Modèle OSI

Le but de l'OSI(ISO) est de créer un modèle idéal ou chaque couche effectue une tâche définie et dépend des services de la couche inférieure. Chaque couche donc fournit ses propres services à la couche supérieure.

```
OSI
Application (7)
Présentation (6)
Session (5)
Transport(4)
Réseau(3)
Liaison des données(2)
Physique(1)
```

Couche physique (1) La couche physique transfère les bits à travers un canal de communication. Ses bits encodés peuvent être en numérique mais aussi en analogique. Cette couche transmet les bits venant de la couche de données à l'interface physique et inversément. (support physique : Paire torsadée, coaxial, FO...)
Couche liaison de données (2) La couche liaison de données prend les données de la couche physique et fournit ses services à la couche réseau. Les bits reçus sont assemblés en trames1. (liaison possible : Ethernet, Frame Relay, X.25, PPP...)
Couche réseau (3) La couche réseau gère les connexions entre les noeuds du réseau. Un routeur, par exemple, travaille au minimum dans cette couche. Dans le modèle TCP/IP, la fonction de la couche réseau est assurée par IP2. (IPv4 ou IPv6)
Couche transport (4) La couche de transport offre des services supplémentaires par rapport à la couche réseau. Cette couche garantit l'intégrité des données. Son travail consiste à relier un sous-réseau non fiable à un réseau plus fiable. Dans le modèle TCP/IP, la fonction de la couche transport est assurée par TCP3 et par le protocole UDP4.
Couche session (5) La couche de session gère les connexions entre les applications coopérantes. Le modèle TCP/IP ne possède pas de couche de session car TCP fournit une grande partie des fonctionnalités de session. Mais le service NFS, par exemple, peut utiliser le protocole RPC qui lui, est dans la couche de session. Beaucoup d'applications TCP n'utilisent pas les services de la couche session.
Couche présentation (6) La couche de présentation gère la représentation des données. Pour représenter les données, il existe ASCII, EBCDIC... Un langage commun doit être utilisé pour une bonne compréhension entre les différents noeuds du réseau. Par exemple, il existe le langage ASN.1 pour la représentation des données en SNMP (XDR pour NFS, Base64 pour SMTP...). Plusieurs applications TCP n'utilisent pas les services de cette couche.
Couche d'application (7) La couche d'application fournit les protocoles et les fonctions nécessaires pour les applications clients. Il existe un nombre important de services fournis par la couche d'application. Dans le modèle TCP/IP, on peut citer comme services : FTP,SMTP,POP3,HTTP5.

Le protocole IP de la couche Réseau

Le rôle fondamental de la couche réseau (niveau 3 du modèle OSI) est de déterminer la *route* que doivent emprunter les paquets. Cette fonction de recherche de chemin nécessite une identification de tous les hôtes connectés au réseau. De la même façon que l'on repère l'adresse postale d'un bâtiment à partir de la ville, la rue et un numéro dans cette rue, on identifie un hôte réseau par une *adresse* qui englobe les mêmes informations.
Le modèle TCP/IP utilise un système particulier d'adressage qui porte le nom de la couche réseau de ce modèle : *l'adressage IP*. Le but de cet article est de présenter le fonctionnement de cet adressage dans sa version la plus utilisée IPv4.
De façon très académique, on débute avec le format des adresses IP. On définit ensuite les classes d'adresses IP, le premier mode de découpage de l'espace d'adressage. Comme ce mode de découpage ne convenait pas du tout au développement de l'Internet, on passe en revue la chronologie des améliorations apportées depuis 1980 : les sous-réseaux ou *subnetting*, la traduction d'adresses ou *Native Address Translation* (NAT) et enfin le routage inter-domaine sans classe.

3. Le format des adresses IP

Les adresses IP sont composées de 4 octets. Par convention, on note ces adresses sous forme de 4 nombres décimaux de 0 à 255 séparés par des points.
L'originalité de ce format d'adressage réside dans l'association de l'identification du réseau avec l'identification de l'hôte.

• La partie réseau est commune à l'ensemble des hôtes d'un même réseau,
• La partie hôte est unique à l'intérieur d'un même réseau.

Prenons un exemple d'adresse IP pour en identifier les différentes parties :

Tableau 1. Exemple : adresse IP 192.168.1.1

Adresse complète 192.168.__1.__1
Masque de réseau 255.255.255.__0
Partie réseau 192.168.__1.___
Partie hôte ___.___.___.__1
Adresse Réseau 192.168.__1.__0
Adresse de diffusion 192.168.__1.255

Le masque de réseau

Le masque de réseau sert à séparer les parties réseau et hôte d'une adresse. On retrouve l'adresse du réseau en effectuant un ET logique bit à bit entre une adresse complète et le masque de réseau.

L'adresse de diffusion

Chaque réseau possède une adresse particulière dite de *diffusion*. Tous les paquets avec cette adresse de destination sont traités par tous les hôtes du réseau local. Certaines informations telles que les annonces de service ou les messages d'alerte sont utiles à l'ensemble des hôtes du réseau.

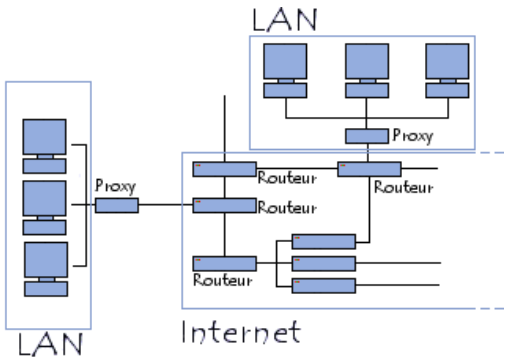
Un routeur est un élément intermédiaire dans un réseau informatique assurant le routage des paquets entre réseaux indépendants. Ce routage est réalisé selon un ensemble de règles formant la table de routage.
C'est un équipement de couche 3 par rapport au modèle OSI. Il ne doit pas être confondu avec un commutateur (couche 2) !

Un **routeur** est un équipement d'interconnexion de réseaux informatiques permettant d'assurer le routage des paquets entre deux réseaux ou plus afin de déterminer le chemin qu'un paquet de données va emprunter.

Lorsqu'un utilisateur appelle une URL, le client Web (navigateur) interroge leserveur de noms, qui lui indique en retour l'adresse IP de la machine visée.

Son poste de travail envoie la requête au routeur le plus proche, c'est-à-dire à la passerelle par défaut du réseau sur lequel il se trouve. Ce routeur va ainsi déterminer la prochaine machine à laquelle les données vont être acheminées de manière à ce que le chemin choisi soit le meilleur.

Pour y parvenir, les routeurs tiennent à jour des tables de routage, véritable cartographie des itinéraires à suivre en fonction de l'adresse visée. Il existe de nombreux protocoles dédiés à cette tâche.



En plus de leur fonction de routage, les routeurs permettent de manipuler les données circulant sous forme de datagrammes afin d'assurer le passage d'un type de réseau à un autre. Or, dans la mesure

où les réseaux n'ont pas les mêmes capacités en terme de taille de paquets de données, les routeurs sont chargés de fragmenter les paquets de données pour permettre leur libre circulation.

Fonctionnalités de la couche réseau

-Le routage: déterminer le chemin (/ la route) des paquets à travers le réseau

• Sous réseaux hétérogènes:

- Segmentation peut être nécessaire

• Le contrôle de congestion: éviter les embouteillages

- **Les routeurs sont connectés à plusieurs réseaux**
- **Le routage :**
  - **comment décider de la route à prendre?**
  - **c'est à dire dans un routeur (ou un host) comment répondre à la question : quel est le prochain routeur à qui envoyer le paquet**
- **Deux fonctions distinctes**
  - **Décider au vue d 'informations locales (table de routage) et de l 'adresse destination du paquet à qui envoyer le paquet et sur quel réseau le reémettre**
  - **Construire la table de routage**

- **Service orienté connexion**
  - **Une connexion de niveau réseau s'appelle circuit virtuel.**
  - **Le chemin associé au circuit virtuel dans le réseau est alloué à l'établissement de la connexion. La décision de routage n'est prise qu'au cours de la phase d'établissement de la connexion.**
  - **Tous les paquets circulant sur le même circuit virtuel empruntent le même chemin.**
  - **Exemple : protocole ATM (Asynchronous Transfer Mode)**

- **Service sans connexion (Unité de donnée: *datagramme*)**
  - **Chaque paquet est envoyé indépendamment des autres et routé séparément.**
  - **Des paquets successifs peuvent donc suivre des routes différentes et il peut y avoir alors déséquencement des paquets**
  - **Exemple: le protocole IP (Internet Protocol)**

Fonctions WAN d'un Routeur

Un routeur détermine, à partir de l'adresse logique contenue dans le paquet, le meilleur chemin pour atteindre le destinataire

Un routeur connecte des réseaux utilisant des technologies différentes au niveau de la couche liaison

Fonction LAN d'un Routeur (1)

Segmente un réseau LAN en augmentant le nombre de domaines de broadcast mais en diminuant leur taille

- Domaine de collisions : liè à Ethernet ; zone réseau dans laquelle voyagent des trames qui peuvent rentrer en collision avec d'autres

- Domaine de broadcast : Ensemble de tous les dispositifs qui recevront des trames de diffusion provenant de n'importe quel des dispositifs faisant partie de cet ensemble

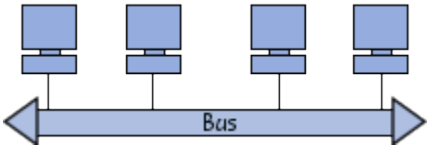
Protocoles routés / de routage

- Les protocoles routés (routables) sont des protocoles prenant en charge les fonctions de la couche réseau (`IP, IPX, AppleTalk`)

- Les protocoles de routages fournissent les mécanismes de partage et de gestion des tables de routage entre les routeurs (`RIP, IGRP, EIGRP, OSPF`)

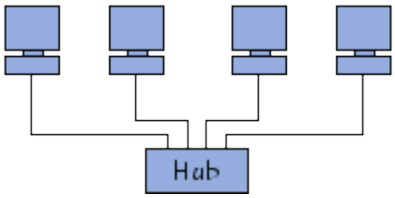
La **topologie logique**, par opposition à la topologie physique, représente la façon dont les données transitent dans les lignes de communication. Les topologies logiques les plus courantes sont Ethernet, Token Ring et FDDI.

Une **topologie en bus** est l'organisation la plus simple d'un réseau. En effet, dans une topologie en bus tous les ordinateurs sont reliés à une même ligne de transmission par l'intermédiaire de câble, généralement coaxial. Le mot « bus » désigne la ligne physique qui relie les machines du réseau.



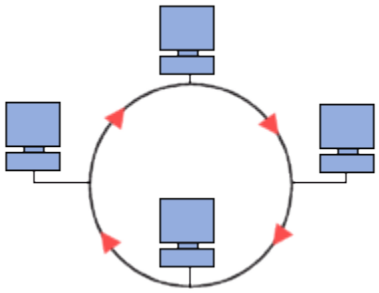
Cette topologie a pour avantage d'être facile à mettre en oeuvre et de posséder un fonctionnement simple. En revanche, elle est extrêmement vulnérable étant donné que si l'une des connexions est défectueuse, l'ensemble du réseau en est affecté.

Dans une **topologie en étoile**, les ordinateurs du réseau sont reliés à un système matériel central appelé **concentrateur** (en anglais *hub*, littéralement*moyen de roue*). Il s'agit d'une boîte comprenant un certain nombre de jonctions auxquelles il est possible de raccorder les câbles réseau en provenance des ordinateurs. Celui-ci a pour rôle d'assurer la communication entre les différentes jonctions.

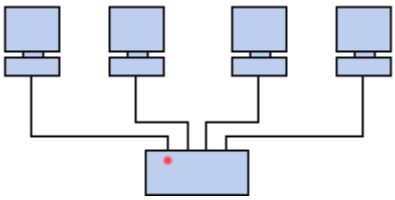


Contrairement aux réseaux construits sur une topologie en bus, les réseaux suivant une topologie en étoile sont beaucoup moins vulnérables car une des connexions peut être débranchée sans paralyser le reste du réseau. Le point névralgique de ce réseau est le concentrateur, car sans lui plus aucune communication entre les ordinateurs du réseau n'est possible.
En revanche, un réseau à topologie en étoile est plus onéreux qu'un réseau à topologie en bus car un matériel supplémentaire est nécessaire (le hub).

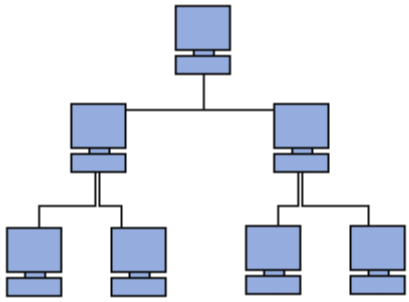
Dans un réseau possédant une **topologie en anneau**, les ordinateurs sont situés sur une boucle et communiquent chacun à leur tour.



En réalité, dans une topologie anneau, les ordinateurs ne sont pas reliés en boucle, mais sont reliés à un **répartiteur** (appelé *MAU*, *Multistation Access Unit*) qui va gérer la communication entre les ordinateurs qui lui sont reliés en impartissant à chacun d'entre-eux un temps de parole.



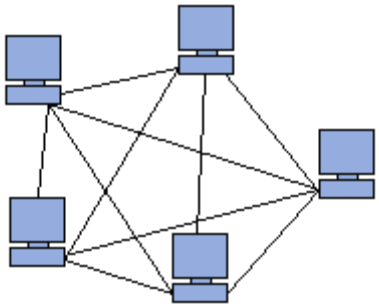
Les deux principales topologies logiques utilisant cette topologie physique sont Token ring (anneau à jeton) et FDDI.
Aussi connu sous le nom de *topologie hiérarchique*, le réseau est divisé en niveaux. Le sommet, le haut niveau, est connectée à plusieurs nœuds de niveau inférieur, dans la hiérarchie. Ces nœuds peuvent être eux-mêmes connectés à plusieurs nœuds de niveau inférieur. Le tout dessine alors un arbre, ou une arborescence.



Topologie maillée

Une topologie maillée, est une évolution de la topologie en étoile, elle correspond à plusieurs liaisons point à point. Une unité réseau peut avoir (1,N) connexions point à point vers plusieurs autres unités. Chaque terminal est relié à tous les autres. L'inconvénient est le nombre de liaisons nécessaires qui devient très élevé.
Cette topologie se rencontre dans les grands réseaux de distribution (Exemple : Internet). L'information peut parcourir le réseau suivant des itinéraires divers, sous le contrôle de puissants superviseurs de réseau, ou grâce à des méthodes de routage réparties.
L'armée utilise également cette topologie, ainsi, en cas de rupture d'un lien, l'information peut quand même être acheminée.

Elle existe aussi dans le cas de couverture Wi-Fi. On parle alors bien souvent de topologie mesh mais ne concerne que les routeurs WiFi.



Topologie du bus
Avantages de la topologie de bus
Il est facile à manipuler et à mettre en œuvre.
Il est plus adapté pour les petits réseaux.

Inconvénients de la topologie de bus
La longueur du câble est limitée. Cela limite le nombre de stations qui peuvent être connectés.
Cette topologie de réseau peut effectuer ainsi que pour un nombre limité de nœuds.

Topologie en anneau
Avantage de Topologie en anneau
Les données étant transmises entre deux noeuds passe par tous les noeuds intermédiaires. Un serveur central n'est pas requis pour la gestion de cette topologie.

Inconvénients de la Topologie en anneau
La défaillance d'un seul nœud du réseau peut entraîner l'ensemble du réseau à l'échec.
Le mouvement ou les modifications apportées aux noeuds de réseau affecte le rendement de l'ensemble du réseau.

Topologie maillée
Avantage de topologie maillée
L'agencement des noeuds de réseau est telle qu'il est possible de transmettre des données d'un noeud à plusieurs autres noeuds dans le même temps.

Inconvénient de topologie maillée
L'arrangement où chaque nœud du réseau est connecté à tous les autres nœuds du réseau, la plupart des connexions ne servent à rien majeure. Cela conduit à la redondance de la plupart des connexions réseau.

Topologie en étoile
Avantages de la topologie en étoile
En raison de son caractère centralisé, la topologie offre une simplicité de fonctionnement.
Il réalise également un isolement de chaque périphérique du réseau.

Inconvénient de topologie en étoile
Le fonctionnement du réseau dépend du fonctionnement de la plate-forme centrale. Par conséquent, l'échec de la plate-forme centrale conduit à l'échec de l'ensemble du réseau.

Le routeur, est un équipement réseau permettant d'acheminer les données d'un réseau à un autre. Le routeur possède une table contenant les chemins que doivent emprunter les données pour arriver à destination. Représenter vous un routeur comme un bureau de poste où le courrier représente les données. Vous déposez une enveloppe dans la boite aux lettres, le bureau de poste regarde la destination et détermine comment acheminer le courrier à destination puis à un autre bureau de poste. Un routeur réalise la même chose mais avec des données informatiques. Il reçoit une donnée, regarde la destination, il étudie sa table de routage pour chercher le meilleur chemin, et transmet les données à un autre routeur.

Un routeur est un système à microprocesseur qui possède les composants suivants :
· RAM/DRAM : contient le système d'exploitation décompressé ; stocke les tables de routage, le cache ARP, etc. ; stocke également la configuration active (running-config) du routeur. Le contenu de la RAM est perdu lorsque le routeur est éteint ou redémarré.
· NVRAM (non volatile RAM) : mémoire flash qui contient un fichier de configuration de démarrage/sauvegarde (startup-config). Le contenu n'est pas perdu lorsque l'équipement est éteint ou redémarré.
· Flash : emplacement par défaut de l'image du système d'exploitation (IOS file).
· ROM : contient le programme de diagnostic de démarrage (power-on self test, POST) ainsi que le bootstrap ou boot-loader. Contient aussi une version minimal du système d'exploitation en cas d'effacement de la flash.
· Interfaces : connexions réseau à travers lesquelle les paquets entrent et sortent du routeur ; peut être sur la carte mère ou sur un module séparé.
· Port console : fournit un accès au routeur, à travers une ligne RS-232 (ligne série asynchrone), pour la gestion et la configuration.

Unité centrale (CPU) L'unité centrale, ou le microprocesseur, est responsable de l'exécution

du système d'exploitation (chez Cisco, c'est IOS) du routeur. Le système d'exploitation prend aussi bien en charge les protocoles que l'interface de commande via une session telnet. La puissance du microprocesseur est directement liée à la puissance de traitement du routeur .
Mémoire Flash La flash représente une sorte de ROM effaçable et programmable. Sur beaucoup de routeurs, la flash est utilisé pour maintenir une image d'un ou plusieurs systèmes d'exploitation. Il est tout à fait possible de maintenir plusieurs images sur la même flash (suivant la taille de la flash). La mémoire flash est pratique car elle permet une mise à jour de la mémoire sans changer des "chips". La flash peut se présenter sous forme de barette mais aussi sous forme de carte.

ROM La ROM contient le code pour réaliser les diagnostics de démarrage (POST : Power On Self Test). En plus, la ROM permet le démarrage et le chargement du système d'exploitation contenu sur la flash. On change rarement la ROM. Si on la change, on doit souvent enlever des "chips" et les remplacer.

RAM La RAM est utilisé par le système d'exploitation pour maintenir les informations durant le fonctionnement. Elle peut contenir les tampons (buffer), les tables de routage, la table ARP, la configuration mémoire et un nombre important d'autres choses. Et comme c'est de la RAM, lors de la coupure de l'alimentation, elle est effacée.

NVRAM (RAM non volatile) Le problème de la RAM est la non-conservation des données après la coupure de l'alimentation. La NVRAM solutionne le problème, puisque les données sont conservées même après la coupure de l'alimentation. L'utilisation de la NVRAM permet de ne pas avoir de mémoire de masse (Disques Durs, Floppy). Cela évite donc les pannes dues à une partie mécanique. La configuration est maintenue dans la NVRAM.

Portes I/O La structure même d'un routeur est l'ouverture donc l'interfaçage vers le monde extérieur est important. Il existe un nombre impressionant d'interfaces possibles pour un routeur (Liaison série asynchrone, synchrone, ethernet, tokenring, ATM, Sonet, FO, ...). La vitesse du bus qui interconnecte les I/O avec les différents composants du routeur marque aussi la puissance de traitement du routeur.

Le système d'exploitation des équipements Cisco est appelé Internetwork Operating System (IOS). Les routeurs sont configurés et gérés à l'aide de l'interface en ligne de commandes (command-line interface, CLI).

Les composants	Les fonctions
Le processeur	Le processeur (UC) exécute les instructions du système d'exploitation IOS. Ses principales fonctions sont, entre autres, l'initialisation du système, le routage et le contrôle de l'interface réseau. L'UC est un microprocesseur. Les grands routeurs sont généralement multiprocesseurs.
Mémoire flash	La mémoire flash est utilisée pour le stockage d'une image complète de la plate-forme logicielle Cisco IOS. Le routeur obtient normalement l'IOS par défaut de la mémoire flash. Ces images peuvent être mises à niveau en chargeant en mémoire flash une nouvelle image. L'IOS peut être au format non compressé ou compressé. Dans la plupart des routeurs, une copie exécutable de l'IOS est transférée vers la mémoire vive au cours du processus de démarrage. Dans d'autres routeurs, l'IOS peut être exécuté directement à partir de la mémoire flash. L'ajout ou le remplacement des

	modules SIMM de mémoire flash ou des cartes PCMCIA permet de mettre à niveau la quantité de mémoire flash.
la mémoire vive (RAM)	La mémoire vive, également appelée mémoire vive dynamique (DRAM), possède les caractéristiques et les fonctions suivantes: · elle contient les tables de routage, · elle contient le cache ARP, · elle contient la mémoire cache à commutation rapide, · elle effectue la mise en mémoire tampon des paquets (RAM partagée), · elle gère les files d'attente de paquets, · elle sert de mémoire temporaire pour le fichier de configuration à la mise sous tension du routeur, · elle perd son contenu à la mise hors tension ou au redémarrage du routeur.
La mémoire vive rémanente (NVRAM)	La mémoire vive rémanente (NVRAM) possède les caractéristiques et fonctions suivantes: · elle assure le stockage du fichier de configuration de démarrage, · elle conserve son contenu à la mise hors tension ou au redémarrage du routeur. La mémoire flash possède les caractéristiques et fonctions suivantes: · elle contient l'image du système d'exploitation (IOS), · elle permet de mettre à jour le logiciel sans suppression ni remplacement de puces sur le processeur, · elle conserve son contenu à la mise hors tension ou au redémarrage du routeur, · elle peut stocker plusieurs versions de la plate-forme logicielle IOS, · elle constitue un type de ROM programmable et effaçable électroniquement (EEPROM).
	La mémoire morte (ROM) possède les caractéristiques et fonctions suivantes:

La mémoire morte (ROM)	· elle gère les instructions du test automatique de mise sous tension (POST), · elle stocke le programme d'amorçage (bootstrap) et le logiciel de système d'exploitation de base, · elle nécessite un remplacement des puces enfichables sur la carte mère pour procéder aux mises à jour logicielles.
Les interfaces	Les interfaces possèdent les caractéristiques et fonctions suivantes: · elles connectent le routeur au réseau pour l'entrée et la sortie des paquets, · elles peuvent se trouver sur la carte mère ou sur un module séparé

Porte console

La configuration de base d'un routeur Cisco (et des autres aussi) se fait en général via la porte console. La porte console, sur un routeur, est configurée comme une interface DTE (Data Terminal Equipment). Mais la porte RS232 d'un PC est aussi une interface DTE, c'est pour cela que vous ne pouvez connecter un cable série directement sur la porte console. La solution est d'utiliser un cable croisé (entre le fil 2 & 3) avec les différents fils de signaux. Le cable de console est souvent fourni en standard avec les routeurs Cisco. La connexion s'effectue, en standard, à 9600bauds avec 8 bits de data, 1 bit stop et pas de parité. Vous pouvez utiliser votre émulateur de terminal favori.

Les fichiers de configuration

Dans un routeur cisco (en général), il existe différents fichiers de configuration. Il y a un fichier de configuration dans la nvram (startup-config), qui est lu au démarrage du routeur et copié en mémoire. Il y a un autre fichier de configuration dans la mémoire vive (running-config).
La "startup-config" est conservée dans la nvram sous forme ASCII. Tandis que la "running-config" est dans la ram sous forme binaire.

Interpreteur de commande (CLI exec)

L'interpreteur de commande, comme son nom l'indique, est responsable de l'interprétation des commandes que vous tapez. La commande interprétée, si elle est correcte, réalise l'opération demandée.

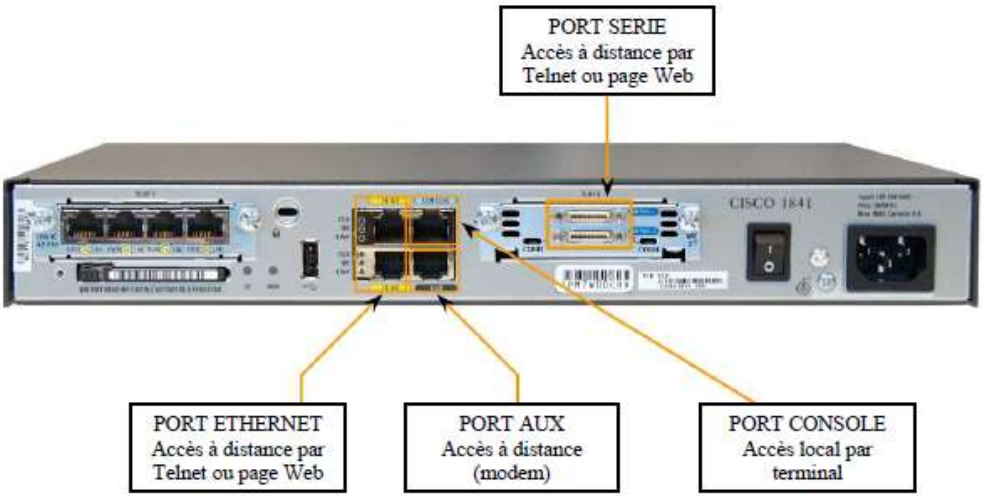
Si lors de la configuration initiale un (ou des) password a été configuré, vous devez introduire ce password pour accéder à l'interpreteur de commande.
Il y a 2 modes d'execution sur un routeur Cisco :
1. Le mode utilisateur (prompt : >)
2. Le mode privilégié (prompt : #)

Lors de la connexion initiale avec le routeur, vous arrivez dans le mode utilisateur. Pour passer au mode privilégié, vous devez introduire la commande enable et ensuite introduire un mot de passe. Le mode utilisateur sert uniquement à la visualisation des paramètres (pas de la configuration) et des différents status du routeur. Par contre, le mode privilégié permet, en plus de la visualisation des paramètres, la configuration du routeur et le changement de

paramètres dans la configuration.
L'interpreteur de commande des routeurs Cisco est très souple et vous permet de demander les commandes disponibles. Vous désirez savoir les commandes qui commencent par "ho", rien de plus simple, ho ? <enter>. Il est aussi possible d'utiliser l'expansion de commande comme sous Unix (avec la touche de tabulation). Si il n'y pas de confusions possibles, vous pouvez utiliser les abbréviations de commande. Par exemple, sh ip int brie au lieux de show ip interface brief. Cela permet de gagner du temps et de rendre la vie un peu plus facile.

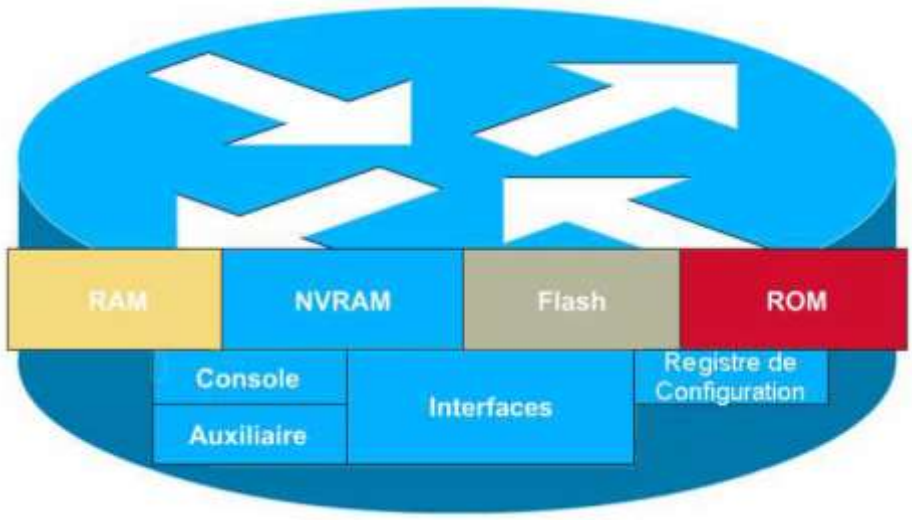
Un routeur (ou un commutateur) Cisco peut être administré/paramétré de différentes façons :

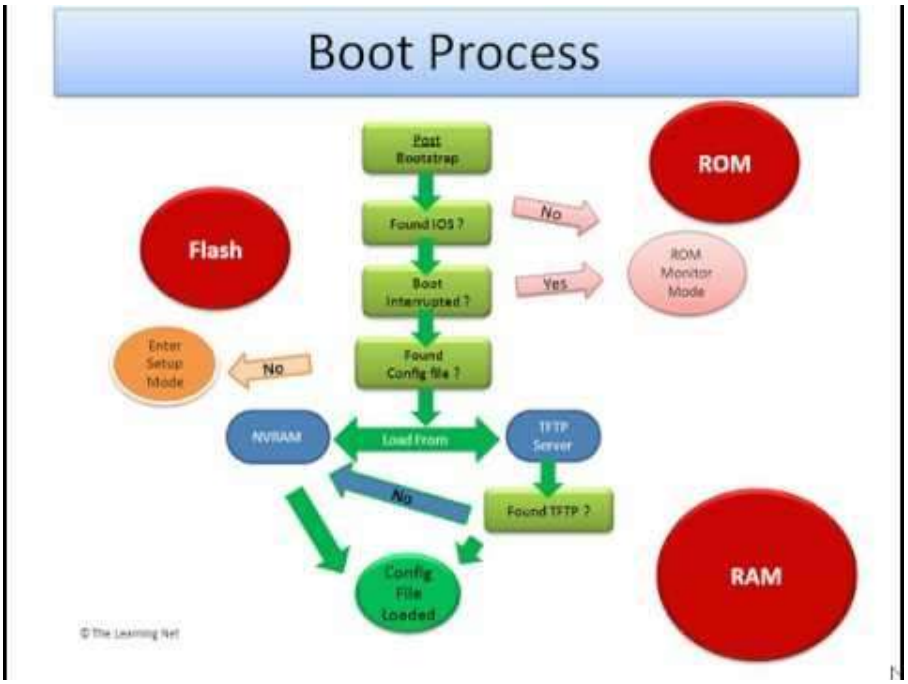
- Localement ou à distance.
- Par page web ou en ligne de commande(CLI).



1.1. Configuration locale.

Le port Console: Il est utilisé pour relier directement un PC avec HyperTerminal ou Putty (par exemple) en utilisant un câble série. Cisco fournit pour cela des câbles plats bleu pâle. **Le port console est indispensable si le routeur n'a pas d'adresse IP de configurée.**

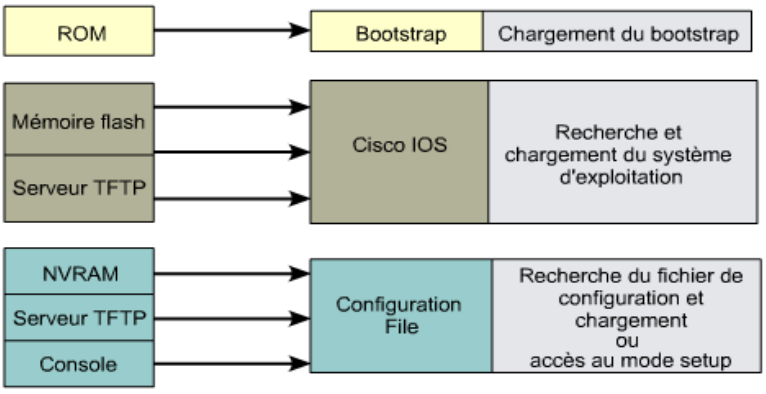


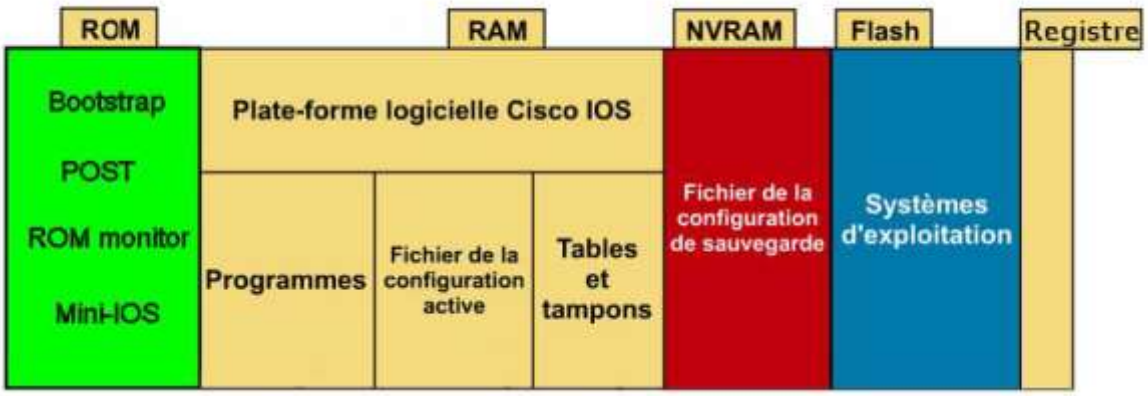


Étapes d'initialisation du routeur

FIGURES

1
2





Contenu de la ROM

- Bootstrap : démarre le routeur et charge le système
- POST (Power-On Self Test) : teste le fonctionnement des composants physiques du routeur (processeur, mémoire, interface)
- ROM monitor : commandes de bas niveau pour tester et administrer le routeur
- Mini-IOS (RXBOOT) : mini-système suffisant pour monter une interface puis charger un système d'exploitation plus complet

Contenu de la RAM

- Le système d'exploitation en cours d'exécution
- Les différentes tables et files d'attente (ARP, routage, etc.)
- Le fichier de configuration active (`running config`)

Contenu de la NVRAM et de la flash

- NVRAM : Le fichier de configuration de démarrage (`startup config`)
- FLASH : Une ou plusieurs images du système d'exploitation (IOS)

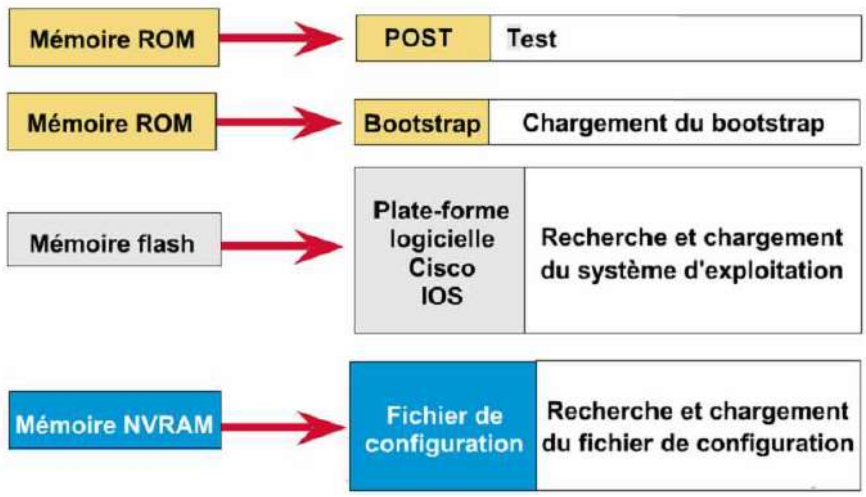
Modification de la séquence de démarrage

- Changement de la valeur du registre de configuration
  - 0Xnnn0 démarrage en moniteur ROM
  - 0Xnnn1 chargement de la première image en flash
  - 0Xnnn2 – 0Xnnnf utilisation des commandes `boot system`
- Commande `boot system` :
  - Situées dans la NVRAM
  - Spécifie la localisation du système chargé lors du démarrage

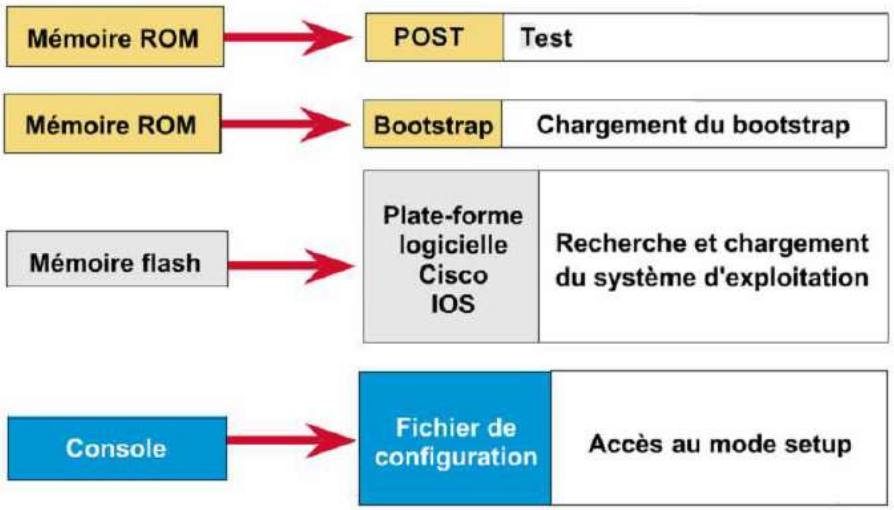
Prompts et modes de démarrage

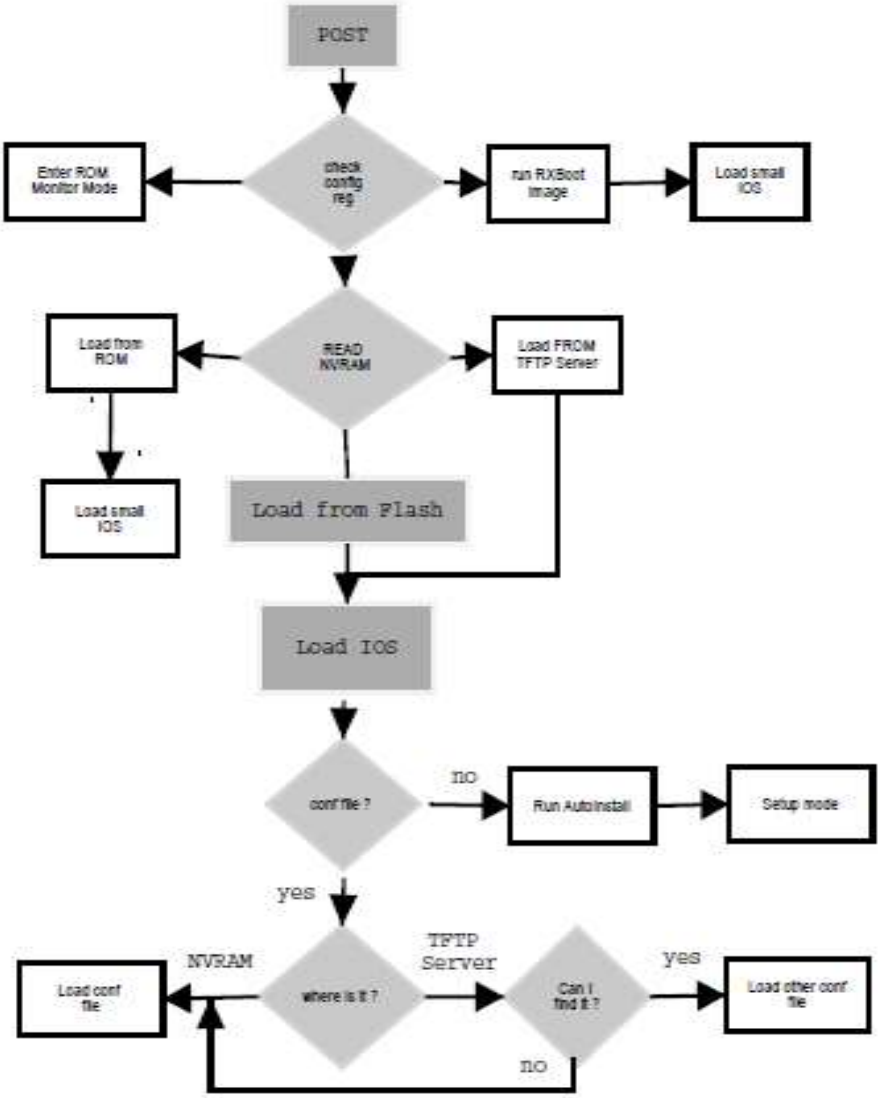
Environnement d'exploitation	Invite	Utilisation
Moniteur ROM	`> or ROMMON>`	Panne ou récupération de mot de passe
Plate-forme logicielle Cisco IOS	`Router>`	Fonctionnement normal

Démarrage « Classique » (OX2102)



Démarrage récupération mot de passe (0x2142)

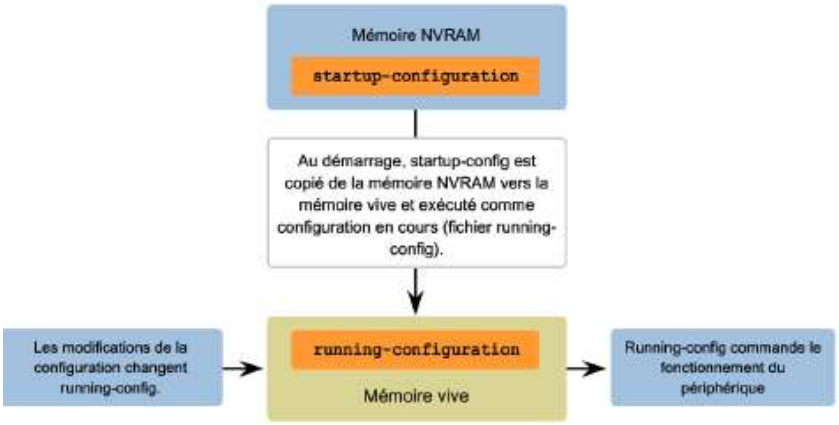




Un routeur (ou un commutateur) contient deux fichiers de configuration.

3.2.1. Startup-config.

Le fichier de configuration initiale (**startup-config**) est utilisé au démarrage du système pour configurer le périphérique. Le fichier de configuration initiale, appelé startup-config, est stocké en mémoire vive non volatile (NVRAM).



Le fichier de configuration **running-config** représente la configuration en cours de fonctionnement. Si on modifie un paramètre, on modifie ce fichier.

☞ Pour sauvegarder la configuration en cours avant extinction du routeur, il faut la taper la commande suivante:

Router# copy running-config startup-config

Ainsi, lors du prochain redémarrage, on récupèrera la configuration sauvegardée.

☞ Pour récupérer la configuration initiale du routeur, il faut la taper la commande suivante:

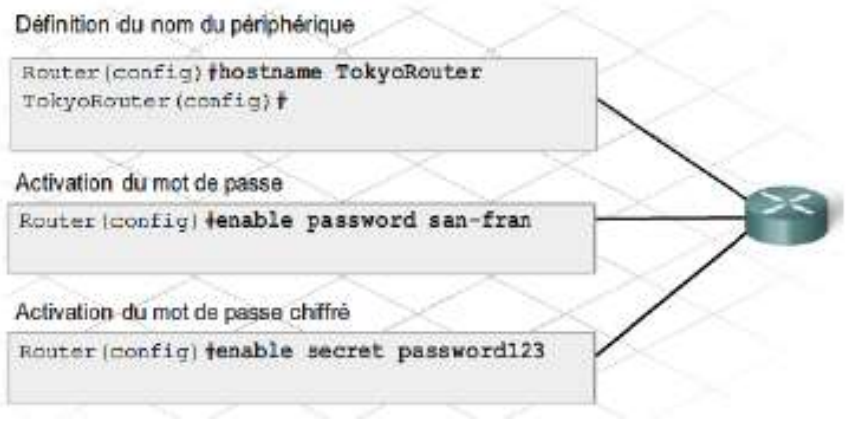
Router# copy running-config startup-config

☞ Pour effacer la configuration initiale du routeur, il faut la taper la commande suivante:

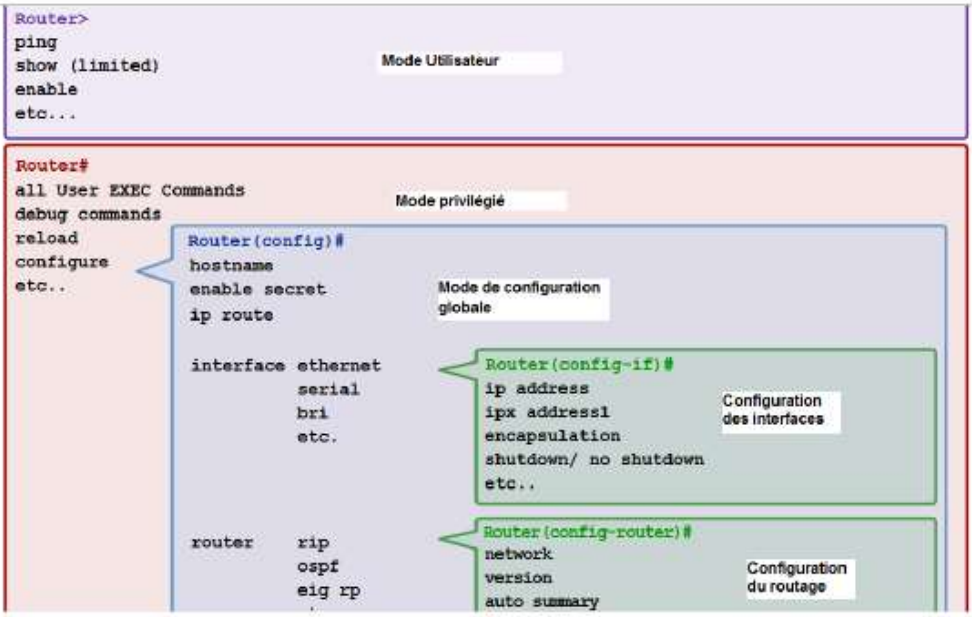
Router# wr erase

☞ Pour recharger la config startup, il faut taper:

Router# reload



La figure ci-dessous montre la structure hiérarchique des modes IOS avec des invites et des fonctionnalités classiques.



Les étapes de configuration d'une interface sont les suivantes :

Étape 1. Spécification du type d'interface et du numéro de port de l'interface
Étape 2. Spécification d'une description de l'interface
Étape 3. Configuration de l'adresse IP et du masque de sous-réseau de l'interface
Étape 4. Définition de la fréquence d'horloge si vous configurez une interface série en tant que DCE
Étape 5. Activation de l'interface

```
Router(config)#interface fastethernet 0/0
Router(config-if)#description connection to Admin LAN
Router(config-if)#ip address 192.168.2.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface serial 0/0/0
Router(config-if)#description connection to Router2
Router(config-if)#ip address 192.168.1.125 255.255.255.0
Router(config-if)#clock rate 64000
Router(config-if)#no shutdown
```

POUR LA BANNIERE

```
Marseille(config)# banner motd $ Bienvenue sur
   Marseille, accès autorisé uniquement $
```

⌘Encryption de tous les mots de passes

```
Router(config)#service password-encryption
```

Suppression de l'adresse ip d'une interface:

```
Router(config)#interface fastEthernet 0/0
Router(config-if)#no ip address
```

2.2.8 Configuration des interfaces routages

La configuration des protocoles de routage est réalisé de la même manière que les interfaces.

```
router leprotocolederoutage
```

Protocole de routage	Description
bgp	Border gateway protocol
egp	Exterior gateway protocol
igrp	Interior gateway protocol
isis	ISO IS-IS
iso-igrp	IGRP pour les réseaux OSI
ospf	Open shortest path first
rip	Routing information protocol
static	Static CLNS routing

```
ip-int-gw>enable
password :
ip-int-gw#configure terminal
ip-int-gw(config)#router ospf 303
ip-int-gw(config-router)#network 145.30.6.0
ip-int-gw(config-router)#exit
ip-int-gw(config)#exit
ip-int-gw#
```

Un mot de passe est créé pour se loguer au différentes lignes.

```
Routeur-cisco(config)#enable secret m02p@55E
Routeur-cisco(config)#line con 0
Routeur-cisco(config-line)#password P@55w0rdcon5
Routeur-cisco(config-line)#login
Routeur-cisco(config-line)#exit
Routeur-cisco(config)#line vty 0 4
Routeur-cisco(config-line)#password P@55w0rdcon5
Routeur-cisco(config-line)#login
Routeur-cisco(config-line)#end
Routeur-cisco#
```

Afficher les utilisateurs connectés au routeur

```
Routeur-cisco#show users
Line User Host(s) Idle Location
* 0 con 0 idle 00:00:00

Interface User Mode Idle Peer Address

Routeur-cisco#
```

Suppression de la configuration - réinitialisation du routeur Cisco

```
Router#write erase
Erasing the nvram filesystem will remove all configuration files!
Continue? [confirm]
[OK]
Erase of nvram: complete
Router#
```

La fonctionnalité principale de la couche Réseau consiste à transmettre des paquets de données issu d'un émetteur à destination d'un (ou plusieurs) récepteurs, paquets qui doivent traverser un réseau composé de nombreux noeuds intermédiaires (routeurs).

A chaque réception d'un paquet, un routeur doit choisir vers quel prochain routeur il doit retransmettre le paquet entrant pour que celui-ci arrive à destination.

- En mode datagramme, le choix est effectué indépendamment pour chaque paquet.
- En mode circuit virtuel, le choix est fixé à l'établissement de la connexion et pour toute la durée de la connexion.

Dans chaque routeur (commutateur), ce choix est effectué en se servant d'informations contenues dans une table de routage (commutation).

Les entrées d'une table de routage sont renseignées soit manuellement, soit automatiquement à l'aide d'algorithme de mise à jour des tables de routage en se basant sur différents critères (débit possible, disponibilité de la ligne, taux d'erreurs, nombre de noeuds intermédiaires, ...)

Fonctions d'un routeur :

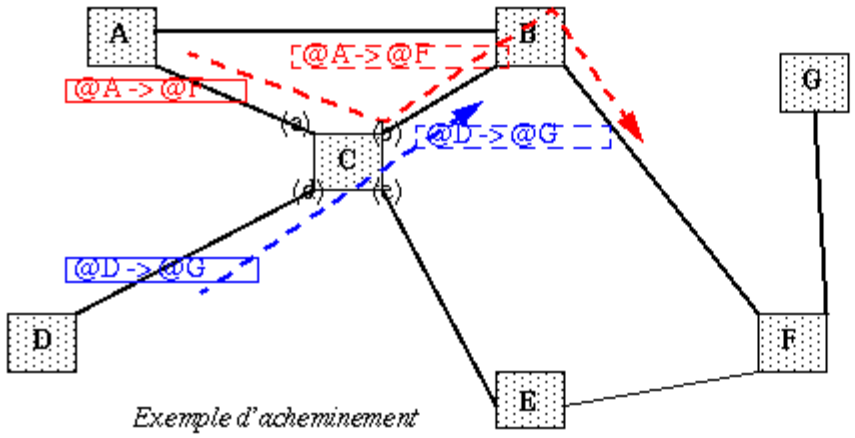
- acheminement des paquets ("datagram forwarding"), c-à-d transmission des paquets.
- mise à jour des tables de routage - algorithme de routage.

4.2. L'acheminement par datagramme

Chaque routeur est muni d'une table de routage. Cette table reflète l'état (perçu par le routeur) de la topologie du réseau à un moment donné.

Actions effectuées lors de la réception d'un paquet:

- extraction de l'adresse de destination,
- recherche dans la table de routage,
- retransmission du paquet vers le prochain routeur



Exemple d'acheminement

Table de routage de C

Destination	Prochain routeur	Informations complémentaires
@A	@A	(a)
@G	@B	(b)
...		
@D	@B	(b)
@F	@E	(e)
...		

4.3. Le procédé d'acheminement par circuit virtuel

Le ciurcuit virtuel (CV) relie l'émetteur au destinataire. Chaque tronçon de CV est identifié par un nº de voie logique (NVL).

Les numéros de VL sont réservés lors de l'établissement de la connexion. Ils sont rendus lors de la libération de la connexion.

Actions effectuées lors de la réception d'un paquet :

- extraction du NVL, recherche dans la table de circuit virtuel
- échange du NVL, retransmission du paquet

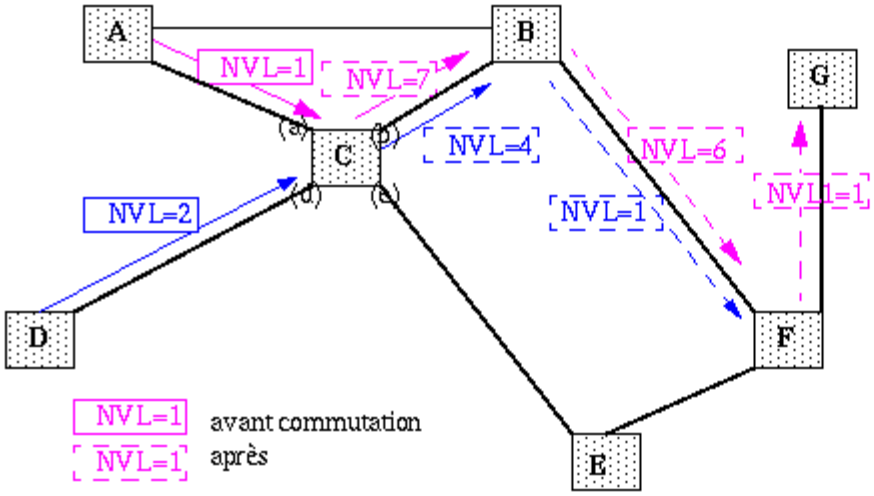


Table de commutation de C

Entrée		Sortie	
Origine	nºVL	Prochain	nºVL
(a)	1	(b)	7
(b)	1	(a)	1
(b)	2	(d)	1
(d)	1	(b)	2
(d)	2	(b)	4
(e)	4	(d)	2

4.4. Services et procédés

On confond souvent services et procédés.

Deux services d'acheminement :

- en mode connecté ou en mode non connecté

Deux procédés d'acheminement :

- Par circuit virtuel ou par datagramme

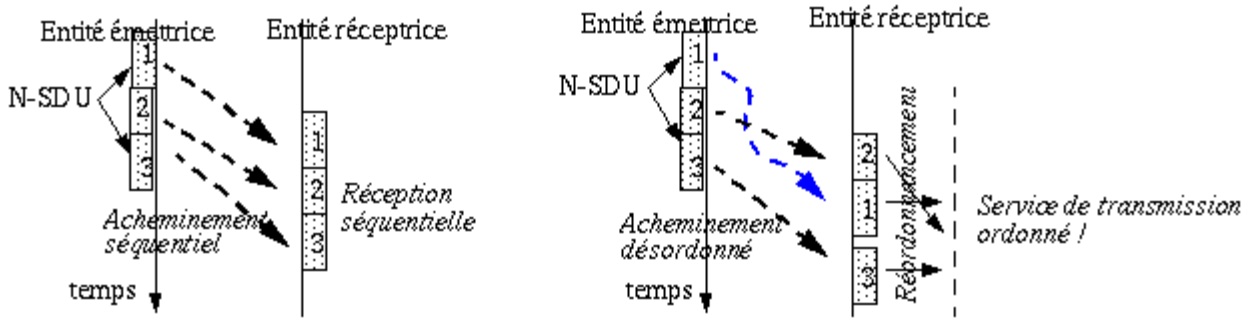
4.4.1 Le service non connecté

1. Les paquets (N-SDU) sont reçus et délivrés par les entités Réseau indépendamment les uns des autres.
   - Utilise généralement le procédé d'acheminement par datagramme,
   - Généralement pas de service d'augmentation de la fiabilité.
     - Les services de protection contre les erreurs, de contrôle de flux et le ré-ordonnancement des paquets sont éventuellement reportés dans les couches supérieures.

4.4.2 Le service connecté

1. Les entités d'une même connexion partagent un même contexte :
   - par exemple au sein d'une connexion une entité connaît le numéro du prochain paquet envoyé par l'autre entité.
   - Les paquets (N-SDU) appartenant à la même connexion sont délivrés dans l'ordre où ils ont été émis. Et généralement, un contrôle de flux et d'erreur y est associé.
   - Utilise généralement le procédé d'acheminement par circuit virtuel.

Le mode d'acheminement par datagramme et service ordonné ne sont pas contradictoires :

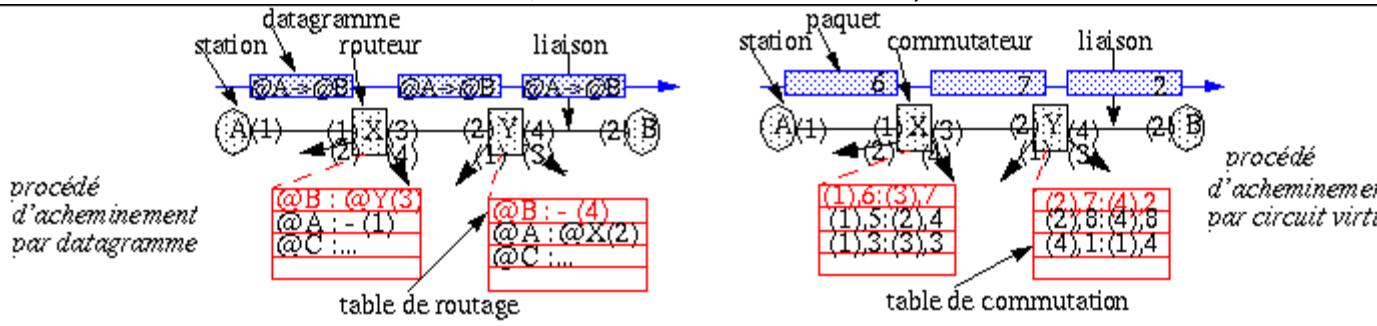


4.4.3 Le procédé d'acheminement par datagramme :

1. Les paquets (N-PDU) sont transmis indépendamment les uns des autres au sein du réseau.
    - Leur routage est effectué grâce à l'adresse de destination figurant dans l'entête du paquet,
    - Le routage des paquets (entre deux mêmes stations) est adaptatif,
    - Généralement, les routeurs effectuent peu ou pas de traitement de contrôle.

4.4.4 Le procédé d'acheminement par circuit virtuel :

1. Les paquets (N-PDU) sont souvent acheminés séquentiellement grâce à un circuit virtuel ouvert au sein du réseau.
    - Leur commutation est effectuée grâce à un identificateur de circuit virtuel figurant dans l'entête du paquet (c'est le numéro de voie logique : NºVL),
    - La phase d'établissement du circuit virtuel réserve les ressources (notamment le numéro de voie logique) au sein de chaque commutateur,
    - Tous les paquets utilisant un circuit virtuel suivent le même chemin,
    - Les paquets sont transmis sur ce circuit virtuel dans l'ordre,
    - Généralement, un contrôle de flux et d'erreur y est associé.



- Note : une table de routage est nécessaire lors de l'établissement de la connexion pour réserver le numéro de circuit virtuel!

4.5. Comparaisons

4.5.1 Circuit virtuel et datagramme, adresse et identificateur de CV

- Un numéro de voie logique identifie un tronçon de CV (pour une seule liaison entre 2 systèmes intermédiaires). Le chemin suivi par un CV est identifié par une suite de nº de VL.
- Le numéro de voie logique est généralement de plus faible taille qu'une adresse
- La table de commutation est plus petite que la table de routage.

- La durée le vie de l'association entre numéro de VL et circuit virtuel est celle de la connexion.
- La réservation d'un nº de VL est effectuée localement pour chacune des liaisons formant le circuit virtuel. Sinon :
    - des réservations multiples de nº risqueraient d'apparaître,
    - la résolution des conflits de numérotation serait complexe et longue.
- Grâce au circuit virtuel :
    - la commutation est plus rapide,
    - le contrôle du trafic est aisé,
    - la taxation est plus facile.

4.5.2 Comparaison des deux types de service de transmission Réseau

service en mode connecté ou non

Fonctionnalités	Service en mode non connecté	Service en mode connecté
Etablissement/Initialisation	Inutile	Nécessaire
Adresse du destinataire	Dans chaque paquet	Dans le paquet d'initialisation
Séquencement des paquets	Non garanti, généralement	Garanti, généralement
Contrôle d'erreur/Contrôle de flux	Non fournis, effectués (si besoin) dans les couches supérieures	Fourni, généralement
Possibilité de négociation des options	Non	Oui
Utilisation d'identificateurs de connexion (NVL)	Non	Oui, dans tous les paquets

4.6. Les paquets errants

Certains paquets peuvent errer dans le réseau :

- notamment si le service Réseau est en mode datagramme
- les paquets suivent des chemins indépendants
- le mécanisme de retransmission produit des doubles
- certaines portions du réseau peuvent se trouver isolées du reste :
- soit par panne de routeur ou par rupture de liaisons
- soit à cause de l'instabilité (vitesse de convergence) des algorithmes de routage
- les routeurs doivent mémoriser les paquets qu'ils ne peuvent temporairement acheminer

Dans ce cas, la durée de vie des paquets est volontairement limitée.

Exemple IP :

- chaque datagramme est muni d'un champ spécifique : TTL ("Time to live"),
- initialisé à une certaine valeur : sa duré de vie maximale,
- décrémenté toutes les secondes de résidence dans un routeur et à chaque réception,
- le datagramme est détruit lorsque la valeur devient nulle.

Routage IP

1.3.1 Concept

En théorie, le routage IP est simple, particulièrement dans le cas d'une workstation. Si une machine de destination est directement connectée à une autre machine (par exemple : une liaison PPP) ou sur un réseau partagé (par exemple : Ethernet), alors le datagramme IP

est envoyé sans intermédiaire à cette destination. Par contre, le routage est plus complexe sur un routeur ou sur un machine avec plusieurs interfaces.
Le routage IP est effectué sur le base de “saut à saut” (hop to hop routing). Les étapes du routage IP peuvent être découpées de cette manière :
1. Recherche, dans une table de routage, de l’entrée associée à l’adresse IP de destination. S’il trouve une correspondance entre la table de routage et l’adresse de destination, le datagramme IP est envoyé au routeur de “saut suivant”(next-hop router). Ce cas de figure est utilisé pour les liaisons point à point.
2. Recherche, dans la table de routage, de l’entrée correspondant exactement à l’indentificateur du réseau de destination. Si cette adresse est localisée, envoi du paquet au routeur de saut suivant indiqué ou à l’interface directement connecté (par exemple : si l’interface existe sur le routeur). C’est ici aussi que l’on tient compte des masques de sous-réseau.
3. Recherche, dans la table de routage, de l’entrée par défaut. Envoi du paquet au routeur “de saut suivant” si cette entrée est configurée.
Si le déroulement de ces 3 phases est correct, alors le datagramme IP est délivré au prochain routeur ou host. Par contre, si cela n’est pas le cas, un message ICMP (host unreachable ou network unreachable) est envoyé au host d’origine et le datagramme IP est jeté.

La route par défaut est la route qui sera utilisée lorsque aucune route spécifique pour aller vers la destination spécifiée n'aura été trouvée. Ainsi, dans le cas précédent, si je voulais atteindre l'adresse 193.253.25.46, aucune entrée de ma table de routage ne m'aurait indiqué comment y aller... Ce qui fait que ma machine n'aurait pas su vers qui envoyer le paquet et qu'il serait allé directement à la poubelle :-(

En indiquant en plus une route par défaut, cela aurait permis à ma machine d'avoir une destination, même quand aucune entrée de la table de routage ne correspondait à l'adresse demandée. J'aurais donc envoyé mon paquet vers ma route par défaut, en fait vers le prochain routeur à utiliser, et c'est ce prochain routeur qui se serait occupé de continuer à router le paquet. Si lui non plus n'avait pas eu de route spécifiée pour l'adresse de destination demandée, il aurait envoyé le paquet à son propre routeur par défaut, et ainsi de suite jusqu'à tomber sur un routeur connaissant la route !
La table de routage pour le routeur 1 devient alors:
Réseau Masque Interface Passerelle
192.168.0.0 255.255.255.0 ethernet 1 ethernet 1
172.16.0.0 255.255.0.0 ethernet 2 ethernet 2
10.0.0.0 255.0.0.0 ethernet 2 172.16.0.254
défaut 0.0.0.0 ethernet 2 172.16.0.254

Cette ligne peut parfois être aussi écrite:
0.0.0.0 0.0.0.0 ethernet 2 172.16.0.254

Route statique IP

Les routes statiques IP se définissent grâce à la commande ip route du mode global de configuration. La syntaxe générale est la suivante :
ip route prefix mask {ip-address | interface-type interface-number}
On indique l'adresse IP du prochain routeur à l'aide de ip-address ou l'interface de sortie (interfacetype interface-number) lorsque le réseau est directement connecté et que le type de réseau est point à point.
Dans l'exemple, trois routes sont configurées :
Router(config)#ip route 10.1.0.0 255.255.0.0 192.168.2.1
Router(config)#ip route 192.168.1.0 255.255.255.0 FastEthernet0/1
Router(config)#ip route 192.168.2.0 255.255.255.0 FastEthernet0/2
Le réseau 192.168.1.0/24 est directement relié au routeur par l'intermédiaire de la première interface FastEthernet.
Le réseau 10.1.0.0/16 est atteignable en passant par l'interface 192.168.2.1 d'un autre routeur.

Lorsqu’un réseau atteint une taille assez importante, il est très lourd de devoir ajouter les entrées dans les tables de routage à la main. La solution est le routage dynamique. Cela permet de mettre à jour les entrées dans les différentes tables de routage de façon dynamique.

RIPv1(Routing Information Protocol) C’est le protocole (distance vector protocol) le plus vieux mais qui est toujours implanté sur beaucoup de sites. C’est un protocole de type IGP (Interior Gateway Protocol) qui utilise une algorithme permettant de trouver le chemin

le plus court. Il supporte un maximum de 15 noeuds traversés (il n'est pas adapté au réseau de grande taille). Il fonctionne par envoi de messages toutes les 30 secondes. Les messages RIP permettent de dresser une table de routage.
RIPv2 (Routing Information Protocol) C'est une version améloriée pour ajouter le support des sous-réseaux (subnets), des liaisons multipoints et de l'authentification.
EIGRP Ce protocole (Hybrid link-state & distance vector protocol) de routage a été developpé par Cisco pour améliorer RIP et le rendre plus stable. Il fonctionne très bien mais il est bien sûr uniquement compatible avec les produits Cisco.
OSPF(Open Shortest Path First) C'est la deuxième génération de protocole de routage (Link-state protocol). Il est beaucoup plus complexe que RIP mais ses performances et sa stabilité sont supérieures. Le protocole OSPF utilise une base de données distribuées, qui garde en mémoire l'état des liaisons. Ces informations forment une description de la topologie du réseau et de l'état de l'infrastructure. Le protocole RIP est adapté pour des réseaux de taille raisonnable par contre OSPF est de meilleure facture pour les réseaux de taille importante (par exemple ISP).
BGP (Border Gateway Protocol) BGP est utilisé sur Internet pour le routage entre, par exemple, les différents systèmes autonomes OSPF. Ce protocole a été créé pour des besoins propres à Internet suite à la grande taille du réseau lui-même.

Principe du routage IP

- Le routage s'effectue sur deux opérations :
  - La sélection du meilleur chemin (optimal)
    - Niveau 3 du modèle OSI
    - Métrique: nombre de sauts, bande passante, délai, etc
  - La commutation du paquet sur l'interface appropriée

La politique d'acheminement de paquet

- **Déterministe** :
  - Une seule route est possible par rapport à la destination.
  - Les tables de routage peuvent être fixées à la configuration du réseau
  - Les mises à jour périodiquement par le(s) centre(s) de gestion (gestion centralisée ou décentralisée)
- **Adaptative** :
  - Aucun chemin n'est prédéterminé, le chemin sera fixé au moment du routage en fonction de données sur l'état du réseau (charge, indisponibilité d'un nœud, …)
- **Mixte** :
  - La politique est adaptative à l'établissement du chemin et déterministe durant le reste de la session
  - Cette technique est utilisée dans les réseaux en mode orienté connexion

Classification des algorithmes de routage

- **Routage statique**
  - Mise à jour manuelle de tous les équipements réseau
  - Pour les réseaux les plus stable
  - Complexe et risque d'erreur pour les grand réseaux (> 10 routeurs)

- **Routage dynamique**
  - Adaptation dynamique à l'évolution du réseau :
    - Changement de la topologie réseau
    - Changement des conditions réseau (paramètres de Qualité de Service)
  - Nécessite un protocole de routage

Routage IP statique

- Une route statique est basée sur :
  - L'adresse du réseau + Le masque de sous-réseau du réseau distant
  - L'adresse du routeur du tronçon suivant (next-hop) + l'interface de sortie

- **Route par défaut**
  - Facilite la circulation des données sur un réseau de grande taille
  - Pour atteindre une destination inconnue
  - Utilisée si le prochain saut ne figure pas explicitement dans la table de routage

Routage IP statique

Problèmes du routage statique

- Mise à jour manuelle de tous les équipements du réseau
- Une station ne peut atteindre que les réseaux qu'on lui indique par la commande route
- Boucles de routage
- Routages asymétriques

- **Recommandations générales**
  - Stations, Routeurs d'extrémité => Routage statique
  - Routeurs => Routage dynamique

Routage IP statique

Avantages d'un routage statique

- Sécurité par masquage de certains parties d'un inter-réseau

- Moins de surcharge par rapport au routage dynamique

Routage IP dynamique

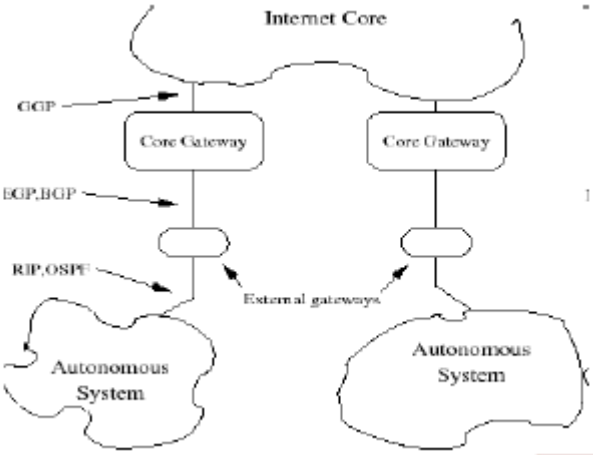
- Plusieurs routes possibles pour rejoindre une destination
  => l'usage d'un protocole de routage dynamique

- Une route statique privilégie (une seule route) et ignore les autres

- Existence de plusieurs routes est une nécessité pour assurer la redondance du service, voire même l'équilibrage du trafic sur plusieurs liens

- **Objectifs des protocoles de routage :**
  - Sélectionner les meilleures routes
  - Eliminer les boucles de routage
  - Eviter la configuration manuelle
  - Gérer dynamiquement le changement des routes
  - Maintenir la cohérence des informations associées aux routes
  - Limiter la taille des tables de routage pour réduire le temps de traitement
  - Réduire la consommation de la bande passante et du CPU
    - Hiérarchie des échanges d'informations
      - Notion du système autonome
      - Classification des protocoles : IGP et EGP

GGP: Gateway to Gateway *Protocol*
EGP: Exterior Gateway Protocol
BGP: Border Gateway Protocol
RIP: Routing Information Protocol
OSPF: Open Shortest Path First

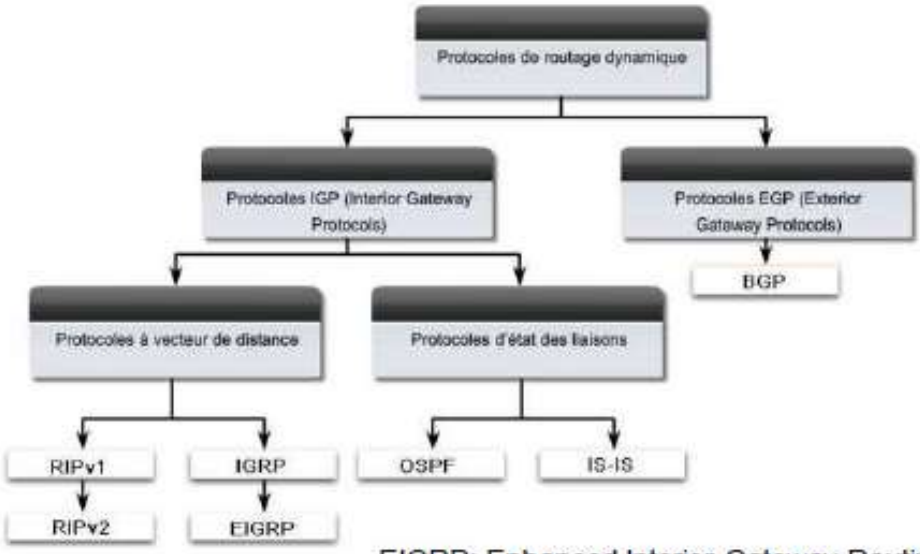


Un AS, le monde extérieur et intérieur

- Tous les routeurs de même AS :
  - sont interconnectés entre eux
  - échangent leur tables de routage

- Deux familles de protocoles de routage
  - Protocoles entre routeurs d'un AS (Intra AS)
    - IGP : Interior Gateway Protocol (RIP, OSPEF, etc)
  - Protocoles de routage entre AS (Inter AS)
    - EGP : Exterior Gateway Protocol (EGP, BGP)

- Deux grandes classes de protocoles de routage
  - **Distance Vector** (Vecteur de distance)
    - Plus court chemin calculé à l'aide du nombre de sauts et de manière distribuée
    - Envoi périodique de tables de routage aux voisins
  - **Link State** (état des liaisons)
    - Chaque routeur envoie une liste complète des routeurs voisins et des coûts des liens (ex. bande passante) contenue dans sa base de données
    - Construction du graphe localement
    - Calcul du plus court chemin dans le graphe avec l'algorithme Dijkstra



EIGRP: Enhanced Interior Gateway Routing Protocol

IS-IS : Intermediate System to Intermediate System

Protocoles à vecteur de distance

- Algorithme Belman-Ford : calcul distribué des routes
- Routeur diffuse régulièrement les routes qu'il connaît pour ses voisins
- Une route est composée de :
  - L'adresse du réseau de destination
  - L'adresse du prochain routeur (next-hop)
  - La métrique : nombre de sauts = nombre de routeurs traversés pour atteindre la destination
  - Le routeur compare les routes qu'ils reçoivent avec les siennes => MAJ sa propre table de routage si :
    - La route reçue est nouvelle
    - La route reçue est meilleure (métrique inférieure)

Protocoles à vecteur de distance «Distance-Vector»

- **Avantages**
  - Algorithme simple
  - Totalement décentraliser
  - Interopérabilité (stations/routeurs)

- **Inconvénients**
  - Convergence lente pour les grands réseaux
  - La taille des informations de routage est proportionnel au nombre de réseau
  - Pas de chemins de multiples
  - Coût des routes externes est arbitaire
  - Bouclage à l'infini

- **Solutions aux inconvénients**

  - Fixer une valeur finie pour l'infinie (16)

  - Le routeur n'envoie pas à un voisin les information qui passe par la voie pour joindre ce voisin
    (**Split Horizon : L'horizon coupé**)

Protocoles d'état des liaisons

- Algorithme à état des liens de **Dijkstra**
- Chaque routeur communique à tous les routeurs l'état des liens avec ses voisins directs
- Métrique: débit, délai, charge, fiabilité, distance

- Les étapes à suivre pour chaque routeur
  - Découvrir les voisins directs
  - Evaluer les coûts pour les atteindre
  - Diffuser ces informations à tous les autres routeurs
  - Construire la matrice des coûts (représente la topologie réseau)
  - Calculer le plus court chemin vers tous les routeurs

- Etape 1: Découverte des voisins
  - Envoi du paquet HELLO sur toutes les liaisons
  - Chaque routeur reçoit ce paquet répond pour se présenter

- Etape 2 : Mesure le coût du lien (état du lien)
  - Calcul du temps d'aller-retour du paquet Echo
    - Avec/sans prise en compte de la charge du réseau

- Etape 3 : Formation du paquet d'état du liens à transmettre
  - Emetteur, liste des routeurs voisins directs et le coût associé

- Etape 4 : Diffusion de ces informations à tout le réseau
  - Par inondation (flooding)
- Etape 5 : Calcul de la matrice de coûts
  - Constitue une représentation de la topologie réseau
- Une route peut avoir trois états :
  - Validé : à partir de la source il n'existe aucun autre chemin pour atteindre la destination
  - Découverte : nouvelle route pour joindre le nœud suivant (next-hop) à partir d'un nœud validé
  - En attente : nouvelle route dont on ne sait pas si elle peut être validée ou pas
- **Avantage**
  - Convergence rapide et sans boucle
  - Possibilité de chemins multiples
  - Plusieurs métriques précises couvrant différents besoins
  - Chaque routeur calcule ses routes indépendamment des autres
  - Les algorithmes d'états de liaisons sont mieux adaptés au facteur d'échelle que les algorithmes de Vector-Distance
- **Inconvénients**
  - Complexe à mettre en ouvre
  - Consommation de ressources non négligeable

2. Compostion d'une table de routage.

Une table de routage est une sorte de "panneau indicateur" qui donne les routes (les réseaux) joignables à partir du "carrefour" que constitue un routeur. Les paquets arrivent sur une interface de la machine. pour "router" le paquet, le routeur fondera sa décision en deux temps : d'abord il regarde dans l'en-tête IP le réseau de destination et compare toutes les entrées dont il dispose dans sa table de routage; ensuite, si le réseau de destination est trouvé, il commute le paquet sur le bon port de sortie; si ce réseau n'est pas trouvé, le paquet est jeté.

Une table de routage réside en RAM. Elle constituée des éléments suivants :

- Méthode de routage : type de protocole qui a appris la route.
- Réseau et masque : destination.
- Distance administrative : Préférence d'une route par un protocole sur un autre. Chaque protocole a sa valeur par défaut.
- Valeur de métrique : valeur d'une route sur une autre parmi toutes celles apprises par un protocole de routage.
- Via prochaine interface (Gateway).
- Interface de sortie du routeur.

2.1. Métrique

La métrique d'une route est la valeur d'une route en comparaison d'autres routes apprises par le protocole de routage. Plus sa valeur est faible, meilleure est la route. Chaque protocole dispose de sa méthode de valorisation. On peut trouver toute une série de composante de métrique parmi :

- nombre de sauts (RIP)

- bande passante (IGRP - EIGRP)
- délai (IGRP - EIGRP)
- charge (IGRP - EIGRP)
- fiabilité (IGRP - EIGRP)
- MTU (IGRP - EIGRP)
- coût (OSPF - ISIS)

2.2 Distance administrative

La distance administrative est la préférence dans une table de routage des routes apprises par un protocole de routage par rapport aux mêmes routes apprises par un autre protocole de routage. Plus la valeur est faible et plus le protocole est préféré. Chaque protocole dispose de sa valeur par défaut sur les routeurs Cisco :

Méthode de routage	**Distance administrative**
Interface directement connectée	0
Route statique	1
Ext-BGP	20
Int-EIGRP	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
Int-BGP	200
Inconnu	255

La **distance administrative** est utilisée sur les routeurs afin de choisir la meilleure route possible lorsque plusieurs routes, originaires de protocoles de routage différents et ayant la même destination, existent.

La **distance administrative** définit un indice de confiance pour chacun des protocoles de routage, ainsi les protocoles sont classés du plus fiable au moins fiable en fonction de cet indice. Plus la distance administrative est basse, plus le protocole est de confiance.

Par exemple, une route apprise en OSPF, qui a une distance administrative de 110, est préférée à une route apprise en RIP dont la distance administrative est 120.

La distance administrative est souvent abrégée par l'acronyme "**AD"** pour "Administrative Distance" en anglais.

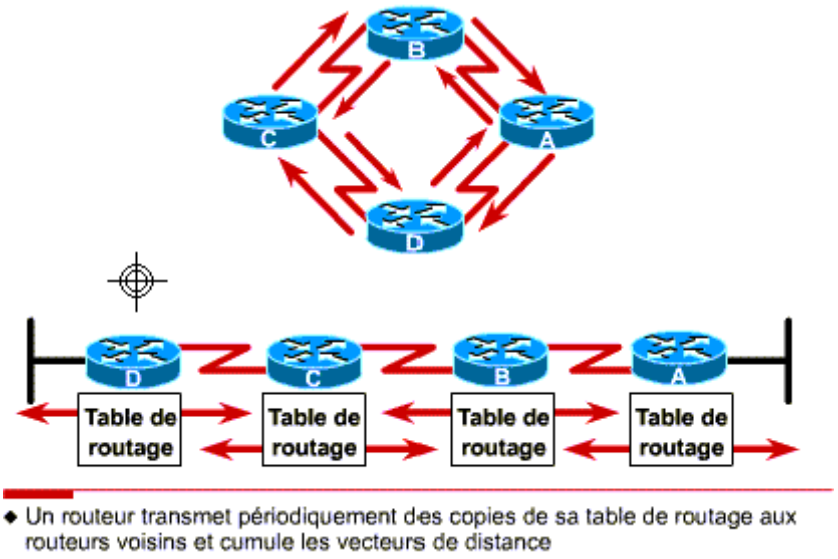
Résumé sur le routage à vecteur de distance

Les algorithmes à vecteur de distance entrent dans la catégorie des algorithmes d'optimisation qui nécessitent plus de bande passante que de puissance en processus. Cette caractéristique fait en sorte que le routage converge plus lentement mais aussi qu'il est plus simple à implémenter. On citera RIP et IGRP comme protocoles de routage utilisant l'algorithme. Les protocoles à vecteur de distance sont particulèrement sensibles aux boucles de routage. Diverses solutions sont proposées pour pallier à cette faiblesse.

1. Concepts de base

Les algorithmes de routage à vecteur de distance (Bellman-Ford) transmettent d'un routeur à l'autre des copies périodiques d'une table de routage. Ces mises à jour régulières entre les routeurs permettent de communiquer les modifications de topologie. Chaque routeur reçoit une table de routage des routeurs voisins auxquels il est directement connecté.

L'algorithme cumule les distances afin de tenir à jour la base de données contenant les informations de topologie du réseau. Toutefois, les algorithmes de routage à vecteur de distance ne permettent pas à un routeur de connaître la topologie exacte d'un interréseau.



◆ Un routeur transmet périodiquement des copies de sa table de routage aux routeurs voisins et cumule les vecteurs de distance

1.1. Découverte d'un réseau à vecteur de distance

Chaque entrée de la table de routage pour chaque réseau correspond à un vecteur de distance cumulé, qui indique la distance au réseau dans une direction donnée. Chaque réseau directement connecté à un routeur à une valeur de 0 et ainsi de suite.

1.2. Mise à jour des tables de routage

- Les mises à jour s'effectuent de *routeurs en routeurs*.
- Les mises à jour s'effectuent *périodiquement*.
- Les mises à jour consistent en des envois des *tables entières*.
- Les mises à jour sont envoyées à *l'adresse de diffusion (broadcast) 255.255.255.255*

2. Le problème des boucles de routage (routing loops) et mesure infinie (counting to infinity).

Une boucle de routage est une route diffusée pour des paquets qui n'atteignent jamais leur destination : ils passent de façon répétée par la même série de nœuds de réseau. Ce phénomène est dû à une convergence lente des informations de routage. Un routeur éloigné fait croire à des routeurs bien informés d'une route modifiée qu'il dispose d'une nouvelle route (à coût plus élevé) vers ce réseau.
Une métrique de mesure infinie est le résultat d'une boucle de routage qui engage les routeurs à incrémenter à l'infini la métrique de mesure.

3. Solutions

- Définir un **nombre maximum de sauts**
- **Route poisoning :** lorsqu'une route vers un réseau tombe, le réseau est immédiatement averti d'une métrique de distance infinie (le maximum de sauts +1), plus aucune incrémentation n'est possible.
- **Split horizon :** puisque toutes les interfaces d'un routeur sont censées envoyer des mises à jour de routage, le mécanisme Split horizon empêche à un routeur d'envoyer des informations (de métrique plus élevée) à travers l'interface de laquelle elle a appris l'information.
- **Compteur de retenue (Holddown Timer) :** Après avoir retenu qu'une route vers un réseau est tombée, le routeur attend une certaine période de temps avant de croire n'importe quelle autre information de routage à propos de ce réseau.

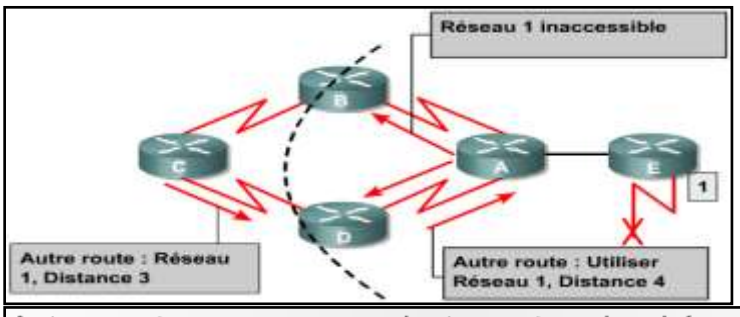
Si l'information d'une route tombée redevenant accessible est apprise du même voisin endéans le délai, la route est réinscrite dans la table de routage. Si l'information d'une route de nouveau accessible provient d'un autre voisin avec une meilleure métrique, la route est réinscrite dans la table de routage et le compteur est arrêté.

- **Triggered Update :** Une mise à jour est envoyée immédiatement plutôt qu'avant l'expiration du compteur lorsque une route est tombée. Utilisée avec la mesure de métrique infinie , cette solution assure que tous les routeurs ont la connaissance des routes tombées avant que n'importe quel compteur expire.
- **Split Horizon avec Poison Reverse :** le protocole de routage avertit de toutes les routes sortant d'une interface, mais celles qui ont été apprises d'une mise à jour plus récente venant dans cette interface sont marquée d'une métrique de distance infinie.

Des boucles de routage peuvent apparaître lorsque des tables de routage incohérentes ne sont pas mises à jour en raison d'une convergence plus lente dans un environnement réseau changeant. Juste avant la panne du réseau 1, tous les routeurs disposent d'une base de connaissances cohérente et de tables de routage correctes. On dit alors que le réseau a convergé. Pour la suite de cet exemple, supposons que le meilleur chemin du routeur C vers le réseau 1 passe par le routeur B et que la distance entre le routeur C et le réseau 1 soit égale à 3.

Lorsque le réseau 1 tombe en panne, le routeur E envoie une mise à jour au routeur A. Ce dernier cesse d'acheminer des paquets vers le réseau 1, mais les routeurs B, C et D continuent de les acheminer car ils n'ont pas encore été informés de la panne. Lorsque le routeur A transmet sa mise à jour, les routeurs B et D cessent d'acheminer des paquets vers le réseau 1. Toutefois, le routeur C n'a toujours pas reçu de mise à jour. Pour lui, le réseau 1 est toujours accessible via le routeur B.

À présent, le routeur C envoie une mise à jour périodique au routeur D pour lui indiquer un chemin vers le réseau 1 passant par le routeur B. Le routeur D modifie sa table de routage pour refléter cette information erronée et la transmet au routeur A. Ce dernier la transmet à son tour aux routeurs B et E, et ainsi de suite. Tous les paquets destinés au réseau 1 génèrent alors une boucle à partir du routeur C vers les routeurs B, A et D, qui revient au routeur C.



Autres routes, convergence lente, routage incohérent

7.1.4 Élimination des boucles de routage grâce à la fonction split horizon

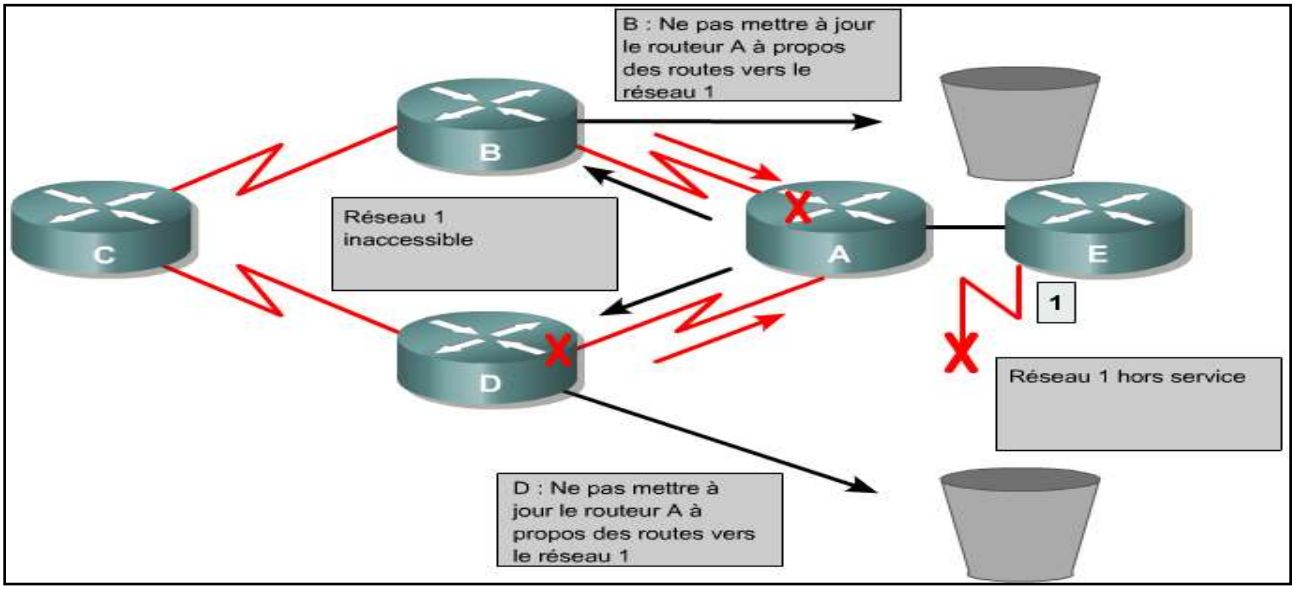
Une boucle de routage peut également se créer lorsqu'un routeur reçoit des informations erronées qui contredisent les informations correctes qu'il a envoyées initialement. Ce problème survient de la façon suivante:

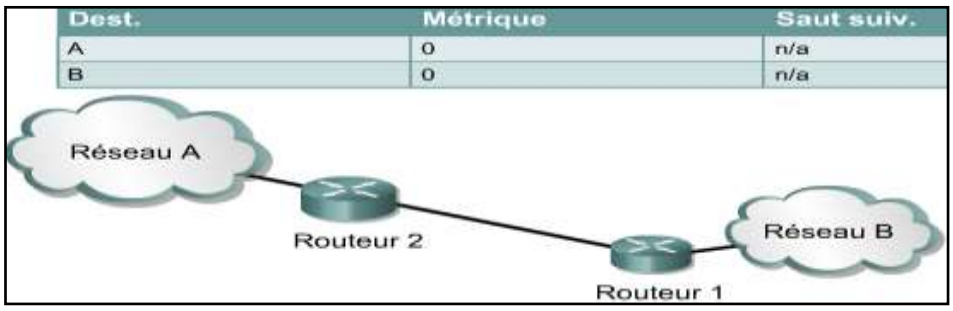
- Le routeur A transmet une mise à jour aux routeurs B et D indiquant que le réseau 1 est arrêté. Cependant, le routeur C transmet une mise à jour au routeur B indiquant que le réseau 1 est disponible à une distance de 4, via le routeur D. Ce chemin ne transgresse pas les règles de la solution split horizon.

- Le routeur B en conclut, à tort, que le routeur C dispose toujours d'un chemin valide vers le réseau 1, bien que la métrique soit beaucoup moins favorable. Le routeur B transmet une mise à jour au routeur A pour lui indiquer la nouvelle route jusqu'au réseau 1.

- Le routeur A détermine maintenant qu'il peut envoyer des paquets au réseau 1 via le routeur B. Ce dernier détermine qu'il peut les envoyer au réseau 1 via le routeur C, et celui-ci détermine qu'il peut les envoyer au réseau 1 via le routeur D. Tous les paquets introduits dans cet environnement tourneront en boucle entre les routeurs.

- La solution split horizon tente d'éviter cette situation. Si une mise à jour de routage relative au réseau 1 arrive du routeur A, le routeur B ou D n'est pas en mesure de renvoyer au routeur A les informations relatives au réseau 1. La solution split horizon réduit ainsi les informations de routage erronées, ainsi que la charge de routage.



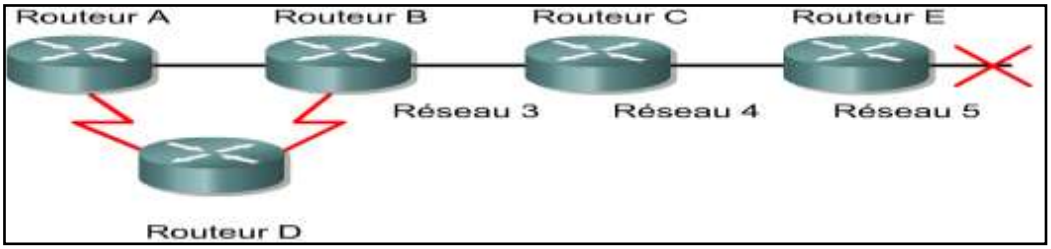


En " split-horizon " simple, les mises à jour de routage envoyées par un routeur à son voisin ne contiennent pas les informations qui ont été précédemment apprises grâce à ce routeur voisin. Supposons, par exemple, que le routeur 1 annonce qu'il connaît une route vers le réseau A. Le routeur 2 reçoit la mise à jour du routeur 1 et insère cette information sur le réseau A dans sa table de routage. Lors des mises à jour régulières des informations de routage envoyées au routeur 1, le routeur 2 n'inclura pas l'entrée concernant le réseau A, puisque c'est ce routeur 1 qui lui avait indiqué une route vers ce réseau A.

7.1.5 Mode poison reverse

Le mode « poison reverse » est utilisé par différents protocoles à vecteur de distance afin d'éviter les grandes boucles de routage et d'offrir des informations explicites en cas d'inaccessibilité d'un sous-réseau ou d'un réseau. En règle générale, ce mode ajoute 1 au nombre maximal de sauts.

Le mode poison reverse constitue l'un des moyens d'éviter les mises à jour incohérentes. Lorsque le réseau 5 tombe en panne, le routeur E passe en mode poison reverse en créant une entrée de table de métrique 16 (inaccessible) pour ce réseau. De cette manière, le routeur C n'est plus susceptible de transmettre des mises à jour incorrectes concernant la route vers le réseau 5. Lorsqu'il reçoit un message poison reverse en provenance du routeur E, il renvoie à ce dernier une mise à jour poison reverse. Cela permet de s'assurer que toutes les routes du segment ont bien reçu les informations sur la route inaccessible.



Lorsque le réseau 5 tombe en panne, le routeur E passe en mode " poison reverse " en créant une entrée de table de métrique 16 (inaccessible).

Grâce au mode poison reverse et aux mises à jour déclenchées, le temps de convergence est plus rapide car les routeurs voisins n'ont pas à attendre 30 secondes avant d'annoncer la route inaccessible.

En mode poison reverse, un protocole de routage annonce les routes inaccessibles avec une métrique de mesure infinie. Ce mode n'est pas contraire aux règles split horizon. La méthode split horizon avec poison reverse consiste essentiellement à empêcher l'utilisation d'une route, mais elle concerne plus particulièrement les routes que les règles split horizon n'autoriseraient pas normalement pour la transmission des informations de routage. Dans chacun des cas, les routes inaccessibles sont annoncées avec des métriques de mesure infinie.

7.1.6 Comment empêcher les boucles de routage avec les mises à jour déclenchées

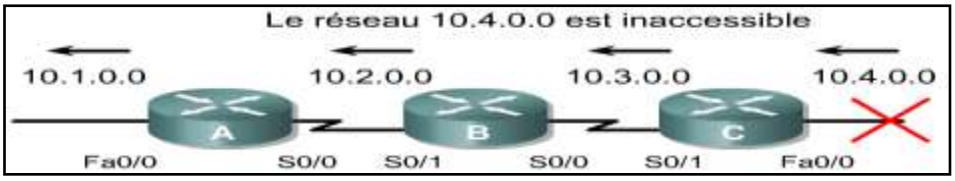
Les nouvelles tables de routage sont envoyées régulièrement aux routeurs voisins. Par exemple, les mises à jour RIP ont lieu toutes les 30 secondes. Toutefois, une mise à jour déclenchée est envoyée immédiatement en réponse à certaines modifications de la table de routage. Le routeur qui détecte une modification topologique envoie immédiatement un message de mise à jour aux routeurs adjacents qui, à leur tour, génèrent des mises à jour déclenchées pour signaler la modification à leurs routeurs voisins.

En cas d'échec d'une route, une mise à jour est envoyée immédiatement, sans attendre l'expiration du délai du compteur de mise à jour. Les mises à jour déclenchées, associées à la fonction poison reverse,

permettent de s'assurer que tous les routeurs ont connaissance des routes inaccessibles avant l'expiration du délai des compteurs de retenue.

Les mises à jour déclenchées continuent à envoyer des mises à jour en raison d'un changement des informations de routage, sans attendre l'expiration du délai du compteur. Le routeur envoie une autre mise à jour de routage sur ses autres interfaces, sans attendre l'expiration du délai du compteur de mise à jour de routage. Cela entraîne la transmission des informations relatives à l'état de la route qui a changé et le déclenchement plus rapide des compteurs de retenue sur les routeurs voisins. La vague de mises à jour se propage sur l'ensemble du réseau.

Le routeur C déclenche une mise à jour pour annoncer que le réseau 10.4.0.0 est inaccessible. Lorsqu'il reçoit cette information, le routeur B annonce l'indisponibilité de ce réseau via l'interface S0/1. Le routeur A envoie à son tour une mise à jour à partir de l'interface Fa0/0.



Avec le concept de mise à jour déclenchée, les routeurs envoient des messages dès qu'ils remarquent un changement dans leur table de routage.

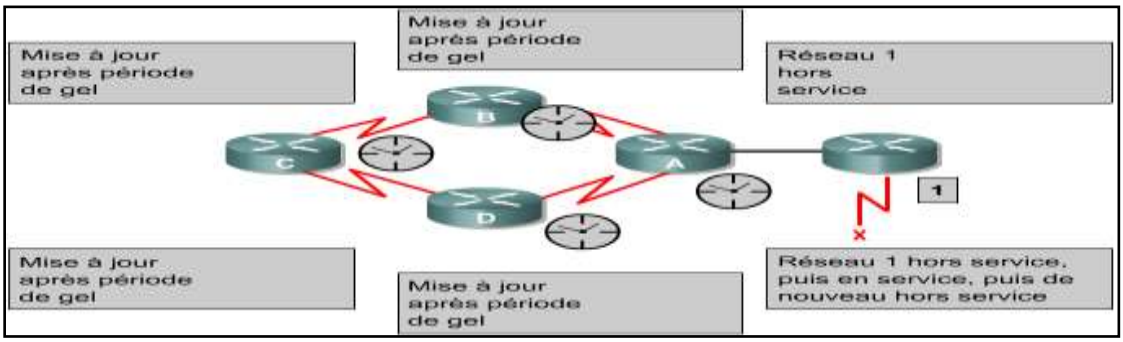
7.1.7 Comment éviter les boucles de routage grâce aux compteurs de retenue

L'utilisation de compteurs de retenue permet d'éviter les problèmes de métrique de mesure infinie:

- Lorsqu'un routeur reçoit une mise à jour d'un routeur voisin lui indiquant qu'un réseau auparavant accessible est devenu inaccessible, il marque la route comme étant inaccessible et déclenche un compteur de retenue. Si, avant l'expiration du délai de retenue, le routeur reçoit une mise à jour du même voisin indiquant que le réseau est de nouveau accessible, il marque le réseau comme étant accessible et désactive le compteur de retenue.

- Si une mise à jour provenant d'un autre routeur voisin indique une métrique meilleure que celle initialement enregistrée pour le réseau, le routeur marque le réseau comme étant accessible et désactive le compteur de retenue.

- Si, avant l'expiration du délai de retenue, une mise à jour provenant d'un autre routeur voisin indique une métrique inférieure, elle est ignorée. Le fait d'ignorer une telle mise à jour alors qu'un compteur de retenue est actif permet de disposer de plus de temps pour transmettre à l'ensemble du réseau les informations relatives à une modification perturbatrice.



Concevoir une architecture LAN en couche hiérarchique	> Expliquer l'intérêt du découpage en 3 couches hiérarchique dans une topologie réseau > Justifier l'utilisation de 1, 2 ou 3 couches en fonction de différents paramètres (cout, besoin, dimension, etc.) > Choisir le matériel adéquat en fonction de la couche où il sera installé
Proposer une solution de réseau sans fil sécurisée	> Connaitre les principales technologies qui concernent le WIFI (famille de normes 802.11) > Expliquer les principales technologies et chiffrements de sécurisation du WIFI (WEP, WPA, WPA2, RC4, AES, TKIP, EAP) > Configurer ces méthodes sur des matériels afin de les intégrer en production