Laboratoire SUPINFO des Technologies Cisco

CCNA 3 - Essentiel

Commutation et routage intermédiaire

Auteurs : TOURRES Grégoire, BODIN Laurent et VERNERIE Matthieu
Relecture : BODIN Laurent
Version 2.5 – 26 Octobre 2005

SUPINFO - Ecole Supérieure d'Informatique de Paris
23. rue de Château Landon 75010 Paris
Site Web : http://www.supinfo.com

Laboratoire SUPINFO des Technologies Cisco
Site Web : www.labo-cisco.com – E-mail : labo-cisco@supinfo.com

Table des matières

1. Routage Classless

1.1. Introduction au routage Classless

Au début des années 90, Internet subissait une croissance exponentielle annonçant un épuisement des adresses IPv4, notamment celles de classe B.

Cette pénurie d'adresse est principalement due au découpage fixe de l'espace d'adressage total IPv4 en classes (classe A, classe B, classe C) qui fige le nombre de réseaux possibles et le nombre d'hôtes maximum par réseau.

En effet, lorsque l'on utilise un **adressage classful,** les masques de sous-réseaux ne sont pas envoyés sur le réseau. Les équipements réseaux utilisent donc des masques de sous-réseaux par défaut qui sont les suivants :

- Classe A : 255.0.0.0 ou /8
- Classe B : 255.255.0.0 ou /16
- Classe C : 255.255.255.0 ou /24

Il est dans ce cas impossible de créer des sous-réseaux et de former des groupes d'utilisateur de différentes tailles au sein d'un réseau d'entreprise.

Ce problème est résolu avec l'utilisation d'un **adressage classless** (sans classe) qui permet d'envoyer le masque de sous-réseau utilisé aux autres équipements et de ce fait, de créer des sous-réseaux de taille variable.

Le CIDR et le VLSM sont des exemples de procédures utilisant un adressage classless. Bien que complémentaires, celles-ci sont différentes. Le VLSM peut d'ailleurs être vu comme une extension du CIDR au niveau d'une organisation.

Le VLSM permet en effet d'éviter le gaspillage d'adresse au sein d'une organisation en utilisant des masques de taille variable, tandis que le CIDR permet de diminuer significativement le nombre d'entrées des tables de routage en utilisant des agrégations de routes.

Il existe cependant des règles à suivre concernant la création et l'utilisation de sous-réseaux. Ces règles sont régies par les RFC 950 (règle du 2^n-2) et RFC 1878 (règles du 2^n-1 et du 2^n) :

- **Règle du 2^n - 2** → impossible d'utiliser le premier sous-réseau ainsi que le dernier sous-réseau
- **Règle du 2^n - 1** → impossible d'utiliser le premier sous-réseau
- **Règle du 2^n** → utilisation de tous les sous-réseaux

L'utilisation d'une de ces règles par rapport à une autre dépend uniquement des capacités techniques des équipements. De nos jours la majorité des réseaux utilisent la règle du 2^n puisqu'elle permet de limiter au maximum le gaspillage d'adresses IP.

1.2. CIDR

L'expansion d'Internet a entraîné l'augmentation de la taille des tables de routage sur de nombreux routeurs, notamment les routeurs des fournisseurs d'accès à Internet.

Pour alléger de manière considérable ces tables de routage, une solution permettant d'agréger plusieurs routes en une seule a dû être mise en place : c'est le principe du **CIDR** (Classless Inter-Domain Routing).

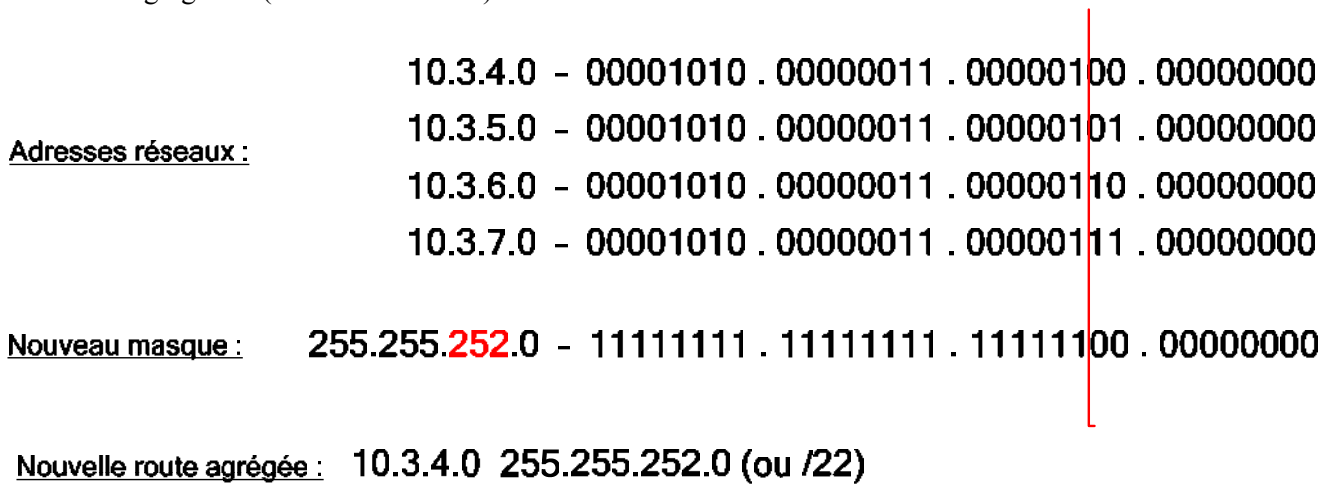
Pour ce faire, une comparaison binaire de l'ensemble des adresses à agréger est nécessaire. Il faut en effet arriver à déterminer les bits de la partie réseau qui sont en commun dans toutes ces adresses et mettre à zéro tous les bits restant.

De cette manière une délimitation entre la partie réseau commune et le reste de l'adresse sera effectuée. Celle-ci permettra de déterminer l'adresse agrégée ainsi que le nouveau masque de sous-réseau à utiliser.

L'exemple suivant illustre l'utilisation d'une agrégation de quatre adresses réseaux en une seule adresse. Il faut en effet agréger les 4 réseaux ci-dessous :

- 10.3.4.0 255.255.255.0 (ou /24)
- 10.3.5.0 255.255.255.0 (ou /24)
- 10.3.6.0 255.255.255.0 (ou /24)
- 10.3.7.0 255.255.255.0 (ou /24)

Processus d'agrégation (ou summarization) de routes en une seule :



Cependant l'emploi de CIDR n'est possible que si :

- Le protocole de routage utilisé transporte les préfixes étendus dans ses mises à jour.
- Les routeurs implémentent un algorithme de la correspondance la plus longue.
- Un plan d'adressage hiérarchique est appliqué pour l'assignation des adresses afin que l'agrégation puisse être effectuée.
- Les hôtes et les routeurs supportent le routage classless.

1.3. VLSM

L'utilisation du masque de sous-réseau à taille variable (**V**ariable **L**ength **S**ubnet **M**ask) permet à un réseau classless d'utiliser différents masques de sous-réseaux au sein d'une organisation et d'obtenir par conséquent des sous-réseaux plus appropriés aux besoins.

Cependant, certaines conditions sont requises pour utiliser le VLSM :

- Il est nécessaire d'employer un protocole de routage supportant le VLSM. **RIPv.2**, **OSPF**, **IS-IS**, **EIGRP, BGP** ainsi que le **routage statique** supportent VLSM. Les protocoles de routage classless, contrairement aux protocoles de routage classful (RIPv.1, IGRP), transmettent dans leurs mises à jour de routage, le masque de sous-réseau pour chaque route.

- Les routeurs doivent implémenter un algorithme de la correspondance la plus longue. En effet, les routes qui ont le préfixe le plus élevé sont les plus précises. Les routeurs dans leurs décisions d'acheminement doivent être capables de déterminer la route la plus adaptée aux paquets traités.

- Un plan d'adressage hiérarchique doit être appliqué pour l'assignation des adresses afin que l'agrégation puisse être effectuée.

VLSM repose sur l'agrégation. C'est-à-dire que plusieurs adresses de sous-réseaux sont résumées en une seule adresse. L'agrégation est simple, l'on retient simplement la partie commune à toutes les adresses des sous-réseaux.

Pour conceptualiser un réseau conforme VLSM, il faut:

- Recenser le nombre total d'utilisateurs sur le réseau (prévoir une marge pour favoriser l'évolutivité du réseau).
- Choisir la classe d'adresse la plus adaptée à ce nombre.
- Partir du plus haut de l'organisation (couche principale) et descendre au plus près des utilisateurs (couche accès).
- Décompter les entités au niveau de chaque couche. Par exemple, les grandes agglomérations, avec pour chaque agglomération, les villes, le nombre de bâtiments dans chaque ville, le nombre d'étages par bâtiment et le nombre d'utilisateur par étage.
- Pour chacune de ces entités, réserver le nombre de bits nécessaire en prévoyant l'évolutivité du réseau.
- Calculer le masque de sous-réseau à chaque niveau de l'organisation.

1.4. Procédure de réalisation

Les procédures de réalisation de plan d'adressage avec du VLSM symétrique puis asymétrique sont expliquées. Néanmoins, il faut savoir que le VLSM symétrique n'est qu'une étude de cas scolaire et que le VLSM asymétrique est ce qui est réellement utilisé dans la réalité.

1.4.1. VLSM Symétrique

Le VLSM symétrique est un plan d'adressage qui fait un découpage récursif du la topologie du réseau de l'entreprise sachant que les différents découpages sont similaires.
Exemple : si l'entreprise a deux bâtiments par ville, on devra avoir deux bâtiments dans chaque ville.

Dans cette procédure, on parle de sous réseau uniquement pour les parties les plus proches des utilisateurs. Tous les autres niveaux de la hiérarchie seront considérés comme une adresse agrégée.

Procédure :

- **Etape 1 : Identifier le besoin :**
Recenser les différents niveaux hiérarchiques de l'entreprise et dessiner la topologie.

- **Etape 2 : Au niveau utilisateur :**
Connaître la taille du sous-réseau.

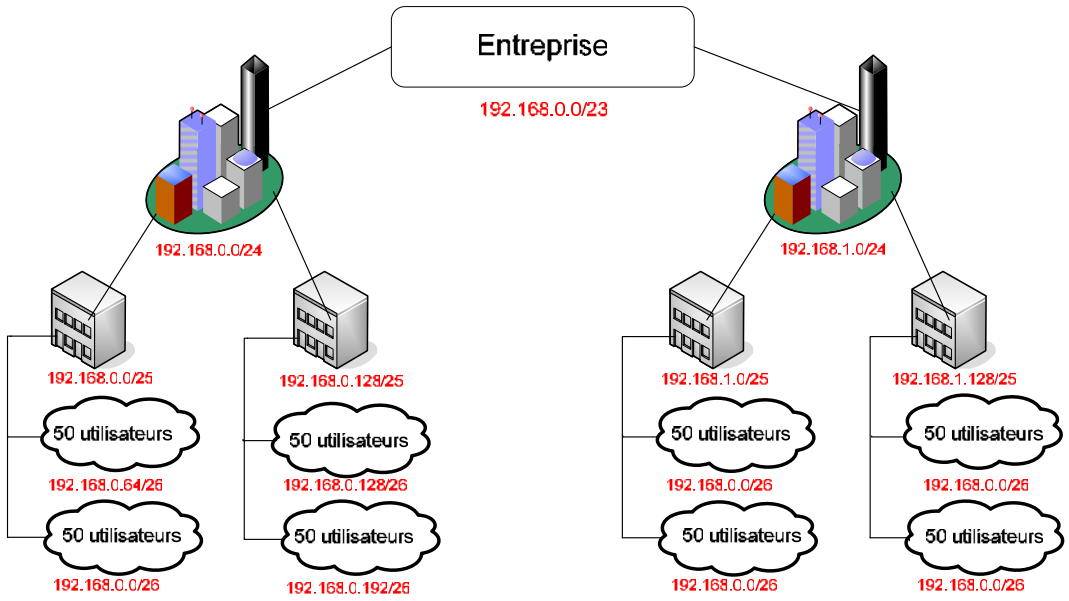
- **Etape 3 : Recensement :**
Déterminer le nombre de bits nécessaires pour recenser chaque instance du niveau hiérarchique.

- **Etape 4 : Classe d'adresse utilisée :**
Déterminer la classe d'adresse ou l'agrégat d'adresses (le choix dépendant du contexte), en additionnant tous les bits nécessaires pour identifier chaque niveau hiérarchique de l'entreprise.

- **Etape 5 :**
On procède ensuite au découpage de la classe d'adresse de l'entreprise et de l'attribution à chaque instance du niveau hiérarchique.

Cette procédure est valable quelque soit la méthode d'adressage utilisée (RFC 950 ou 1878) à une différence prêt, si on applique la règle du 2^n-1 ou 2^n-2, il faudra l'appliquer une seule fois sur toute la topologie au niveau hiérarchique limitant la perte (induit par le nombre de bits de ce niveau hiérarchique).

Exemple :



Etape 1 : Une entreprise dans deux villes. Deux bâtiments par ville. Deux étages par bâtiment. 50 utilisateurs par étage.
Etape 2 : 50 utilisateurs / sous-réseau +1 adresse pour le broadcast +1 adresse pour le réseau +1 adresse pour la passerelle = 53 adresses IP.
Etape 3 : 2^x >=53 x=6 Il faut donc 6 bits par sous-réseau soit un /26 (255.255.255.192)
Etape 4 : Dans ce contexte, on peut découper une classe B (beaucoup de gaspillage) ou agréger plusieurs classe C. On choisira une classe C
Etape 5 : Chaque instance du niveau hiérarchique se voit attribuer un préfixe et un masque. (en rouge sur le dessin)

1.4.2. VLSM Asymétrique

Le VLSM Asymétrique, ou plus simplement, VLSM, correspond à une topologie d'entreprise ou les différents niveaux hiérarchiques et les instances ne sont pas similaires (nombre, taille etc.)

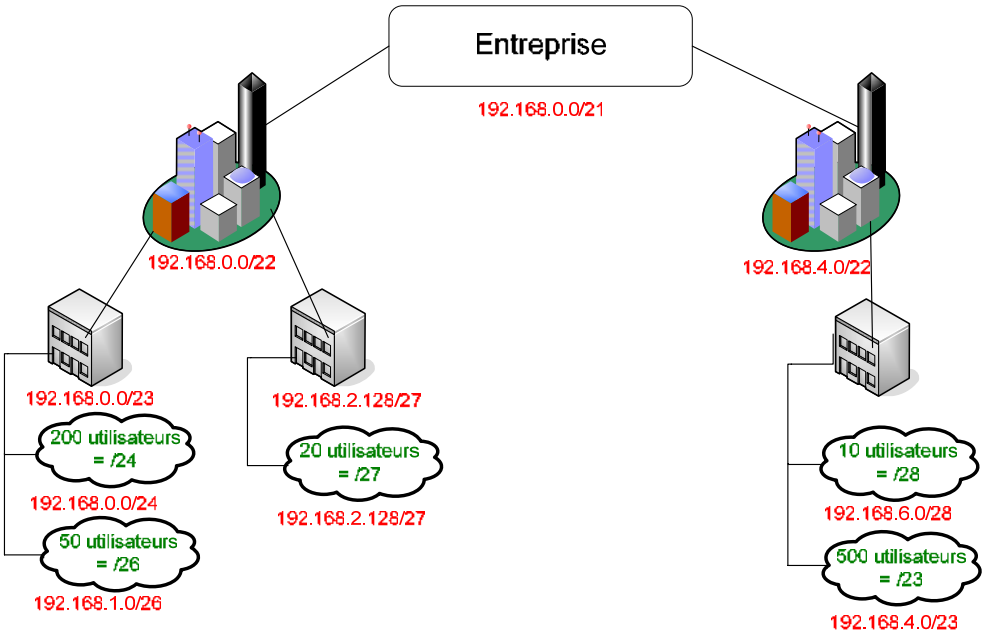
Procédure :

- **Etape 1 : Identifier le besoin :**
Dessiner la topologie, identifier les besoins a chaque niveau hiérarchique.

- **Etape 2 : Recensement :**
Connaître le nombre d'utilisateurs pour chaque sous-réseau (puisqu'ils peuvent être différents à chaque niveau maintenant), ce qui revient à connaître la taille de chaque sous-réseau (ne pas oublier qu'on ne peut pas utiliser la première ni la dernière adresse et qu'il faut une adresse IP pour la passerelle).
Si le nombre d'utilisateur n'est pas connu a chaque niveau de la hiérarchie, on peut suivre un processus descendant ('top down') : repartir équitablement le nombre d'utilisateur pour un niveau hiérarchique supérieur vers le niveau directement inférieur.

- **Etape 3 : Classe d'adresse utilisée :**
Déterminer la classe d'adresse ou l'agrégat d'adresses (le choix dépendant du contexte), en additionnant tous les bits nécessaires pour identifier chaque niveau hiérarchique de l'entreprise.

- **Etape 4 :**
En suivant un processus remontant récursif maintenant, on va agréger les différents instances d'un niveau pour obtenir l'identifiant réseau du niveau hiérarchique directement supérieur jusqu'a obtenir l'adresse agrégée de toute l'entreprise.



Etape 1 : Une entreprise dans deux villes. Deux bâtiments dans la première ville, un seul bâtiment dans la deuxième ville. Tous les bâtiments ont deux étages sauf un qui en a qu'un seul. Le nombre d'utilisateur varie d'un étage a l'autre.

Etape 2 : Recensement (en vert). Ne pas oublier l'adresse pour le broadcast, l'adresse pour le réseau et l'adresse pour la passerelle.

Etape 3 : Dans ce contexte, on peut découper une classe B (beaucoup de gaspillage) ou agréger plusieurs classe C. On choisira une classe C

Etape 4 : En remontant, on adresse chaque étage, chaque bâtiment etc. (en rouge)

1.5. Configuration

Lorsque la règle du 2^n-1 est appliquée, il est convenu de ne pas utiliser le premier sous-réseau pour éviter toute confusion. En effet, l'adresse réseau du premier sous-réseau correspond à l'adresse réseau de toute la plage d'adresse.

Pour limiter le gaspillage d'adresse, en utilisant la règle du 2^n, il suffit d'utiliser la commande **ip subnet-zero** qui permet l'utilisation du premier sous-réseau calculé. Cette fonctionnalité est active par défaut depuis la version 12.0 de l'IOS.

- **ip subnet-zero**
  - Mode de configuration globale
  - Permet d'utiliser le premier sous-réseau (2^n)

Par ailleurs, la commande **ip classless** active la prise en charge des informations ne respectant pas le découpage d'adresses en classes. C'est-à-dire qu'elle permet d'activer le support des masques de sous-réseau et d'une route par défaut. Cette commande est active par défaut.

- **ip classless**
  - Mode de configuration globale
  - Permet d'activer le support des masques de sous-réseau et d'une route par défaut

Lors de l'emploi du VLSM, il faut avant tout s'assurer du bon calcul des masques de sous-réseaux. Une fois cette étape effectuée nous pouvons configurer les interfaces.

- **interface {type} {numéro}**
  - Mode de configuration globale
  - Permet de passer dans le mode de configuration d'interface

- **ip address {IP} {masque}**
  - Mode de configuration d'interface
  - Permet d'attribuer une adresse IP à cette interface

2. Protocole RIPv2

2.1. Rappels sur RIPv1

RIPv1 est un protocole de routage intérieur classful, à vecteur de distance qui base ses décisions d'acheminement sur une métrique qui emploie essentiellement le nombre de saut. Le nombre maximum de saut est de 15.

- Il transmet des mises à jour de routage complètes toutes les 30 secondes. D'autre part, il lui faut entre 3 et 5 minutes pour converger. Le tableau suivant récapitule les principales caractéristiques de RIPv.1:
- RIPv1 est un protocole de routage intérieur (IGP).
- C'est est un protocole de routage à vecteur de distance
- Il utilise une métrique basée sur le nombre de saut.
- Toutes les 30 secondes, il diffuse sa mise à jour de routage par broadcast.
- RIPv1 a une convergence lente.
- Il utilise une métrique de mesure infini (maximum hop count), le split horizon ainsi que des compteurs de retenue (hold down timers) mais aussi le route poisoning pour limiter les effets des boucles de routage.
- RIPv1 est un protocole de routage classful et par conséquent ne supporte pas VLSM et CIDR.

2.2. Spécifications de RIPv2

RIPv2 est une version améliorée de son prédécesseur et partage donc certaines caractéristiques :

- Tous deux sont des IGP (Interior Gateway Protocol).
- RIPv1 et RIPv2 sont des protocoles de routage à vecteur de distance.
- Ils utilisent une métrique basée sur le nombre de saut.
- Ils emploient un nombre maximum de saut, des compteurs de retenue d'on la valeur est fixé à 180s par défaut, ainsi que le split horizon et le route poisoning pour limiter les effets de boucles de routage.
- Leur configuration est aisée.

RIPv2 apporte également des fonctionnalités supplémentaires tels que :

- Le support du routage classless.
- La diffusion du masque réseau dans les mises à jour de routage.
- Le support de VLSM.
- La diffusion des mises à jour de routage par multicast avec l'adresse de classe D 224.0.0.9.
- L'authentification de la source de la mise à jour de routage par un texte en clair **(actif par défaut)**, ou un texte crypté suivant l'algorithme MD5 (Message-Digest 5).
- L'utilisation d'indicateurs de route externe **(route tag)** afin de pouvoir différencier les routes apprises d'autre protocole de routage et redistribué dans RIP.

2.3. Configuration

2.3.1. Commandes générales

- **router rip**
  - Mode de configuration globale
  - Active le protocole RIP.

- **version 2**
  - Mode de configuration du protocole de routage
  - Permet d'utiliser RIPv2 à la place de RIPv1

- **network {adresse réseau}**
  - Mode de configuration du protocole de routage
  - Permet d'indiquer les réseaux directement connectés au routeur.

- **ip default-network {adresse réseau}**
  - Mode de configuration du protocole de routage
  - Permet de spécifier une route par défaut.

- **default-information originate**
  - Mode de configuration du protocole de routage
  - Permet de propager la route par défaut dans les mises à jour de routage.

- **no auto-summary**
  - Mode de configuration du protocole de routage
  - Désactive l'auto-agrégation.

2.3.2. Authentification

- **key-chain {nom}**
  - Mode de configuration globale
  - Permet d'identifier un groupe de clef d'authentification.

- **key {id}**
  - Mode de configuration de clé
  - Permet de créer une clef dans un groupe de clef. L'identifiant de clef peut prendre une valeur de 0 à 2147483647. L'identifiant de clef peut ne pas être consécutif.

- **key-string {mot de passe}**
  - Mode de configuration de clé
  - Permet de définir un mot de passe pour une clef.

- **ip rip authentication key-chain {nom}**
  - Mode de configuration d'interface
  - Active l'authentification RIP sur une interface

- **ip authentication mode {text | md5}**
  - Mode de configuration d'interface
  - Permet de spécifier le type d'authentification en clair ou crypté.

3. Protocole OSPF

3.1. Caractéristiques

Le protocole **OSPF** (Open Shortest Path First) est un protocole de routage à état de lien crée en 1988 par l'IETF (RFC 2328). C'est à l'heure actuelle l'**IGP** (Interior Gateway Protocol) le plus répandu. OSPF est un protocole libre.

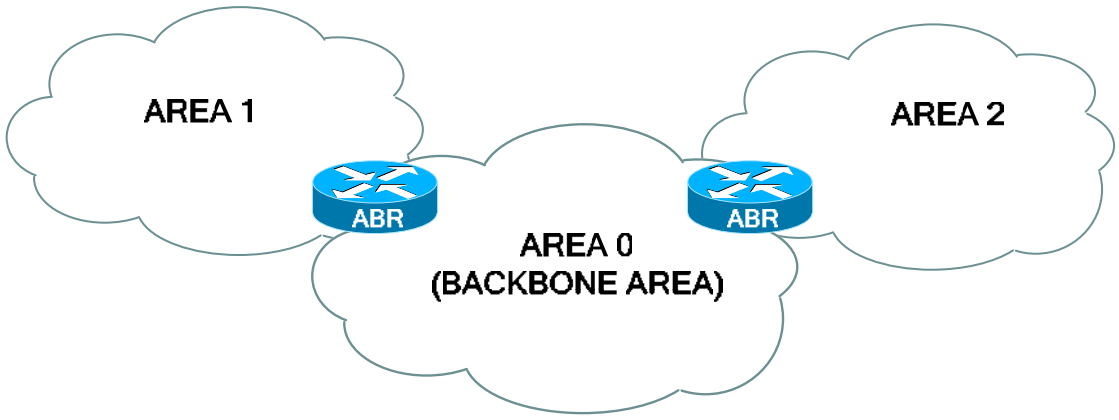
Principales caractéristiques d'OSPF :

- Emission des mises à jour déclenchées par modification(s) topologique(s).
- Connaissance exacte et complète de la topologie du réseau.
- Chaque nœud connaît l'existence de ses voisins adjacents.
- Utilisation d'un arbre du plus court chemin d'abord (SPF Tree) et d'un algorithme du plus court chemin d'abord (Algorithme SPF appelé aussi l'algorithme de Dijkstra) pour générer la table de routage.
- Envoi des mises à jour topologiques via une adresse multicast et non broadcast.
- Utilisation moindre de la bande passante
- Protocole de routage classless supportant le VLSM.
- Requiert des routeurs plus puissants.
- Domaines de routage exempts de boucles de routage
- Métrique utilisée : le coût (chaque liaison a un coût).
- Détermination et utilisation d'un ou plusieurs domaines de routage appelés Areas (ou aires) au sein d'un même système autonome (AS).

Les interfaces OSPF distinguent quatre types de réseaux :

- Les réseaux multi-accès broadcast comme Ethernet.
- Les réseaux point-à-point.
- Les réseaux multi-accès non broadcast ou encore Nonbroadcast multi-access (NBMA), tel que Frame Relay.
- Les réseaux point-à-multipoint configuré manuellement par un administrateur

L'établissement de la base de données topologique, ainsi que le calcul du plus court chemin d'abord impose une grande charge de traitements pour chaque routeur. Pour diminuer la taille de la base donnée topologique, les routeurs peuvent être regroupés en plusieurs aires (**area**) au sein d'un même système autonome (**SA**). On parle alors de **multiple area OSPF** (voir schéma ci-dessous)**,** mais le cursus CCNA 3 ne s'attarde que sur l'emploi de **single area OSPF**.



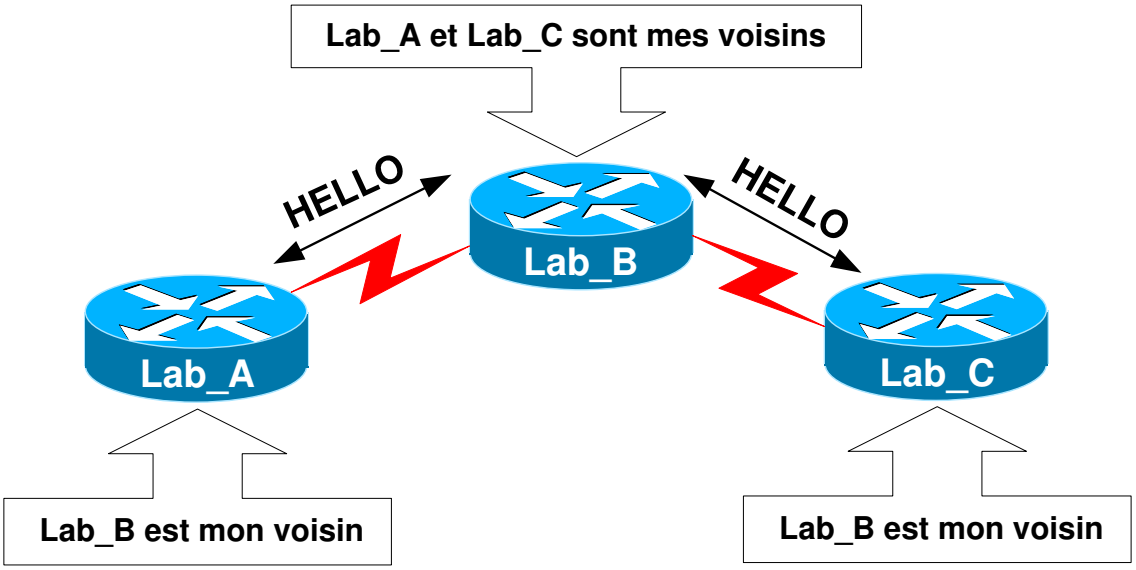
3.2. Définitions

- **Neighbor**
  - Routeur voisin sur le même réseau.
- **HELLO**
  - Protocole permettant la découverte et le maintient de liens entre les voisins. Les paquets HELLO sont transmis toutes les 10s pour un réseau de type broadcast multi-access et toutes les 30s pour un réseau de type NBMA.
- **LSU**
  - Paquet de mise à jour de données topologique. Permet d'avoir des informations sur l'évolution topologique du réseau.
- **LSA**
  - Contenu dans les LSUs ils permettent d'avertir qu'une modification topologique à lieu.
- **SPF tree**
  - L'arbre du plus court chemin d'abord résultant de l'application de l'algorithme de Dijkstra.
- **Algorithme de Dijkstra**
  - L'algorithme de Dijkstra (ou algorithme SPF), publié par le scientifique allemand du même nom en 1959 est utilisé pour le calcul de l'arbre du plus court chemin d'abord.
- **Adjacencies database**
  - Base de données contenant les informations relatives aux voisins.
- **Topological database**
  - Base de données qui contient toutes les informations sur la topologie du réseau.
- **Routing table**
  - Table de routage avec les meilleures routes à destination de tous les sous-réseaux de la topologie.
- **Flooding**
  - Processus qui consiste à envoyer par tous les ports.
- **DR (Designated Router)**
  - Routeur élu pour centraliser toutes les informations topologiques.
- **BDR (Backup Designated Router)**
  - Routeur élu pour prendre le relais du DR en cas de panne.
- **NBMA (Non Broadcast Multi-access)**
  - Réseau multi-accès Non broadcast tel que Frame Relay.
- **ABR (Area Border Router)**
  - Routeur situé à la bordure d’une ou plusieurs aires.

3.3. Fonctionnement dans un réseau ne comportant qu'une aire

3.3.1. Découverte des routeurs voisins

Avant tout échange d'informations de données topologiques, le routeur implémentant OSPF doit s'assurer qu'il existe d'autres routeurs adjacents à celui-ci qui utilisent eux aussi OSPF. Ces routeurs adjacents sont appelés des « voisins » et chacun d'entre eux peut être voisin d'un ou de plusieurs routeurs.



Pour découvrir leurs voisins, chaque routeur utilisant OSPF comme protocole de routage va devoir recourir au protocole **HELLO** qui permet d'établir et de maintenir un échange avec les routeurs voisins.

Celui-ci va permettre à chaque routeur d'envoyer des paquets HELLO à intervalles réguliers sur chacune de leurs interfaces en utilisant l'adresse multicast **224.0.0.5**. Les voisins découverts seront ensuite enregistrés dans une base de données de voisinage appelée **Neighbor Database**.

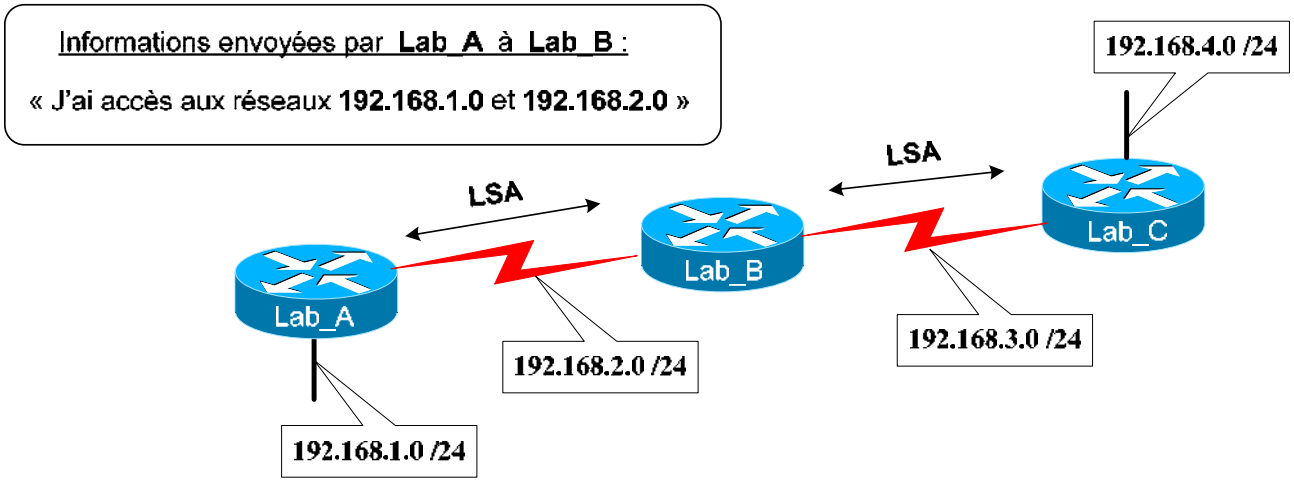
3.3.2. Etablissement des bases de données topologiques

3.3.2.1. Dans un réseau point-à-point

Une fois que chaque routeur a appris l'existence de ses voisins, il va leur envoyer les informations concernant tous les réseaux directement connectés à celui-ci.

Ces informations envoyées vont permettre à chaque nœud de mettre rapidement à jour leur base de données topologique (**Topological Database**) et d'obtenir ainsi une connaissance complète de la topologie réseau.

Ces mises à jour topologiques, déclenchées à l'initialisation du protocole OSPF sur les routeurs et par la suite lors de chaque modification topologique, se font grâce à l'envoi de paquets LSU (Link State Update) contenant des LSA (Link State Advertisement) comme le montre le schéma ci-dessous.



3.3.2.2.Dans un réseau multi-accès

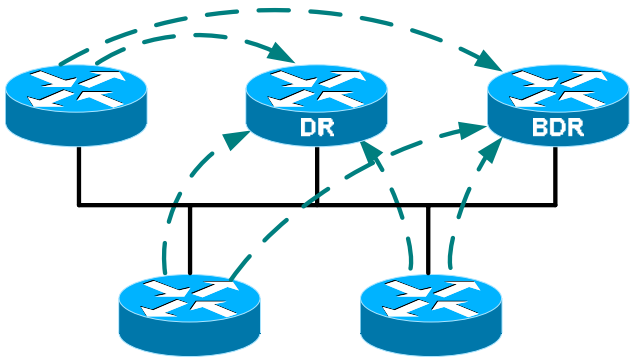
Les réseaux multi-accès fonctionnent suivant le même principe que les réseaux point-à-point à la différence que dans les réseaux multi-accès tous les routeurs sont voisins.

Cela pose cependant un problème puisque chaque routeur maintient un lien avec tous ses voisins pour l'échange d'informations topologiques. Par conséquent plus il y a de routeurs sur le réseau, plus ces derniers sont sollicités à envoyer des paquets de mises à jour topologiques.

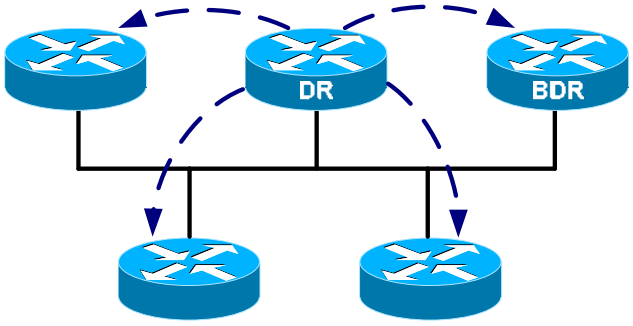
Pour palier à ce problème, le protocole HELLO va élire un **DR** (Designated Router) qui sera chargé de centraliser toutes les informations de modifications topologiques et de les retransmettre par la suite à tous les autres routeurs.

Il y aura ensuite l'élection d'un **BDR** (Backup Designated Router) servant de secours au cas où le DR ne pourrait plus assurer son rôle.

Tous les routeurs transmettront donc leurs informations topologiques au DR (ainsi qu'au BDR) en utilisant l'adresse multicast 224.0.0.6, tandis que le DR redistribuera ces informations avec l'adresse multicast 224.0.0.5 à tous les autres routeurs comme indiqué ci-dessous.



Envoi de paquets LSA au DR et au BDR en utilisant l'adresse multicast 224.0.0.6



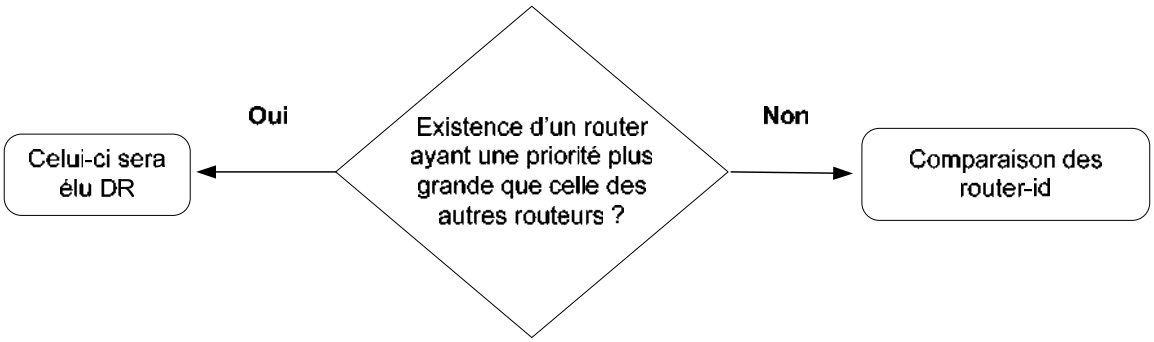
Envoi de paquets LSA à tous les routeurs en utilisant l'adresse multicast 224.0.0.5

3.4. Opérations OSPF

3.4.1. Election du DR / BDR

Un routeur doit répondre à plusieurs critères pour être désigné DR dans le réseau multi-accès. L'élection se fait grâce aux paquets HELLO qui contiennent l'ID du routeur et une priorité.

Lors du processus d'élection, le routeur ayant la plus grande priorité sur le réseau multi-accès sera élu DR. Dans le cas d'une égalité des priorités, les routeurs devront comparer leur router-id. Le routeur qui aura dans ce cas le plus grand router-id sera élu DR.



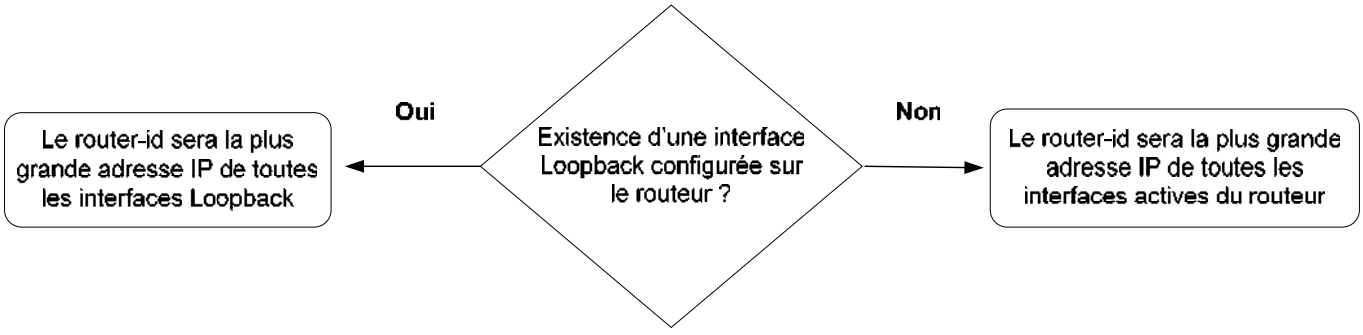
Une fois le DR désigné, le processus d'élection devra ensuite déterminer le BDR, correspondant au routeur ayant la deuxième plus haute priorité ou le deuxième plus grand router-id sur le réseau multi-accès.

3.4.2. Détermination du Router-ID

Lorsqu'une instance OSPF est initialisée, un identifiant de routeur appelé router-id est déterminé. Ce router-id n'est autre qu'une adresse IP qui servira d'identifiant à un routeur sur les réseaux auxquels il est raccordé.

Le router-id est déterminé selon les critères suivant :

- S'il y a présence d'une ou plusieurs interfaces Loopback sur le routeur, son router-id correspondra à la plus grande adresse IP de toutes les interfaces Loopback configurées sur celui-ci.
- Si aucune interface Loopback n'est présente sur le routeur alors son router-id sera la plus grande adresse IP de toutes les interfaces actives configurées sur celui-ci.



Pour fonctionner, un processus OSPF nécessite qu'il y ait au moins une interface active configurée sur le routeur. Il est donc conseillé, pour éviter toute interruption du processus OSPF, de faire usage des interfaces Loopback lorsque l'on configure ce protocole de routage sur un équipement.

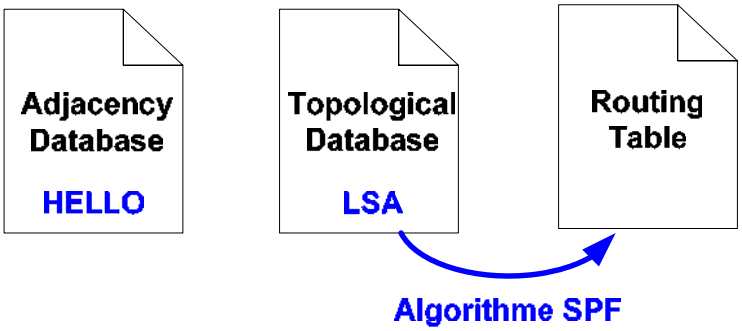
3.5. Construction de la table de routage

Une fois que tous les routeurs ont convergé, c'est-à-dire qu'ils ont tous la même vu complète du réseau, chacun d'entre eux va construire, à partir de sa base de données topologique, un arbre du plus court chemin d'abord (**SPF Tree**).

Cette construction va être réalisée grâce à l'algorithme **SPF** (Shortest Path First), aussi appelé l'algorithme de Dijkstra, qui va parcourir la base de données topologique et considérer chaque routeur comme étant des sommets reliés par des liens point-à-point. Le routeur qui l'implémente sera placé à la racine de l'arbre du plus cours chemin d'abord.

La métrique utilisée par OSPF étant le coût, calculée par les composants Cisco à l'aide de la formule suivante : **coût=10^8/bande passante** (s'exprime en bps), chaque lien va donc avoir un coût. La métrique d'une route est par conséquent calculée en faisant la somme de la bande passante de chaque lien de la route.

L'algorithme de Dijkstra va parcourir ensuite cet arbre du plus court chemin afin de déterminer les meilleures routes pour atteindre chaque réseau de destination (routes dont le coût est le plus bas). Ces routes seront ensuite ajoutées à la table de routage.



Au niveau de la table de routage, chaque route apprise par le protocole de routage OSPF se manifestera par la lettre « O » devant celle-ci et aura une distance administrative de 110.

3.6. Commandes

3.6.1. Commandes générales

- **router ospf {id de processus}**
  - Mode de configuration globale
  - Active le protocole OSPF.
  - Plusieurs processus peuvent être lancés sur un routeur.

- **network {préfixe}**
  - Mode de configuration du routeur
  - Permet de spécifier les réseaux devant participer au processus de routage.
  - Le préfixe doit être un réseau directement connecté au routeur

- **interface loopback {number}**
  - Mode de configuration globale
  - Permet de créer une interface logique.

- **bandwidth**
  - Mode de configuration d'interface
  - Permet de spécifier la bande passante sur l'interface.

- **ip ospf priority {number}**
  - Mode de configuration d'interface
  - Permet de modifier la priorité d'une interface pour l'élection du DR.
  - La valeur peut aller de 0 à 255. Attention, une priorité de 0 empêche le routeur d'être élu DR.

- **ip ospf cost {number}**
  - Mode de configuration d'interface
  - Permet de spécifier la valeur du coût.

3.6.2. Authentification

- **area {numéro de l'aire} authentication**
  - Mode de configuration du routeur
  - Active l'authentification OSPF pour le mot de passe en clair.

- **area {numéro de l'aire} authentication message-digest**
  - Mode de configuration du routeur
  - Active l'authentification pour le mot de passe encrypté.

- **ip ospf message-digest-key {key-id} md5 {type d'encryption}**
  - Mode de configuration d'interface
  - Permet l'encryption du mot de passe.

- **ip ospf authentication-key {mot de passe}**
  - Mode de configuration d'interface
  - Spécifie le mot de passe utilisé pour générer les données d'authentification de l'entête de paquets OSPF.

3.6.3. Timers

- **ip ospf hello-interval {intervalle}**
  - Mode de configuration d'interface
  - Définit la fréquence d'émission des paquets HELLO.

- **ip ospf dead-interval {intervalle}**
  - Mode de configuration d'interface
  - Définit la durée pendant laquelle un lien sera considéré comme actif, après que le routeur est reçu un paquet HELLO d'un routeur voisin.

3.6.4. Commandes show associées

- **show ip ospf interface**
  - Mode privilégié
  - Permet d'afficher la priorité de l'interface.

- **show ip protocols**
  - Mode privilégié
  - Affiche les informations sur les protocoles de routage configurés sur le routeur.

- **show ip route**
  - Mode privilégié
  - Affiche la table de routage du routeur.

- **show ip ospf**
  - Mode privilégié
  - Affiche la durée pendant laquelle le protocole est activé, ainsi que la durée durant laquelle il n'y a pas eu de modification topologique.

- **show ip ospf neighbor detail**
  - Mode privilégié
  - Affiche une liste détaillée des voisins, leur priorité et leur statut.

- **show ip ospf database**
  - Mode privilégié
  - Affiche le contenu de la base de données topologique (router-Id, process-Id).

4. Protocole EIGRP

4.1. Caractéristiques

EIGRP (Enhanced IGRP), protocole propriétaire Cisco, est une version améliorée d'IGRP qui utilise la même technologie à vecteur de distance. Les améliorations portent principalement sur :

- Les propriétés de convergence
- L'efficacité des opérations du protocole

Les changements apportés correspondent à beaucoup des caractéristiques des protocoles de routage à état des liens, et ont pour buts de faciliter l'évolutivité et d'accélérer le temps de convergence des réseaux. De ce fait, il est référencé dans la catégorie des protocoles de routage hybride, ou, d'après Cisco, à vecteur de distance évolué.

Les caractéristiques principales d'EIGRP sont :

- Protocole de routage Classless, avec support du VLSM
- Algorithme DUAL
- Mises à jour incrémentales, avec adressage multicast, et de façon fiable (via RTP)
- Utilisation de la bande passante réduite par rapport à IGRP
- Utilisation d'une métrique composite
- Découverte de voisins
- Principe de successeur, avec de multiples FS
- Agrégation de routes manuelle
- Etat des routes (Active et Passive)
- Partage de charge entre chemins n'ayant pas les mêmes métriques
- Compatibilité avec IGRP
- Distance administrative de 90

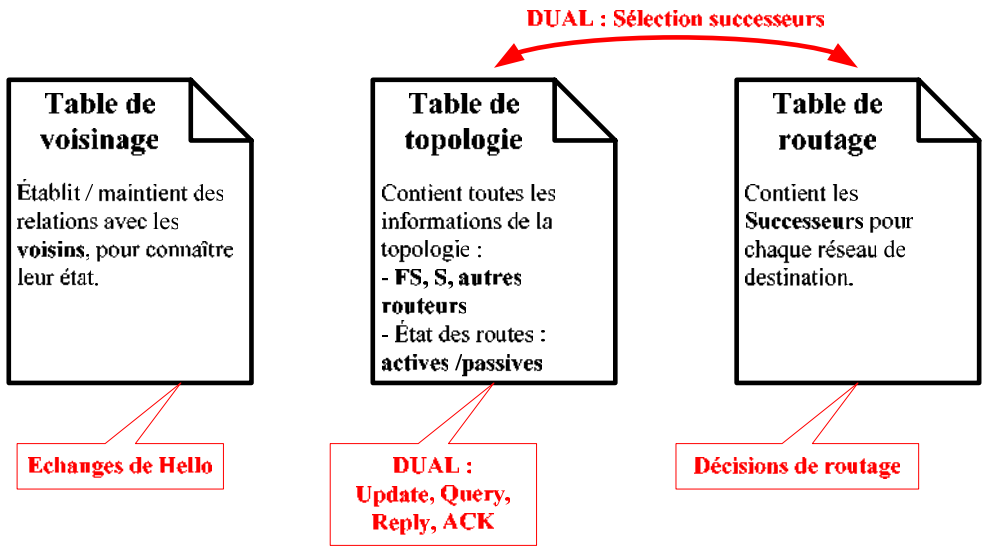
Pour chaque protocole routé utilisé, EIGRP maintient 3 tables distinctes :

- Table de voisinage (Neighbor Table)
- Table de topologie (Topology Table)
- Table de routage (Routing Table)

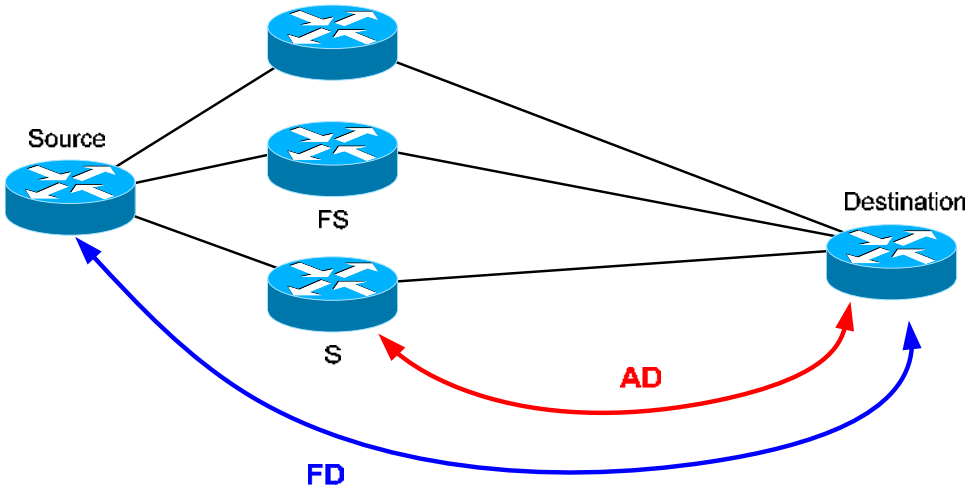
4.2. Termes et définition

EIGRP utilise beaucoup de termes génériques et spécifiques que nous détaillons et définissons ci-dessous :

- **Neighbor (voisin)**
  - Routeur voisin directement connecté qui utilise aussi EIGRP.
- **Neighbor Table (table de voisinage)**
  - Table contenant une liste de tous les voisins. Cette table est élaborée en fonction des informations contenues dans les Hello reçus par les voisins.
- **Route Table (table de routage)**
  - Table de routage pour un protocole routé précis.
- **Topology Table (table de topologie)**
  - Table contenant tous les réseaux appris par les voisins. Cette table sert à remplir la table de routage en fonction de certains critères.
- **Hello**
  - Message utilisé pour découvrir les voisins et les maintenir dans la table de voisinage.
- **Update**
  - Paquet du protocole Hello contenant les informations sur les changements du réseau.
- **Query**
  - Paquet du protocole Hello demandant aux voisins l'existence d'un FS.
- **Reply**
  - Paquet du protocole Hello répondant à un paquet Query.
- **ACK (accusé de réception)**
  - Paquet du protocole Hello accusant réception des autres messages du protocole Hello. Le fenêtrage de RTP est fixé à 1. Ceci signifie que chaque paquet Update doit être suivi d'un ACK.
- **Holdtime**
  - Valeur incluse dans les paquets Hello indiquant le temps qu'un routeur attend un signe d'un voisin avant de le considérer comme indisponible. Ca valeur est 3 fois celle de l'intervalle de transmission des messages Hello. Passé ce délai, le voisin sera considéré comme mort.
- **Reliable Transport Protocol (RTP)**
  - Condition de délivrance d'un paquet par séquence avec garantie.
- **Diffusing Update ALgorithm (DUAL)**
  - Algorithme appliqué sur la table de topologie pour converger le réseau.



- **Advertised Distance (AD)**
  - Métrique diffusée par un voisin dans sa mise à jour de routage. Elle correspond à la métrique depuis ce voisin, connu localement comme le prochain saut.
- **Reported Distance (RD)**
  - Autre nom pour l'AD.
- **Feasible Distance (FD)**
  - Plus petite métrique pour une destination donnée. C'est la métrique pour la route actuellement dans la table de routage.
- **Feasible Condition (FC)**
  - Condition vérifiée quand un voisin informe une AD plus petite que la FD du routeur local pour une même destination.
- **Feasible Successor (FS)**
  - Voisin vérifiant la FC. Il est potentiellement éligible en tant que successeur.
- **Successor**
  - Voisin utilisé comme prochain saut pour une destination donnée. C'est le FS ayant la plus petite métrique.
- **Stuck In Active (SIA) (aussi appelé Query Scoping)**
  - Etat d'un routeur lorsqu'une route reste active après dépassement d'un certain temps.



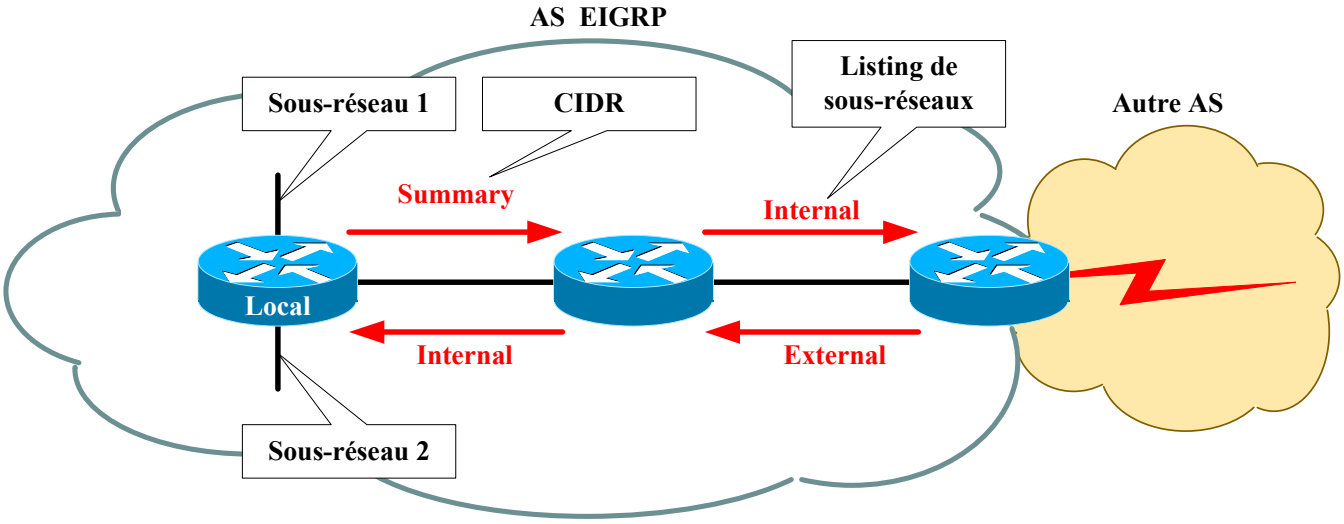
Représentation schématique de quelques définitions

4.3. Métriques

Les métriques sont très similaires à celles employées par IGRP. La grande différence est que la valeur métrique est maintenant un nombre sur 32 bits. Les décisions prises peuvent donc être plus fines ou détaillées.

Il peut y avoir jusqu'à 6 routes pour une même destination dans la table de routage, et que ces routes peuvent être de 3 types :

- **Internal** : Route interne à l'AS
- **Summary** : Routes internes mises sous la forme d'un unique agrégat de routes
- **External** : Route externe à l'AS qui a été redistribuée dans l'AS EIGRP (inclus aussi les routes statiques redistribuées)



Ces routes sont représentées ainsi dans la table de routage :

- **D** : Routes internes et agrégées
- **D EX** : Routes externes

La formule pour le calcul d'une métrique EIGRP est la suivante :

Métrique = (K1 × Bandwidth + K2 × Bandwidth ÷ (256 – Load) + K3 × Delay) + K5 ÷ (Reliability + K4)

Les différents paramètres de cette formule sont les suivants :

- **K1** : Coefficient rattaché à la bande passante (valeur par défaut = 1)
- **K2** : Coefficient rattaché à la charge (valeur par défaut = 0)
- **K3** : Coefficient rattaché au délai (valeur par défaut = 1)
- **K4** : Coefficient rattaché à la fiabilité (valeur par défaut = 0)
- **K5** : Coefficient rattaché au MTU (valeur par défaut = 0)
- **Bandwidth** : Valeur correspondant à la plus petite bande passante de liaison entre les hôtes source et destination. Cette valeur est calculée avec la formule $\mathbf{10^7 \div BP \times 256}$, avec BP la bande passante exprimée en Kbps.
- **Load** : Charge sur la liaison. C'est un pourcentage binaire dont la valeur peut aller de 0 à 255.
- **Delay** : Délai de transmission sur le chemin exprimé en microsecondes (µs). C'est la somme des délais de toutes les liaisons entre les hôtes source et destination. Cette valeur est calculée via la formule $\mathbf{\Sigma_{délais} \times 256}$.
- **Reliability** : Fiabilité de la liaison. C'est aussi un pourcentage binaire dont la valeur peut aller de 0 à 255 et qui est déterminée par le ratio entre le nombre de paquets corrects et le nombre de paquets transmis sur le média.

Ainsi, avec les valeurs par défaut, on arrive à la formule simplifiée suivante :

Métrique = Bandwidth + Delay
Métrique = $(10^7 \div BP + \Sigma_{délais}) \times 256$

On peut donc remarquer que, avec les paramètres par défaut, une métrique d'EIGRP est 256 fois plus grande qu'une métrique d'IGRP pour une même destination.

4.4. Protocole Hello

Le protocole Hello permet l'échange des informations de routage entre les routeurs utilisant le protocole EIGRP ainsi que la découverte dynamique des voisins. Certains messages utilisent RTP afin d'assurer la bonne réception des informations.

Les paquets du protocole Hello utilisant le multicast se servent de l'adresse 224.0.0.10 pour leur transmission.

Plusieurs types de messages, ou plus précisément paquets, existent et se distinguent de part leur utilité :

- **Hello**
  - Emis périodiquement
  - Non orienté connexion
  - Toutes les 5 secondes sur les liaisons LAN
  - Toutes les 60 secondes sur les liaisons WAN

- **Update**
  - Contient les informations des différents réseaux connus par un routeur EIGRP. Ces informations sont à destination de ces voisins, afin qu'ils puissent compléter leur table de topologie.
  - Orienté connexion avec RTP
  - S'il s'agit d'un nouveau voisin, alors le ou les paquets Update envoyés vers ce voisin sont en unicast. Dans les autres cas, le paquet Update est envoyé en multicast.

- **Query**
  - Requête vers un voisin en vue d'obtenir des informations sur les différents réseaux connus par ce dernier. Celui-ci répondra, via un ou plusieurs paquets Reply.
  - Envoyé lorsqu'une ou plusieurs destinations passent à l'état Active
  - Orienté connexion avec RTP
  - Ce type de paquet est toujours envoyé en multicast.
  - Ce type de paquet est généralement envoyé afin d'enquêter sur un réseau suspect (plus accessible, changement d'états et/ou de chemin, etc.).

- **Reply**
  - Identique à un paquet Update sauf que celui-ci est envoyé uniquement en réponse à un paquet Query.
  - Orienté connexion avec RTP
  - Ce paquet est un unicast vers le voisin ayant émis le paquet Query.

- **ACK**
  - Accusé de réception pour les paquets envoyés orientés connexion
  - Envoyé sous la forme d'unicast
  - C'est un paquet Hello sans données qui contient un numéro d'accusé de réception différent de 0.
  - Le fenêtrage a une valeur par défaut de 1. Ceci implique donc que chaque paquet Update, Query et Reply devront être suivi de ce paquet ACK de chaque voisin afin d'en assurer la remise à ces derniers. Le cas échéant, le paquet Update, Query ou Reply envoyé précédemment sera réémis en unicast.
  - Après 16 essais de retransmissions unicast, le routeur marquera le voisin incriminé comme mort.

La capacité à envoyer des retransmissions unicast diminue le temps qu'il faut pour construire les différentes tables, car tous les voisins n'ont pas à traiter et accuser réception de chaque retransmission.

4.4.1. Neighbor Table

Un routeur est considéré comme voisin si :

- **Un paquet Hello** ou ACK est reçu de ce voisin.
- Le **numéro d'AS** est identique pour les deux routeurs.
- Les paramètres de **métrique sont identiques** sur les deux routeurs.

La réception en continu des paquets Hello en provenance des voisins permet de maintenir à jour la table de voisinage, sachant que cette table contient les champs suivants :

- **Adresse** : Adresse de couche 3 du voisin
- **Interface** : Interface locale par laquelle le paquet Hello de ce voisin a été reçue
- **Holdtime** : Temps d'attente d'un signe de vie du voisin avant de le considérer comme mort
- **Uptime** : Temps écoulé depuis la découverte de ce voisin
- **Nombre de paquets en file d'attente (Q Count)** : Permet la visualisation d'une possible congestion vers ce voisin
- **Numéro de séquence** : Numéro de séquence pour les paquets (Utilisant RTP) entrants et sortants. EIGRP garde donc en mémoire deux numéros de séquence différents.

4.4.2. Topology Table

Cette table permet de garder en mémoire tous les réseaux accessibles par les différents voisins (y compris les dupliqués). Elle est complétée grâce aux paquets Update ou Reply (en réponse à un paquet Query) reçus des voisins et enregistre les paquets qui ont été envoyés par le routeur à ses voisins.

L'avantage de posséder la table de routage de tous les voisins dans cette table est la diminution de la surcharge réseau ainsi que des calculs. Ceci permet donc une convergence très rapide.

Cette table permet de gérer la sélection des routes à ajouter dans la table de routage parmi toutes celles disponibles en faisant appel à l'algorithme DUAL.

Elle contient les informations suivantes :

- Etat de la route (Active ou Passive)
- Qu'un paquet Update a été envoyé aux voisins
- Qu'un paquet Query a été envoyé aux voisins. Si ce champ est positif, alors au moins une route doit être marquée comme étant à l'état Active.
- Si un paquet Query a été envoyé, un autre champ indiquera si un paquet Reply a été reçu des voisins
- Qu'un paquet Reply a été envoyé en réponse à un paquet Query reçu d'un voisin
- Les réseaux distants
- Le masque (ou préfix) pour ces réseaux
- La métrique vers chaque réseau (FD)
- La métrique pour chaque réseau avertie par les voisins (AD)
- Le prochain saut pour chaque réseau
- L'interface locale par laquelle sortir pour atteindre ce prochain saut
- Les successeurs, à savoir le chemin jusqu'à la destination, exprimé en sauts

Les métriques incluses dans la table de topologie sont celles indiquées dans les paquets reçus par les voisins (AD). Cela signifie que c'est la table de routage qui calculera la métrique totale vers la destination.

Elle est mise à jour car le routeur obtient ou perd la connectivité directe avec un voisin ou car un changement topologique a été détecté grâce à la communication réseau d'EIGRP. Il existe trois raisons menant à la recalculation de cette table de topologie :

- **Un nouveau réseau est disponible** :
  - Un paquet Update avertit de l'existence d'un nouveau réseau.
  - Une interface locale devient fonctionnelle pour un protocole de couche 3 supporté par EIGRP, et ce dernier est configuré avec les commandes de réseaux appropriées.

- **Le routeur change le successeur** dans la table de topologie ainsi que dans la table de routage :
  - Un paquet Reply ou Query est reçu, modifiant ainsi une ou plusieurs entrées dans la table de topologie.
  - Il y a modification du coût pour une interface locale via configuration.

- **Un réseau devient inaccessible** :
  - Un paquet Update, Query ou Reply reçu informe la table de topologie qu'un réseau est inaccessible.
  - Aucun paquet Hello n'est reçu d'un voisin menant à ce réseau avant expiration du Holdtime.
  - Le réseau est directement connecté et l'interface du routeur perd le signal de porteuse.

4.5. DUAL

Cet algorithme a pour buts de maintenir la table de topologie à jour et de (re)créer la table de routage.

La mise à jour de la table de routage est effectuée différemment en fonction de l'état du ou des réseaux traités :

- **Passive** : Il y a une recherche dans la table de topologie d'une route acceptable pour remplacer l'ancienne présente dans la table de routage :
  - Toutes les entrées pour une même destination sont examinées afin de trouver tous les FS (ceux qui vérifient la FC, à savoir que leur AD doit être inférieure à la FD indiquée dans l'ancienne version de la table de routage).
  - Après examen, il existe au moins un FS.
  - Le FS proposant la plus petite AD sera alors choisi comme successeur à l'entrée non valide de l'ancienne table de routage.

- **Active** : Il n'y a pas de routes acceptables dans la table de topologie pour remplacer l'ancienne présente dans la table de routage. Le routeur interroge alors ses voisins via un paquet Query afin d'obtenir des informations sur des chemins possibles de remplacement :
  - Toutes les entrées pour une même destination sont examinées afin de trouver tous les FS (ceux qui vérifient la FC, à savoir que leur AD doit être inférieure à la FD indiquée dans l'ancienne version de la table de routage).
  - Après examen, il n'existe aucun FS. Le routeur passe en mode actif et envoie des paquets Query à ses voisins.
  - Si un ou plusieurs voisins répondent en indiquant une ou plusieurs nouvelles routes vérifiant la FC (AD > FD), alors les voisins menant à ces routes deviennent des FS.
  - Le FS proposant la plus petite AD sera alors choisi comme successeur à l'entrée non valide de l'ancienne table de routage.

4.6. Commandes

Les commandes de configuration d'EIGRP sont les suivantes :

- **router eigrp {n° AS}**
  - Mode de configuration globale
  - Active l'algorithme du protocole de routage pour IP.
  - Permet de passer en mode de configuration de ce protocole de routage.

- **network {réseau} [masque générique]**
  - Mode de configuration du protocole de routage
  - Spécifie la ou les interfaces interagissant avec ce protocole de routage. Une interface émettra et recevra donc des mises à jour de routage EIGRP si leur adresse IP fait partie du réseau indiqué en paramètre.
  - Inclut les informations concernant ces réseaux dans les mises à jour de routage transmises.
  - Le réseau indiqué en paramètre doit obligatoirement être directement connecté au routeur, mais il peut englober plusieurs sous-réseaux à la fois (via CIDR) en l'associant à un masque générique.

- **[no] auto-summary**
  - Mode de configuration du protocole de routage
  - Permet d'activer (par défaut) ou de désactiver l'agrégation de routes automatique aux frontières Classful.

- **ip summary-address eigrp {n° AS} {réseau} {masque}**
  - Mode de configuration d'interface
  - Permet de configurer manuellement un agrégat de routes à une frontière Classless.
  - Pour que l'effet de cette commande fonctionne, il faut obligatoirement que l'agrégation de routes automatique soit désactivée (commande **no auto-summary**).

- **variance {multiplicateur}**
  - Mode de configuration du protocole de routage
  - Indique la variance que peut avoir au maximum les routes qui seront incluses dans la table de routage à de fins de partage de charge.
  - Le multiplicateur est un entier pouvant aller de 1 (valeur par défaut) à 128.

- **maximum-paths {nombre}**
  - Mode de configuration du protocole de routage
  - Indique le nombre, allant de 1 (par défaut) à 6, de routes à métrique égale (à plus ou moins la variance) pouvant être mises au maximum dans la table de routage pour une même destination à des fins de partage de charge.

- **bandwidth {BP}**
  - Mode de configuration d'interface
  - Informe les protocoles de routage utilisant la bande passante pour le calcul des métriques de la véritable bande passante de la liaison.
  - La bande passante d'une liaison n'est pas détectée, et a une valeur par défaut de 1544 Kbps (T1) pour les interfaces série haut débit.
  - Le paramètre **BP** est exprimé en Kbps.

- **passive-interface {type} {numéro}**
  - Mode de configuration du protocole de routage
  - Empêche l'émission et la réception de mises à jour de routage en empêchant la formation d'une relation de voisinage sur l'interface spécifiée.

- **metric weights {TOS} {K1} {K2} {K3} {K4} {K5}**
  - Mode de configuration du protocole de routage
  - Modifie des coefficients entrants en jeu dans le calcul des métriques d'EIGRP.
  - La valeur de **TOS** doit toujours être de 0.

Pour la visualisation de l'état du protocole EIGRP, nous avons à notre disposition les commandes suivantes :

- **show ip route [eigrp [n° AS]]**
  - Visualise uniquement les routes EIGRP de la table de routage.
- **show ip eigrp neighbors [{type} {numéro} [n° AS]] [detail]**
  - Fournit toutes les informations sur les voisins, l'état de la relation de voisinage ainsi que les interfaces et adresses par lesquelles ils communiquent.
- **show ip eigrp topology [all | n° AS | [IP] masque]**
  - Affiche les informations concernant la table de topologie. Il est possible d'afficher les informations pour les destinations connues en fonction du paramètre optionnel (**all** affiche toutes les routes ainsi que tous les chemins alternatifs).
- **show ip eigrp traffic [n° AS]**
  - Donne les informations regroupées sur le trafic total envoyé depuis et vers le processus EIGRP.
- **show ip eigrp interfaces [n° AS] [detail]**
  - Informations relatives aux interfaces participant au processus de routage d'EIGRP. Ceci inclut mais ne se limite pas au nombre de voisins et le SRTT.

A des fins de dépannage, les commandes **debug** suivantes sont disponibles :

- **debug eigrp packet**
  - Affiche les paquets EIGRP émis et reçus, sachant que le type de message peut être précisé.
- **debug eigrp neighbors**
  - Affiche les paquets Hello émis et reçus par le routeur ainsi que les voisins découverts.
- **debug ip eigrp**
  - Idem que **debug ip eigrp route**
- **debug ip eigrp route**
  - Affiche les changements dynamiques apportés à la table de routage.
- **debug ip eigrp summary**
  - Affiche un résumé des informations concernant EIGRP telles que les voisins, le filtrage et la redistribution.
- **debug eigrp events**
  - Affiche les types de paquets émis et reçus et les statistiques sur les décisions de routage.

4.7. Configuration

La procédure de configuration du protocole EIGRP est la suivante :

- Activer le protocole EIGRP (commande **router eigrp**)
- Indiquer les interfaces devant participer au processus de routage d'EIGRP (commande **network**)
- Optionnel : Spécifier la bande passante réelle de la liaison (commande **bandwidth**)
- Optionnel : Désactiver l'émission/réception des informations de routage vers les interfaces connectées à des réseaux moignons (commande **passive-interface**)
- Optionnel : Meilleure gestion des routes (commandes **maximum-paths**, **variance** et **metric weights**)
- Optionnel : Agrégation de routes manuelle (commandes **no auto-summary** et **ip summary-address**)

5. Design de LAN

5.1. Présentation

La conception d'un réseau est un des facteurs les plus importants pour en assurer la stabilité. Les objectifs de cette conception incluent des facteurs tels que :

- **La fonctionnalité**
  - Un réseau doit apporter aux utilisateurs les fonctionnalités suffisantes et nécessaires à leurs besoins
- **L'évolutivité**
  - Un réseau doit pouvoir prendre en charge de nouvelles fonctionnalités sans pour autant devoir reconsidérer la structure initiale
- **L'adaptabilité**
  - Un réseau doit pouvoir s'adapter sans nécessiter de trop complexes configurations
- **La facilité de gestion**
  - Un réseau doit être relativement simple à administrer

Au cours de ce chapitre, nous allons analyser les différents points à observer lors de la conception d'un réseau local. L'analyse portera sur les points suivants :

- Fonctions et emplacements des serveurs
- Détection des collisions (couche 2)
- Segmentation (couche 2 et 3)
- Domaines de broadcast (couche 3)

5.2. Méthodologie de conception

Pour qu'un réseau local soit efficace et réponde aux besoins des utilisateurs, il doit être mis en œuvre selon une suite d'étapes systématiquement planifiées, comprenant notamment les étapes suivantes :

- Le regroupement des besoins et des attentes des utilisateurs
- L'analyse des besoins
- La conception de la structure LAN des couches 1 à 3
- La création de documents sur la mise en œuvre logique et physique du réseau

La première étape de conception d'un réseau consiste à recueillir des données sur la structure de l'organisation. Ces informations comprennent :

- L'historique et l'état en cours de l'organisation
- La croissance prévue
- Les politiques d'exploitation et les procédures de gestion
- Les procédures et les systèmes administratifs ainsi que les points de vue des futurs utilisateurs du réseau local.

Un réseau local est un outil qui sera utilisé par les différents membres de l'entreprise. Le niveau de compétence de ces derniers ainsi que l'utilisation qu'ils comptent faire du réseau sont des éléments déterminants dans la conception.

Ces informations contribuent à identifier et à clarifier les problèmes. Vous devez également déterminer s'il existe des documents sur les politiques déjà en place. Le bon sens et une étude approfondie des besoins des utilisateurs sont les clefs d'un réseau efficace.

Il est également vital de prévoir le rôle des personnes qui vont participer à l'administration du réseau (adressage, maintenance, etc..). Par exemple, la présence d'une tierce entreprise utilisée pour la maintenance est un élément important.

Les ressources d'une organisation pouvant affecter la mise en œuvre d'un nouveau réseau local sont classées en deux catégories : les ressources matérielles/logicielles et les ressources humaines.

Le matériel informatique et les logiciels existants de l'organisation doivent être répertoriés par écrit, et les besoins futurs dans ce domaine doivent être définis. Un rapport écrit sur ces besoins permet d'évaluer les coûts et d'établir un budget pour la mise en place du réseau local. Un schéma présentant la topologie logique du réseau est également un élément important qui permet de bien visualiser le réseau dans son intégralité.

Un schéma logique représente le modèle de la topologie du réseau sans les détails relatifs au parcours d'installation précis des câbles. Il s'agit du plan de base du réseau local. La topologie logique comprend les éléments suivants :

- L'emplacement exact des locaux techniques du répartiteur principal MDF et des répartiteurs intermédiaires IDF.

- Le type et le nombre de câbles utilisés pour interconnecter le répartiteur principal MDF et les répartiteurs intermédiaires IDF ainsi que le nombre de câbles de réserve disponibles pour accroître la bande passante entre les locaux techniques.

- Un document décrivant en détail tous les parcours de câbles, les numéros d'identification et le port de l'interconnexion horizontale ou verticale auquel aboutissent les câbles.

5.3. Fonction et emplacements des serveurs

On distingue 2 types de serveurs :

- Les serveurs d’entreprise :
  - Serveurs dédiés à une application
  - Prennent en charge tous les utilisateurs du réseau (Exemple : DNS, messagerie)
  - Doivent être installés dans le répartiteur principal (MDF)

- Les serveurs de groupes de travail :
  - Offrent des services tels que l’impression ou encore le partage de fichiers
  - Prennent en charge un ensemble spécifique d’utilisateurs
  - Doivent être installés dans les répartiteurs intermédiaires (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.

5.4. Conception de 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 comprennent le type de câble à utiliser (généralement, des câbles de cuivre ou à fibre optique) ainsi que la structure globale du câblage.

Les médias de câblage de couche 1 comprennent le câble à paires torsadées blindées (ou non) de catégorie 5 et le câble à fibre optique, avec la norme TIA/EIA-568-A pour la disposition et la connexion des méthodes de câblage.

En plus des limites de distance, vous devez évaluer avec soin les points forts et les points faibles des diverses topologies, car l'efficacité d'un réseau est directement liée au câblage sous-jacent. Si vous prévoyez d'apporter des modifications importantes à un réseau, il est essentiel d'effectuer une vérification complète des câbles pour identifier les zones qui nécessitent une mise à niveau ou une réinstallation.

Qu'il s'agisse de la conception d'un nouveau réseau ou de la réinstallation du câblage d'un réseau existant, vous devez utiliser des câbles à fibre optique dans le réseau de backbone et le câblage vertical, avec des câbles à paires torsadées blindées (ou non) de catégorie 5 pour le câblage horizontal.

La mise à niveau des câbles doit être prioritaire sur toutes les autres modifications à apporter. En outre, il est impératif de s'assurer, sans exception, que ces systèmes sont conformes aux normes en vigueur.

Dans une topologie en étoile simple comportant un seul local technique, le répartiteur principal MDF comprend un ou plusieurs tableaux d'interconnexions horizontales. Les câbles d'interconnexion horizontale servent à relier le câblage horizontal de la couche 1 aux ports du commutateur LAN de la couche 2.

Le port uplink du commutateur LAN qui, selon le modèle, diffère des autres ports parce qu'il n'est pas interconnecté, est connecté au port Ethernet du routeur de la couche 3 via un câble de raccordement. À ce stade, l'hôte d'extrémité est doté d'une connexion physique complète au port du routeur.

Lorsque des hôtes de grands réseaux dépassent la limite des 100 mètres fixée pour le câble à paires torsadées non blindées de catégorie 5, il n'est pas rare d'installer plusieurs locaux techniques.

La création de plusieurs locaux techniques entraîne la création de plusieurs zones d'interconnexion de réseaux (IDF).

Les normes TIA/EIA568-A 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 permet d'interconnecter les divers répartiteurs intermédiaires IDF au répartiteur principal (MDF).

Comme les câbles verticaux sont en général plus longs que la limite des 100 mètres imposée pour les câbles à paires torsadées non blindées de catégorie 5, le câble à fibre optique est habituellement utilisée.

5.5. Conception de couche 2

L'objectif des équipements de couche 2 est d'assurer la commutation ainsi que la détection des erreurs et la réduction des congestions du réseau. Les deux équipements de couche 2 les plus courants (autres que la carte réseau dont chaque hôte du réseau doit être doté) sont les ponts et les commutateurs LAN. Les équipements de cette couche déterminent la taille des domaines de collision et de broadcast.

Les collisions et la taille du domaine de collision sont deux facteurs qui nuisent aux performances d'un réseau. La commutation LAN permet de micro segmenter le réseau afin d'éliminer les collisions et de réduire la taille des domaines de collision.

Grâce à une autre caractéristique importante, 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.

Si vous installez un commutateur LAN au répartiteur principal MDF et aux répartiteurs intermédiaires IDF ainsi qu'un câble vertical entre le répartiteur principal et les répartiteurs intermédiaires, le câble vertical acheminera tout le trafic de données entre le répartiteur principal et les répartiteurs intermédiaires.

La capacité de ce parcours doit être supérieure à celle des parcours reliant les répartiteurs intermédiaires IDF et les stations de travail. Les câbles horizontaux utilisent des paires torsadées non blindées de catégorie 5 et aucun branchement de câble ne doit dépasser 100 mètres de longueur de façon à obtenir des liaisons à des débits de 10 Mbits/s ou de 100 Mbits/s. Dans un environnement normal, un débit de 10 Mbits/s convient pour le câble de branchement horizontal.

Comme les commutateurs LAN asymétriques permettent de combiner des ports à 10 Mbits/s et à 100 Mbits/s sur un même commutateur, l'étape suivante consiste à déterminer le nombre de ports à 10 Mbits/s et à 100 Mbits/s nécessaires pour le répartiteur principal MDF et pour chacun des répartiteurs intermédiaires IDF.

Vous pouvez déterminer ce nombre en consultant les besoins des utilisateurs spécifiant le nombre de câbles de branchement horizontaux par salle dans chaque zone d'interconnexion de réseaux ainsi que le nombre de câbles verticaux.

L'autre méthode permettant de mettre en œuvre une commutation LAN consiste à installer des concentrateurs LAN partagés sur les ports du commutateur et de connecter plusieurs hôtes à un seul port du commutateur. Tous les hôtes connectés au concentrateur LAN partagé partagent le même domaine de collision et la même bande passante.

Les concentrateurs à média partagé sont généralement utilisés dans un environnement de commutateurs LAN pour créer davantage de points de connexion à l'extrémité des câbles horizontaux.

Cette solution est acceptable, mais vous devez vous assurer que la taille des domaines de collision n'augmente pas et que les besoins de l'hôte en matière de bande passante respectent les spécifications définies à l'étape des besoins du processus de conception du réseau.

5.6. Conception de couche 3

Les équipements de couche 3, tels que les routeurs, peuvent être utilisés pour créer des segments LAN uniques et permettre la communication entre les segments sur la base de l'adressage de couche 3, tel que l'adressage IP. La mise en œuvre des équipements de couche 3, tels que les routeurs, permettent de segmenter le réseau local en réseaux physiques et logiques uniques.

Les routeurs fournissent également la connectivité aux réseaux WAN tels qu'Internet. Le routage de couche 3 détermine également le flux du trafic entre les segments physiques uniques du réseau en fonction de l'adressage de couche 3 (par exemple, un réseau IP ou un sous-réseau).

Le nombre total de broadcasts, tels que les requêtes ARP, est une question importante dans un réseau. Grâce aux VLAN, vous pouvez limiter le trafic de broadcast au sein de chaque VLAN et, par conséquent, créer des domaines de broadcast plus petits.

Les VLAN permettent également de sécuriser le réseau en créant des groupes de VLAN selon leur fonction. Une association à un port physique est utilisée pour mettre en œuvre l'attribution de VLAN statiques. Comme le routeur détermine si le réseau VLAN 1 peut communiquer avec le réseau VLAN 2, vous pouvez créer un système de sécurité fondé sur l'attribution des VLAN.

Les routeurs fournissent une évolutivité au réseau parce qu'ils servent de pare-feu vis-à-vis des broadcasts. De plus, comme les adresses de couche 3 ont généralement une structure, ils accroissent l'évolutivité en divisant les réseaux et les sous-réseaux, ce qui renforce la structure de ces adresses.

Une fois les réseaux divisés en sous-réseaux, l'étape finale consiste à développer et à expliquer par écrit le système d'adressage IP à utiliser. La technologie de routage filtre les broadcasts et les multicasts de liaison de données. En ajoutant des ports de routeur ainsi que des adresses réseau ou de sous-réseau, vous pouvez, si nécessaire, segmenter l'inter réseau.

Les routeurs permettent de créer des sous-réseaux IP pour renforcer la structure des adresses. Avec des ponts et des commutateurs, toutes les adresses inconnues encombrant chaque port doivent être évacuées.

Avec des routeurs, les hôtes utilisant des protocoles d'adressage de couche réseau peuvent résoudre la recherche d'hôtes sans provoquer d'encombrement réseau :

- Si l'adresse de destination est locale, l'hôte émetteur peut encapsuler le paquet dans un en-tête de liaison de données et transmettre une trame d'unicast directement à la station. Le routeur ne voit pas la trame et, bien sûr, n'a pas besoin de la traiter. L'hôte émetteur peut utiliser une requête ARP. Dans ce cas, un broadcast est généré. Cependant, comme il s'agit d'un broadcast local, le routeur ne le transmet pas.

- Si la destination n'est pas locale, la station émettrice transmet le paquet au routeur. Le routeur envoie la trame à destination ou au saut suivant en fonction de sa table de routage.

En raison de cette fonctionnalité de routage, il est évident que les grands réseaux locaux évolutifs doivent comporter quelques routeurs.

6. Commutation

6.1. Concepts et fonctionnement

Au début des LAN, les équipements de réseau utilisaient un seul bus électrique. En effet, tous les équipements du LAN partageaient la bande passante d'un seul bus. C'est le cas des normes Ethernet 10Base2, 10Base5 et 10Base-T.

Dans une réunion, quand plusieurs personnes prennent la parole en même temps, cela crée une cacophonie et il devient très difficile, voire impossible de comprendre les interlocuteurs. Il faut donc appliquer une convention afin qu'il n'y ait qu'une personne à la fois qui prenne la parole.

La même problématique se retrouve dans les LAN où les équipements du réseau se partagent le même espace de « discussion ». Quand 2 hôtes envoient un signal en même temps, ceux-ci se chevauchent rendant impossible leur interprétation : on parle de collision.

Pour résoudre ce problème, l'algorithme **CSMA/CD** (Carrier Sense Multiple Access with Collision Detection) est appliqué et définit de quelle façon accéder au bus. Malgré l'apport de CSMA/CD l'utilisation du réseau n'était pas optimale. Les LAN étaient confrontés aux problèmes de collisions, congestions, latence et de remise de données de type broadcast.

Les ponts transparents, puis les commutateurs (ou **switch**) dans un second temps permirent de résoudre ces phénomènes.

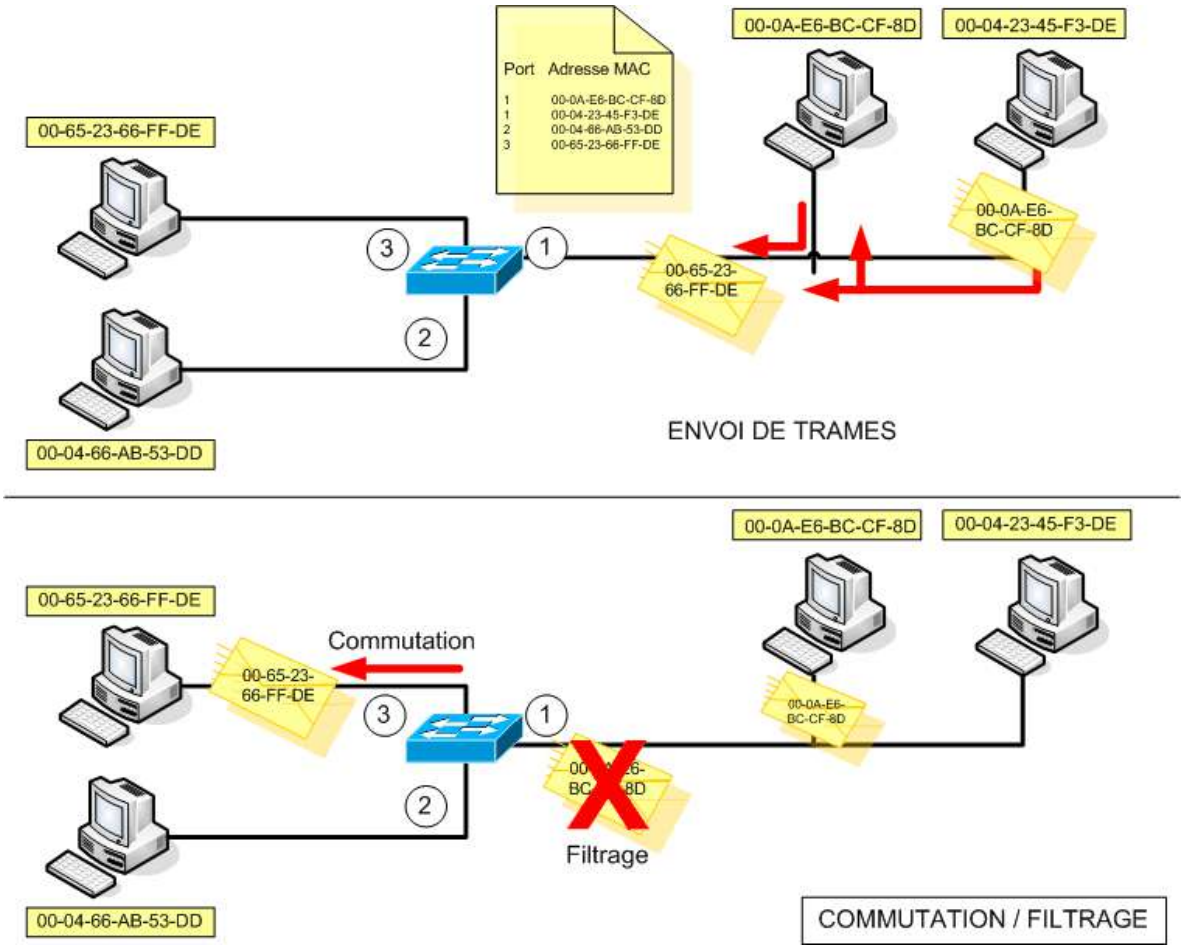
Les ponts offrent principalement les avantages suivants:
- La réduction de la taille des domaines de collisions par la segmentation.
- L'augmentation de la bande passante (due à la réduction de la taille des domaines de collision).

Les ponts et les commutateurs ont la même logique de fonctionnement, d'ailleurs un commutateur est un pont multiport.

Contrairement à un concentrateur qui se contente de régénérer, resynchroniser et retransmettre les bits sur le média, le pont est capable de prendre des décisions d'acheminement. Pour cela, il utilise les adresses **MAC** (Media Access Control). De ce fait, les ponts, comme les commutateurs, sont des équipements de couche 2 du modèle OSI.

Quand un pont reçoit une trame, il examine l'adresse MAC (Media Access Control) de destination et détermine s'il doit filtrer ou transmettre la trame. Les décisions d'acheminements se fondent sur une table de pontage où le pont inscrit toutes les adresses MAC et le port par lequel elles sont arrivées.

Quand une trame arrive à un port, le pont va consulter sa table de pontage pour connaître le port par lequel la trame doit être envoyée à l'adresse MAC de destination. Dans ce cas, si :
- Le port de destination est le même que celui qui a reçu la trame, la trame ne sera pas transmise sur d'autres ports : c'est le **filtrage**.
- Le port de destination est un port différent de celui par lequel la trame a été reçue, le pont transmet cette trame sur le port correspondant : c'est la **commutation**.



Le fonctionnement du commutateur est identique. L'apprentissage des adresses MAC se déroule comme suit :

- Lorsque le commutateur reçoit une trame par un de ses ports, il inscrit dans sa table de pontage la correspondance entre l'adresse MAC source et le port associé.
- Supposons que la table de pontage soit déjà créée et complète. Le commutateur examine l'adresse physique de destination de la trame reçue et cherche dans sa table l'entrée associée à l'adresse.
- Une fois le port de destination identifié, le commutateur commute la trame sur le port correspondant.

S'il n'y a pas d'entrée dans la table de pontage, le commutateur crée une entrée correspondante et transmet les données par tous ses ports excepté le port source. Quand le destinataire répondra à l'émetteur, le commutateur pourra inscrire l'entrée correspondante.

L'IEEE a définit trois catégories d'adresses MAC :

- Adresse **unicast** : adresse physique identifiant une seule carte réseau.
- Adresse de **broadcast** : avec cette adresse tous les noeuds du LAN doivent traiter la trame. L'adresse de broadcast a pour valeur FFFF.FFFF.FFFF
- Adresse **multicast**. Permet à un ensemble de noeuds de communiquer entre eux. L'adresse multicast a pour valeur 0100.5Exx.xxxx où x peut prendre n'importe quelle valeur.

En transmettant les trames reçues à un autre port, le commutateur crée un bus unique entre la source et la destination (micro segmentation). L'utilisation de la bande passante est optimale, 100% de la bande passante est utilisée.

L'algorithme CSMA/CD n'est plus employé car il n'y a pas de collision. On peut alors utiliser le mode de fonctionnement full-duplex, c'est-à-dire que la source et la destination peuvent émettre et recevoir en même temps.

6.2. Commutateurs

6.2.1. Présentation

Un commutateur est un équipement réseau de couche 2. Il en existe une grande variété avec des caractéristiques différentes :

- Nombre de ports
- Type de port (10/100 Mbits, gigabit)
- Type de commutation (Strore and Forward, Cut Through)
- Facilité d'installation en armoire etc…

Les différents types de commutation :

- **Store and forward**: Le commutateur attend d'avoir reçu toute la trame avant de la transmettre. Cette méthode offre une grande vérification d'erreur car le commutateur a le temps de vérifier la valeur FCS. Cependant ce traitement augmente la latence réseau.

- **Cut Through**: Dès que l'adresse de destination est connue, la trame commence à être commutée. Ce mode est plus rapide que le précédent. Il existe différentes variantes de ce type de commutation:

    - **Fragment Free**: Filtrage des fragments de collision (inférieur à 64 octets). Le commutateur attend d'avoir reçu les 64 premiers octets avant de commencer à transmettre la trame. La détection des collisions subies doit être détectée au niveau des 64 premiers octets.

    - **Fast Forward**: Pas de vérification d'erreurs. La trame est transmise dès que l'adresse de destination est identifiée.

6.2.2. Démarrage

Avant le démarrage du système d'exploitation une procédure POST (Power On Self Test) est lancée pour tester le bon état du matériel.

Le voyant indique l'échec ou la réussite du POST : une lumière ambre indique l'échec, alors qu'une couleur verte indique que la procédure s'est terminée avec succès.

6.2.3. Configuration de base

Pour configurer un commutateur il convient de se connecter via le port console à l'aide d'un câble du même nom. Une fois la connexion lancée, ont se retrouve sur une interface de ligne de commande : la CLI (Command-Line Interface).

A l'instar de l'IOS des routeurs, il existe différents modes de configuration : le mode utilisateur, le mode privilégié et le mode de configuration globale. Les mêmes commandes sont utilisées pour accéder à ces différents modes.

6.2.4. Voyants d'un commutateur

Voyant	Etat et signification	
Système	Voyant éteint : le système est hors tension.	
	Voyant vert : le système est sous-tension.	
	Voyant ambre : problème suite au POST.	
RPS (Remote Power Supply)	Ce voyant indique si l'alimentation de sécurité est utilisée.	
Port	Chaque port a son voyant qui donne des indications sur l'état du port selon le mode choisi.	
Bouton mode	Permet de choisir entre les 4 modes: Stat, Util, Duplex et Speed.	
Bouton mode	Stat	Donne des informations sur l'état des ports. Une lumière verte indique que le port est opérationnel. Quand elle clignote elle témoigne d'une activité. Si la lumière est éteinte le port est non opérationnel.
	Util	Ce mode utilise l'ensemble des voyants de ports pour donner des informations sur l'utilisation générale du commutateur.
	Duplex	Quand le voyant est allumé le port fonctionne en mode full duplex. Eteint, c'est le mode half duplex qui est employé.
	Speed	Un voyant allumé indique un débit de 100 Mbits, un voyant éteint un débit de 10Mbits.

Face avant et arrière d'un commutateur Cisco Catalyst 2950

6.2.5. Commandes

- **enable**
  - Depuis le mode utilisateur permet d'accéder au mode privilégié.
- **configure terminal**
  - Depuis le mode privilégié permet d'accéder au mode de configuration globale.
- **show version**
  - Permet de vérifier la version de l'IOS et la valeur du registre de configuration.
- **show running-config**
  - Permet d'afficher le fichier de configuration actif.
- **show interface FastEthernet [numéro de l'interface]**
  - Affiche le statut de l'interface, le débit, l'auto négociation et les statistiques de l'interface.
- **show flash ou dir:flash**
  - Affiche la version de l'image de l'IOS contenue dans la mémoire flash, la taille de la mémoire et la mémoire utilisée.
- **show interface status**
  - Affiche le mode opérationnel du port.
- **show controllers ethernet-controller**
  - Affiche les statistiques sur les données reçues et envoyées au niveau matériel.
- **show post**
  - Indique si le routeur a effectué le POST.
- **reload**
  - Redémarre le commutateur.
- **erase startup-config**
  - Efface le fichier de configuration de sauvegarde.
- **delete flash:vlan.dat**
  - Supprime la base de donnée de VLAN. Sûr les Catalyst 1900 c'est la commande delete nvram qui est employée.
- **show mac-address-table**
  - Permet d'afficher les adresses MAC apprises par le commutateur.
- **clear mac-address-table**
  - Permet d'effacer les entrées de tables configurées par l'administrateur.
- **mac-address table static [adresse MAC de l'hôte] interface Fast Ethernet [numéro de l'interface] vlan [numéro du vlan]**
  - Permet d'attribuer une adresse MAC statique à une interface.
- **show port security**
  - Permet de vérifier le statut de sécurité appliqué aux ports.
- **interface [type] [numéro/sous numéro]**
  - Permet de passer dans le mode configuration de l'interface.
- **interface range [type] [numéro/premier numéro – dernier numéro]**
  - Permet de passer dans le mode de configuration de plusieurs interfaces.

6.2.6. Procédure de récupération des mots de passe

- Appuyez sur le bouton mode en même temps que la mise sous tension du commutateur.
- Pour initialiser la flash tapez **flash_init**, puis **load_helper** et enfin **dir:flash**.
- Ensuite renommez le fichier de configuration avec la commande **rename flash: config.txt flash: config.old**.

Le fichier de configuration ne sera pas chargé au prochain démarrage du commutateur.
Pour des raisons d'espace, pensez à supprimer le fichier config.old avec la commande : **delete flash: config.old**.

6.3. Protocole Spanning-Tree

Les topologies redondantes sont mises en place pour palier à des liaisons interrompues. En effet, plusieurs chemins peuvent permettre d'accéder au même lien.

Mais si ces chemins redondants ne sont pas correctement gérés, les trames peuvent boucler indéfiniment. Le protocole Spanning-Tree permet d'y remédier.

6.3.1. Théorie concernant Spanning-Tree

Les commutateurs implémentent le protocole **IEEE 802.1D Spanning-Tree**. Il apporte une réponse au problème de bouclage. Pour ce faire, **STP** (Spanning-Tree Protocol) empêche certains ports de transmettre en mettant les ports dans un état de blocage ou dans un état de transmission, afin qu'il n'y ait qu'un seul chemin possible entre deux segments de LAN.

Un port bloqué ne peut ni recevoir ni émettre et inversement en mode de transmission. En premier lieu, des **BPDUs (Bridge Protocol Data Unit)** sont envoyés toutes les 2 secondes sur tous les ports.

Le commutateur qui détient l'identifiant de pont le plus bas (Bridge ID) est élu racine. Le Bridge ID de 8 octets est composé d'une priorité sur 2 octets (32768 par défaut), suivi par l'adresse MAC du port émetteur. Tous les ports du commutateur racine sont placés en état de transmission par le protocole STP.

Le commutateur racine transmet par tous ses ports des BPDUs. Ces messages sont transmis par les commutateurs non racine. A chaque réception de BPDU, le champ du coût est incrémenté, ce qui permet aux commutateurs non racine de connaître la valeur de l'itinéraire jusqu'à la racine.

Le port de chaque commutateur qui reçoit le BPDU comportant le coût le plus bas (donc le plus proche du commutateur racine) est élu port racine pour le segment de LAN auquel il est connecté.

Le calcul de la route se base sur la vitesse. Plus elle est grande, plus le coût est bas. Le port par lequel arrivent les BPDU portant le moindre coût vers la racine est mis en état de transmission. Les autres ports sont mis en état de blocage, pour éliminer toute route redondante et ainsi éviter qu'il y ait des boucles actives.

Les ports prennent d'autres états. Voici un tableau récapitulatif des états appliqués aux ports :

Etat	Description
Transmission	Le port émet et reçoit les trames.
Ecoute	Le port écoute les BPDU pour s'assurer qu'il n'y ait pas de boucle. Ce processus a une durée de vie de 15 secondes.
Apprentissage	Le port écoute les BPDU pour découvrir les adresses MAC. Ce processus a une durée de vie de 15 secondes également.
Désactivé	Le port n'est pas utilisé pour des raisons administratives.
Blocage	Le port ne peut ni émettre ni recevoir les trames.

Un réseau interconnecté est dit convergent lorsque tous les ports ont pris un état de blocage ou de transmission. Le processus de convergence prend 15 secondes pour le processus d'écoute, plus 15 secondes pour le processus de découverte et 20 secondes pour bloquer les ports ou les mettre dans l'état de transmission.

Lorsqu'une modification topologique est détectée l'arbre est recalculé et le trafic ne reprend totalement qu'après le temps de convergence nécessaire.

6.3.2. Théorie concernant Rapid Spanning-Tree

Le protocole RSTP (Rapid Spanning Tree Protocol) est défini par le standard IEEE 802.1w. Il diffère principalement de STP de part sa convergence plus rapide. En effet, RSTP offre une convergence au minimum 5 fois plus rapide que STP. RSTP prend moins de 10 secondes pour converger.

RSTP et STP partagent certaines similitudes:

- Election d'un commutateur racine suivant le même processus.
- Ils élisent le port racine des commutateurs non racine de la même manière.
- Ils élisent le port désigné pour un segment de LAN de la même façon.
- Ils placent tous les ports dans un état de blocage ou de transmission, à la différence que RSTP utilise l'appellation discarding pour l'état de blocage.

RSTP définit aussi des types de liaisons et de bordures. Les liaisons sont les connections physique entre les commutateurs et les bordures les connections physiques entre un commutateur et un hôte ou un concentrateur. On distingue:

- Les liaisons point-à-point, c'est-à-dire entre deux commutateurs.
- Les liaisons partagées, c'est-à-dire entre un et plusieurs commutateurs.
- Les bordures point-à-point, entre un hôte et un commutateur.
- Les bordures partagées, entre un concentrateur et un commutateur.

Les ports des liaisons point-à-point et des bordures point-à-point sont immédiatement placés dans l'état de transmission. Ce qui permet d'améliorer la vitesse de convergence des commutateurs.

6.3.3. Commandes et configuration de Spanning-Tree

- **spanning-tree {identifiant de vlan} root**
  - Depuis le mode de configuration globale, permet de désigner le commutateur racine. A l'issue de cette commande la priorité du commutateur sera modifiée pour être plus basse que le commutateur qui devrait être racine.

- **spanning-tree {identifiant de vlan} [priority priorité]**
  - Depuis le mode de configuration globale, permet de changer le niveau de priorité.

- **spanning-tree cost {coût}**
  - Depuis le mode de configuration spécifique de l'interface, permet de modifier le coût STP.

- **channel-group {numéro du groupe de canal} mode [auto | desirable | on]**
  - Active l' Etherchannel (agrégation de liens) de l'interface.

- **show spanning-tree**
  - Affiche des informations détaillées sur le protocole STP en cours ainsi que l'état de chaque port.
- **show spanning-tree interface {interface}**
  - Affiche les informations Spanning-tree du port spécifié.
- **show spanning-tree vlan {vlan id}**
  - Affiche les informations Spanning-tree du VLAN spécifié.
- **debug spanning-tree**
  - Affiche les informations de changement topologique STP.
- **show etherchannel {numéro de groupe de canal} [brief | detail | port | port-channel | summary]**
  - Affiche les informations sur le statut des EtherChannels sur le commutateur.

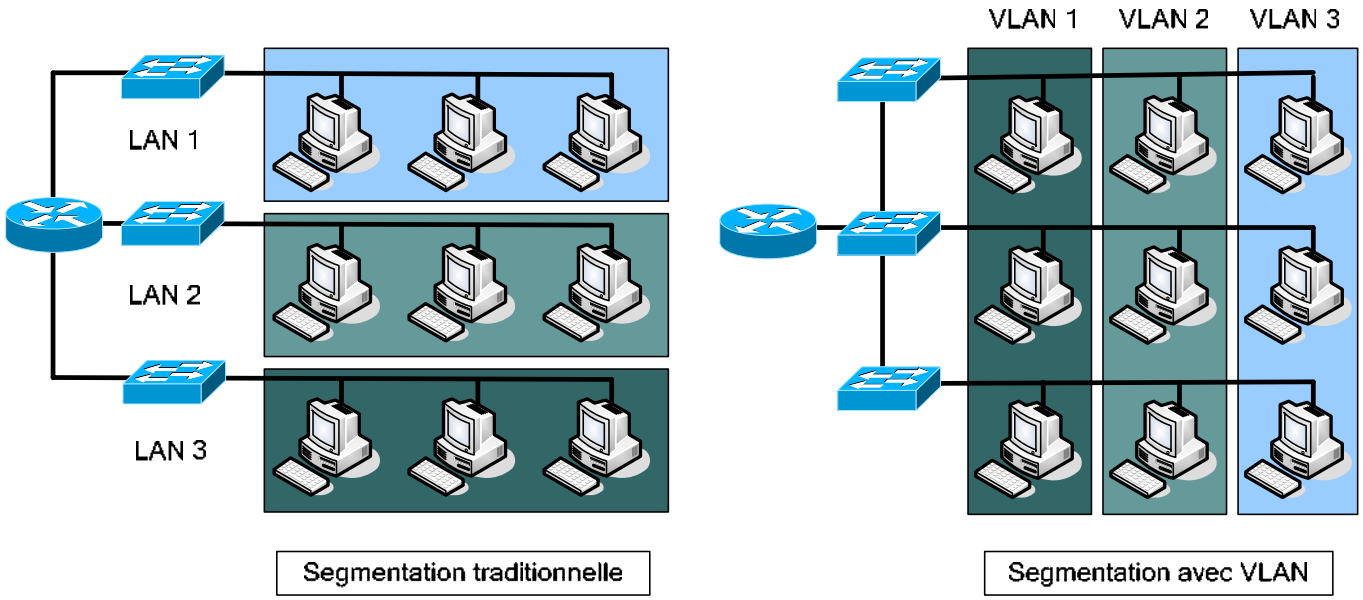
6.4. VLAN

6.4.1. Concepts

Un LAN virtuel est un ensemble d'unités regroupées en domaine de broadcast quelque soit l'emplacement de leur segment physique.

Les principales différences entre la commutation traditionnelle et les LAN virtuels sont:

- Les LAN virtuels fonctionnent au niveau des couches 2 et 3 du modèle OSI.
- La communication inter LAN virtuels est assurée par le routage de couche 3.
- Les LAN virtuels fournissent une méthode de contrôle des broadcasts.
- Les LAN virtuels permettent d'effectuer une segmentation selon certains critères:
  - Des collègues travaillant dans le même service.
  - Une équipe partageant le même applicatif.
- Les LAN virtuels peuvent assurer la sécurité des réseaux en définissant quels nœuds réseaux peuvent communiquer entre eux.



Il est donc possible de segmenter le réseau en plusieurs domaines de broadcast afin d'en améliorer les performances.

On distingue 2 méthodes de création pour les LAN virtuels :

- **LAN statiques** : ces VLAN sont dits accès sur les ports. L'appartenance à un VLAN est en effet fonction du port sur lequel est connecté un utilisateur (corrélation de couche 1 : port <-> VLAN). La configuration des commutateurs se fait donc en attribuant un port à un VLAN.

- **LAN dynamiques** : dans cette configuration, l'appartenance à un VLAN est déterminée par une information de couche supérieure : 2 ou plus (corrélation de couche>=2 <-> VLAN). Typiquement, on peut baser l'appartenance à un VLAN en fonction de l'adresse MAC de l'utilisateur. Cette configuration nécessite un logiciel d'administration réseau (ex : CiscoWorks 2000) basé sur un serveur. Lors de la connexion d'un hôte au commutateur, ce dernier enverra une requête au serveur lui indiquant, par exemple, l'adresse MAC du nouvel hôte connecté. Le serveur, grâce à une base de donnée liant MAC et VLAN (remplie par l'administrateur), renverra alors le VLAN d'appartenance au commutateur.

6.4.2. Commandes générales

- **vlan database**
  - Mode privilégié
  - Permet d'accéder au mode de configuration de VLAN.

- **vlan vlan_id [name { nom du vlan }]**
  - Mode de configuration des VLAN (vlan database)
  - Permet de créer et nommer les VLANs.

- **switchport mode {access | dynamic {auto | desirable} | trunk}**
  - Mode de configuration d'interface
  - Permet de configurer une interface pour le trunking ou pour un VLAN.

- **switchport access vlan vlan-id**
  - Mode de configuration d'interface
  - Permet de configurer un VLAN statique sur une interface.

6.4.3. Commandes show associées

- **show interfaces [interface-id | vlan vlan-id] [switchport | trunk]**
  - Affiche les statuts du trunking.

- **show vlan [brief | id vlan-id | name vlan-name | summary]**
  - Liste les informations sur le VLAN.

- **show vlan [vlan]**
  - Affiche des informations sur le VLAN.

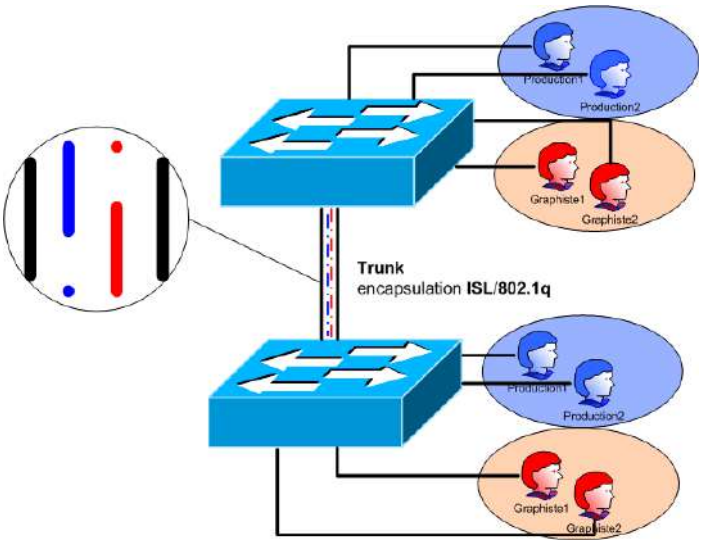
- **show spanning-tree vlan vlan-id**
  - Affiche les informations spanning-tree pour le VLAN spécifié.

6.4.4. Configuration

- **Configurer un VLAN statique**
  - Entrez dans le mode de configuration de VLAN à l'aide de la commande **vlan database**.
  - Créez le VLAN avec la commande **vlan** {vlan number}.
  - Entrez dans le mode de l'interface que vous souhaitez associer au VLAN.
  - Spécifiez le mode du port pour un VLAN : **switchport mode access**.
  - Spécifiez le VLAN avec la commande **switchport access vlan** vlan-id.

- **Sauvegarder la configuration VLAN**
  - Les configurations de VLAN sont automatiquement sauvegardées dans la flash dans le fichier **vlan.dat**.

6.5. Trunking



Le trunking permet, dans des réseaux comportant plusieurs commutateurs, de transmettre à un autre commutateur via un seul port, le trafic de plusieurs VLAN (dont les membres sont dispatchés sur plusieurs commutateurs). Le problème étant que différents trafics isolés (de différents VLAN) doivent emprunter un seul câble.

On a donc plusieurs trafics logiques sur une liaison physique : on appelle cette notion un trunk.
Afin d'identifier l'appartenance des trames aux VLAN, on utilise un système d'étiquetage (ou encapsulation) sur ce lien.

Il en existe deux protocoles :

- **ISL** (Inter Switch Link) qui est un protocole propriétaire Cisco.
- **802.1q** qui est un standard de l'IEEE.

6.5.1. Protocole ISL

Cisco avait développé bien avant l'IEEE son protocole ISL. Comme ISL est un protocole propriétaire Cisco, il ne peut être appliqué qu'à des commutateurs Cisco.

Avec l'emploie d'ISL, la trame originelle est encapsulée entre un en-tête de 26 octets et un en-queue de 4 octets.

Trame ISL

En-tête ISL 26 octets	Trame Ethernet encapsulée	FCS 4 octets

Composition de l'en-tête ISL

DA 40 bits	Type 4 bits	Util. 4 bits	SA 48 bits	LEN 16 bits	AAAA03 24 bits	HSA 24 bits	VLAN 16 bits	BPDU 1 bit	INDEX 16 bits	RES 16 bits

- DA : Adresse multicast de destination qui prend la valeur 0x01-00-0C-00-00 ou 0x03-00-0C-00-00.
- Type : Indique le type de trame (Ethernet, Token Ring, etc.).
- Util : Indique la priorité de traitement de la trame.
- SA : Adresse MAC source.
- LEN : Longueur de la trame encapsulé moins les 18 bits des champs DA, Type, Util., SA, LEN et FCS.
- AAAA03 : Champ SNAP d'une valeur fixe 0xAAAA03.
- HSA : Contient la portion constructrice de l'adresse MAC source.
- VLAN : Identifiant de VLAN.
- BPDU : Utilisé par l'algorithme Spanning Tree pour déterminer les informations topologiques.
- INDEX : Employé à des fins diagnostiques uniquement.
- RES : Utilisé quand une trame Token Ring ou FDDI est encapsulé dans une trame ISL.

6.5.2. Protocole 802.1q

Contrairement à ISL le protocole développé par L'IEEE 802.1q n'encapsule pas la trame Ethernet originale, mais insère un en-tête additionnel de 4 octets qui contient un champ d'identification du VLAN.

Le champ de contrôle de trame (FCS) doit être recalculé à cause de l'ajout de l'en-tête additionnel.

Trame Ethernet avec 802.1q.

Dest	Src	Etype	Tag	Long/Type Ether	Données	FCS

En-tête Tag.

Priorité		ID VLAN

6.5.3. Comparaison entre ISL et IEEE 802.1q

ISL	IEEE 802.1q
Encapsule la trame d'origine.	Ajoute un en-tête additionnel à la trame d'origine.
Comporte un champ d'identification de VLAN de 12 bits.	
Utilisation de PVST (Per VLAN Spanning Tree) pour obtenir un arbre STP par VLAN.	

6.5.4. Commandes associées

- **switchport mode trunk**
  - Depuis le mode de configuration spécifique du port, active le trunking.
- **switchport trunk [allowed | encapsulation | native | pruning]**
  - Quand l'interface est en mode trunking permet respectivement, de spécifier le type de caractéristiques VLAN, le type d'encapsulation (ISL, 802.1q), les caractéristiques natives et les caractéristiques de pruning des VLANs.

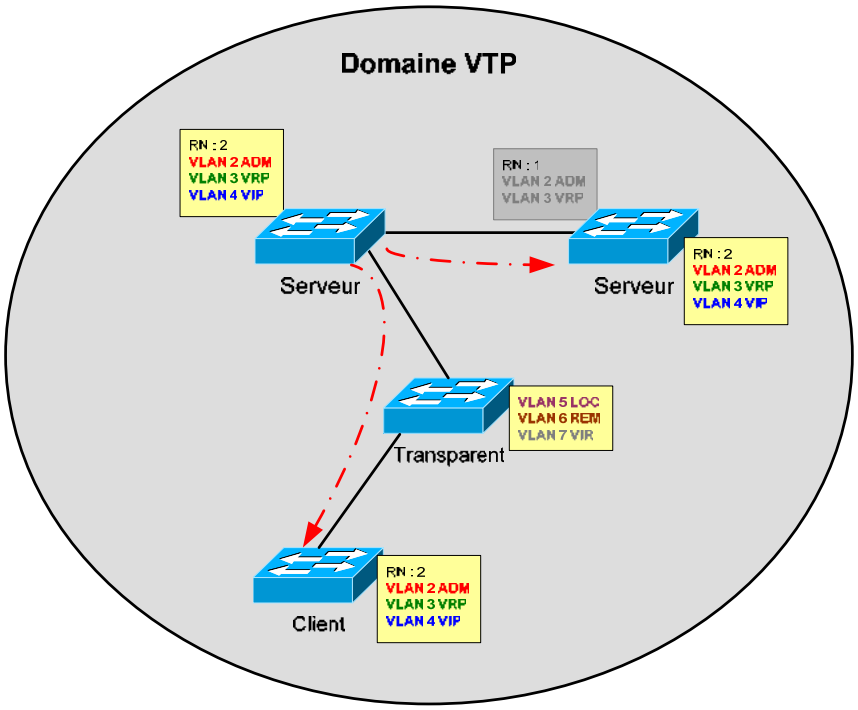
- **show port capabilities [numéro/sous-numéro]**
  - Affiche les fonctionnalités supportées par l'interface.
- **show trunk**
  - Permet de vérifier la configuration du trunking.

6.6. VTP

6.6.1. Théorie sur le protocole VTP

VTP (Virtual Trunking Protocol), protocole propriétaire Cisco permet, aux commutateurs et routeurs qui l'implémentent, d'échanger des informations de configuration des VLAN.

Il permet donc de redistribuer une configuration à d'autres commutateurs, évitant par la même occasion à l'administrateur de faire des erreurs, en se trompant par exemple de nom de VLAN. VTP diffuse ses mises à jour au sein du domaine VTP toutes les 5 min ou lorsqu'une modification a lieu.



Les mises à jour VTP comportent:

- Un numéro de révision (**Revision Number**) qui est incrémenté à chaque nouvelle diffusion. Cela permet aux commutateurs de savoir s'ils sont à jour.
- Les noms et numéro de VLAN.

Dans un domaine VTP, on distingue une hiérarchie comprenant trois modes de fonctionnement :

- VTP **serveur**
- VTP **client**
- VTP **transparent**

Les commutateurs qui font office de serveur VTP peuvent créer, modifier, supprimer les VLAN et d'autres paramètres de configuration. Ce sont eux qui transmettront cette configuration aux commutateurs en mode client (ou serveur) dans leur domaine VTP.

Les commutateurs fonctionnant en mode client ne peuvent que recevoir et transmettre les mises à jour de configuration.

Le mode transparent, lui, permet aux commutateurs de ne pas tenir compte des mises à jour VTP. Ils sont autonomes dans le domaine VTP et ne peuvent configurer que leurs VLAN (connectés localement). Cependant, ils transmettent aux autres commutateurs les mises à jour qu'ils reçoivent.

Les commutateurs en mode serveur et client mettent à jour leur base de données VLAN, si et seulement si, ils reçoivent une mise à jour VTP concernant leur domaine et contenant un numéro de révision supérieur à celui déjà présent dans leur base.

Fonction	Mode Serveur	Mode Client	Mode Transparent
Envoi de messages VTP	OUI	NON	NON
Réception des messages VTP ; Synchronisation VLAN	OUI	OUI	NON
Transmission des messages VTP reçus	OUI	OUI	OUI
Sauvegarde de configuration VLAN (en NVRAM ou Flash)	OUI	NON	OUI
Edition des VLANs (création, modification, suppression)	OUI	NON	OUI

Lorsqu'un hôte d'un VLAN envoie un broadcast, celui-ci est transmit à tous les commutateurs du domaine VTP. Il peut arriver que dans ce domaine, des commutateurs n'ait pas le VLAN concerné sur un de leur port.

Ce broadcast leur est alors destiné sans aucune utilité. Le **VTP pruning** empêche la propagation de ces trafics de broadcast aux commutateurs qui ne sont pas concernés.

6.6.2. Commandes associées

- **vlan database**
  - Mode privilégié
  - Permet d'accéder au mode de configuration de VLAN.

- **vlan vlan_id [name { nom du vlan }]**
  - Mode de configuration de VLAN
  - Permet de créer et nommer les VLANs.

- **vtp domain nom de domaine { password mot de passe | pruning | v2-mode | {server | client | transparent}}**
  - Mode de configuration de VLAN
  - Spécifie les paramètres VTP.

- **show vtp status**
  - Mode privilégié
  - Affiche la configuration VTP et le statut du processus.