP	Type de protocole
FD	Feasible Distance - distance possible
RD	Reported Distance - distance annoncée par le routeur voisin
Successor	Route principale vers la destination
FS	Feasible Successor (successeur possible) - Route de secours vers la destination

Structure de données EIGRP

Les cinq types de paquets EIGRP sont les suivants:

- HELLO
- Accusé de réception
- Mise à jour
- Requête
- Réponse

EIGRP recourt aux paquets HELLO pour découvrir, vérifier et redécouvrir les routeurs voisins. Sur les réseaux IP, les routeurs EIGRP envoient des HELLO à l'adresse IP multicast **224.0.0.10**

Bande passante	Exemple de liaison	Intervalle HELLO par défaut	Délai de conservation par défaut
1,544 Mbits/s ou moins	Frame Relay multipoint	60 secondes	180 secondes
Supérieure à 1,544 Mbits/s	T1, Ethernet	5 secondes	15 secondes

Un routeur EIGRP stocke des informations sur les voisins dans la table de voisinage. La table de voisinage inclut le champ de numéro de séquence (Seq No) où est enregistré le numéro du dernier paquet EIGRP reçu que chaque voisin a envoyé. La table de voisinage inclut également un champ de délai de conservation qui enregistre l'heure à laquelle le dernier paquet a été reçu.

➔ Pour que l'état Passif soit maintenu, les paquets doivent être reçus dans l'intervalle du délai de conservation. L'état Passif est un état accessible et opérationnel.

L'OSPF requiert que les routeurs voisins possèdent les mêmes intervalles HELLO et d'arrêt pour communiquer. L'EIGRP n'a pas cette restriction. Les routeurs voisins prennent connaissance de chaque compteur respectif en échangeant des paquets HELLO.

Un routeur EIGRP utilise des paquets d'accusé de réception pour indiquer la réception de n'importe quel paquet EIGRP au cours d'un échange fiable. Contrairement aux HELLO multicast, les paquets d'accusé de réception sont unicast.

Les paquets de mise à jour sont utilisés lorsqu'un routeur *découvre un nouveau voisin*. Un routeur EIGRP envoie des paquets de mise à jour unicast à ce nouveau voisin afin de pouvoir l'ajouter à sa table topologique.

Les paquets de mise à jour sont également utilisés lorsqu'un routeur *détecte un changement topologique*. Dans ce cas, le routeur EIGRP envoie un paquet de mise à jour multicast à tous les voisins, qui leur signale le changement. Tous les paquets de mise à jour sont envoyés de manière fiable.

Un routeur EIGRP utilise des paquets de requête chaque fois qu'il a besoin d'informations spécifiques sur un ou plusieurs de ses voisins. Un paquet de réponse est utilisé pour répondre à une requête (par exemple des informations pour déterminer un nouveau successeur).

Configuration EIGRP

Configuration IGRP :

Router(config)#**router eigrp numéro-du-système-autonome**

Router(config-router)#**network numéro-réseau** → (uniquement des réseaux connectés).

Lors de la configuration de liaisons série à l'aide d'EIGRP, il est important de configurer le paramètre de bande passante sur l'interface. Si la bande passante de ces interfaces n'est pas modifiée, l'EIGRP sélectionne la bande passante par défaut sur la liaison plutôt que la bande passante réelle.

Router(config-if)#**bandwidth kbits/s**

Cisco recommande également l'ajout de la commande suivante à toutes les configurations :

Router(config-if)#**eigrp log-neighbor-changes**

Cette commande active la journalisation des changements de contiguïté de voisins pour surveiller la stabilité du système de routage et pour mieux détecter les problèmes.

Configuration des résumés EIGRP

La fonction de résumé automatique est avantageuse → elle permet de conserver des tables de routage aussi compactes que possible.

Avec certains sous-réseaux non contigus, le résumé automatique doit être désactivé pour que le routage fonctionne correctement.

Router(config-router)#**no auto-summary**

→ L'adresse résumée peut ensuite être définie avec la commande :

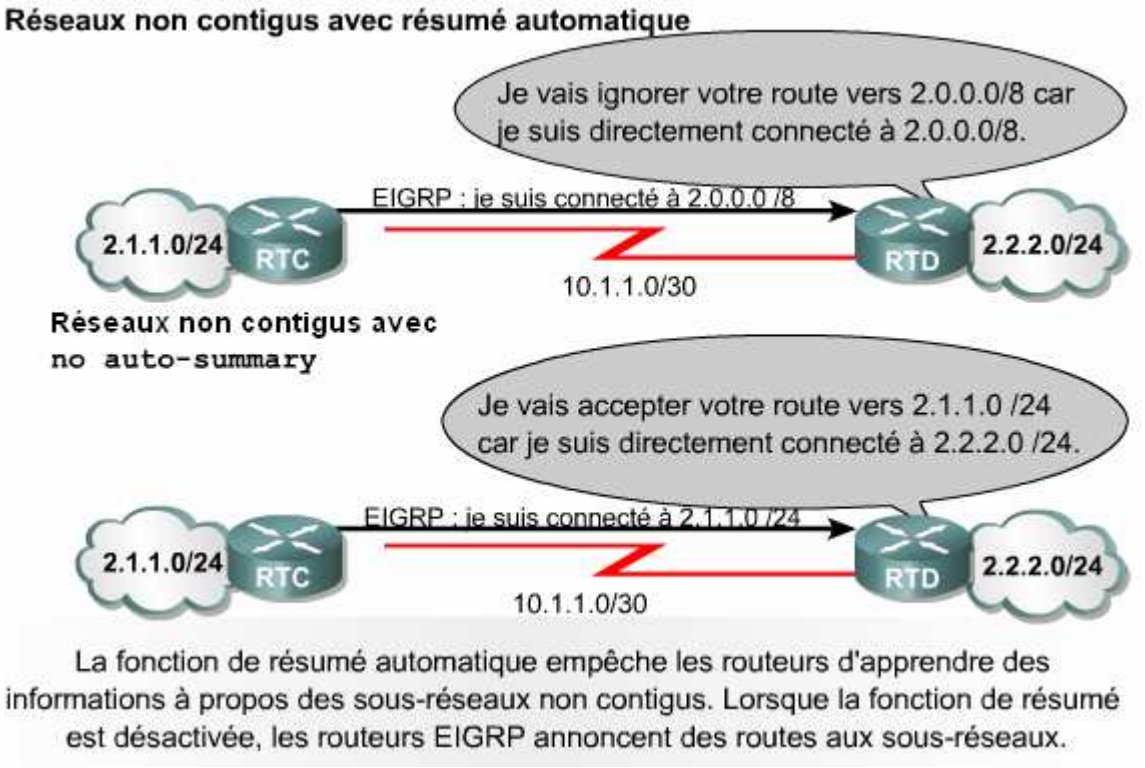
Router(config-if)#**ip summary-address eigrp {numéro-sa} {adresse-ip} {masque} [distance-administrative]**

Remarque : Les routes résumées EIGRP ont par défaut une distance administrative de 5.

Le routeur ajoutera alors une route à sa table, comme suit (exemple) :

```
D 2.1.0.0/16 is a summary, 00:00:22, Null0
```

Remarque : Notez que la route résumée provient de Null0 et pas d'une interface réelle. Cela est dû au fait que cette route est utilisée à des fins d'annonce et qu'elle ne représente pas un chemin qu'on peut emprunter pour atteindre ce réseau.



La fonction de résumé automatique empêche les routeurs d'apprendre des informations à propos des sous-réseaux non contigus. Lorsque la fonction de résumé est désactivée, les routeurs EIGRP annoncent des routes aux sous-réseaux.

Vérification de l'EIGRP de base

Commande	Description
show ip eigrp neighbors *[type number]* **[details]**	Affiche la table de voisinage EIGRP. Utilisez les options " type " et " numéro " pour indiquer une interface. Le mot-clé " details " étend le résultat.
show ip eigrp interfaces *[type number]* *[as-number]* **[details]**	Affiche des informations EIGRP pour chaque interface. Les mots-clés facultatifs limitent l'affichage des informations à une interface ou à un système autonome spécifique. Le mot-clé " details " entraîne l'affichage d'informations détaillées.
show ip eigrp topology *[as-number | [[ip-address] mask]]*	Affiche tous les successeurs possibles dans la table topologique EIGRP. Les mots-clés facultatifs peuvent filtrer les informations affichées sur la base du numéro de système autonome ou d'une adresse réseau spécifique.
show ip eigrp topology [active | pending | zero-successors]	Selon le mot-clé utilisé, affiche toutes les routes de la table topologique qui sont actives, en attente ou sans successeurs.

show ip eigrp topology all-links	Affiche toutes les routes, et non simplement les successeurs possibles, dans la topologie EIGRP.
show ip eigrp traffic *[as-number]*	Affiche le nombre de paquets Enhanced IGRP envoyés et reçus. Les informations affichées par la commande peuvent être filtrées à l'aide d'un numéro de système autonome facultatif.

Commande	Description
debug eigrp fsm	Cette commande indique l'activité des successeurs possibles EIGRP permettant de déterminer si des mises à jour de routage sont en cours d'installation et de suppression par le processus de routage.
debug eigrp packet	Les informations affichées par cette commande reflètent l'envoi et la réception de paquets EIGRP. Ces paquets peuvent être de type HELLO, mise à jour, requête ou réponse. Les numéros de séquence et d'accusé de réception utilisés par l'algorithme de transport fiable EIGRP sont indiqués dans les informations affichées.

Dépannage des protocoles de routage :

Processus de dépannage de protocole de routage :

1. Faites un énoncé clair lors de l'analyse du problème.
2. Isoler les causes possibles.
3. Examinez les problèmes possibles.
4. Créez un plan d'action basé sur les problèmes potentiels restants.
5. Mettez en œuvre le plan d'action.
6. Analysez les résultats afin de déterminer si le problème a été résolu.
7. Si le problème n'a pas été résolu, élaborez un plan d'action basé sur le problème suivant le plus probable de la liste. Retournez à l'étape 4, modifiez une variable à la fois, et répétez le processus jusqu'à ce que le problème soit résolu.
8. Une fois la cause réelle du problème identifiée, essayez de le résoudre.

Les routeurs Cisco fournissent diverses commandes intégrées pour vous aider à surveiller et à dépanner un interréseau :

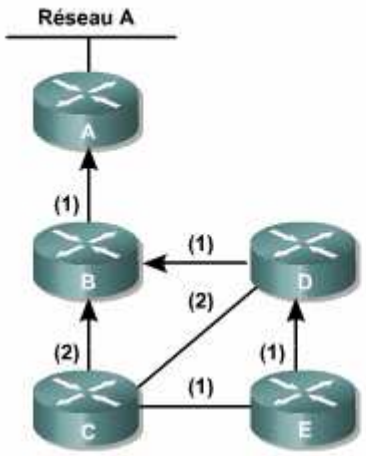
- Les commandes **show** permettent de surveiller le comportement à l'installation et le comportement normal du réseau, ainsi que d'isoler des zones problématiques
- Les commandes **debug** permettent d'identifier précisément les problèmes de protocole et de configuration.
- Les outils de réseau TCP/IP tels que **ping**, **traceroute** et **telnet**

Module 3+

l'algorithme DUAL

Exemple de L'algorithme DUAL :

Etat Stable :



Numéros entre () = métrique

C EIGRP	FD	RD	Topologie
Réseau A	3		(FD)
via B	3	1	(Successeur)
via D	4	2	(FS)
via E	4	3	

D EIGRP	FD	RD	Topologie
Réseau A	2		(FD)
via B	2	1	(Successeur)
via C	5	3	

E EIGRP	FD	RD	Topologie
Réseau A	3		(FD)
via D	3	2	(Successeur)
via C	4	3	

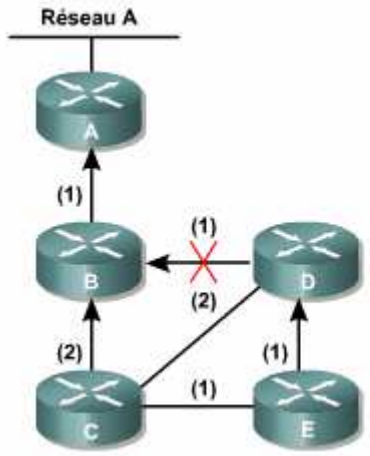
Légende	
EIGRP	Type de protocole
FD	Feasible Distance - distance possible
RD	Reported Distance - distance annoncée par le routeur voisin
Successor	Route principale vers la destination
FS	Feasible Successor (successeur possible) - Route de secours vers la destination

- Le routeur C a une route successeur en passant par le routeur B.
- Le routeur C a une route successeur possible en passant par le routeur D.
- Le routeur D a une route successeur en passant par le routeur B.
- Le routeur D n'a pas de route successeur possible.
- Le routeur E a une route successeur en passant par le routeur D.
- Le routeur E n'a pas de route successeur possible.

La route reliant le routeur D au routeur B est interrompue :

Dans le routeur D:

- La route passant par le routeur B est supprimée de la table topologique.
- C'est la route successeur. Le routeur D n'a pas de route successeur possible identifiée.
- Le routeur D doit effectuer un nouveau calcul de route.



C	EIGRP	FD	RD	Topologie
Réseau A		3		(FD)
	via B	3	1	(Successeur)
	via D	4	2	(FS)
	via E	4	3	

D	EIGRP	FD	RD	Topologie
Réseau A		2		(FD)
	~~via B~~	~~2~~	~~1~~	~~(Successeur)~~
	via C	5	3	

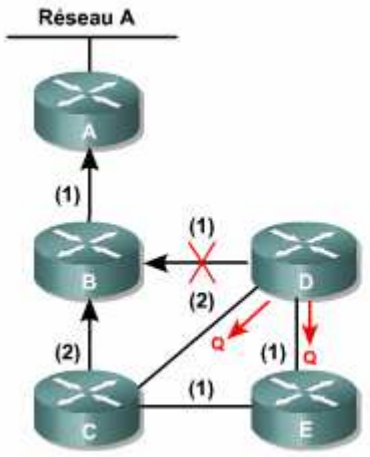
E	EIGRP	FD	RD	Topologie
Réseau A		3		(FD)
	via D	3	2	(Successeur)
	via C	4	3	

Dans le Routeur C:

- La route vers le routeur A passant par le routeur D est interrompue.
- La route passant par le routeur D est supprimée de la table.
- C'est une route successeur possible pour le routeur C.

Dans le routeur D:

- Le routeur D n'a pas de route successeur possible. Il ne peut commuter vers une route de secours identifiée.
- Le routeur D doit recalculer la topologie du réseau. Le chemin vers le réseau de destination A est défini à l'état Actif.
- Le routeur D envoie un paquet de requête à tous les voisins connectés, le routeur C et le routeur E, pour leur demander des informations topologiques.
- Le routeur C n'a pas une entrée précédente pour le routeur D.
- Le routeur D n'a pas une entrée précédente pour le routeur E.



C	EIGRP	FD	RD	Topologie
Réseau A		3		(FD)
	via B	3	1	(Successeur)
	via D			
	via E	4	3	

D	EIGRP		FD	R	Topologie
Réseau A	**ACTIF**	-1	2		(FD)
	via B				(q)
	via C		5	3	(q)

E	EIGRP	FD	RD	Topologie
Réseau A		3		(FD)
	~~via D~~	~~3~~	~~2~~	(Successeur)
	via C	4	3	

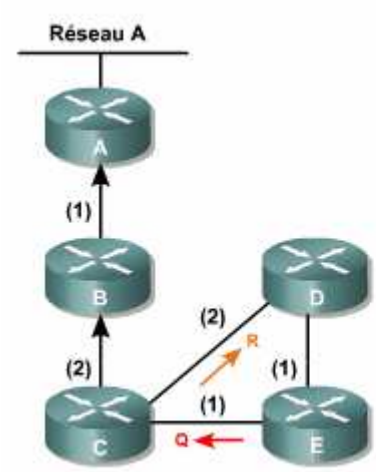
Dans le Routeur E:

- La route vers le réseau A passant par le routeur D est interrompue.

- La route passant par le routeur D est mise hors fonction.
- C'est la route successeur pour le routeur E.
- Le routeur E n'a pas de route possible identifiée.
- Notez que le coût de la distance annoncée du routage via le routeur C est 3, soit le même coût que la route successeur passant par le routeur D.

Dans le Routeur C:

- Le routeur E envoie un paquet de requête au routeur C.
- Le routeur C supprime le routeur E de la table.
- Le routeur C répond au routeur D avec une nouvelle route vers le réseau A.



C	EIGRP	FD	RD	Topologie
Réseau A		3		(FD)
	via B	3	1	(Successeur)
	via D			
	via E			

D	EIGRP		FD	R	Topologie
Réseau A	**ACTIF**	-1			(FD)
	via B				(q)
	via C		5	3	(q)

E	EIGRP		FD	R	Topologie
Réseau A	**ACTIF**	-1			(FD)
	via D				
	via C		4	3	(q)

Dans le routeur D:

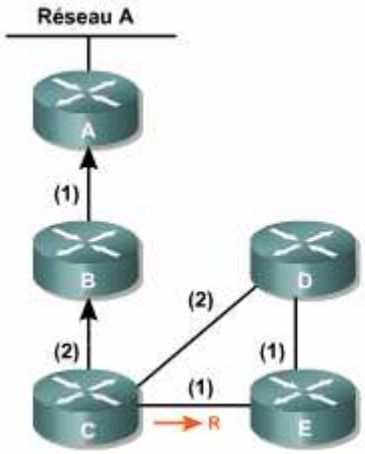
- L'état de la route vers le réseau de destination A est toujours marqué comme Actif. Le calcul n'est pas encore terminé.
- Le routeur C a répondu au routeur D pour confirmer qu'une route vers le réseau de destination A est disponible au coût de 5.
- Le routeur D attend toujours une réponse du routeur E.

Dans le Routeur E:

- Le routeur E n'a pas de route successeur possible pour atteindre le réseau de destination A.
- Le routeur E, par conséquent, étiquette l'état de la route vers le réseau de destination comme étant Actif.
- Le routeur E devra recalculer la topologie du réseau.
- Le routeur E supprime de la table la route qui passe par le routeur D.
- Le routeur E envoie un requête au routeur C, lui demandant des informations topologiques.
- Le routeur E a déjà une entrée via le routeur C. Son coût de 3 est identique à celui de la route successeur.

Dans le Routeur E:

- Le routeur C répond avec une distance signalée de 3.
- Le routeur E peut à présent définir la route passant par le routeur C comme nouvelle route successeur avec une distance possible de 4 et une distance signalée de 3.
- Le routeur E remplace l'état « Actif » de la route vers le réseau de destination A par un état « Passif ». Notez qu'un routeur a un état « Passif » par défaut tant que des paquets HELLO sont reçus. Dans cet exemple, seules les routes dont l'état est «Actif» sont étiquetées.



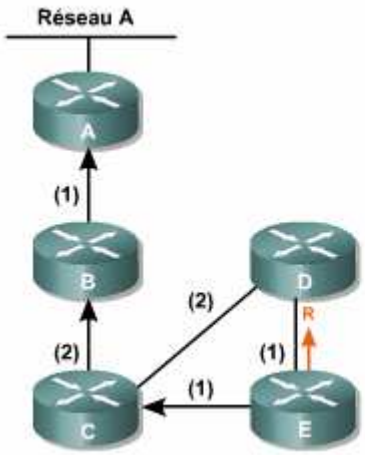
C	EIGRP	FD	RD	Topologie
Réseau A		3		(FD)
	via B	3	1	(Successeur)
	via D			
	via E			

D	EIGRP	FD	RD	Topologie
Réseau A	**ACTIF**	-1		(FD)
	via B			(q)
	via C	5	3	

E	EIGRP	FD	RD	Topologie
Réseau A	**ACTIF**	4		(FD)
	via C	4	3	(Successeur)
	via D			

Dans le Routeur E:

- Le routeur E envoie une réponse au routeur D, lui indiquant les informations topologiques du routeur E.



C	EIGRP	FD	RD	Topologie
Réseau A		3		(FD)
	via B	3	1	(Successeur)
	via D			
	via E			

D	EIGRP	FD	RD	Topologie
Réseau A		5		(FD)
	via C	5	3	(Successeur)
	via E	5	4	

E	EIGRP	FD	RD	Topologie
Réseau A		4		(FD)
	via C	4	3	(Successeur)
	via D			

Dans le routeur D:

- Le routeur D reçoit le paquet de réponse du routeur E lui indiquant les informations topologiques du routeur E.
- Le Routeur D entre ces données pour la route vers le réseau de destination A passant par le routeur E.

- Cette route devient une route successeur supplémentaire étant donné que son coût est identique au routage passant par le routeur C et que la distance signalée est inférieure au coût de distance possible de 5.

La convergence a été atteinte entre tous les routeurs EIGRP à l'aide de l'algorithme DUAL.

Module 4

Concepts de commutation

Présentation des réseaux LAN Ethernet 802.3 :

Développement des réseaux LAN :

→ Utilisation des *câbles* épais et fins partagés pour interconnecter des réseaux.
→ Utilisation des *équipements de couche 1* pour étendre les distances des réseaux.
→ Utilisation des *équipements de couche 2* pour segmenter les réseaux et optimiser les performances.

Les ponts et les commutateurs prennent des décisions de transmission sur la base des adresses MAC (Media Access Control) « table de pontage ».

- Ils créent des domaines de collision plus petite → efficacité accrue du réseau.
- Ils renforcent néanmoins le contrôle du trafic au sein d'un réseau

Les commutateurs créent un circuit virtuel entre deux unités connectées qui souhaitent communiquer. Une fois ce circuit créé, un chemin de communication dédié est établi entre les deux unités.

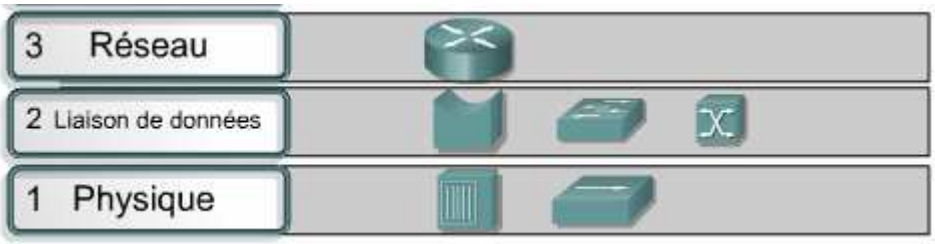
- Il crée un environnement exempt de collisions entre la source et la destination, ce qui permet d'optimiser l'utilisation de la bande passante disponible.
- Il facilite la création de multiples connexions simultanées de circuits virtuels

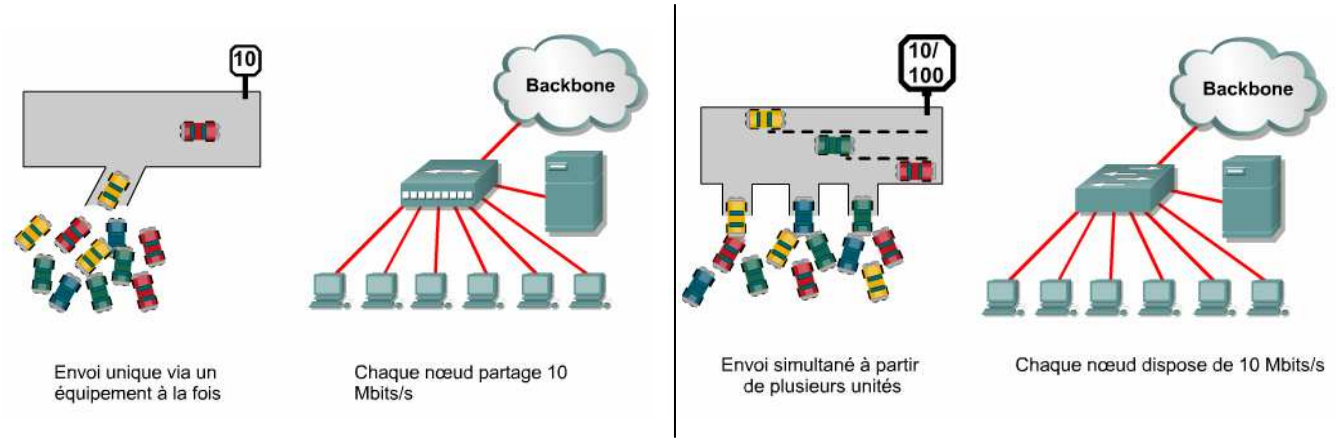
Remarque : les équipements de couche 2 présentent l'inconvénient de transmettre des trames de broadcast à tous les équipements connectés au réseau.

Un routeur (couche 3) assure toutes les fonctions suivantes:

- il examine les paquets de données entrants de couche 3.
- il sélectionne le meilleur chemin pour ces paquets sur le réseau
- il les commute vers le port de sortie approprié

Remarque : Les routeurs n'acheminent pas par défaut les paquets broadcast à moins d'être configurés explicitement pour le faire.





Facteurs ayant une incidence sur les performances du réseau

- L'environnement multitâche des systèmes d'exploitation
- Croissance d'Internet.
- Utilisation des applications client/serveur.
- Croissance du nombre d'Utilisateurs.
- Utilisation des logiciels multimédia.

Modes de transmission :

➔ Réseaux half-duplex

Ethernet était initialement une technologie half-duplex : un hôte pouvait soit transmettre, soit recevoir, mais ne pouvait pas transmettre et recevoir simultanément.

Chaque hôte Ethernet vérifie si des données sont en cours de transmission sur le réseau avant de transmettre d'autres données. Si le réseau est en cours d'utilisation, la transmission est retardée. Malgré le report de transmission, plusieurs hôtes Ethernet peuvent transmettre simultanément, ce qui *engendre une collision*.

En cas de collision :

- Une collision se produit
- l'hôte qui détecte la collision en premier envoie aux autres hôtes un signal de bourrage.
- Dès réception de ce signal, chaque hôte arrête de transmettre pendant une période aléatoire définit par l'algorithme de temporisation.

➔ Transmission full duplex :

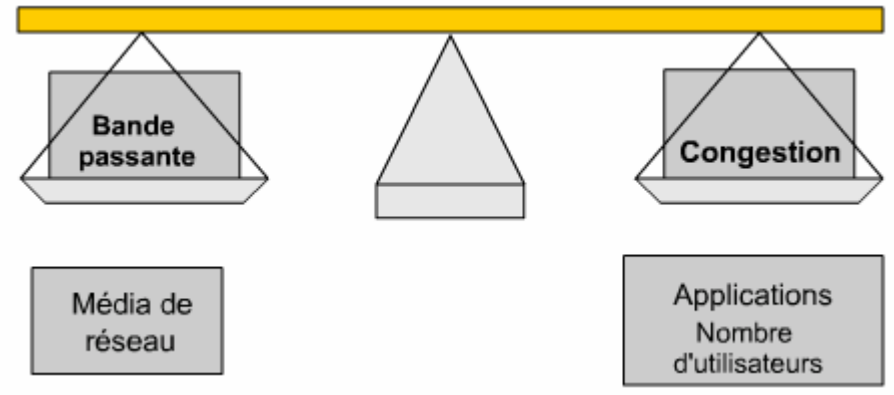
Le mode Ethernet full duplex permet de transmettre un paquet et d'en recevoir un autre simultanément. Les transmissions et réceptions simultanées nécessitent l'utilisation d'un

câble à deux paires de fils et d'une connexion commutée entre chaque nœud (*pas de collision*).

Généralement, Ethernet utilise seulement de 50 à 60 % des 10 Mbits/s de bande passante disponible en raison des collisions et de la latence.

➔ Le mode Ethernet full duplex offre 100 % de la bande passante dans les deux directions.

Congestion d'un réseau :



La congestion du réseau se traduit par un ralentissement des temps de réponse et des transferts de fichiers, ainsi que par une diminution de la productivité des utilisateurs du réseau.

➔ Pour décongestionner un réseau, il convient d'accroître la bande passante ou d'utiliser plus efficacement la bande passante disponible

Latence d'un réseau

La latence, parfois appelée délai, est le temps nécessaire à une trame ou à un paquet pour circuler entre sa station d'origine et sa destination finale.

Il existe au moins trois causes de latence:

- le temps nécessaire à la carte réseau d'origine pour placer des impulsions électriques sur le fil, plus le temps nécessaire à la carte réseau réceptrice pour interpréter ces impulsions. (1 microseconde pour les cartes réseau 10BaseT).
- le délai de propagation réel du signal traversant le câble. En général, (0,556 microseconde par 100 m de l'UTP cat 5.
- le temps de latence dépendant des unités réseau de couche 1, 2 ou 3 ajoutées sur le chemin entre les deux ordinateurs qui communiquent.

Temps de transmission Ethernet 10BaseT

La durée d'un bit « tranche de temps » est l'unité de base au cours de laquelle UN bit est envoyé. Pour que les équipements électroniques ou optiques soient en mesure de reconnaître un 1 ou un 0 binaire, il doit exister une période minimale durent laquelle le bit est actif ou non.

Le temps de transmission = nombre de bits envoyés * la durée d'un bit d'une technologie

Une autre manière de visualiser le temps de transmission est de considérer l'intervalle de temps entre le début et la fin d'une transmission ou encore, l'intervalle entre le début de transmission d'une trame et une collision. Le temps de transmission des trames de petite taille est plus court que celui des trames de grande taille.

→ La durée de transmission dépend alors de la taille d'une trame ainsi la technologie utilisée.

Exemple : Pour Ethernet 10 Mbits/s la durée du bit = 100 ns.

Taille de trame en octets	Durée de transmission en microsecondes
64	51.2
512	410
1000	800
1518	1214

Introduction à la commutation LAN :

Segmentation LAN :

La segmentation c'est le fait de diviser un réseau en plusieurs segments plus petite afin de :

- réduire significativement la congestion du réseau au sein de chaque segment.
- partager la totalité de la bande passante disponible sur chaque segment.

Les données échangées entre les segments sont transmises au *backbone* du réseau via un pont, un routeur ou un commutateur.

Segmentation LAN à l'aide de ponts :

→ L'utilisation d'un pont augmente de dix à trente pour cent la latence d'un réseau. Cette latence résulte du processus de prise de décision qui a lieu avant l'envoi d'un paquet.

→ Un pont est considéré comme un équipement de type Store-and-Forward, car il doit examiner le champ d'adresse de destination et calculer le code de redondance cyclique (CRC) dans le champ de séquence de contrôle de trame avant l'envoi d'une trame. Si le port de

destination est occupé, le pont peut stocker temporairement la trame jusqu'à ce que le port soit de nouveau disponible.

Segmentation LAN à l'aide de routeurs

→ Les routeurs assurent la segmentation des réseaux en ajoutant un coefficient de latence de 20 à 30 % sur un réseau commuté. Cette latence accrue est due au fonctionnement d'un routeur au niveau de la couche réseau qui utilise l'adresse IP pour déterminer le meilleur chemin.

Avantages : Domaines de Broadcast plus petites + permet la communication entre les SR.

Segmentation LAN à l'aide de commutateurs

→ Les commutateurs utilisent la microsegmentation afin de réduire les domaines de collisions et le trafic réseau.

→ Lorsque deux nœuds établissent une liaison, ou circuit virtuel, ils accèdent au maximum de bande passante disponible. Ces liaisons offrent un débit plus important que les LAN Ethernet connectés via des ponts ou des concentrateurs.

Fonctionnement de base d'un commutateur

Une unité de commutation exécute deux fonctions de base :

- La commutation de trames de données – Opération qui consiste à recevoir une trame sur une interface du commutateur, de sélectionner l'interface de sortie et de finalement transmettre la trame.
- Gestion des tables de commutation – Les commutateurs créent et gèrent des tables de commutation.

Latence des commutateurs Ethernet :

La latence d'un commutateur est l'intervalle de temps à partir de l'entrée du début d'une trame dans le commutateur jusqu'à la sortie de la fin de la trame correspondante. Cette période est directement liée au processus de *commutation configuré* et au *volume du trafic*.

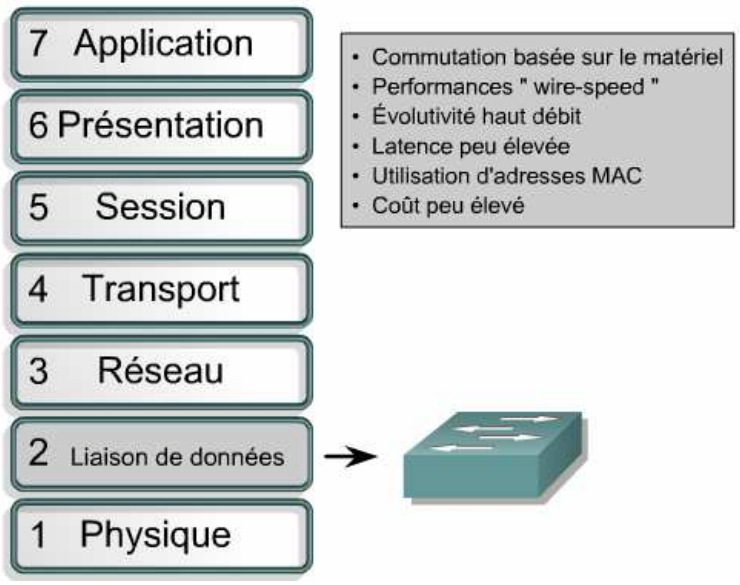
Commutation des couches 2 et 3

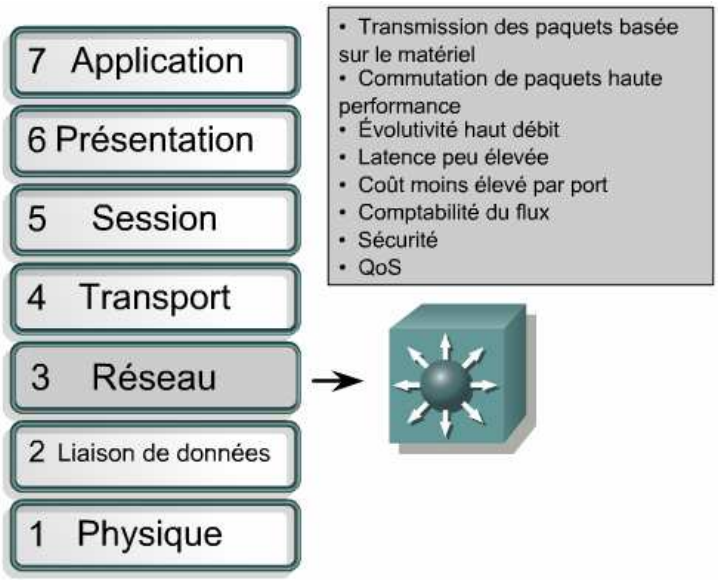
- Les routeurs et les commutateurs de couche 3 utilisent la commutation de couche 3.
- Les commutateurs de couche 2 et les ponts utilisent la commutation de couche 2.

La différence entre les deux réside au niveau du type d'information utilisé dans la trame pour déterminer l'interface de sortie appropriée (MAC ou IP)

La principale **différence entre le processus de commutation** de paquet d'un **routeur** et d'un **commutateur de couche 3** se situe au niveau de l'implémentation physique.

- Dans la plupart des *routeurs*, la commutation de paquet s'effectue au niveau logiciel par l'entremise d'un microprocesseur.
- Un *commutateur de couche 3* effectue la commutation de paquet directement au niveau matériel en ayant recourt à des circuits intégrés spécialisés (ASIC).





Commutation symétrique et asymétrique

La commutation symétrique ou asymétrique d'un réseau LAN dépend de la façon dont la bande passante est allouée aux ports de commutateur.

→ La commutation symétrique fournit des connexions commutées entre des ports de même débit.

→ Un commutateur LAN asymétrique fournit des connexions commutées entre des ports de débit différent, par exemple entre une combinaison de ports de 10 Mbits/s et de 100 Mbits/s.

- nécessite l'utilisation de la mémoire tampon pour conserver les trames contiguës.

Mise en mémoire tampon

La zone de mémoire dans laquelle le commutateur stocke les données s'appelle la mémoire tampon.

→ Recourir à la mise en mémoire tampon : lorsque le port de destination est occupé + le cas de la commutation asymétrique.

Cette mémoire peut utiliser deux méthodes pour acheminer les trames :

- la mise en mémoire tampon axée sur les ports
- la mise en mémoire tampon partagée.

• Dans le cas de la mise en mémoire tampon axée sur les ports, les trames sont placées dans des files d'attente liées à des ports entrants spécifiques.
• La mise en mémoire partagée stocke toutes les trames dans une mémoire tampon commune que partagent tous les ports du commutateur.

Le commutateur tient à jour une carte de liaisons entre une trame et un port, indiquant l'emplacement vers lequel un paquet doit être acheminé.

Fonctionnement d'un commutateur :

Fonctions des commutateurs Ethernet

Un commutateur apprend les hôtes qui sont connectés à un port en lisant l'adresse MAC comprise dans les trames. Il ouvre un circuit virtuel uniquement entre les nœuds d'origine et de destination, ce qui limite la communication à ces deux ports sans affecter le trafic des autres ports.

Les principales fonctions d'un commutateur Ethernet sont les suivantes:

- Il isole le trafic entre des segments.
- Il augmente la bande passante pour chaque utilisateur.

1- Chaque segment utilise le mode d'accès CSMA/CD pour gérer le trafic des données entre les utilisateurs sur le segment.

2- La microsegmentation permet la création de segments réseau dédiés comportant un seul hôte par segment. Chaque hôte reçoit ainsi toute la bande passante du lien

Modes de transmission de trame

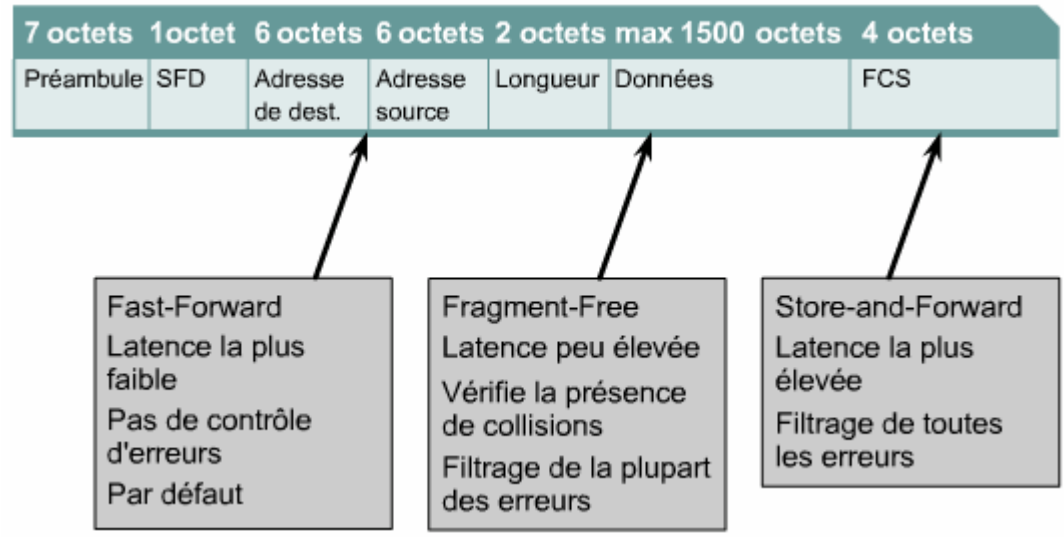
Il existe 3 modes de transmission d'une trame :

➔ **Commutation Cut-through** – La trame est acheminée avant d'avoir été entièrement reçue. Ce mode réduit la latence de la transmission mais diminue aussi le potentiel de détection d'erreurs de commutation. Il y a deux types de commutation "cut-through" :

- *Commutation "Fast-forward"* – il achemine une trame dès la réception de l'adresse MAC de destination. Dans ce mode, la latence est mesurée à partir du premier bit reçu jusqu'au premier bit transmis (c'est la méthode du premier entré, premier sortie ou "FIFO").
- *Commutation "Fragment-free"* – il filtre les fragments de collision avant que l'acheminement ne puisse commencer (fragment < 64 octets), la trame reçue doit être jugée comme n'étant pas un fragment de collision pour être acheminée.

➔ **Store-and-Forward** – Dans ce mode, la trame doit être reçue entièrement pour qu'elle puisse être acheminée. Le commutateur dispose du temps nécessaire pour vérifier les erreurs, ce qui améliore la détection des erreurs.

➔ **Adaptive Cut-through** – il combine les modes Store-and-Forward et Cut-through. Dans ce mode, le commutateur utilise le mode Cut-through jusqu'à ce qu'il détecte un nombre d'erreurs donné. Une fois le seuil d'erreurs atteint, il passe en mode Store-and-Forward.



Apprentissage des adresses par les commutateurs et les ponts :

Lorsqu'un pont est activé, des messages de broadcast sont transmis pour demander à toutes les stations du segment local du réseau de répondre.

Lorsque les stations renvoient le message de broadcast, le pont crée une table d'adresses locales. Ce processus est appelé ***apprentissage***.

Les adresses apprises et l'interface ou le port associé sont stockés dans la table d'adressage.

Remarque : La table d'adressage se trouve dans la mémoire associative (CAM) « Content Addressable Memory ».

Une adresse est *horodatée* chaque fois qu'elle est enregistrée. Cela permet de stocker les adresses pendant une période déterminée.

Le processus suivi par la mémoire associative (CAM) :

→ Si l'adresse n'est pas trouvée, le pont achemine la trame sur chaque interface à l'exception de l'interface sur laquelle la trame a été reçue. Ce processus est appelé inondation.

→ Si l'adresse est trouvée dans la table d'adresses et que l'adresse est associée à l'interface de réception, la trame est rejetée. Elle doit nécessairement avoir déjà été reçue par la destination.

→ Si l'adresse est trouvée dans la table d'adresses et que l'adresse est associée à une interface autre que celle de réception, le pont l'achemine sur l'interface en question.

Lorsque deux hôtes connectés veulent communiquer, le commutateur consulte la table de commutation et établit une *connexion virtuelle* (micosegment) entre les deux ports. Le circuit virtuel est maintenu jusqu'à ce que la session soit terminée.

Filtrage des trames par les commutateurs et les ponts

- Une trame est dite filtrée lorsqu'elle est ignorée.
- Une trame est dite transmise lorsqu'elle est copiée.

La plupart des ponts et des commutateurs ont maintenant la capacité de filtrer des trames selon des critères visant presque n'importe quel champ de la couche 2

Exemple : → Traiter les paquets de broadcast et de multicast inutiles.

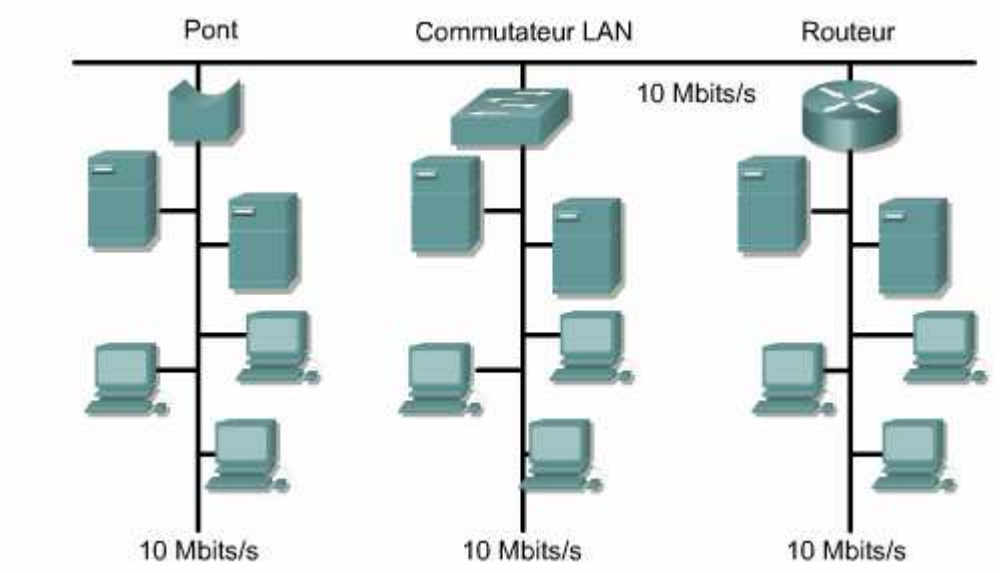
Les ponts et les commutateurs qui peuvent filtrer les trames sous la base des adresses MAC peuvent aussi filtrer les trames Ethernet selon qu'il s'agisse d'une adresse broadcast ou multicast. Ce filtrage est accompli par la mise en œuvre de LAN virtuels (VLAN).

→ Rendre les tempêtes de broadcast moins dangereuse.

Les commutateurs actuels sont également capables de filtrer en fonction du protocole de couche réseau « pont-routeur »

Remarque : Les ponts-routeurs filtrent en examinant les informations de la couche réseau mais n'utilisent pas de protocole de routage

Pourquoi segmenter les réseaux LAN ?



- Isoler le trafic entre les segments.
- Fournir davantage de bande passante par utilisateur par la création de domaines de collision de petite taille.

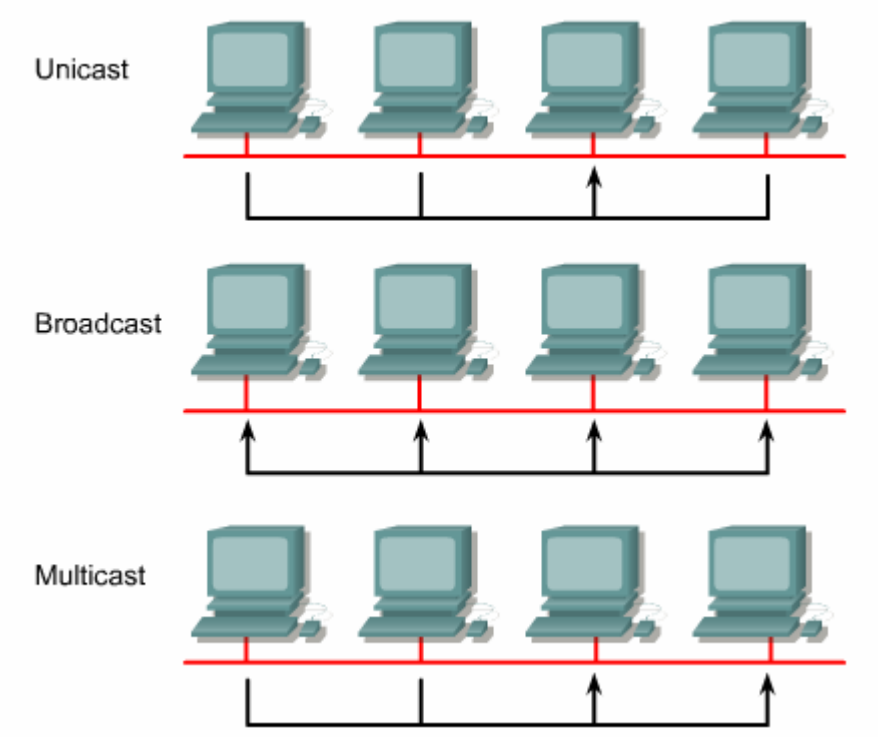
Commutateurs et domaines de collision

La zone du réseau d'où proviennent les trames qui entrent en collision est appelée domaine de collision. Tous les environnements à média partagé sont des domaines de collision.

Quand un hôte est connecté à une interface d'un commutateur, le commutateur crée alors une connexion dédiée. Cette connexion est considérée comme un domaine de collision individuel.

Commutateurs et domaines de broadcast

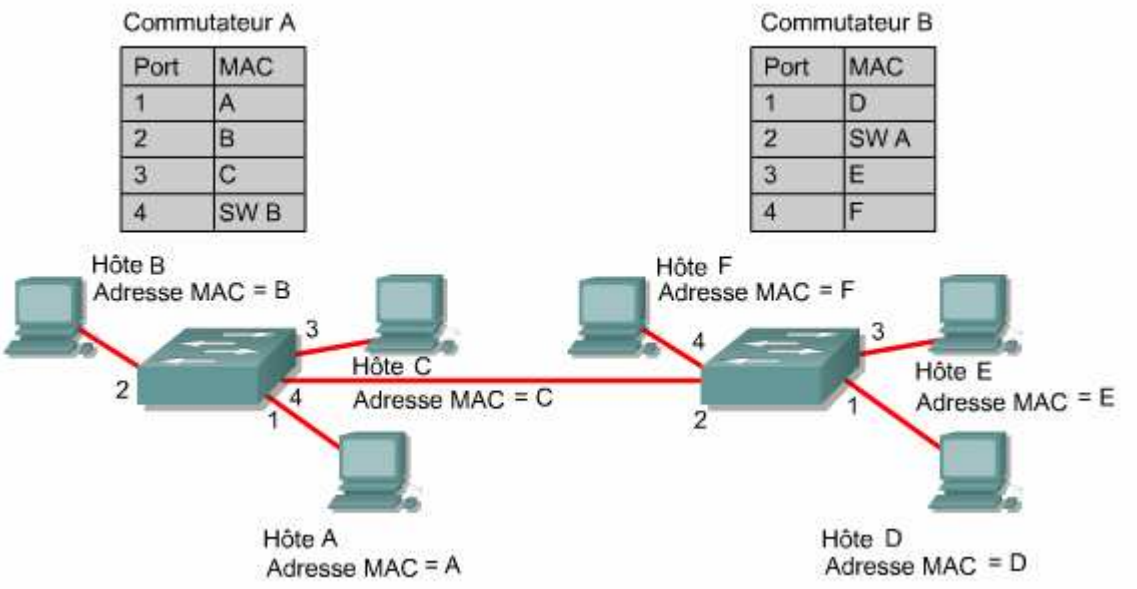
Il existe 3 modes de transmission sur un réseau :



Unicast → un émetteur tente d'atteindre un récepteur.

Multicast → un émetteur tente d'atteindre un sous-ensemble, un groupe ou un segment entier.

Broadcast → un émetteur tente d'atteindre tous les récepteurs du réseau..



Module 5

Commutateurs

Conception LAN :

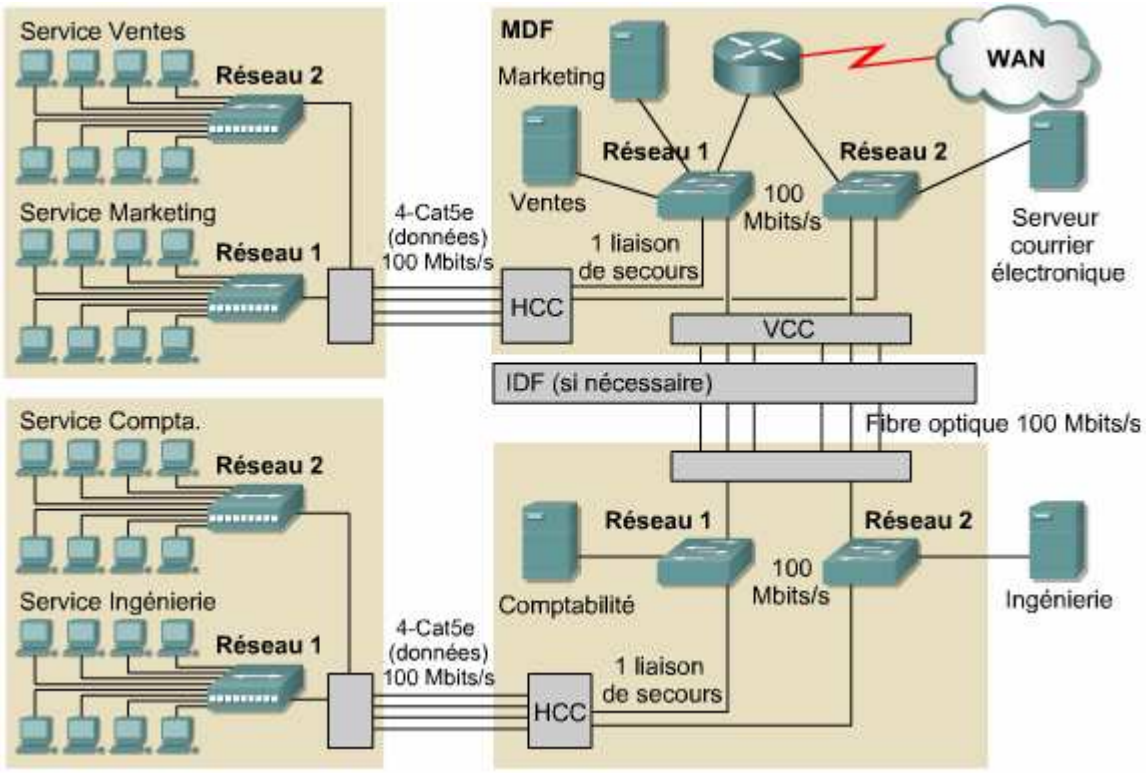
Objectifs de la conception LAN :

- **Fonctionnalité** – Le réseau doit être fonctionnel. Il doit fournir une connectivité fiable entre les utilisateurs ainsi qu'entre les utilisateurs et les applications, avec un débit raisonnable.
- **Évolutivité** – Le réseau doit présenter une capacité d'extension. La conception initiale doit pouvoir s'étendre sans qu'il soit nécessaire d'apporter des modifications importantes à la conception globale.
- **Adaptabilité** – Le réseau doit être conçu de façon à s'adapter aux futures technologies
- **Facilité de gestion** – Un réseau doit être conçu pour faciliter la surveillance et la gestion du réseau.

Choix de conception LAN :

Afin de maximiser la bande passante et les performances LAN, il faut prendre en compte les aspects de conception LAN suivants :

- la *fonction* et *l'emplacement* des *serveurs*
- *Problématique* des *domaines de collision*
- les *problèmes* de *segmentation*.
- les *problèmes* de *domaine de broadcast*.



Les serveurs fournissent des services de partage de fichiers, d'impression, de communication et d'application. On peut distinguer deux catégories de serveurs :

- les serveurs d'entreprise et les serveurs de groupe de travail.

→ Un serveur d'entreprise prend en charge tous les utilisateurs du réseau en leur offrant des services tels que le courrier électronique ou le système de noms de domaine (DNS), dont tous les membres ont besoin, car il s'agit de fonctions centralisées (installés dans le **MDF**)

→ Un serveur de groupe de travail prend en charge un ensemble spécifique d'utilisateurs et offre des services tels que le traitement de texte et le partage de fichier (installés dans les **IDF**)

➔ Dans le répartiteur principal MDF et les répartiteurs intermédiaires IDF, les commutateurs LAN de couche 2 liés à ces serveurs doivent avoir un débit minimal de 100 Mbits/s.

Méthodologie de conception de réseau LAN

Pour qu'un réseau local réponde aux besoins des utilisateurs, il doit être mis en œuvre en respectant une série d'étapes systématiquement planifiées :

- recueillir les impératifs et les attentes
- analyser les besoins et les données
- concevoir la structure LAN des couches 1, 2 et 3 (c'est-à-dire la topologie)
- créer des documents sur la mise en œuvre logique et physique du réseau

Le processus de recueil de l'information permet de clarifier et d'identifier tout problème de réseau actuel, ainsi que les points de vue des futurs utilisateurs du réseau local.

- Qui seront les futurs utilisateurs du réseau local ?
- Quel est leur niveau de compétence ?
- Comment se comportent-ils vis-à-vis des ordinateurs et des applications ?
- Certaines données sont-elles d'une importance vitale ?
- Certaines opérations sont-elles d'une importance vitale ?
- Quels sont les protocoles autorisés sur le réseau ?
- Certains types d'ordinateur de bureau sont-ils les seuls hôtes supportés par le réseau?
- Qui est responsable de l'adressage, de l'attribution de noms, de la conception de la topologie et de la configuration du réseau LAN ?
- Quelles sont les ressources matérielles, logicielles ainsi que les ressources humaines?
- Quel est le lien entre ces ressources et de quelle façon sont-elles partagées?
- Quelles sont les ressources financières de l'organisation?

La constitution de documentation sur les exigences suivantes permet d'établir une estimation de coûts et des délais pour la mise en œuvre de la conception LAN projetée.

De nombreux éléments peuvent affecter la disponibilité, notamment les suivants:

- le débit
- le temps de réponse

- l'accès aux ressources.

L'étape suivante consiste à *choisir une topologie LAN globale* capable de répondre aux besoins des utilisateurs.

La conception d'une topologie LAN peut être divisée en trois catégories uniques du modèle de référence OSI :

- la couche réseau,
- la couche liaison de données
- la couche physique.

L'étape suivante consiste à *constituer la documentation de la topologie physique et logique* du réseau.

- La topologie physique du réseau se rapporte à la façon dont les divers composants LAN sont connectés ensemble.
- La conception logique du réseau fait référence au flux de données dans un réseau.

La documentation d'une conception LAN importante inclut les éléments suivants:

- la carte topologique de la couche OSI
- la carte logique du réseau LAN
- la carte physique du réseau LAN
- les feuilles d'identification des câbles
- la carte logique du VLAN
- la carte logique de la couche 3
- les cartes d'adressage

Schéma logique

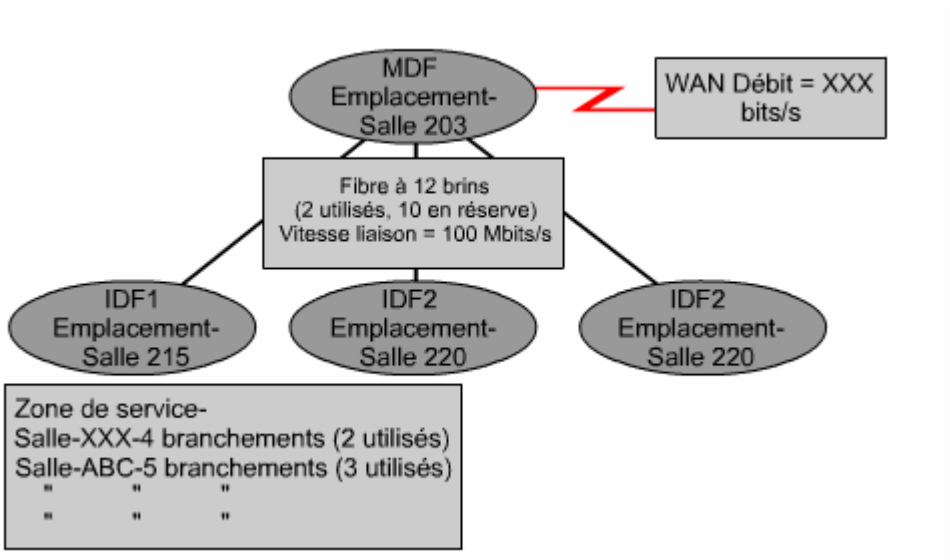
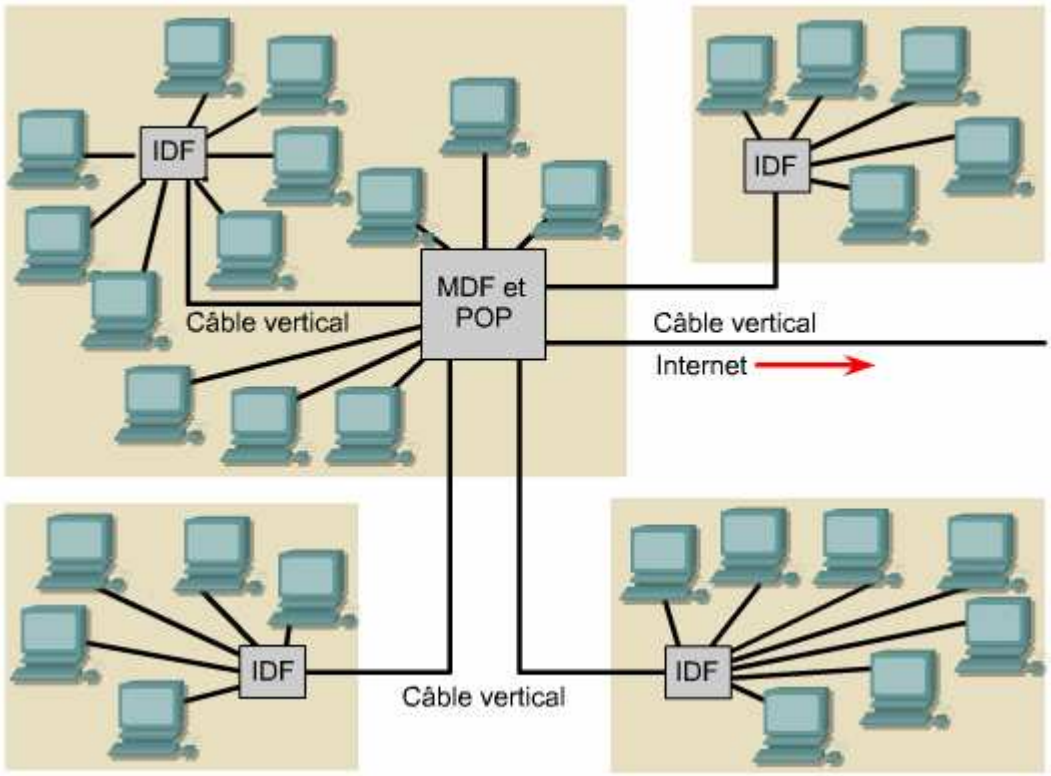


Schéma physique :

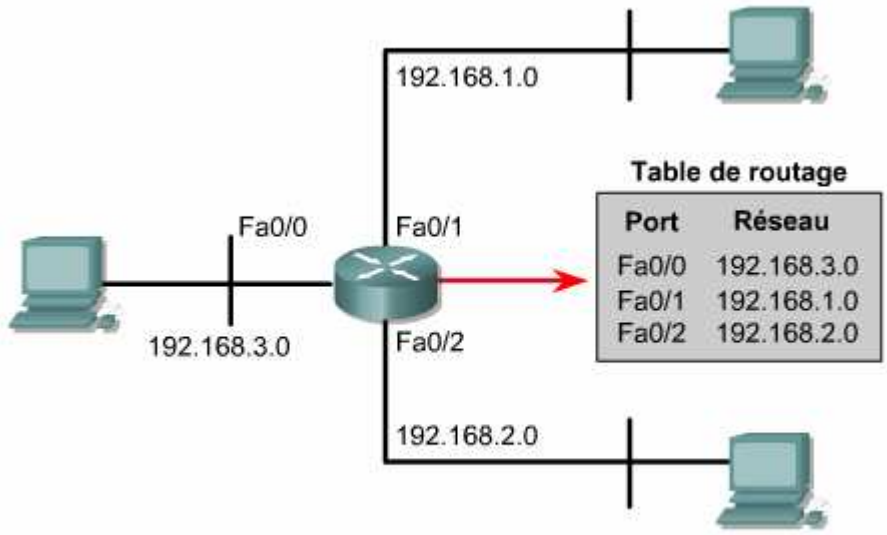


Feuille d'identification des câbles :

IDF1
Emplacement-
Salle XXX

Connexion	ID câble	Interconnexion Raccord/Port	Type de câble	État
IDF1 à salle 203	203-1	HCC1/Port 13	UTP cat. 5	Utilisé
IDF1 à salle 203	203-2	HCC1/Port 14	UTP cat. 5	Non utilisé
IDF1 à salle 203	203-3	HCC2/Port 3	UTP cat. 5	Non utilisé
IDF1 à MDF	IDF1-1	VCC1/Port 1	Fibre multimode	Utilisé
IDF1 à MDF	IDF1-2	VCC1/Port 2	Fibre multimode	Utilisé

la carte logique de la couche 3



Conception de la couche 1

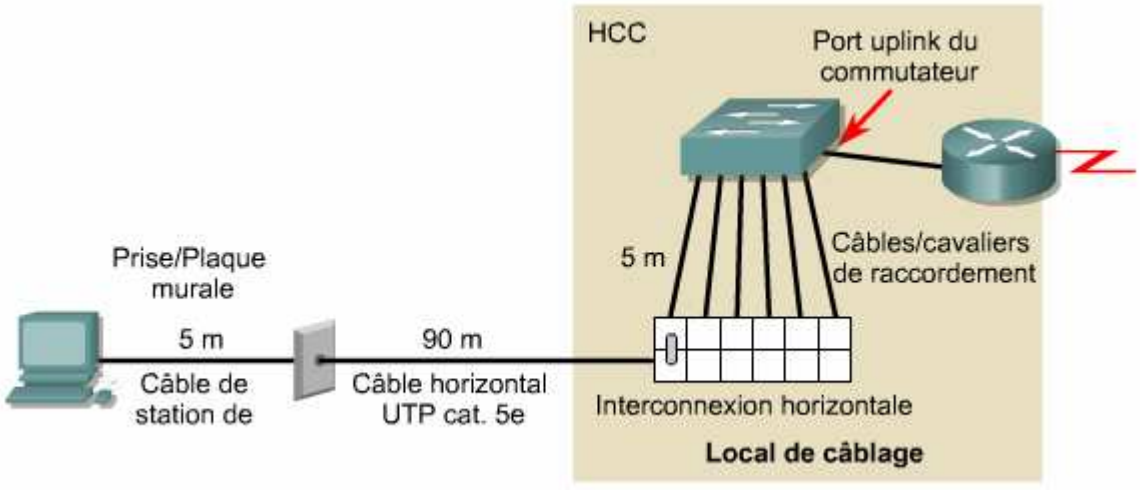
Le câblage physique est l'un des éléments les plus importants à prendre en considération lors de la conception d'un réseau.

Les questions relatives à la conception au niveau de la couche 1 comprennent le type de câble à utiliser (généralement, des câbles de cuivre ou à fibre optique) ainsi que la structure globale du câblage.

→ Vous devez évaluer les points forts et les faiblesses des diverses topologies.

→ Vous devez s'assurer que ces systèmes sont conformes aux normes de l'industrie, telles que la norme TIA/EIA-568-B.

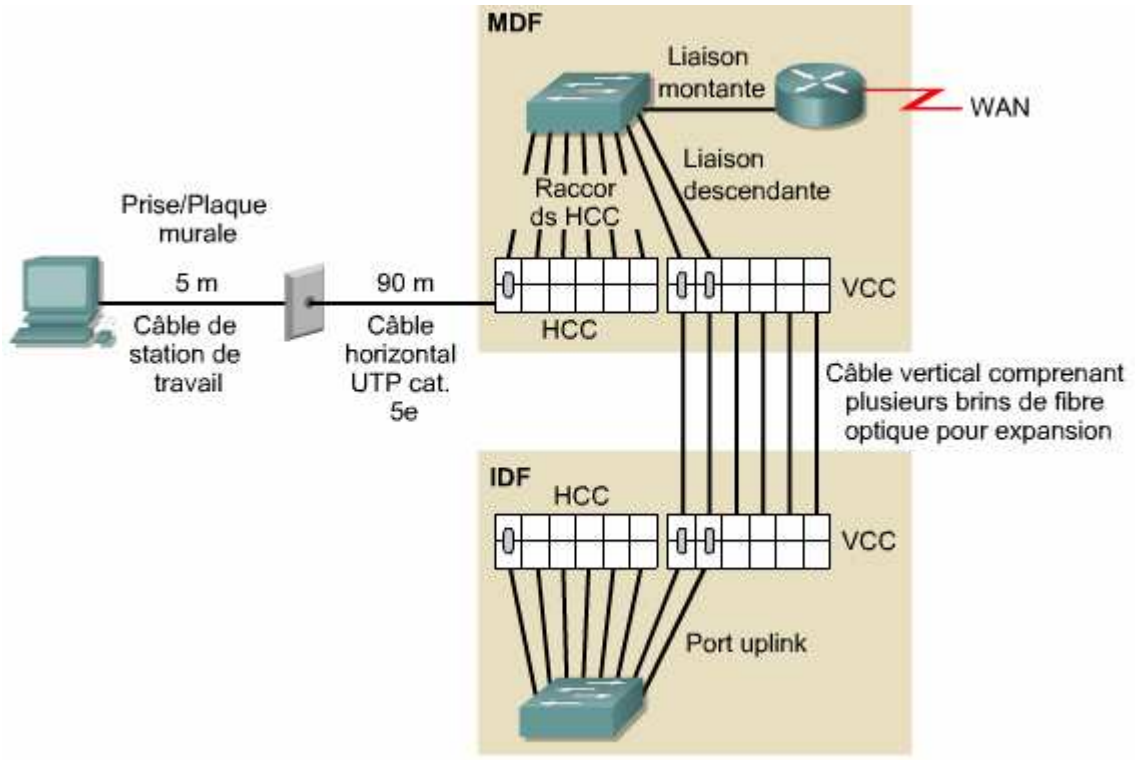
Dans une topologie en étoile simple comportant un seul local technique, le répartiteur principal MDF comprend un ou plusieurs tableaux d'interconnexions horizontales (horizontal cross-connect ou HCC).



Pour étendre la superficie du réseau, il faut créer plusieurs locaux techniques (IDF).

Les normes TIA/EIA568-B précisent que les répartiteurs intermédiaires IDF doivent être connectés au répartiteur principal MDF par le biais d'un *câblage vertical* appelé *câblage de backbone.*

Une interconnexion verticale (vertical cross-connect ou VCC) permet d'interconnecter les divers répartiteurs intermédiaires IDF au répartiteur principal MDF.



Le schéma logique représente le modèle de la topologie du réseau sans les détails relatifs au parcours d'installation précis des câbles « inclut les éléments suivants » :

- L'emplacement exact et l'identification des locaux techniques MDF et IDF.
- Le type et le nombre de câbles utilisés pour interconnecter le MDF et les IDF.
- Le nombre de câbles de réserve disponibles pour accroître la bande passante.
- Une documentation détaillée de tous les parcours de câbles, les numéros d'identification et le port de l'interconnexion horizontale ou verticale.

Conception de la couche 2

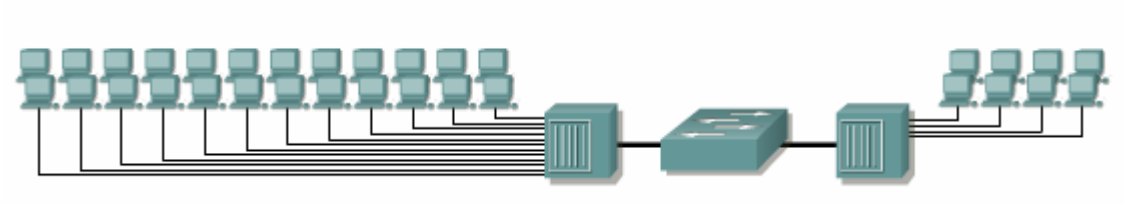
L'objectif est d'augmenter les performances d'un groupe de travail ou d'un backbone.

Utiliser des commutateurs asymétriques : Un commutateur LAN peut attribuer la bande passante par port, ce qui laisse davantage de bande passante aux câbles verticaux, aux liaisons montantes (*uplinks*) et aux serveurs.

Le câble vertical acheminera tout le trafic de données entre le répartiteur principal et le répartiteur intermédiaire. La capacité souhaitée d'un câble vertical est supérieure à celle d'un câble horizontal.

L'étape suivante consiste à déterminer le nombre de ports nécessaires pour le répartiteur principal MDF et pour chacun des répartiteurs intermédiaires IDF.

→ On peut également utiliser des concentrateurs de couche 1 mais en utilisant un commutateur pour connecter ces concentrateurs (limiter un petit peu les collisions)



Conception de la couche 3 :

Les routeurs (couche 3) fournissent une évolutivité au réseau parce qu'ils servent de pare-feu vis-à-vis des broadcasts. Ils peuvent également favoriser l'évolutivité en divisant les réseaux en sous-réseaux.

Les routeurs résolvent les problèmes liés au nombre excessif de broadcasts, aux protocoles qui n'évoluent pas correctement, à la sécurité et à l'adressage de la couche réseau.

Une fois qu'un modèle d'adressage IP a été développé pour un client, il doit faire l'objet d'une documentation claire et précise. Une convention standard doit être définie pour l'adressage des hôtes importants du réseau.

Adresse logique	Unités du réseau physique
x.x.x.1-x.x.x.10	Ports de routeur, LAN et WAN
x.x.x.11-x.x.x.20	Commutateurs LAN
x.x.x.21-x.x.x.30	Serveurs d'entreprise
x.x.x.31-x.x.x.80	Serveurs de groupe de travail
x.x.x.81-x.x.x.254	Hôtes

Ce système d'adressage doit être cohérent pour l'ensemble du réseau. Les cartes d'adressage fournissent un cliché du réseau.

Adresse IP réseau 172.16.0.0
Masque de sous-réseau = 255.255.255.0

Rectorat XYZ

École ABC	École DEF
172.16.1.0 à 172.16.10.0	172.16.11.0 à 172.16.21.0
Masque de sous-réseau = 255.255.255.0	Masque de sous-réseau = 255.255.255.0
Nom du routeur = Routeur ABC	Nom du routeur = Routeur DEF
Fa0/0 = 172.16.1.1	Fa0/0 = 172.16.11.1
Fa0/1 = 172.16.2.1	Fa0/1 = 172.16.12.1

→ La création de cartes physiques vous aide à dépanner le réseau.

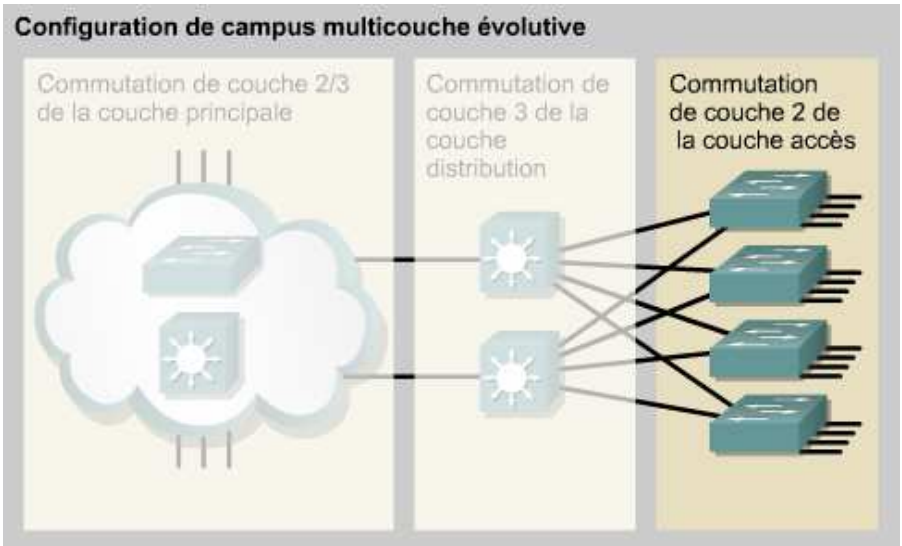
Commutateurs LAN :

LAN commutés :

L'utilisation d'un *modèle de conception hiérarchique* permettra d'apporter plus facilement des modifications au réseau au fur et à mesure de la croissance de l'organisation.

Le modèle de conception hiérarchique comprend les trois couches suivantes :

- ***La couche accès*** permet aux utilisateurs répartis dans les groupes de travail d'accéder au réseau.
- ***La couche distribution*** assure une connectivité basée sur les politiques d'administration et de sécurité.
- ***La couche principale*** assure l'optimisation du transport entre les sites. La couche principale est souvent appelée backbone.



Vue d'ensemble de la couche accès :

La couche accès est le point d'entrée au réseau pour les stations de travail utilisateur et les serveurs. Dans un réseau LAN de campus, l'équipement utilisé au niveau de la couche accès peut être un commutateur (BP commutée) ou un concentrateur (BP partagée).

Fonctions :

- Bande passante partagée
- Bande passante réservée
- Filtrage de la couche MAC
- Microsegmentation

Commutateurs de la couche accès

Les commutateurs de la couche accès fonctionnent au niveau de la couche 2 du modèle OSI et fournissent des services tels que l'appartenance au VLAN. Le commutateur de couche accès a pour principal objectif d'autoriser l'accès des utilisateurs finaux sur le réseau.

- faible coût
- une densité de port élevée

- Gamme Catalyst 1900
- Gamme Catalyst 2820
- Gamme Catalyst 2950
- **Gamme Catalyst 4000**
- Gamme Catalyst 5000

Vue d'ensemble de la couche distribution

Elle a pour rôle de définir les limites à l'intérieur desquelles le traitement des paquets peut avoir lieu. Elle segmente également les réseaux en domaines de broadcast. Des politiques de traitement peuvent être appliquées et des listes de contrôle d'accès peuvent filtrer les

paquets. Les commutateurs de cette couche fonctionnent au niveau de la couche 2 et de la couche 3

Fonctions :

- le regroupement des connexions du local technique,
- la définition des domaines de broadcast et de diffusion multipoint (multicast),
- le routage des LAN virtuels (VLAN),
- le changement de média, si nécessaire,
- la sécurité.

Commutateurs de la couche distribution

Les commutateurs de la couche distribution sont les points de regroupement de plusieurs commutateurs de la couche accès. Le commutateur doit être en mesure de supporter la totalité du trafic des équipements de la couche accès.

- La couche distribution doit avoir des performances élevées
- «*commutateurs multicouches*» combinent en un seul équipement les fonctions d'un routeur et d'un commutateur.

- Catalyst 2926G
- Catalyst 3550
- Gamme Catalyst 5000
- **Gamme Catalyst 6000**

Vue d'ensemble de la couche principale

La couche principale est un backbone de commutation à haut débit.

→ Cette couche du réseau ne doit pas effectuer de tâches liées au traitement de paquets.

→ L'établissement d'une infrastructure principale avec des routes redondantes procure de la stabilité au réseau pour pallier une éventuelle défaillance d'un équipement

→ Des commutateurs ATM ou Ethernet peuvent être utilisés.

Commutateurs de la couche principale

Les commutateurs de couche principale sont conçus pour fournir en cas de besoin une fonctionnalité de couche 3 efficace.

- Gamme Catalyst 6500
- Gamme Catalyst 8500
- Gamme IGX 8400
- **Lightstream 1010**

Module 6

Configuration d'un commutateur

Démarrage du commutateur :

Démarrage physique du commutateur Catalyst :

Les commutateurs sont des ordinateurs dédiés et spécialisés qui contiennent un CPU, une mémoire RAM et un système d'exploitation.

Un commutateur peut être géré par le biais d'une connexion au port console qui vous permet de consulter et de modifier la configuration.

En règle générale, les commutateurs n'ont pas d'interrupteur d'alimentation permettant de les mettre sous tension ou hors tension. Il y a des modèles avec 12, 24 et 48 ports.

Les deux commutateurs du dessus sont des commutateurs symétriques à configuration fixes dont tous les ports sont de technologie FastEthernet ou 10/100.

Les trois modèles suivants sont asymétriques et comportent deux ports Gigabit Ethernet fixes pour les médias de fibre ou de cuivre.

Les quatre modèles du bas sont des commutateurs asymétriques comportant des emplacements pour interfaces modulaires GBIC (Gigabit Interface Converter) qui peut accommoder une variété d'options pour les médias de fibre ou de cuivre

Indicateurs LED de commutateur

Le panneau avant d'un commutateur comporte différents voyants permettant de surveiller les activités et les performances du système.

Le panneau avant du commutateur comporte les LED suivantes:

- LED système
- LED RPS (Remote Power Supply)
- LED pour le mode des ports
- LED pour l'état des ports

→ La LED système indique si le système est bien alimenté et s'il fonctionne correctement.

→ La LED RPS indique si une source de téléalimentation est utilisée.

→ La LED Mode indique l'état actuel du bouton Mode. Les modes permettent de déterminer comment sont interprétés les LED d'état des ports.

Remarque : La signification des LED correspondant à l'état des ports varie en fonction de la valeur courante du LED Mode.

Led Mode	Couleur	Description
STAT	Désactivé	Aucune liaison
	Vert fixe	Liaison opérationnelle
	Vert clignotant	Le port est en train d'envoyer ou de recevoir des données.
	Alternativement vert/orange	Liaison défectueuse
	Orange fixe	Le port ne transmet pas de données car il a été désactivé par un administrateur ou une violation d'adresse, ou bloqué par le protocole Spanning Tree.
UTIL	Désactivé	Chaque LED éteinte indique une réduction de moitié de la bande passante totale. Les LED sont éteintes de droite à gauche. Si le LED le plus à droite est éteint, le commutateur utilise moins de 50 % de la bande passante totale. Si les deux LED les plus à droite sont éteintes, le commutateur utilise moins de 25 % de la bande passante totale.
	Vert	Si toutes les LED sont vertes, le commutateur utilise au moins 50 % de la bande passante totale.
DUPLX	Désactivé	Le port fonctionne en mode half-duplex.
	Vert	Le port fonctionne en mode full duplex.
SPEED	Désactivé	Le port fonctionne à 10 Mbits/s.
	Vert	Le port fonctionne à 100 Mbits/s.
	Vert clignotant	Le port opère à 1000 Mbits/s

Vérification des LED au cours du test (POST)

LED système
La LED système indique le succès ou l'échec de POST. • Si la LED système est éteinte alors que le commutateur est connecté, le test POST est en cours. • Si la LED système est verte, le test POST a réussi. • Si la LED système est orange, le test POST a échoué.

Les LED d'état des ports peuvent également changer de couleur pendant le test POST du commutateur.

Elles peuvent devenir orange pendant 30 secondes, juste le temps pour le commutateur de découvrir la topologie du réseau et de rechercher d'éventuelles boucles.

- LED **verte** → le commutateur a établi un lien entre le port et une cible
- LED **s'éteigne** → le commutateur a déterminé que rien n'est connecté au port

Affichage des informations après démarrage initial du commutateur

→ Connectez un ordinateur à ce commutateur « un câble à paires inversées »

→ Lancez HyperTerminal sur l'ordinateur et définir les paramètres par défaut.

→ Branchez le commutateur à une prise murale.

Les informations délivrées après le démarrage initial du commutateur devraient s'afficher sur l'écran HyperTerminal. Cet affichage présente des informations sur le commutateur, des détails sur l'état du POST et des données sur le matériel du commutateur.

Aperçu de l'aide de l'interface de commande en ligne du commutateur

? → Afficher la liste des commandes disponibles pour le mode de commande actuel

Aide sur les termes → pour accomplir la suite d'une commande.

Aide à la syntaxe des commandes → fournit des mots clés en fonction d'une commande

Modes de commande des commutateurs

Le mode par défaut est le mode utilisateur (User EXEC mode) « > ».

→ Les commandes disponibles en mode utilisateur sont celles qui permettent de modifier les paramètres du terminal, de réaliser des tests de base et d'afficher les informations système.

Commandes	Description
`show version`	Affiche les informations de version du logiciel et du matériel. Utilisé afin de déterminer exactement le logiciel et les modules en cours d'utilisation.
`show flash:`	Affiche l'information à propros du système de fichiers flash: .
`show mac-address-table`	Affiche les adresses MAC contenues dans la table de con
`show controllers ethernet-controller`	Indique les trames abandonnées ou différées, les erreurs d'alignement, les collisions, etc.

La commande **enable** est utilisée pour passer au mode privilégié. « # ».

Commandes	Description
`show running-config`	Affiche le fichier de configuration courant du commutateur.
`show post`	Indique si commutateur a réussi son test automatique de mise sous tension (POST)
`show vlan`	Vérifie la configuration VLAN.
`show interfaces`	Affiche la configuration et l'état d'une interface.

Configuration des commutateurs :

Vérification de la configuration par défaut du commutateur Catalyst

Par défaut : - Le nom d'hôte est Switch + Aucun mot de passe n'est défini sur les lignes de console ou de terminal virtuel + pas d'adresse IP configurée + Les ports ou interfaces du commutateur sont définis sur le mode automatique + tous les ports du commutateur se trouvent dans le VLAN 1 + Le répertoire flash comporte un fichier qui contient l'image IOS, un fichier nommé env_vars et un sous-répertoire nommé html + Le protocole STP est activé

→ Il est possible de donner une adresse IP à un commutateur pour des raisons d'administration. Il faut configurer cette adresse au niveau de l'interface virtuelle, VLAN 1.

→ Une fois que le commutateur est configuré, le répertoire flash peut également contenir un fichier config.text et une base de données VLAN.

Show running-config → vérifier la configuration actuelle

Show version → vérifier les paramètres de version IOS et du registre de configuration.

Configuration du commutateur Catalyst

Pour réinitialiser la configuration d'un commutateur :

- Supprimez toutes les informations VLAN existantes.
- Supprimez le fichier de configuration sauvegardé startup-config.
- Rechargez le commutateur

Catalyst 2950

```
Switch#delete flash:vlan.dat
Delete filename [vlan.dat]?
Delete flash:vlan.dat? [confirm]
Switch#erase startup-config
<Affichage tronqué>
Switch#reload
```

Catalyst 1900

```
Switch#delete nvram
```

Définir un nom au commutateur + Mots de passe ➔ mêmes commandes qu'un routeur.

Définition des paramètres de vitesse de port et de mode duplex :

Duplex full → pour activer le mode full duplex (à partir du mode d'interface)

Speed {débit} → pour définir la vitesse de l'interface (à partir du mode d'interface).

Configuration à partir d'un navigateur :

Les commutateurs peuvent offrir une interface Web à des fins de configuration et de gestion. Un navigateur Web peut accéder à ce service en utilisant l'adresse IP et le port 80.

Ip http server → pour activer le service Http

Ip http port 80 → pour définir le port utilisé.

Gestion de la table d'adresses MAC

Show mac-address–table → Pour afficher les adresses apprises par un commutateur.

Si aucune trame n'est interceptée avec l'adresse apprise précédemment, l'entrée correspondante est automatiquement supprimée dans la table d'adresses MAC ou expire au bout de 300 secondes.

Pour ne pas surcharger la mémoire et optimiser le fonctionnement du commutateur, les adresses apprises peuvent être supprimées de la table d'adresses MAC.

Clear mac-address-table dynamic → Pour supprimer les entrées apprises dynamiquement

Configuration d'adresses MAC statiques

```
Switch(config)#mac-address-table static <adresse-mac de l'hôte> interface
FastEthernet <numéro Ethernet> vlan <nom vlan>
```

→ Pour affecter une adresse MAC de façon permanente à une interface

Voici certaines de ces raisons pour définir une @MAC :

- L'adresse MAC ne doit jamais être supprimée automatiquement par le commutateur.
- Un serveur spécifique doit être attaché au port et l'adresse MAC est connue.
- Améliorer la sécurité.

Configuration de la sécurité des ports

→ Le nombre d'adresses MAC par port peut être limité à 1. La première adresse apprise par le commutateur de façon dynamique devient l'adresse sécurisée.

Switchport port-security {@MAC} → Configurer la sécurité d'un port (mode d'interface)

Show port security → pour vérifier l'état de sécurité du port.

Exécution d'ajouts, de déplacements et de modifications

Lorsqu'un nouveau commutateur est ajouté à un réseau, configurez les éléments suivants :

- Le nom du commutateur
- L'adresse IP du commutateur dans le VLAN d'administration
- Une passerelle par défaut
- Les mots de passe de ligne

Lorsqu'un hôte passe d'un port ou d'un commutateur à un autre, il est préférable de supprimer les configurations pouvant entraîner un comportement inattendu. La configuration requise peut ensuite être ajoutée.

Gestion du fichier de système d'exploitation du commutateur

Un administrateur devrait documenter et gérer les fichiers de configuration opérationnels des équipements réseau.

→ Le fichier de la configuration courante le plus récent devrait être sauvegardé sur un serveur ou un disque.

→ L'IOS devrait également être sauvegardée sur un serveur local.

➔ S'avérer extrêmement utile le jour où une configuration doit être restaurée.

Procédures de Gestion de fichier de l'IOS :

→ Copie de l'IOS sur un serveur TFTP :

Copy flash:c2900XL-hs-mz-112.8.10-SA6.bin tftp
+ Confirmer + indiquer l'adresse IP + Entrée

→ Copie de l'IOS à partir du serveur TFTP :

Copy tftp flash
+ Indiquer l'@IP du serveur + indiquer le nom du fichier + confirmer
Remarque : Lors du téléchargement du fichier : l'écran affiche des !!!!!!!!!!!!!!!

Procédures de Gestion de fichier de configuration :

→ Copie du fichier sur un serveur TFTP :

Copy start tftp
+ indiquer l'@IP + nom de fichier

Remarque → Pour les Catalyst 1900 **:** copy nvram tftp://192.168.1.3/alswitch-config

→ Copie de l'IOS à partir du serveur TFTP :

1- vous devez d'abord effacer le commutateur
2- Reconfigurez le commutateur avec une adresse IP VLAN 1.
3- tapez la commande copy tftp startup-config

+ indiquer l'@IP du serveur + le nom de fichier.

Procédure de récupération de mots de passe 1900/2950

→ Mettre le commutateur sous tension en maintenant enfoncé le bouton « **MODE** ». Relâchez le bouton dès la LED STAT
→ Pour initialiser le système de fichiers et terminer le chargement :

flash_init
load_helper
dir flash:

Rename flash:config**.text** flash:config**.old** → Renommer le fichier de config :

Reload → Redémarrer le système
Boot → répondre « No » pour annuler le dialogue de configuration.
Rename flash:config.old flash:config.text → Renommer à nouveau le fichier de config

Copy flash: config.text system: running-config → Copier le fichier de conf en mémoire

→ Modifier les anciens mots de passé.
→ Sauvegarder la configuration.
→ Mettez le commutateur hors tension puis sous tension et vérifiez les MDP

Mise à jour du firmware 1900/2950

Show boot → Pour afficher le nom de fichier d'image active

Si aucune image logicielle n'est définie dans le chemin d'amorçage, entrez dir flash : ou Show flash

```
ALSwitch#dir flash:
Directory of flash:/

2 -rwx 1674921 Mar 01 1993 01:28:10 c2950-c3h2s-mz.120-5.3.WC.1.bin
3 -rwx 269 Jan 01 1970 00:00:57 env_vars
4 drwx 10240 Mar 01 1993 00:21:13 html
165-rwx 965 Mar 01 1993 00:22:23 config.text

7741440 bytes total (4778496 bytes free)
```

→ Renommer le fichier IOS existant avec le même nom et avec l'extension **.old**

```
ALSwitch#rename flash:c2950-c3h2s-mz.120-5.3.WC.1.bin flash:c2950-
c3h2s-mz.120-5.3.WC.1.old
```

Dir flash → pour vérifier le nouveau nom
Switch(config)#no ip http server → Désactiver l'accès aux pages HTML du commutateur:
Switch#delete flash:html/* → Supprimer les fichiers HTML existants.

→ Extraire la nouvelle image de l'IOS et les nouveaux fichiers HTML de la mémoire flash:
Switch#archive tar /x tftp://192.168.1.3/c2950-c3h2s-mz.120- 5.3.WC.1.tar flash:

Switch(config)#ip http server → Réactivez l'accès aux pages HTML du commutateur:

→ Associez le nouveau fichier d'amorçage

Switch (config)#boot system flash:**c2950-c3h2s-mz.120-5.4.WC.1.bin**

→ Redémarrer le commutateur et vérifier et supprimer l'ancienne image :

Reload → pour redémarrer Show version → Pour vérifier l'image de démarrage.
Delete flash:c2950-c3h2s-mz.120-5.3.WC.1.old → Supprimer l'image ancienne.

Module 7

Protocole Spanning Tree (STP)

Topologies redondantes :

Redondance :

Beaucoup d'organisations se fixent un objectif de 99,99 pour cent. Ceci signifie qu'en moyenne le réseau n'est pas disponible pour une heure tous les 4000 jours, ou approximativement 5,25 minutes par an.

La fiabilité dans un réseau est obtenue par l'utilisation d'un équipement fiable et par la conception d'un réseau qui tolère les pannes et les défaillances. Le réseau est conçu pour reconverger rapidement, de sorte que la panne soit ignorée.

La tolérance aux pannes est obtenue par *la redondance*.

Topologies commutées redondantes :

Les topologies redondantes éliminent les points de panne isolés. Si une panne survient sur une route ou une unité, la route ou l'unité redondante peut prendre le relais pour les travaux en cours

Une topologie commutée redondante peut provoquer des tempêtes de broadcast, des copies de trames multiples et des problèmes d'instabilité dans la table des adresses MAC.

Tempêtes de broadcast :

Les messages multicast sont traités comme les messages broadcast par les commutateurs. Les trames de broadcast et de multicast sont diffusées sur tous les ports, à l'exception du port sur lequel elles ont été reçues.

En cas d'envoi d'un message de Broadcast (Message ARP par exemple), Les commutateurs continuent à propager le trafic de broadcast encore et encore. C'est ce que l'on appelle une tempête de broadcast.

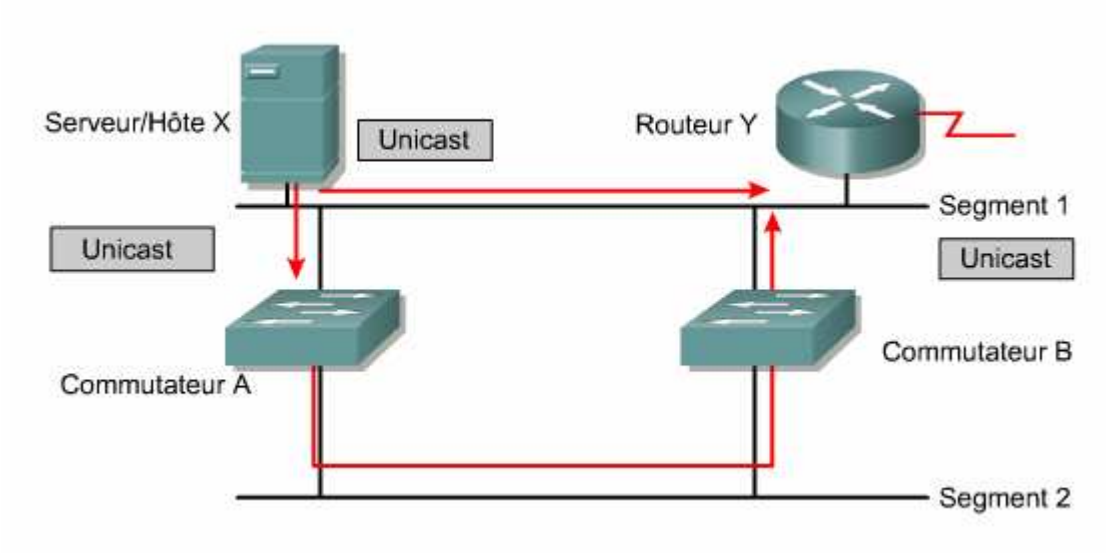
Les commutateurs et les unités d'extrémité sont tellement occupés à traiter les messages de broadcast que le trafic utilisateur ne peut pas être acheminé. Le réseau semble être en panne ou extrêmement ralenti.

Transmissions de trames multiples :

Dans un réseau commuté redondant, il est possible pour une unité d'extrémité de recevoir plusieurs trames.

Supposez que l'adresse MAC du routeur Y ait été supprimée par les deux commutateurs, à cause d'un dépassement du temps de rafraîchissement. Supposez également que l'hôte X dispose encore de l'adresse MAC du routeur Y dans sa mémoire cache ARP et

envoie une trame unicast au routeur Y. Le routeur reçoit la trame, car il figure sur le même segment que l'hôte X.

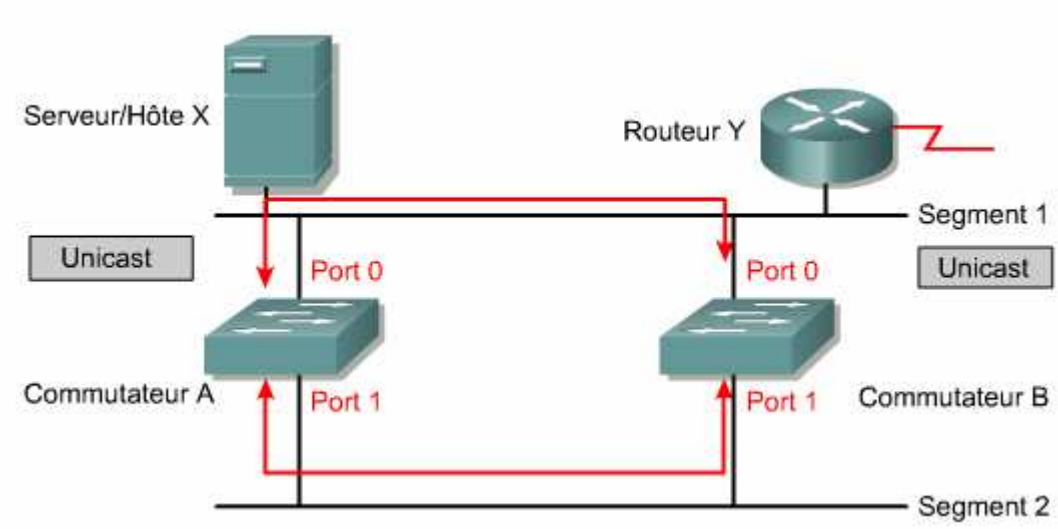


Le commutateur A ne dispose pas de l'adresse MAC du routeur Y et diffuse donc la trame sur ses ports. Le commutateur B ne connaît pas non plus le port du routeur Y. Il diffuse la trame qu'il a reçue et le routeur Y reçoit donc plusieurs copies de la même trame. Cela est le résultat d'opérations inutiles sur toutes les unités.

Instabilité de la base de données MAC :

Il est possible pour les commutateurs d'apprendre des informations erronées (MAC).

Dans cet exemple, l'adresse MAC du routeur Y ne figure pas dans la table d'adresses MAC des commutateurs.



L'hôte X envoie une trame au routeur Y. Les commutateurs A et B apprennent l'adresse MAC de l'hôte X sur le port 0.

La trame destinée au routeur Y est diffusée sur le port 1 des deux commutateurs. Les commutateurs A et B voient cette information sur le port 1 et considèrent à tort que l'adresse MAC de l'hôte X est associée au port 1. Lorsque le routeur Y envoie une trame à l'hôte X, les commutateurs A et B reçoivent également la trame et l'envoient sur le port 1. Cela est inutile, mais les commutateurs ont reçu une mauvaise information « *l'hôte X était sur le port 1* ».

Protocole Spanning Tree (STP)

Topologie redondante et Spanning Tree :

La fiabilité est accrue par la redondance. Un réseau qui est basé sur des commutateurs ou des ponts introduit des liaisons redondantes entre ces commutateurs ou ces ponts pour surmonter la panne d'une liaison unique.

L'en-tête de couche 2 ne comporte pas de durée de vie. Si une trame est envoyée dans une topologie de commutateurs en boucle de couche 2, elle peut tourner indéfiniment. La bande passante est gaspillée et le réseau est inutilisable.

Une topologie physique qui contient des boucles de pontage ou de commutation est nécessaire sur le plan de la fiabilité, mais ***un réseau commuté ne peut pas avoir de boucles***.

La solution → consiste à autoriser les boucles physiques et à créer une topologie logique sans boucle.

→ La topologie logique sans boucle créée est appelée un arbre. Cette topologie logique correspond à l'arbre de recouvrement (Spanning Tree) du réseau « car toutes les unités du réseau sont accessibles ou «recouvertes» »

L'algorithme utilisé pour créer cette topologie logique sans boucle est l'algorithme ***STP***. La convergence de cet algorithme peut prendre du temps.

Un nouvel algorithme appelé algorithme Spanning Tree «rapide» (***RSTP***) est introduit pour réduire la durée de calcul d'une topologie logique sans boucle par un réseau.

Protocole Spanning Tree :

Les ponts et les commutateurs Ethernet peuvent utiliser le protocole Spanning Tree *IEEE 802.1d* et utiliser l'algorithme «Spanning Tree» pour développer un réseau de couche 2 sans boucle utilisant le plus court chemin.

Le plus court chemin est basé sur les coûts de liaison cumulés. Les coûts de liaison sont basés sur la vitesse de la liaison.

Vitesse de liaison	Coût (spéc. IEEE révisée)	Coût (spéc. IEEE précédente)
10 Gbits/s	2	1
1 Gbits/s	4	1
100 Mbits/s	19	10
10 Mbits/s	100	100

Le protocole Spanning Tree établit un nœud racine, appelé pont racine. Il crée une topologie comportant un chemin vers chaque nœud du réseau. L'arbre obtenu part du pont racine. Les liaisons redondantes qui ne font pas partie de l'arbre du plus court chemin sont bloquées.

→ Les trames de données reçues sur les liaisons bloquées sont abandonnées.

STP requiert des unités réseau qu'elles échangent des messages pour détecter les boucles de pontage. Les liaisons qui génèrent une boucle sont bloquées.

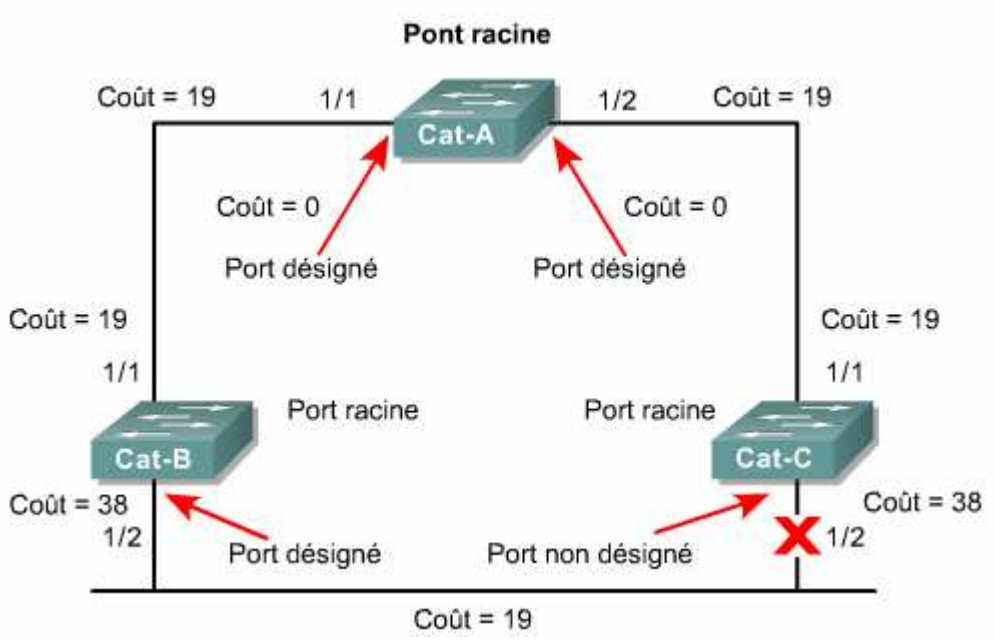
Le message qu'un commutateur envoie, permettant la formation d'une topologie logique sans boucle, est appelé unité ***BPDU*** (Bridge Protocol Data Unit).

Les unités BPDU continuent d'être reçues sur les ports bloqués. Ainsi, si une panne survient sur un chemin ou un équipement actif, un nouveau Spanning Tree peut être calculé.

Les unités BPDU contiennent suffisamment d'informations pour que tous les commutateurs puissent effectuer les opérations suivantes:

- Sélectionner un commutateur devant servir de racine pour le Spanning Tree
- Calculer le chemin le plus court entre lui-même et le commutateur racine
- Désigner un des commutateurs comme étant le plus proche de la racine, pour chaque segment LAN. Ce pont est appelé «commutateur désigné». Le commutateur désigné gère toutes les communications émises sur le réseau LAN en direction du pont racine.
- Choisir un de ses ports comme port racine pour chacun des commutateurs non racine. Il s'agit de l'interface qui fournit le meilleur chemin vers le commutateur racine.
- Sélectionner des ports appartenant au Spanning Tree: les ports désignés.

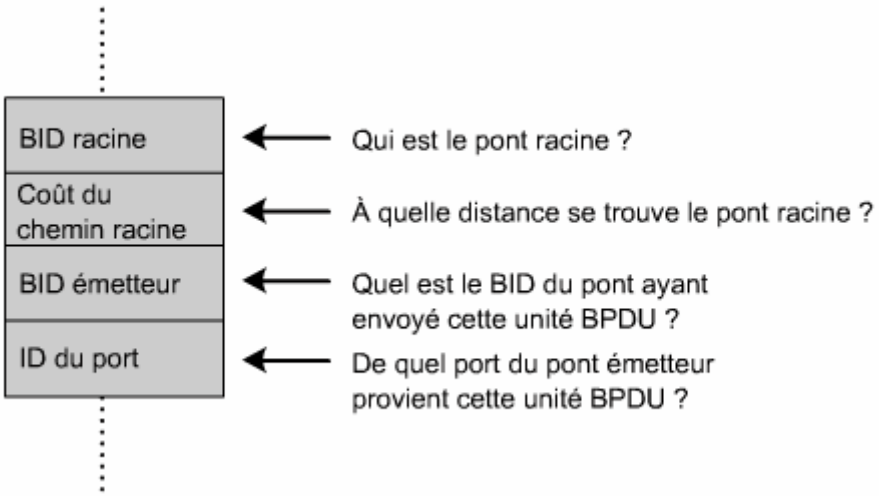
→ Les ports non désignés sont appelés les ports bloqués (B).

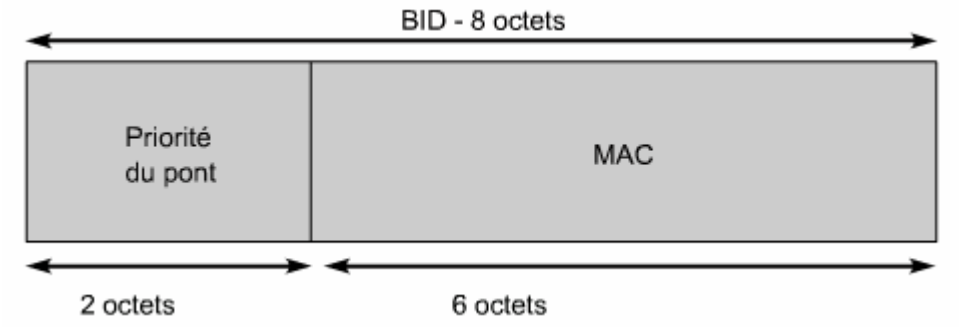


Sélection du pont racine :

Lorsqu'un commutateur est activé, l'algorithme STP est utilisé pour identifier le pont racine. Des unités BPDU sont envoyées avec l'ID de pont (***BID***). Le BID est constitué d'une priorité de pont égale à 32768 par défaut ainsi que de l'adresse MAC du commutateur.

→ Par défaut, les unités BPDU sont envoyées toutes *les deux secondes*.





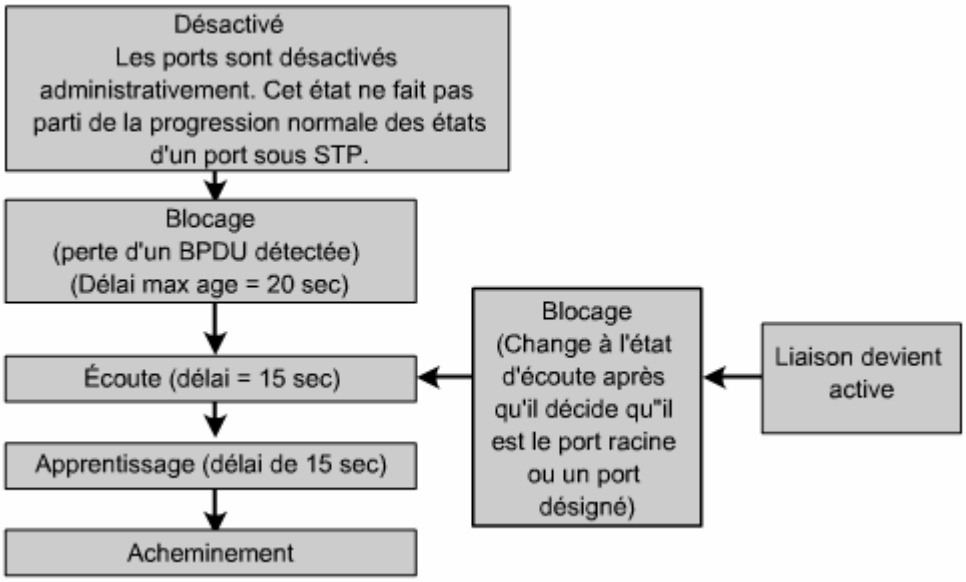
Quand un commutateur démarre, il assume qu'il est le commutateur racine et envoie les BPDU contenant l'adresse Mac du commutateur à la fois dans les champs racine et BID de l'expéditeur. Le commutateur en question transmet les BPDU contenant l'information qu'il est maintenant le pont racine ainsi que le pont désigné.

Tous les commutateurs voient les BID envoyés. Lorsqu'un commutateur reçoit une unité BPDU avec un BID de racine inférieur, il le remplace dans les unités BPDU envoyées. Tous les ponts voient cela et désignent le pont dont la valeur BID est ***la plus petite*** comme pont racine.

→ Un administrateur réseau peut avoir une influence sur cette décision s'il paramètre une valeur de priorité de commutateur inférieure à la valeur par défaut

Étapes des états des ports Spanning Tree :

Un commutateur ne doit pas immédiatement faire passer l'état d'un port d'inactif à actif, car cela peut créer des boucles de données. Chaque port d'un commutateur utilisant le protocole Spanning Tree passe par l'un des cinq états.



→ À l'état de ***blocage,*** les ports peuvent seulement recevoir des unités BPDU. Le passage à un autre état peut prendre jusqu'à 20 secondes.

→ Les ports passent de l'état de blocage à l'état d'***écoute***. Dans cet état, les commutateurs déterminent s'il existe un autre chemin vers le pont racine. Le chemin qui n'est pas le chemin le moins coûteux vers le pont racine retourne à l'état de blocage. La période d'écoute est appelée délai de transmission et dure 15 secondes. À l'état d'écoute, les ports peuvent seulement recevoir des unités BPDU.

→ Les ports passent de l'état d'écoute à l'état d'***apprentissage***. Dans cet état, les données utilisateur ne sont pas transmises, mais les adresses MAC de tout le trafic sont acquises. L'état d'apprentissage dure 15 secondes et est également appelé délai de transmission. Les unités BPDU sont toujours traitées.

→ Un port passe de l'état d'apprentissage à l'état de ***transmission***. Dans cet état, les données utilisateur sont acheminées et les adresses MAC continuent d'être acquises. Les unités BPDU sont toujours traitées.

→ Un port peut être ***désactivé***. Cet état peut survenir lorsqu'un administrateur désactive le port ou lorsque ce dernier tombe en panne.

Recalcul du Spanning Tree :

Un interréseau commuté a convergé lorsque tous les ports de commutateur et de pont sont à l'état de *transmission* ou de *blocage*.

Lorsque la topologie du réseau change, les commutateurs et les ponts recalculent le Spanning Tree, ce qui interrompt le trafic utilisateur

La convergence sur une nouvelle topologie Spanning Tree via la norme IEEE 802.1d peut prendre jusqu'à 50 secondes (20+15+15).

Protocole Spanning Tree rapide (RSTP) :

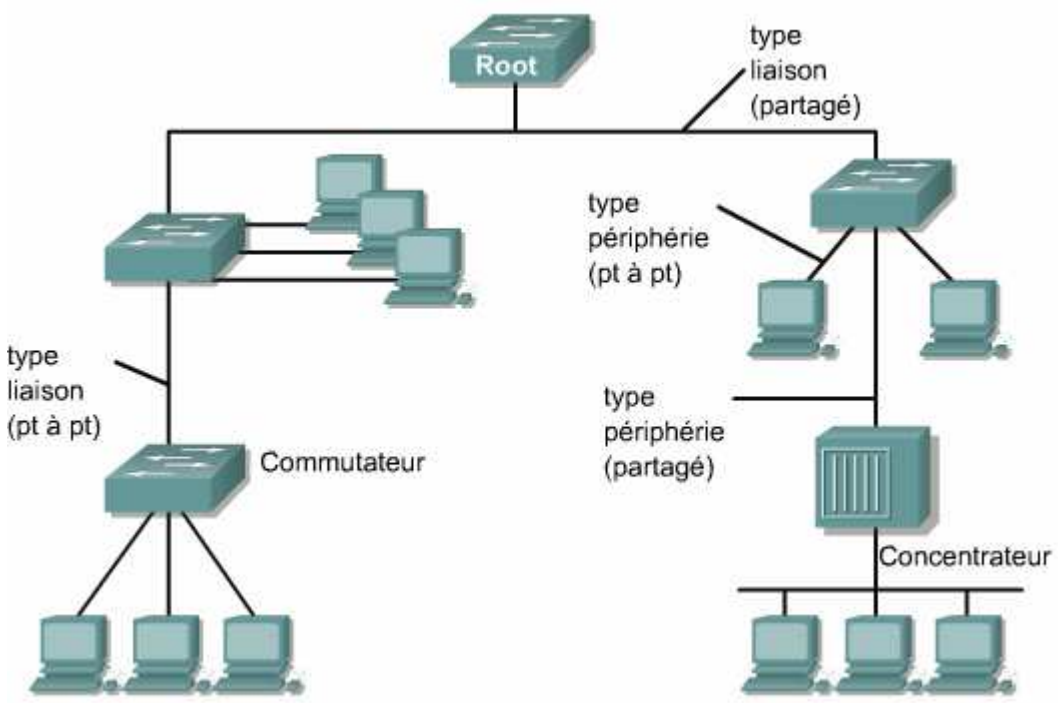
Le protocole Spanning Tree rapide est défini dans la norme LAN IEEE 802.1w. Cette norme et ce protocole introduisent les points suivants:

- Clarification des états et des rôles des ports
- Définition d'un ensemble de types de liaisons pouvant passer rapidement à l'état de transmission
- Concept autorisant les commutateurs, dans un réseau convergé, à générer leurs propres unités BPDU plutôt que de relayer celles du pont racine

L'état de «*blocage*» d'un port est appelé état d'« abandon ». Un *port d'abandon* est un «*port alternatif*».

Les liaisons sont de type *point à point*, *périphérie* et *partagé*. Ces modifications permettent l'apprentissage rapide des échecs de liaison dans les réseaux commutés.

Les liaisons point à point et les liaisons de type périphérie peuvent passer immédiatement à l'état de transmission. (15 secondes)


Root
type
liaison
(partagé)
type
périphérie
(pt à pt)
type
liaison
(pt à pt)
Commutateur
type
périphérie
(partagé)
Concentrateur

Module 8

LAN Virtuels (VLAN)

Concepts VLAN :

Introduction au LAN Virtuel :

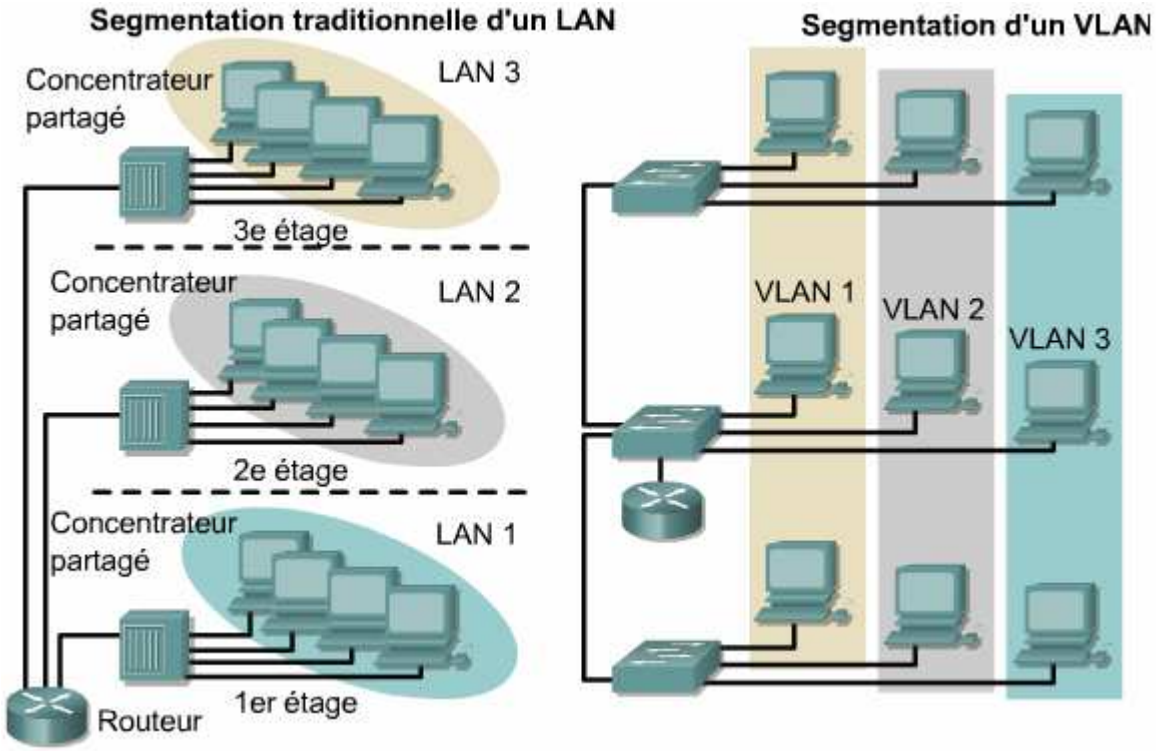
Un LAN virtuel (ou **VLAN**) est un groupe de services réseau qui ne sont pas limités à un segment physique ou à un commutateur LAN.

Les VLAN segmentent les réseaux commutés de manière logique sur la base des fonctions, des équipes de projet ou des applications de l'entreprise, quel que soit l'emplacement physique ou les connexions au réseau.

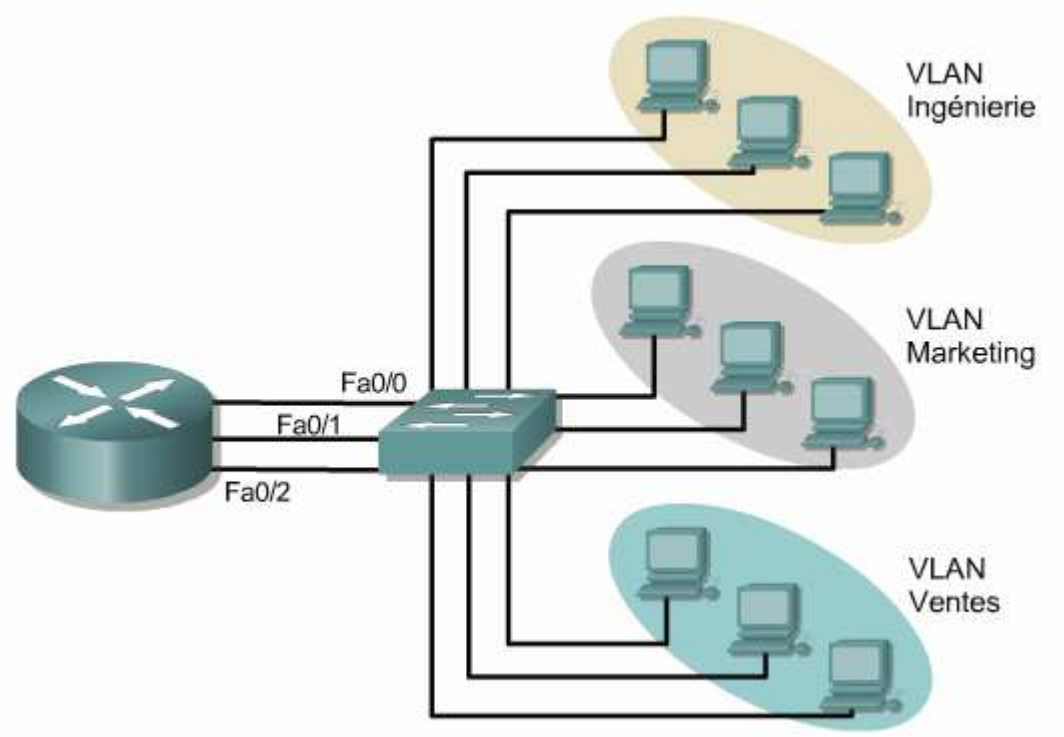
Les LAN virtuels segmentent logiquement le réseau en différents domaines de broadcast. Les commutateurs LAN utilisent des protocoles de pontage avec un groupe de ponts distinct pour chaque VLAN.

Les VLAN sont créés pour fournir des services de segmentation habituellement fournis par les routeurs physiques dans les configurations LAN. Les VLAN répondent aux problèmes d'évolutivité, de sécurité et de gestion des réseaux.

Remarque : Les commutateurs ne peuvent pas acheminer de paquets entre des VLAN par le biais de ponts.



Domaines de broadcast avec VLAN et routeurs :



Dans cet exemple, 3 VLAN sont créés avec un routeur et un commutateur. Toutefois, il y a trois domaines de broadcast séparés. Dans ce scénario, il y a *un routeur* et un commutateur, mais *trois domaines de broadcast* séparés.

Le commutateur transmet les trames aux interfaces du routeur :

- s'il s'agit de trames de broadcast;
- si elles sont destinées à l'une des adresses MAC du routeur.

Si la station de travail 1 du VLAN Ingénierie veut envoyer des trames à la station de travail 2 du VLAN Ventes, celles-ci sont envoyées à l'adresse MAC Fa0/0 du routeur. Le routage est effectué via l'adresse IP sur l'interface de routeur Fa0/0 pour le VLAN Ingénierie

La mise en œuvre de LAN virtuels sur un commutateur *implique* ce qui suit:

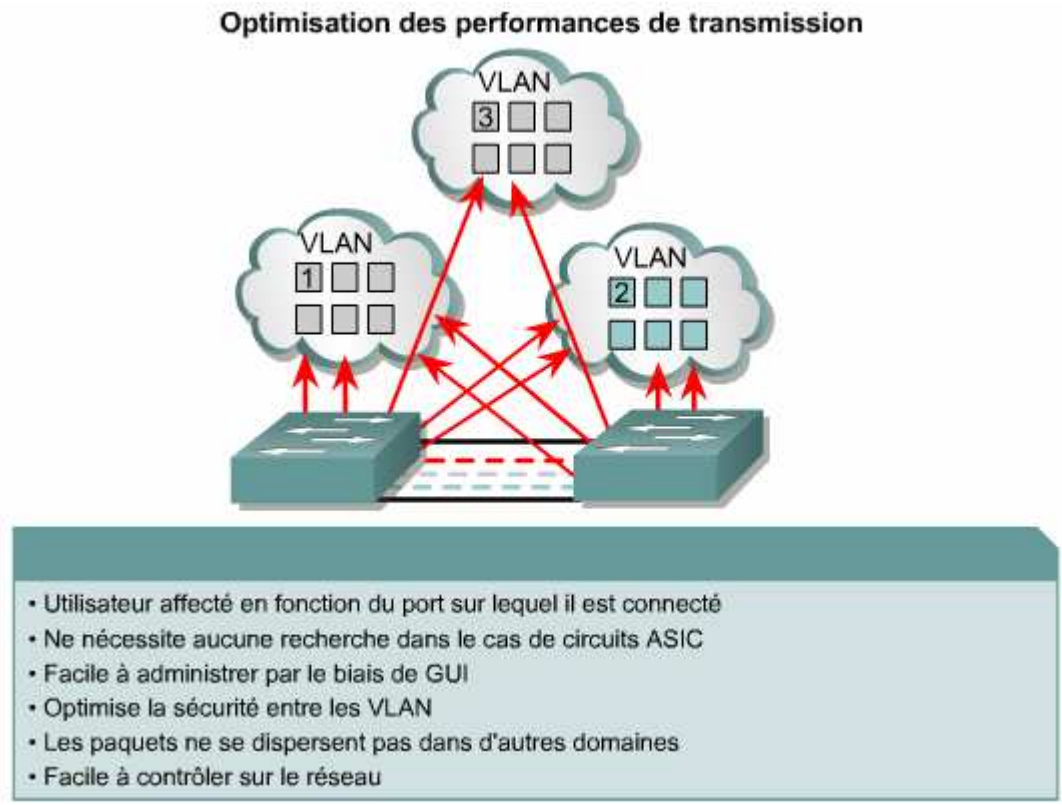
- Le commutateur doit mettre à jour une table de pontage séparée pour chaque VLAN.
- Si la trame arrive sur un port du VLAN 1, le commutateur recherche la table de pontage du VLAN 1.
- Lorsque la trame est reçue, le commutateur ajoute l'adresse source à la table de pontage si elle est inconnue.
- La destination est vérifiée, de sorte qu'une décision de transmission soit prise.
- Pour l'apprentissage et la transmission, la recherche est effectuée uniquement par rapport à la table d'adresses de ce VLAN.

Fonctionnement d'un VLAN :

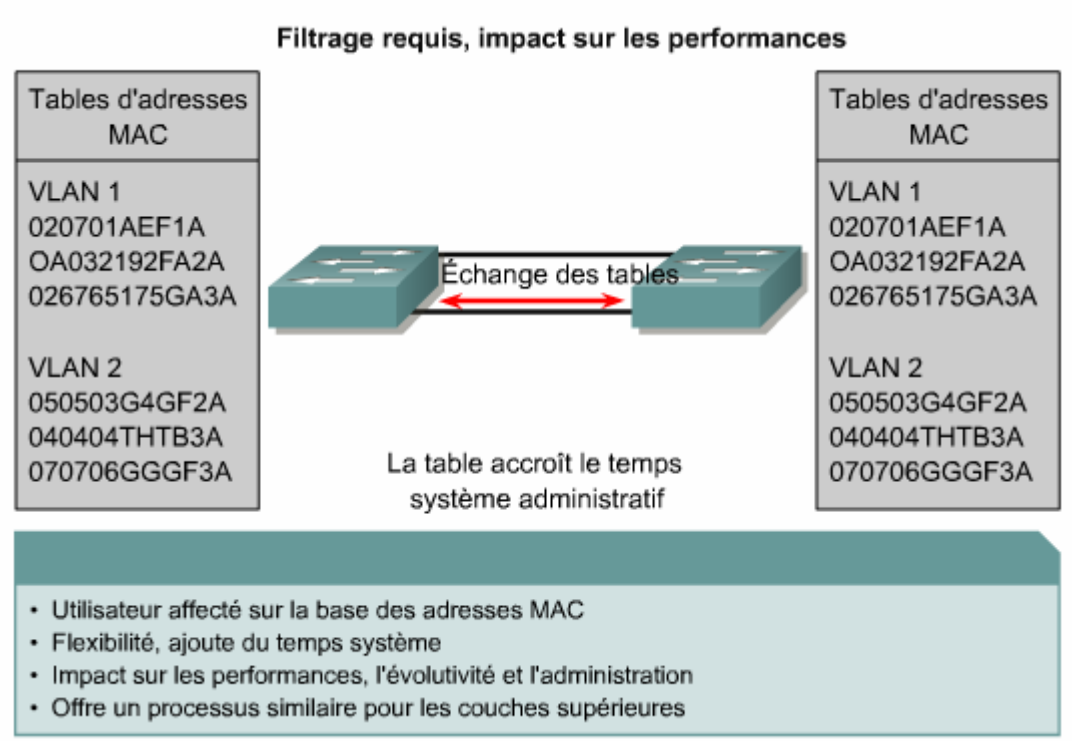
Chaque port de commutateur peut être attribué à un LAN virtuel différent. Les ports affectés au même LAN virtuel partagent les broadcasts.

Les **VLAN statiques** sont dits «*axés sur le port*». Lorsqu'un équipement accède au réseau, il adopte automatiquement le VLAN d'appartenance du port auquel il est connecté.

Les LAN virtuels offrent aux utilisateurs une bande passante plus large qu'un réseau partagé. *Le VLAN par défaut* de chaque port du commutateur est le ***VLAN de gestion***. Par défaut, le VLAN 1 est toujours le VLAN de gestion et ne peut pas être supprimé. Au moins un des ports doit être dans ce VLAN.



Les **VLAN dynamiques** sont créés par l'intermédiaire du logiciel d'administration réseau. CiscoWorks 2000 ou CiscoWorks for Switched Internetworks est utilisé pour créer des VLAN dynamiques. Les VLAN dynamiques permettent une appartenance *axée sur l'adresse MAC* de l'unité connectée au port du commutateur.



Avantages des LAN virtuels (VLAN) :

Le principal avantage des VLAN est qu'ils permettent à l'administrateur réseau d'organiser le LAN de manière logique et non physique. Cela signifie qu'un administrateur peut effectuer toutes les opérations suivantes:

- Déplacer facilement des stations de travail sur le LAN
- Ajouter facilement des stations de travail au LAN
- Modifier facilement la configuration LAN
- Contrôler facilement le trafic réseau
- Améliorer la sécurité

Types de VLAN :

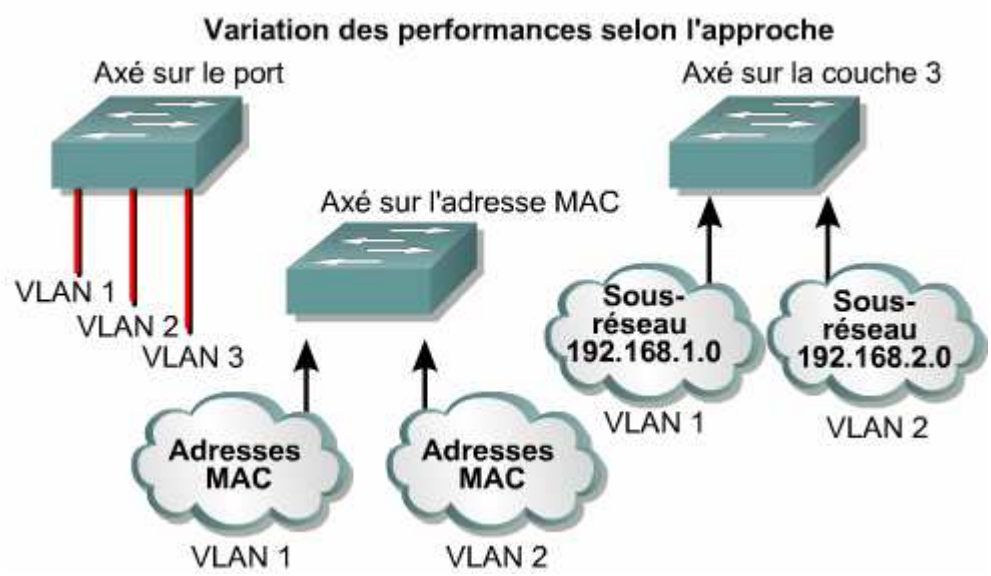
Il existe trois types d'appartenance à un VLAN :

- VLAN *axés sur le port*
- VLAN *axés sur l'adresse MAC*
- VLAN *axés sur le protocole*

Le nombre de VLAN dans un commutateur varie en fonction des facteurs suivants:

- Modèles de trafic
- Types d'application
- Besoins d'administration réseau
- Standardisation de groupes

Le système d'adressage IP est également un facteur important à prendre en compte lors de la définition de la taille du commutateur et du nombre de VLAN.



Types de VLAN	Description
Axé sur le port	• Méthode de configuration la plus courante. • Ports affectés individuellement, par groupes, par rangs ou sur au moins 2 commutateurs. • Facile à utiliser. • Souvent mis en œuvre lorsque que le protocole DHCP (Dynamic Host Control Protocol) est utilisé pour affecter des adresses IP aux hôtes du réseau.
Adresse MAC	• Rarement mis en œuvre de nos jours. • Chaque adresse doit être saisie dans le commutateur et configurée individuellement. • Utile d'après les utilisateurs. • Difficile à administrer, à dépanner et à gérer.
Axé sur le protocole	• Configuré comme les adresses MAC, mais utilise plutôt une adresse logique ou IP. • Plus utilisé en raison du protocole DHCP.

Etiquetage :

Lorsque des trames sont reçus par le commutateur à partir d'une unité de station d'extrémité reliée, un identifiant de trame unique est ajouté dans chaque en-tête. Cette information d'en-tête désigne l'appartenance à un VLAN de chaque trame. La trame est ensuite transmise aux commutateurs ou routeurs appropriés sur la base de l'ID de VLAN et de l'adresse MAC. Sur le nœud de destination, l'ID du VLAN est supprimé du trame par le commutateur contigu et transmis à l'unité connectée.

Étiquetage	Méthode	Médias	Description
ISL (Inter-Switch Link)	Fast Ethernet	L'en-tête ISL encapsule la trame LAN et contient un champ ID de VLAN.	La trame est allongée.
802.IQ	Fast Ethernet	Protocole VLAN Ethernet défini par l'IEEE.	L'en-tête est modifié.
Émulation de LAN (LANE)	ATM	Aucune étiquetage	Une connexion virtuelle implique un ID de VLAN.

Remarque : Les commutateurs Catalyst 2950 ne prennent pas en charge l'agrégation ISL.

Configuration VLAN :

Notions de base sur les VLAN

Une adresse réseau de couche 3 unique doit être affectée à chaque VLAN. Cela permet aux routeurs de commuter les paquets entre les VLAN.

Les VLAN peuvent être créés sous forme de réseaux de bout en bout ou exister à l'intérieur de frontières géographiques.

Les VLAN de bout en bout permettent de regrouper les équipements en fonction de l'utilisation des ressources. Cela inclut des paramètres comme l'utilisation du serveur, les équipes de projet et les services. Le but des VLAN de bout-en bout est de maintenir 80 % du trafic sur le VLAN local.

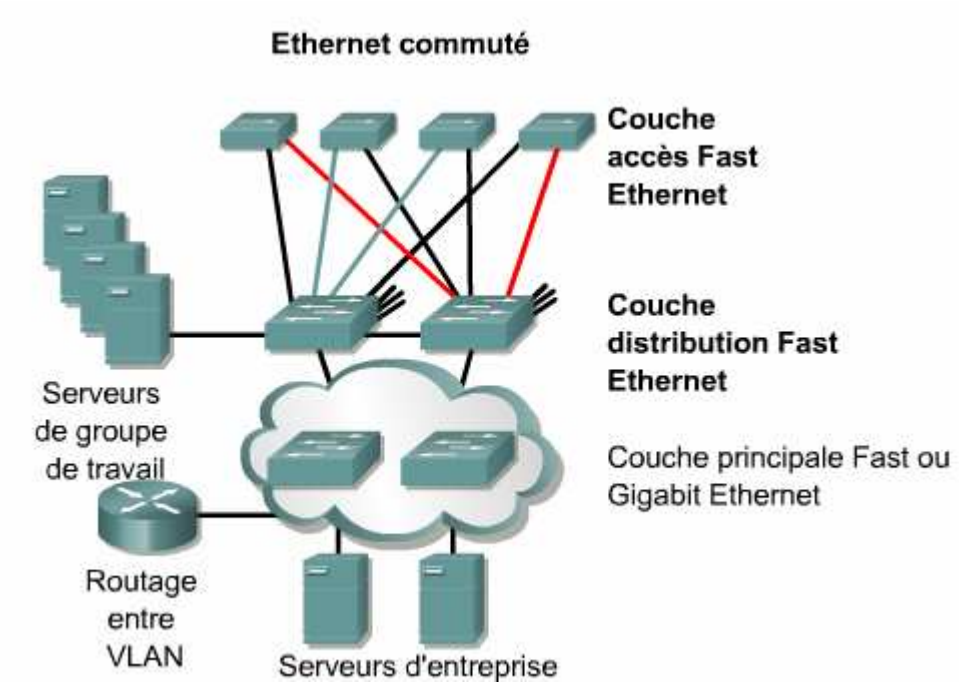
Un réseau VLAN de bout en bout a les caractéristiques suivantes :

- Les utilisateurs sont regroupés en VLAN qui dépendent de leur groupe de travail ou de leur fonction, mais pas de leur localisation physique.
- Tous les utilisateurs d'un VLAN doivent avoir les mêmes modèles de flux de trafic *80/20*.
- Lorsqu'un utilisateur se déplace sur le campus, son appartenance à un VLAN ne doit pas changer.
- Chaque VLAN est caractérisé par un ensemble commun de besoins de sécurité pour tous les membres.

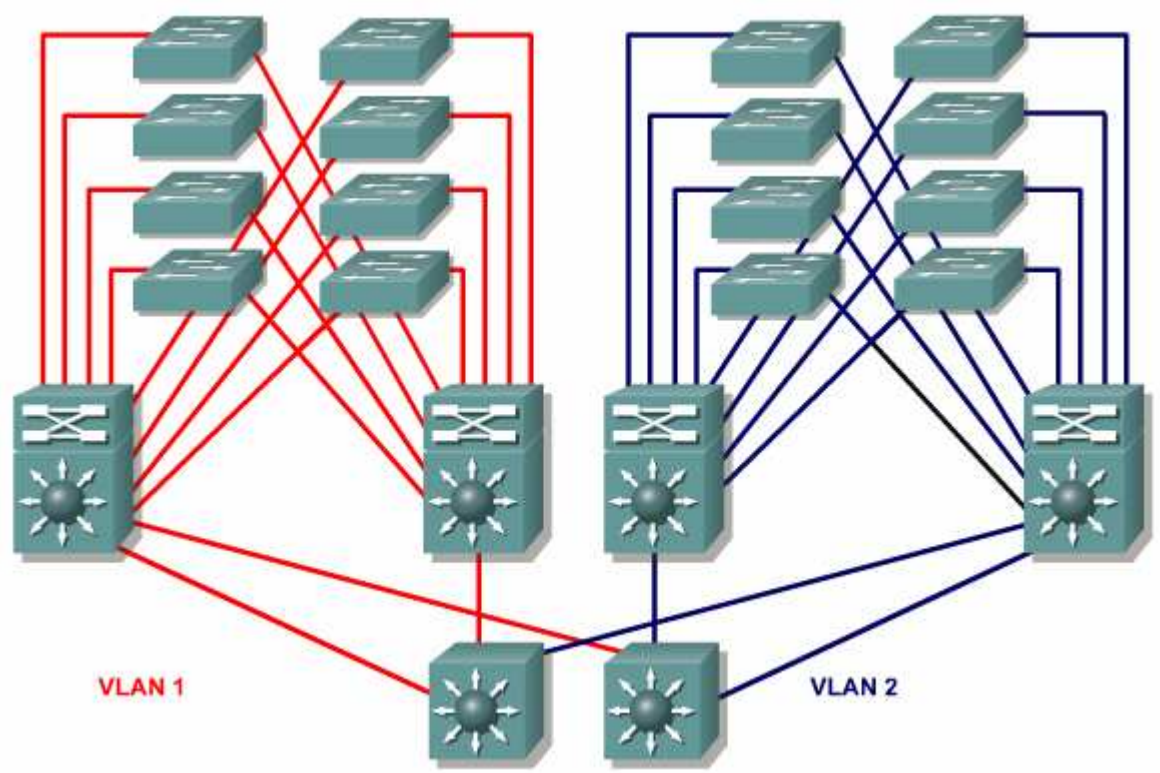
À partir de la couche accès, des ports de commutation sont fournis pour chaque utilisateur. En raison du déplacement des personnes, chaque commutateur devient finalement un membre de tous les VLAN.

Il a été tenté de garder les utilisateurs dans le même VLAN que leur serveur afin d'optimiser les performances de commutation de couche 2 et de centraliser le trafic.

Un routeur de couche principale est utilisé pour acheminer les paquets entre les sous-réseaux. Le réseau est conçu sur la base de modèles de flux de trafic de telle sorte que *80* % du trafic soit contenu au sein d'un VLAN. Les *20* % restants traversent le routeur jusqu'aux serveurs d'entreprise et jusqu'aux réseaux Internet et WAN.



VLAN géographiques



Dans cette structure, la nouvelle règle *20/80* est très fréquemment appliquée. 80 % du trafic est effectué à distance pour l'utilisateur contre 20 % en local. Bien que cette topologie implique pour l'utilisateur de traverser une unité de couche 3 afin d'atteindre 80 % des ressources, cette configuration permet au réseau de fournir une méthode cohérente et déterministe d'accès aux ressources.

Configuration de VLAN statiques

Les lignes directrices suivantes doivent être suivies lors de la configuration de VLAN sur des commutateurs Cisco 29xx:

- Le nombre maximum de VLAN dépend du commutateur.
- Le VLAN 1 est le VLAN Ethernet par défaut.
- Des annonces CDP et VTP sont envoyées sur le VLAN 1.
- L'adresse IP de Catalyst est associée par défaut au domaine de broadcast du VLAN 1.
- Le commutateur doit être en mode serveur VTP pour créer, ajouter ou supprimer des VLAN.

Créer un VLAN :

```
Switch#Vlan database
Switch(vlan)#Vlan {ID_vlan}
Switch(vlan)#Exit
```

Affecter une interface à un VLAN :

```
Switch(config-if)#Switchport mode access vlan
Switch(config-if)#Switchport access vlan {ID_vlan}
```

Vérification de la configuration VLAN

```
Show vlan
Show vlan brief
Show vlan id {ID_vlan}
```

```
SydneySwitch#show vlan

VLAN Name                Status    Ports
---- ------------------- ------- -------------------------------

VLAN Name                Status    Ports
---- ------------------- ------- -------------------------------
1    default             active    Fa0/1, Fa0/2, Fa0/4
2    VLAN2               active    Fa0/3, Fa0/5, Fa0/6, Fa0/7
3    VLAN3               active    Fa0/8, Fa0/9, Fa0/10, Fa0/11,
                                   Fa0/12
1002 fddi-default        active
1003 token-ring-default  active
1004 fddinet-default     active
1005 trnet-default       active
```

Enregistrement de la configuration VLAN

Il est souvent utile de garder une copie de la configuration VLAN sous forme de fichier texte à des fins de sauvegarde ou d'audit.

Suppression de VLAN

Pour enlever une interface d'un VLAN :

```
Switch(config-if)# No switchport access vlan {ID_vlan}
```

Pour enlever un VLAN entièrement d'un commutateur, entrez les commandes:

```
Switch(vlan)#No vlan {ID}
```

Remarque : Lorsqu'un VLAN est supprimé, tous les ports qui lui sont affectés deviennent inactifs. Toutefois, ces ports restent associés au VLAN supprimé jusqu'à ce qu'ils soient affectés à un nouveau VLAN.

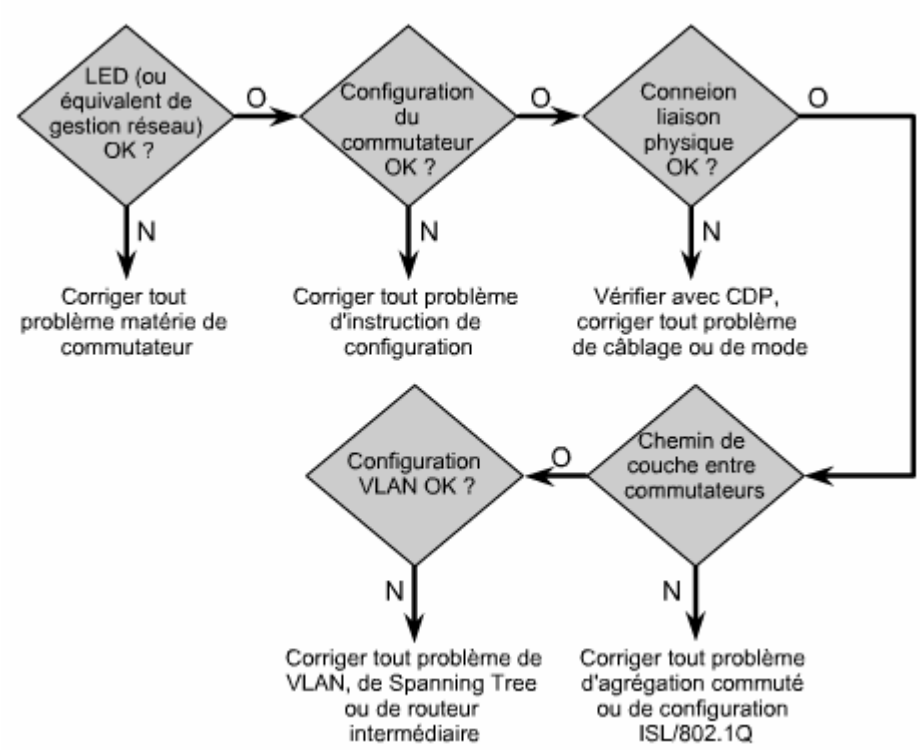
Dépannage des VLAN :

Processus de dépannage d'un VLAN

Les étapes suivantes peuvent aider à identifier un problème sur un réseau commuté:

1. Vérifiez les indications physiques, telles que l'état des LED.
2. Commencez par une configuration simple sur un commutateur, puis élargissez.
3. Vérifiez la liaison de couche 1.
4. Vérifiez la liaison de couche 2.
5. Dépannez les VLAN qui s'étendent sur plusieurs commutateurs.

Rappel : le pont racine détermine les valeurs des messages de configuration, dans les unités BPDU, puis définit les compteurs pour les autres ponts. D'autres ponts désignés déterminent le chemin le plus court vers le pont racine et sont chargés d'annoncer les unités BPDU aux autres ponts par l'intermédiaire de ports désignés.



Comment éviter les tempêtes de broadcast ?

Le contrôle des tempêtes est configuré globalement pour le commutateur, mais est exécuté au niveau de chaque port. Le contrôle des tempêtes est désactivé par défaut.

La prévention contre les tempêtes de broadcast par le paramétrage de valeurs de seuil élevées ou faibles permet d'éliminer l'excès de trafic MAC broadcast, multicast ou unicast.

Les problèmes *STP* incluent les tempêtes de broadcast, les boucles, ainsi que les unités BPDU et les paquets abandonnés.

Remarque : Un port physique sur un routeur ou un commutateur peut faire partie de plusieurs Spanning Tree s'il s'agit d'une agrégation.

Dépannage des VLAN

→ Vérifiez qu'une adresse IP est configurée sur l'interface Fast Ethernet.
→ Des adresses IP sont configurées sur chaque sous-interface d'une connexion VLAN.
→ Vérifiez que la configuration duplex sur le routeur correspond à celle du port ou de l'interface approprié(e) sur le commutateur.

Show vlan → permet d'afficher les informations VLAN du commutateur.
Show spanning-tree → indique la topologie Spanning Tree connue du routeur.

```
MDF_Switch#show spanning-tree

Spanning tree 1 is executing the IEEE compatible
Spanning Tree protocol
  Bridge Identifier has priority 32768, address
  0006.28ab.5e00 Configured hello time 2, max age
  20, forward delay 15 We are the root of the
  spanning tree Topology change flag not set,
  detected flag not set, changes 18
  Times: hold1, topology change 0, notification 2
         hello 2, max age 20, forward delay 15
  Timers:hello 0, topology change 0, notification 0
```

Compteur	Objectif principal	Par défaut
Délai Hello	Délai entre les envois d'unités BPDU de configuration par le pont racine	2 Secs
Délai de transmission	Durée des états d'écoute et d'apprentissage	15 Secs
max_age	Durée de stockage des unités BPDU	20 Secs

La ligne suivante des informations affichées indique que le routeur est la racine du STP :

```
We are the root of the spanning tree.
```

Debug sw-vlan packets → affiche des informations générales sur les paquets VLAN reçus mais non configurés pour prendre en charge le routeur.

Scénario de dépannage d'un VLAN

Problème : Aucun lien multi-VLAN ne peut être établi entre un commutateur et un routeur.

1. Vérifiez que le port est connecté et qu'il ne reçoit pas d'erreurs de couche physique, d'alignement ou de FCS. **show interface** sur le commutateur.
2. Vérifiez que le mode duplex et la vitesse sont correctement paramétrés entre le commutateur et le routeur. **show interface status** sur le commutateur ou **show interfaces** sur le routeur.
3. Configurez l'interface de routeur physique avec une sous-interface pour chaque VLAN qui achemine le trafic. Pour vérifier **show interfaces**. Vérifiez également pour chaque sous-interface du routeur que le type d'encapsulation, le numéro de VLAN, l'adresse IP et le masque de sous-réseau sont correctement configurés. **show interfaces** ou **show running-config** de l'IOS.
4. Vérifiez que le routeur exécute une version de l'IOS qui prend en charge l'agrégation. Pour cela, utilisez la commande **show version**

Module 9

Protocole VTP (VLAN Trunking Protocol)

Agrégation (Trunking) :

Historique de l'agrégation :

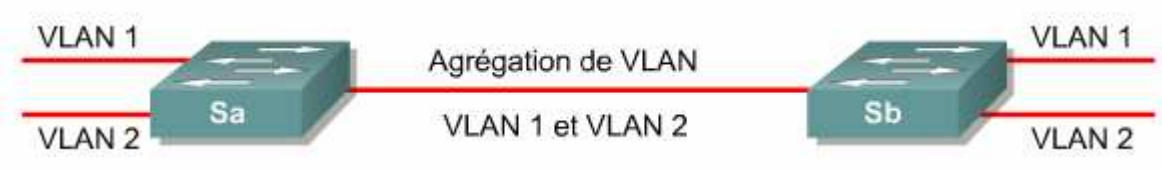
L'apparition de l'agrégation (trunking) remonte aux origines des technologies radio et de téléphonie. Dans les technologies radio, une agrégation est une ligne de communication simple qui transporte plusieurs canaux de signaux radio.

Le même principe d'agrégation est appliqué aux technologies de commutation de réseaux. ***Une agrégation*** est une connexion physique et logique entre deux commutateurs par lesquels le trafic réseau est acheminé.

Concepts d'agrégation :

Une agrégation de VLAN est une liaison point-à-point physique ou logique qui prend en charge plusieurs VLAN.

→ L'objectif d'une agrégation de VLAN est d'économiser des ports lors de la création d'une liaison entre deux unités contenant des VLAN



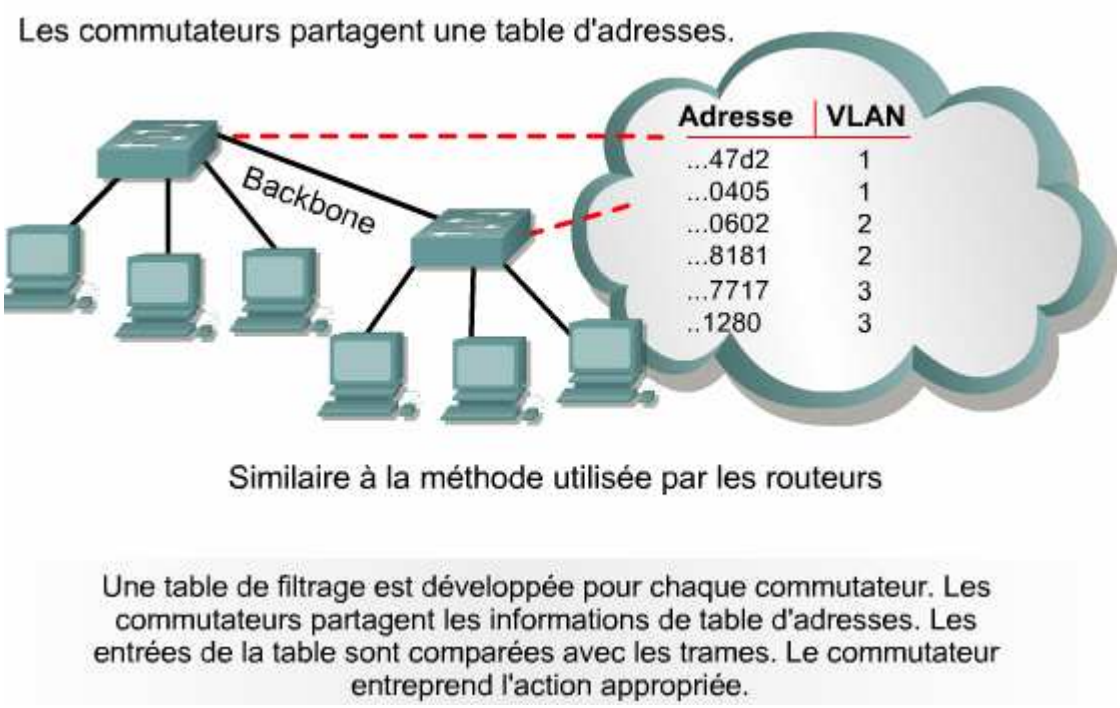
Fonctionnement d'une agrégation de VLAN :

Des ***protocoles d'agrégation*** ont été développés pour gérer efficacement le transfert de trames de différents VLAN sur une liaison physique unique.

Actuellement, il existe deux types de mécanismes d'agrégation: *le filtrage des trames* et *l'étiquetage des trames*. L'étiquetage des trames a été adopté par l'IEEE comme mécanisme d'agrégation standard.

Les systèmes d'étiquetage les plus courants pour les segments Ethernet :

- **ISL** (Inter-Switch Link) – Protocole propriétaire de Cisco
- **802.1Q** – Norme IEEE plus particulièrement traitée dans cette section



Une table de filtrage est développée pour chaque commutateur. Les commutateurs partagent les informations de table d'adresses. Les entrées de la table sont comparées avec les trames. Le commutateur entreprend l'action appropriée.

VLAN et agrégation :

L'utilisation de l'étiquetage de trames comme mécanisme d'agrégation standard, par opposition au filtrage de trames, fournit une solution plus évolutive au déploiement VLAN.

Cette méthode place un identificateur unique dans l'en-tête de chaque trame au moment où celle-ci est acheminée dans le backbone du réseau. L'identificateur est interprété et examiné par chaque commutateur avant tout broadcast ou transmission à d'autres commutateurs, routeurs ou équipements de station d'extrémité. Lorsque la trame quitte le backbone du réseau, le commutateur retire l'identificateur avant de transmettre la trame à la station d'extrémité cible.

Méthode d'identification	Encapsulation	Étiquetage (insertion dans la trame)	Médias
802.1Q	Non	Oui	Ethernet
ISL	Oui	Non	Ethernet
802.10	Non	Non	FDDI
LANE	Non	Non	ATM

Mise en œuvre de l'agrégation de VLAN :

Pour créer ou configurer une agrégation de VLAN sur un commutateur à base de commandes Cisco IOS, configurez d'abord le port en mode d'agrégation de VLAN puis spécifiez l'encapsulation d'agrégation

```
Router#show interface fast 0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Disabled
Access Mode VLAN: 0 ((Inactive))
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: ALL
Trunking VLANs Active: 1,2
Pruning VLANs Enabled: 2-1001
```

VTP (Virtual Trunking Protocol) :

Historique du protocole VTP

Lors d'une modification, une seule affectation de VLAN incorrecte peut engendrer deux types de problème:

- Connexions croisées entre VLAN en raison de l'incohérence des configurations Vlan
- Mauvaise configuration de VLAN sur des environnements à médias mixtes comme Ethernet et FDDI.

Avec ***VTP***, la configuration VLAN est systématiquement mise à jour sur un domaine administratif commun. En outre, VTP facilite la gestion et la surveillance des réseaux VLAN.

Avantages du VTP :

- Cohérence de la configuration des VLAN sur l'ensemble du réseau
- Les VLAN sont réunis en une agrégation sur des médias mixtes. Par exemple, un VLAN Ethernet est associé à un VLAN ATM LANE ou FDDI haut débit.
- Surveillance et suivi précis des VLAN
- Transmission dynamique d'informations sur les VLAN ajoutés à l'ensemble du réseau
- Configuration " plug-and-play " lors de l'ajout de nouveaux VLAN

Concepts VTP :

VTP est un protocole de messagerie qui utilise les trames d'agrégation de *couche 2* pour gérer l'ajout, la suppression et l'attribution de nouveaux noms aux VLAN sur un domaine unique. De plus, VTP autorise les changements centralisés qui sont communiqués à tous les autres commutateurs du réseau.

Les messages VTP sont encapsulés dans des trames de protocole Cisco ISL (Inter-Switch Link) ou IEEE 802.1Q, puis transmis sur des liens multi-VLAN aux autres unités.

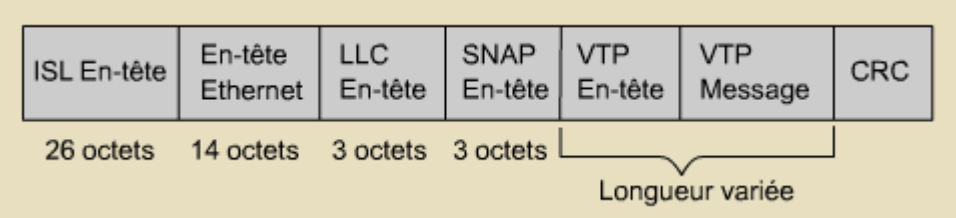
Fonctionnement de VTP :

Un domaine VTP est composé d'un ou de plusieurs équipements interconnectés qui partagent le même nom de domaine VTP.

→ Un commutateur ne peut appartenir qu'à un seul domaine VTP.

L'en-tête VTP varie en fonction du type de message VTP, mais quatre éléments sont généralement inclus dans tous les messages VTP :

- Version du protocole VTP: version 1 ou 2
- Type de message VTP: indique l'un des quatre types
- Longueur du nom de domaine de gestion: indique la taille du nom qui suit
- Nom du domaine de gestion: nom configuré pour le domaine de gestion



→ Les commutateurs VTP exécutent l'un des *trois modes* suivants :

- Serveur
- Client
- Transparent

Les ***serveurs VTP*** peuvent créer, modifier et supprimer un VLAN et des paramètres de configuration VLAN pour l'ensemble du domaine. Les serveurs VTP enregistrent les informations de configuration VLAN dans la mémoire NVRAM du commutateur. Les serveurs VTP envoient des messages VTP par tous les ports multi-VLAN.

Les ***clients VTP*** ne peuvent pas créer, modifier ou supprimer des informations VLAN. Ce mode est utile pour les commutateurs qui manquent de mémoire pour stocker de grandes tables d'informations VLAN. Le seul rôle des clients VTP est de traiter les modifications VLAN et d'envoyer des messages VTP par tous les ports multi-VLAN

Les commutateurs en ***mode transparent VTP*** transmettent des annonces VTP mais ignorent les informations contenues dans le message. Un commutateur transparent ne modifie pas sa base de données lors de la réception de mises à jour et il n'envoie pas de mises à jour indiquant une modification apportée à son état VLAN. Excepté pour la transmission d'annonces VTP, le protocole VTP est désactivé sur un commutateur transparent.

Caractéristique	Serveur	Client	Transparent
Fournir des messages VTP	Oui	Oui	Non
Être à l'écoute des messages VTP	Yes	Oui	Non
Créer des VLAN	Oui	Non	Oui*
Se souvenir des VLAN	Oui	Non	Oui*

*Significatif sur un plan local uniquement

Chaque fois qu'un commutateur reçoit une mise à jour avec un numéro de révision de configuration supérieur, il remplace les informations stockées par les nouvelles informations envoyées dans la mise à jour VTP.

Remarque : Par défaut, les domaines de gestion sont définis sur un mode non sécurisé, ce qui signifie que les commutateurs interagissent sans utiliser de mot de passe. L'ajout d'un mot de passe fait passer automatiquement le domaine de gestion en mode sécurisé.

Mise en œuvre de VTP :

Les trames d'annonce sont envoyées à une adresse multicast, de sorte que toutes les unités voisines puissent recevoir les trames.

Toutes les unités du même domaine de gestion acquièrent des informations sur les nouveaux VLAN configurés dans l'unité émettrice.

Les annonces sur les VLAN par défaut sont basées sur les types de média. Les ports utilisateur ne doivent pas être configurés en tant qu'agrégations VTP.

Chaque annonce commence par le *numéro de révision de configuration* 0. Lorsque des modifications sont apportées, le numéro de révision de la configuration augmente de un (n + 1). Le numéro de révision continue d'augmenter jusqu'au numéro 2 147 483 648. Une fois ce numéro atteint, le compteur est remis à zéro.

Remarque : Pour redéfinir le numéro de révision de configuration sur zéro, le commutateur doit être redémarré.

Il existe deux ***types d'annonce*** VTP:

- les demandes émanant de clients qui réclament des informations au démarrage.
- les réponses des serveurs.

Il existe trois ***types de message*** VTP:

- les demandes d'annonce;
- les annonces de type résumé;
- les annonces de type sous-ensemble.

Avec les demandes d'annonce, les clients demandent des informations VLAN et le serveur répond avec des annonces de type résumé ou sous-ensemble.

Par défaut, les commutateurs serveur et client Catalyst émettent des annonces de type résumé toutes les *5 minutes*. Les serveurs indiquent aux commutateurs voisins ce qu'ils pensent être le numéro de révision VTP actuel. Si les noms de domaine correspondent, le serveur ou client récepteur compare le numéro de révision de la configuration. Si le numéro de révision dans l'annonce est supérieur à celui qui figure actuellement dans le commutateur récepteur, ce dernier émet une demande d'annonce pour les nouvelles informations VLAN.

Les annonces de type sous-ensemble contiennent des informations détaillées sur les VLAN (Identité de l'unité de mise à jour + type de version VTP + nom du domaine + les champs associés + le numéro de révision de la configuration + la clé envoyée avec VTP « MD5 »).

Les événements suivants peuvent créer ces annonces:

- Création ou suppression d'un VLAN
- Arrêt ou activation d'un VLAN
- Modification du nom d'un VLAN
- Modification de la MTU d'un VLAN

Configuration de VTP :

Etapes de configuration VTP de base :

- Détermination du numéro de version
- Sélection du domaine
- Sélection du mode VTP
- Protection du domaine par un mot de passe

→ Deux versions différentes de VTP sont disponibles: la version 1 et la version 2. Les deux versions ne peuvent pas fonctionner ensemble.

- La fonction la plus couramment utilisée (VTP v2) est la prise en charge VLAN Token Ring.
- VTP version 1 est la valeur par défaut.

Vtp v2-mode → pour utiliser la version 2 de VTP (mode VLAN)
Vtp domain {nom entre 1 et 32} → pour créer un domaine vtp (mode VLAN)

→ Le mot de passe peut comporter entre 8 et 64 caractères.

Remarque : Pour ajouter un client VTP à un domaine VTP existant, vérifiez toujours que son numéro de révision de configuration VTP est inférieur à celui des autres commutateurs du domaine VTP.

Show vtp status → Vérifier le numéro de révision de configuration VTP

```
MDF_Switch#show vtp status
VTP Version                          :2
Configuration Revision               :0
Maximum VLANs supported locally      :64
Number of existing VLANs             :7
VTP Operation Mode                   :Server
VTP Domain Name                      :cisco
VTP Pruning Mode                     :Disabled
VTP V2 Mode                          :Disabled
VTP Traps Generation                 :Disabled
MDS digest                           :0x30 0x50
Configuration last modified by 10.1.1.252 a local
updater ID 138.25.13.121 on interface found)
MDF_Switch#exit
```

Etapes d'ajout d'un commutateur à un domaine VTP existant :

- Effacement de la configuration
- Effacement du fichier VTP
- Arrêt puis redémarrage du commutateur
- Configuration du mode et du domaine VTP
- Protection du domaine par un mot de passe

Vtp {client | server | transparent} → Définir le mode VTP (mode VLAN)

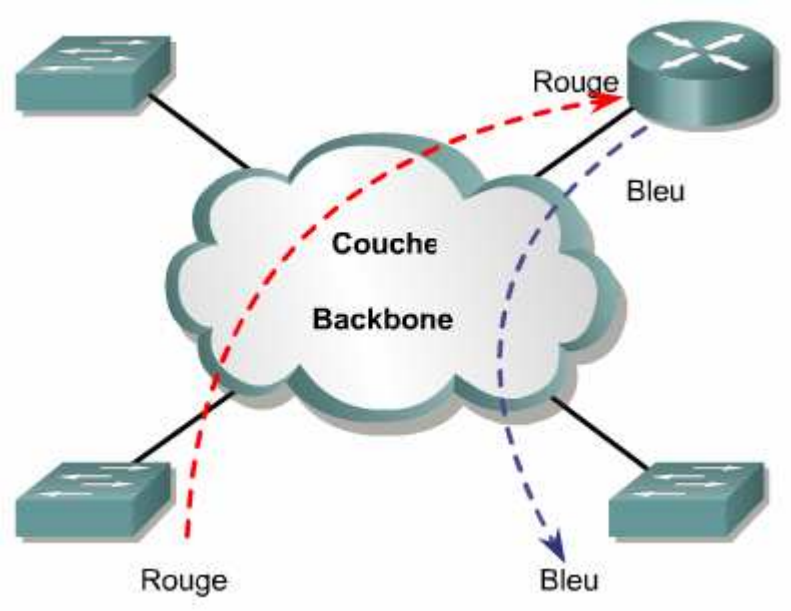
Show vtp counters → pour afficher des statistiques sur les annonces envoyées et reçues.

```
MDF_Switch#show vtp counters
VTP statistics:
Summary advertisments received           :4
Subset advertisments received            :1
Request advertisments received           :2
Summary advertisments transmitted        :7
Subset advertisments transmitted         :4
Request advertisments transmitted        :1
Number of config revision errors         :0
Number of config digest errors           :0
Number of V1 summary errors              :0


VTP pruning statistics:

Trunk               Join Transmitted Join Received
----------------- ----------------- ------------
```

Vue d'ensemble du routage entre VLAN :

Introduction au routage entre VLAN

Lorsqu'un hôte d'un domaine de broadcast souhaite communiquer avec un hôte d'un autre domaine de broadcast, *un routeur doit être utilisé*.



Lorsqu'un VLAN s'étend sur plusieurs équipements, une agrégation est utilisée pour interconnecter les équipements. L'agrégation transporte le trafic de plusieurs VLAN.

Commutateurs, routeurs, serveurs, gestion		
	Établissement de l'appartenance	Commutateurs - Détermination de l'appartenance
	Communication sur la matrice	Agrégation - Échange VLAN commun
	Communications entre VLAN	Routage multiprotocole Échange entre VLAN
	Communication sur les serveurs	Serveurs-Multi - Communication entre VLAN
	Administration centralisée	Gestion - Sécurité, contrôle, administration

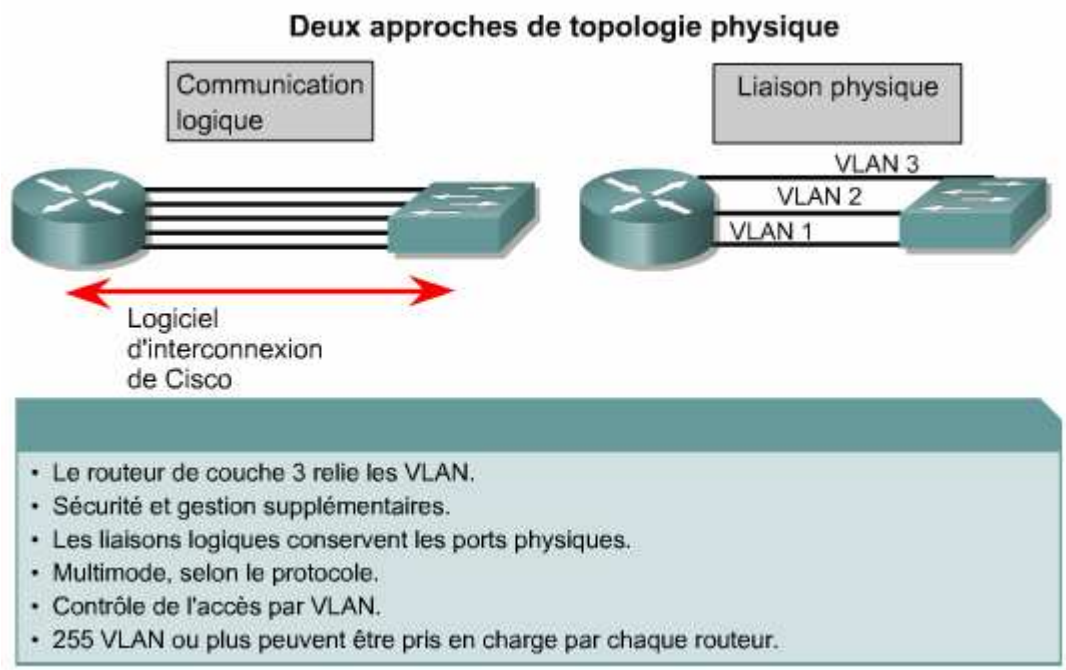
Communication inter-VLAN : Problématique et solutions

Les deux problèmes les plus courants dans un environnement à plusieurs VLAN sont :

- La nécessité pour les unités d'utilisateur final d'atteindre des hôtes non locaux
- La nécessité pour les hôtes de VLAN différents de communiquer entre eux

Les ***premières configurations de VLAN*** reposaient sur des routeurs externes connectés à des commutateurs compatibles VLAN. Avec cette approche, les routeurs traditionnels sont connectés via une ou plusieurs liaisons à un réseau commuté.

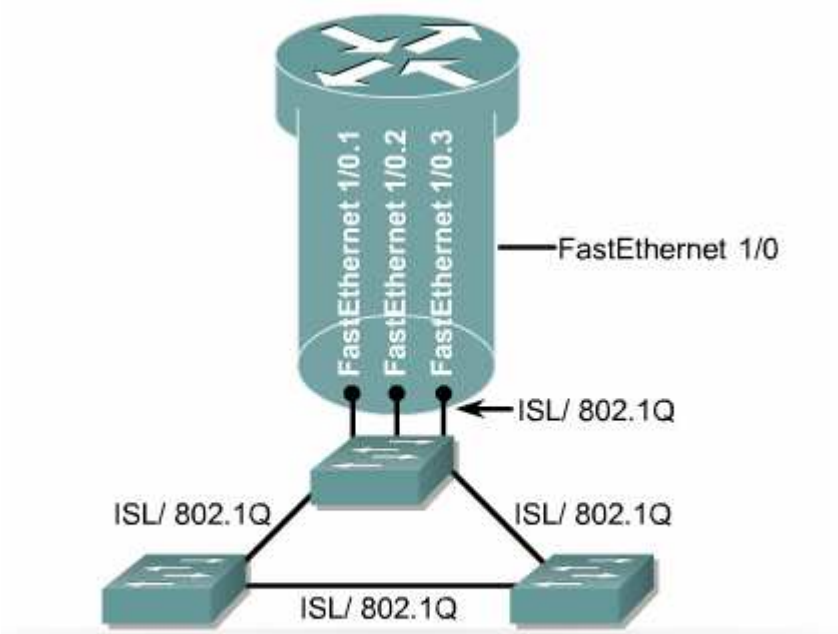
Les configurations «***router-on-a-stick***» utilisent un seul lien multi-VLAN qui connecte le routeur au reste du réseau du campus. Le trafic entre les VLAN doit traverser le backbone de couche 2 pour atteindre le routeur par lequel il peut atteindre les différents VLAN.



Interfaces physiques et logiques :

Le protocole Cisco ISL ainsi que la norme IEEE multifournisseur 802.1Q sont utilisés pour réunir des VLAN en une agrégation sur des liaisons Fast Ethernet.

Les réseaux contenant de nombreux VLAN doivent utiliser le mécanisme d'agrégation de VLAN pour affecter plusieurs VLAN à une interface de routeur unique.



Une interface ISL ou 802.1Q du routeur se connecte à un port multi-VLAN du commutateur.

Le routeur peut prendre en charge de nombreuses interfaces logiques sur des liaisons physiques individuelles. Par exemple, l'interface Fast Ethernet FastEthernet 1/0 pourrait supporter trois interfaces virtuelles s'appelant FastEthernet 1/0.1, 1/0.2 et 1/0.3.

Séparation des interfaces physiques en sous-interfaces

Une ***sous-interface*** est une interface logique au sein d'une interface physique, telle que l'interface Fast Ethernet d'un routeur.

Chaque sous-interface prend en charge un VLAN et dispose d'une adresse IP affectée. Pour que plusieurs unités d'un même VLAN communiquent, les adresses IP de toutes les sous-interfaces maillées doivent être *sur le même réseau ou sous-réseau*.

Configuration du routage entre des VLAN

Pour que le routage entre VLAN fonctionne correctement, tous les routeurs et commutateurs concernés doivent accepter la même encapsulation.

Pour définir des sous-interfaces sur une interface physique, effectuez les tâches suivantes:

- Identifiez l'interface.
- Définissez l'encapsulation VLAN.
- Attribuez une adresse IP à l'interface.

Pour identifier une interface logique :

`Router(config)#interface fastethernet {numéro-port}.{numéro-sous-interface}`

Par exemple : interface fastethernet 0/0.1

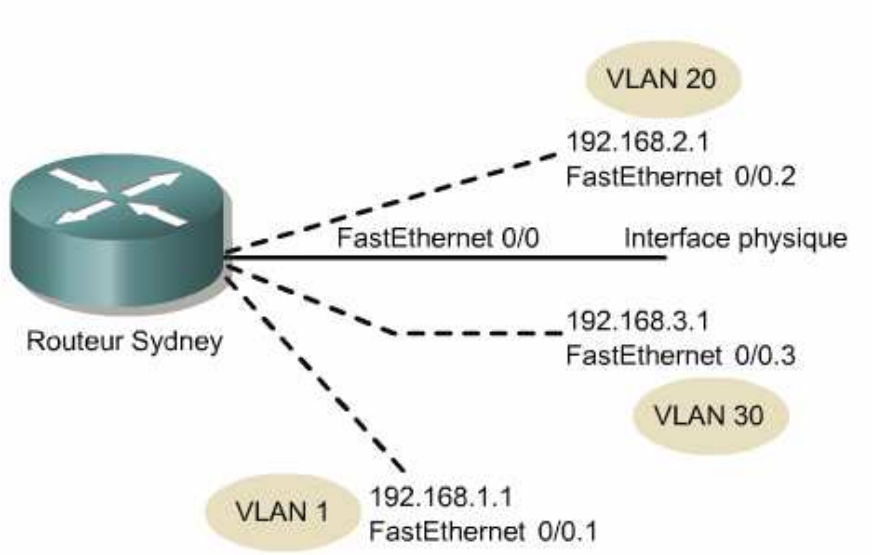
Pour définir l'encapsulation VLAN :

`Router(config-subif)#encapsulation dot1Q {D_VLAN}`

Pour affecter l'adresse IP à la sous-interface :

`Router(config-subif)#ip address {adresse-ip} {masque-sous-réseau}`

Exemple :




```
Sydney(config)#interface FastEthernet 0/0.1
Sydney(config-subif)#description Administration VLAN1
Sydney(config-subif)#encapsulation dot1q 1
Sydney(config-subif)#ip address 192.168.1.1
255.255.255.0
Sydney(config)#interface FastEthernet 0/0.2
Sydney(config-subif)#description Comptabilite VLAN 20
Sydney(config-subif)#encapsulation dot1q 20
Sydney(config-subif)#ip address 192.168.2.1
255.255.255.0
Sydney(config)#interface FastEthernet 0/0.3
Sydney(config-subif)#description Ventes VLAN 30
Sydney(config-subif)#encapsulation dot1q 30
Sydney(config-subif)#ip address 192.168.3.1
255.255.255.0
```