ECOLE SUPERIEURE POLYTECHNIQUE D'ANTANANARIVO

DEPARTEMENT ELECTRONIQUE

MEMOIRE DE FIN D'ETUDES EN VUE DE L'OBTENTION DU DIPLOME D'INGENIEUR

Spécialité : ELECTRONIQUE

Option : Electronique Automatique
Informatique Appliqué

APPLICATION DES SWITCHES CISCO DANS UN RESEAU VLAN (VIRTUAL AREA NETWORK)

Présenté par: ANDRINIAINA Jimmy Rodin

Soutenue le : Vendredi 30 mai 2008

Numéro d'ordre: Année Universitaire : 2006-2007

APPLICATION DES SWITCHES CISCO DANS UN RESEAU VLAN (VIRTUAL AREA NETWORK)

Présenté par : ANDRINIAINA Jimmy Rodin

Le : Vendredi 30 mai 2008

Devant le jury: Madame RABEHERIMANANA Lyliane Irène

Monsieur ANDRIAMANANTSOA Guy Danielson

Monsieur RABEASANDRATANA ANDRIAMIHAJA Mamisoa

Monsieur RATSIMBA Mamy Nirina

Rapporteur : Monsieur RAKOTONDRASOA Justin

RESUME

Auparavant, pour constituer des réseaux locaux indépendants et stables , il était nécessaire de créer des réseaux physiques reliés entre eux par des routeurs, cette obligation liée à la localisation géographique des stations était contraignante pour l'administrateur réseau. Les VLAN(Virtual Local Area Network) ont révolutionné le concept de segmentation des réseaux, ils permettent de constituer autant de réseaux logiques que l'on désire sur une seule infrastructure physique, des réseaux logiques qui auront les mêmes caractéristiques que des réseaux physiques. Mais les VLAN ne sont réalisables qu'avec des commutateurs administrables, et avec l'apparition de ce nouveau matériel, plusieurs éléments essentiels dans la conception de réseau ont changé tant au niveau de l'architecture physique des réseaux, qu'au niveau de la configuration qui ne se fait plus que sur le routeur mais aussi dans ces commutateurs. Bien évidemment, des améliorations ont été implantées dans les logiciels des routeurs pour s'adapter au VLAN et à tous les autres nouveaux principes qui l'accompagnent. En effet, cette évolution des commutateurs a apporté de nouvel atout pour permettre d'introduire d'autre perspective, comme de nouvelle fonction qui serait impossible dans les commutateurs simples, citons par exemple les divers protocoles. L'administrateur doit donc prendre connaissance des nouvelles possibilités pour exploiter au mieux les commutateurs administrables.

Le présent rapport présente les VLAN, traite les avantages de l'utilisation d'une architecture de LAN virtuel et montre comment les appliquer sur des switches configurable CISCO en vue de donner un aperçu dans la nouvelle mode de configuration.

TABLE DES MATIERES

LISTE DES FIGURES

LISTE DES TABLEAUX

LISTE DES ABREVIATIONS

A		
	ARP	Address resolution protocol (Reverse ARP)
	AS	Autonomous System
B		
	BGP	Border Gateway Protocol
	BPDU	Bridge Protocol Data Units
	BRI	Basic Rate Interface
C		
	CCNP	CISCO Certified Network Professional
	CCITT	Comite Consultatif International télégraphique et téléphonique
	CHAP	Challenge Handshake Authentification Protocol
	CSMA/CA	Carrier sense Multiple Access with Collision Avoidance
	CSMA/CD	Carrier sense Multiple Access with Collision detect
	CDP	CISCO Descovery Protocol
D		
	DCE	Data Circuit terminating Equipment
	DTE	Data Terminal Equipment
	DTP	Dynamic Trunking Protocol
E		
	EGP	Exterior Gateway Protocol
	EIGRP	Enhanced Interior Gateway Routing Protocol
F		
	FDDI	Fiber Distributed Data Interface
G		
H		
I		
	ICMP	Internet Control Message Protocol
	IEEE	Institute of Electrical and Electronic Engineers
	IGRP	Interior Gateway Routing Protocol
	IPX	Internetworks Packet Exchange
	ISDN	Integrated Services Digital Network
	ISO	INTERNATIONAL STANDARDIZATION ORGANIZATION
J		
K		
L		
	LAN	Local Area Network (réseau local)
	LLC	Logic link control
M		
	MAC	Medium Access control
	MAN	Metropolitan Area Network (réseaux métropolitains)
	MAU	Media Attachement Unit
N		
O		
	OSI	Open System Interconnection (interconnexion de systèmes ouverts)
	OSPF	Open Shortest Path First

P

PAP	Password Authentification Protocol
PPP	Point to Point Protocol
PPTP	Point to Point Tunnelling Protocol

Q

R

RIP	Routing Information Protocol
RTC	Réseau téléphonique commuté

S

STP	Spanning Tree Protocol

T

U

UIT-T	Union International de Télécommunication

V

VLAN	Virtual Local Area Network (réseau locau virtuel)
VMPS	VLAN Membership Policy Server

W

WAN	Wide Area Network (réseaux étendus)

X

Y

Z

INTRODUCTION

Généralement, un réseau local est configuré en fonction de l'infrastructure physique dont il assure la connexion. Les utilisateurs sont regroupés en fonction de leur emplacement par rapport au concentrateur sur lequel leurs stations sont branchées et en fonction de la façon dont le câble est acheminé vers le local technique. Le routeur qui interconnecte chaque concentrateur partagé, assure habituellement la segmentation et peut servir de pare-feu de domaine de diffusion. Les segments créés par des commutateurs ne peuvent pas jouer ce rôle. La segmentation traditionnelle en LAN ne permet pas de regrouper les utilisateurs en fonction de leur groupe de travail ou de leurs besoins en bande passante. Ils partagent donc le même segment et rivalisent pour utiliser la même bande passante, bien que les besoins en bande passante varient considérablement selon le groupe de travail ou le service.

En plus, ce genre d'architecture que l'on peut dire ancienne, pose beaucoup de problème, comme la congestion à cause du nombre d'utilisateurs croissant. L'union d'ordinateurs et de stations de travail toujours plus puissants et d'applications gourmandes en ressources réseau a créé un besoin pour une capacité réseau, ou bande passante, de loin supérieur à celui disponible sur les LAN traditionnelles. Mais encore, il a été démontré que la sécurité dans ce genre de réseau n'était pas facile à administrer voire très complexe.

Alors, pour résoudre ces problèmes, le concept de réseau local virtuel ou VLAN (Virtual Local Area Network) a été développé par les constructeurs de matériel réseau.

L'idée première de la conception de VLAN est de pouvoir sécuriser et améliorer un réseau local (LAN) en utilisant des divers méthode pour cloisonner les réseaux tout en diminuant le trafic de messages utiles qui y circulent, et le plus important, tout cela devra se faire au niveau d'un seul matériel. Ensuite, l'idée suivante concerne le partage des diverses applications de l'entreprise dans le cas où ce dernier se situe dans de région différente et géographiquement éloignée.

Ainsi, ce présent rapport intitulé «APPLICATION DES SWITCHES CISCO DANS UN RESEAU VLAN (VIRTUAL AREA NETWORK) » a pour objectif principal d'expliquer le fonctionnement du réseau VLAN et de démontrer la possibilité du partage de ressource entre des réseaux VLAN par le biais d'un routeur [19]. Ce document se divise en quatre chapitres bien distincts.

Pour commencer, le premier chapitre rappelle les généralités sur les réseaux, et le second chapitre relate brièvement les éléments constituant un réseau local.

Ensuite, le vif du sujet qui concerne les VLAN est développé dans le chapitre trois.

Enfin, le dernier chapitre montre un aspect pratique et contient une simulation sur un logiciel de simulation réseau Boson Netsim (CCNP)[18].

CHAPITRE I: LES RESEAUX INFORMATIQUES

1- Modèle général de communication :

Au cours des années 70-80, l'évolution des réseaux informatiques a abouti à des plates-formes matérielles et logicielles différentes. Il en a résulté une incompatibilité entre de nombreux réseaux et il est devenu difficile d'établir des communications entre des réseaux fondés sur des spécifications différentes. Pour résoudre ce problème, l'Organisation internationale de normalisation (ISO acronyme de International Standard Organization) a créé un modèle réseau qui aiderait les concepteurs à mettre en œuvre des réseaux capables de communiquer entre eux et d'être interopérable. Le modèle de référence OSI (Open System Interconnection) a été publié en 1984

2- Le modèle de référence OSI :

Le principe de base est la description des réseaux sous forme d'un ensemble de couches superposées les unes aux autres, comme cela, l'étude du tout est réduite à celle des parties, l'ensemble devient plus facile à manipuler [1].

Le modèle permet de voir les fonctions réseau exécutées au niveau de chaque couche et constitue un cadre pour comprendre comment les informations circulent dans un réseau.

Ces couches sont au nombre de sept (7) dans le modèle OSI, chacune d'elle illustrant une fonction réseau bien précise. Cette répartition des fonctions réseau est appelée *organisation en couches*. Le découpage du réseau en sept couches présente les avantages suivants :

- Il permet de diviser les communications sur le réseau en éléments plus petits et plus simples.
- Il uniformise les éléments du réseau afin de permettre le développement et le soutien multiconstructeur.
- Il permet à différents types de matériel et de logiciel réseau de communiquer entre eux.
- Il empêche les changements apportés à une couche d'affecter les autres couches, ce qui assure un développement plus rapide.
- Il divise les communications sur le réseau en éléments plus petits, ce qui permet de les comprendre plus facilement

2-1 - Les 7 couches du modèle OSI

Les 7 couches peuvent être classées selon leur fonction en deux parties comme le montre la figure 1.1:

- Ceux qui se rapportent à la gestion de l'application
- et ceux qui se rapportent à la fonction de transport de données

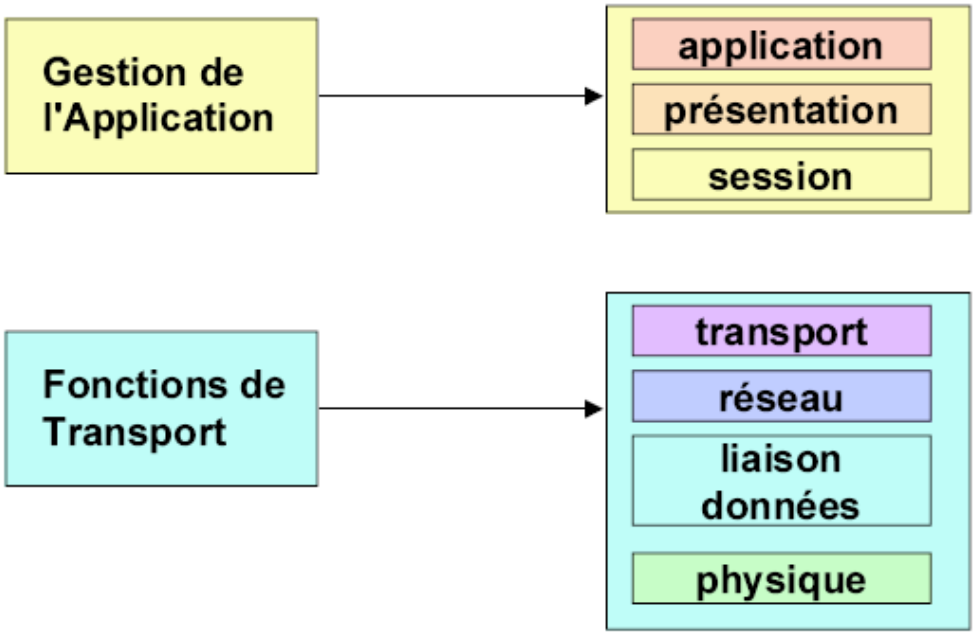


Figure1.1: Classement des 7 couches du modèle OSI selon leur fonction

La figure 1.2 résume et démontre le principe de fonctionnement du modèle OSI

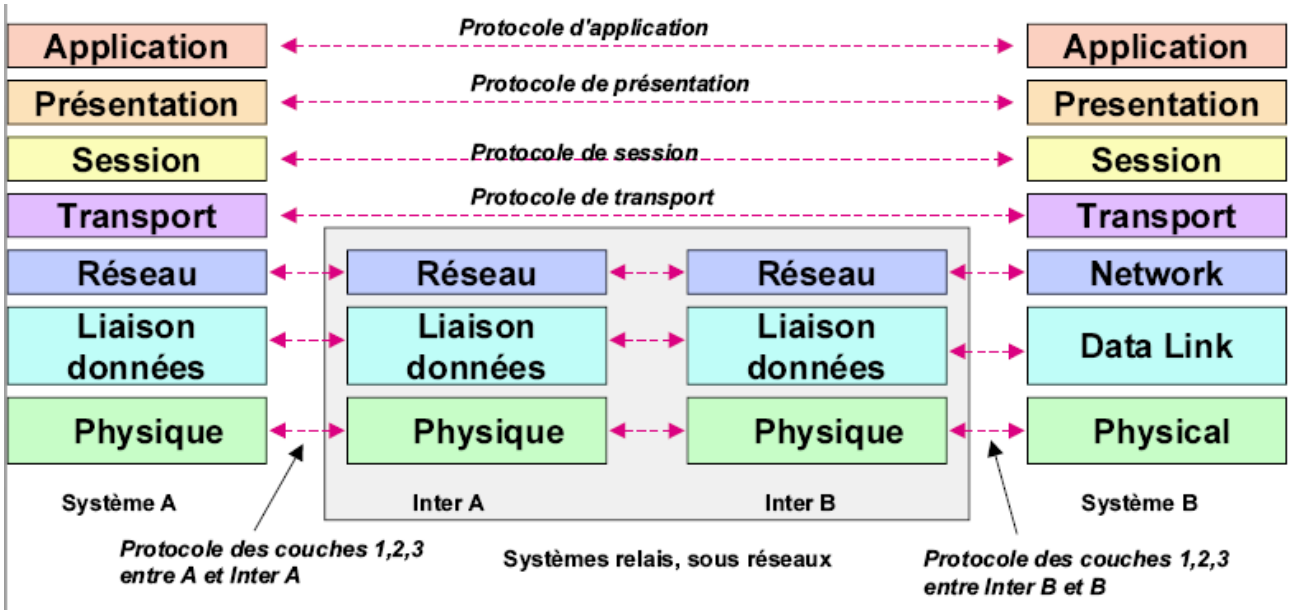


Figure1.2 : Présentation des 7 couches du modèle OSI avec les protocoles correspondants

Un *protocole* consiste en un ensemble de règles, ou conventions, qui déterminent le format et la transmission des données et augmentent l'efficacité des communications au sein d'un réseau. La *couche n* d'un ordinateur communique avec la *couche n* d'un autre ordinateur. Les règles et conventions utilisées lors de cette communication sont collectivement appelées *protocole de couche n*.

a- La couche 7 : La couche application

La couche application est la couche OSI la plus proche de l'utilisateur.

- Elle fournit des services réseau aux applications de l'utilisateur.

- Elle se distingue des autres couches en ce sens qu'elle ne fournit pas de services aux autres couches OSI, mais seulement aux applications à l'extérieur du modèle OSI.

Voici quelques exemples de ce type d'application : tableurs, traitements de texte et logiciels de terminaux bancaires.

- La couche application détermine la disponibilité des partenaires de communication voulus, assure la synchronisation et établit une entente sur les procédures de correction d'erreur et de contrôle d'intégrité des données.

b-La couche 6 : La couche présentation

La couche présentation s'assure que les informations envoyées par la couche application d'un système sont lisibles par la couche application d'un autre système c'est-à-dire qu'elle prend en charge les problèmes associés à la représentation des informations que les applications désirent échanger ou manipuler :

- Elle s'occupe des négociations des syntaxes de transfert de données pour la couche application permettant ainsi à cette dernière de ne se préoccuper que des aspects sémantiques des informations.

- Elle gère les formats de données et effectue les transformations nécessaires sur les structures de données pour les rendre compréhensibles par les équipements hétérogènes.

Exemple : la compression, l'organisation et encryptage des données …

c-La couche 5 : La couche session

- La couche session ouvre, gère et ferme les sessions entre deux systèmes hôtes en communication.

- Cette couche fournit des services à la couche présentation.

- Elle synchronise également le dialogue entre les couches de présentation des deux hôtes et gère l'échange des données.

- Outre la régulation de la session, la couche session assure un transfert efficace des données, une classe de service, ainsi que la signalisation des écarts de la couche session, de la couche présentation et de la couche application.

d-La couche 4 : La couche transport

- La couche transport assure que les messages des utilisateurs connectés au réseau parviennent correctement à leur destinataire, à cette fin elle offre des services supplémentaires de protection de données : c'est la fiabilité du transport des données

- Elle segmente les données envoyées par le système de l'hôte émetteur et les rassemble en flux de données sur le système de l'hôte récepteur.

- En fournissant un service de communication, la couche transport établit et raccorde les circuits virtuels, en plus d'en assurer la maintenance.

- La fourniture d'un service fiable lui permet d'assurer la détection et la correction des erreurs, ainsi que le contrôle du flux d'informations.

- La frontière entre la couche transport et la couche session peut être vue comme la frontière entre les protocoles d'application et les protocoles de flux de données.

e-La couche 3 : La couche réseau

- La couche réseau assure la connectivité et la sélection du chemin entre deux systèmes hôtes pouvant être situés sur des réseaux géographiquement éloignés : Ce sont l'adressage et le routage.

- Elle assure toutes les fonctionnalités de relais et d'amélioration de service à savoir le contrôle de flux et la détection et, la correction d'erreur non réglée dans la couche précédente.

Le contrôle de flux consiste à gérer les paquets pour qu'ils transitent le plus rapidement possible entre l'émetteur et le récepteur. L'objectif est d'éviter les problèmes de congestion du réseau qui surviennent lorsque trop de messages y circulent.

En effet les problèmes de congestion surviennent lorsque des nœuds d'un réseau saturent leur file d'attente et donc perdent des paquets. Si ces paquets sont réexpédiés ou si des messages de gestion de réseau se mettent à circuler en grand nombre, les performances du réseau vont diminuer très vite.

Le routage des paquets dans un réseau maille consiste à fixer par quelle ligne de sortie chaque commutateur réexpédie les paquets qu'il reçoit. Ceci se fait en fonction de la destination finale du paquet et selon une table de routage qui indique pour chaque destination finale quelles sont les voies sorties possible. Pour cela il existe un ensemble des processus algorithmiques devant prendre des décisions dispersées dans le temps et dans l'espace.

f-La couche 2 : La couche liaison de données

La couche liaison de données assure un transit fiable des données sur une liaison physique, pour cela elle fournit les moyens fonctionnels et procéduraux nécessaires à l'établissement, au maintien et à la libération des connexions de liaison de données entre entités du réseau.

- La couche liaison de données s'occupe de :
  - l'adressage physique (plutôt que logique)
  - la topologie du réseau,
  - l'accès au réseau,
  - la notification des erreurs,
  - la livraison ordonnée des trames
  - le contrôle de flux.

g-La couche 1 : La couche physique

La couche physique définit les spécifications électriques, mécaniques, procédurales et fonctionnelles permettant d'activer, de maintenir et de désactiver la liaison physique, destinées à la transmission de bits entre deux entités de liaison de données.

Les caractéristiques telles que les niveaux de tension, la synchronisation des changements de tension, les débits physiques, les distances maximales de transmission, les connecteurs physiques et d'autres attributs semblables sont définies par la couche physique.

Même si le modèle de référence OSI est universellement reconnu, historiquement et techniquement, la norme ouverte d'Internet est le protocole TCP/IP (Transmission Control Protocol/Internet Protocol). Le modèle de référence TCP/IP et la pile de protocoles TCP/IP rendent possible l'échange de données entre deux ordinateurs, partout dans le monde, à une vitesse quasi équivalente à celle de la lumière. Le modèle TCP/IP est basé sur le modèle du DoD (Departement of Defense).

3-Le modèle du DoD :

Le ministère américain de la défense (DoD) a défini un modèle de réseau à quatre couches, chacune d'entre elles comportant le protocole qu'on englobe sous la dénomination suite de protocole TCP/IP (Transmission Control Protocole)[7]. La figure 1.3 donne les 4 couches du modèle DOD en analogie avec le modèle OSI:

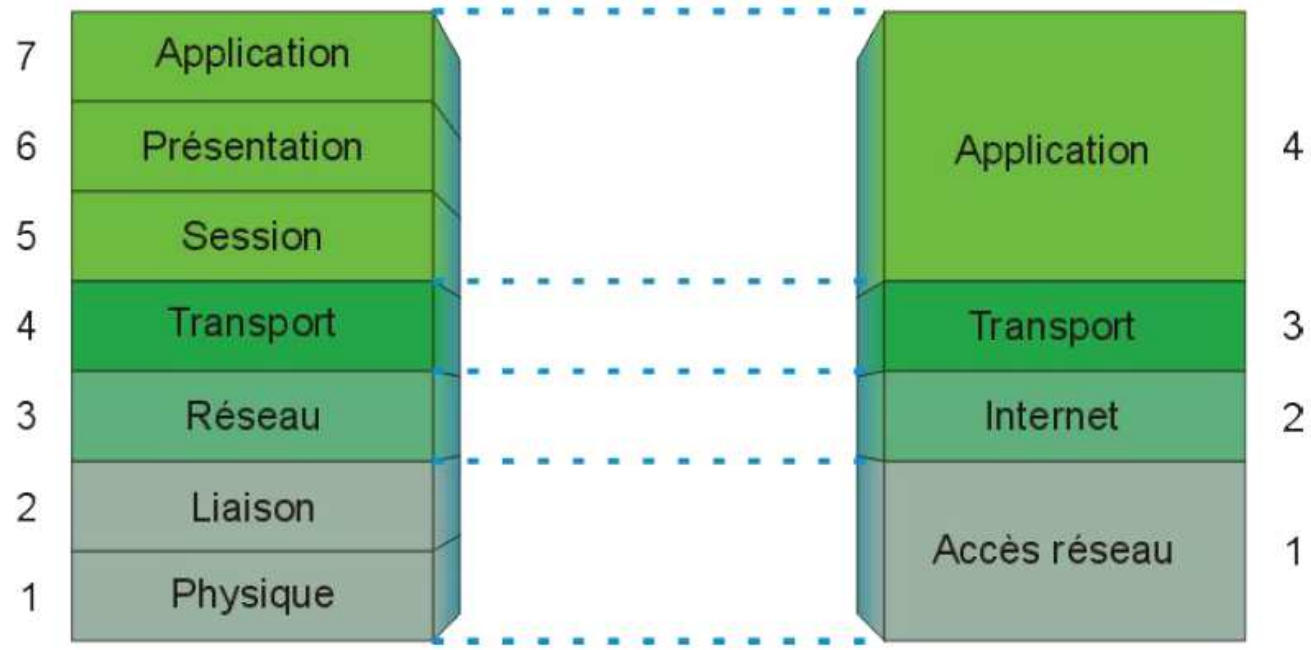


Figure 1.3: Analogie des couches entre le modèle OSI et le modèle DOD

3-1- La couche application :

La couche Application héberge des programmes d'application et sert de fenêtre d'accès au réseau. C'est à travers cette fenêtre que passent tous les échanges d'information signifiante entre les utilisateurs.

Il y a plusieurs protocoles dans la couche Application sur un réseau TCP/IP. Elle correspond en gros aux couches Application, Présentation, et Session du modèle OSI.

Les protocoles implémentes au niveau de cette couche Application sont les suivants :

- TELNET : Service d'émulation de terminal qui permet la connexion à distance. Il est très dangereux du fait que l'on peut piloter une machine à distance.
- FTP (File Transfer Protocol) : un service de transferts interactifs de fichier
- SMTP (Simple Mail Transfer Protocol) : un service de transfert de courrier électronique.
- DNS (Domain Name Service) : un service d'annuaire qui permet de faire correspondre un nom à une adresse IP ;
- RIP (Routage Information Protocoles): service d'annonce des diverses routes possible vers les numéros de réseaux de l'interréseau.
- NFS (Network File System) : Service de partage des catalogues de fichiers d'un ordinateur entre plusieurs machines du réseau.

- HTTP (Hypper Text Transfer Protocol) : Ce protocole est utilisé pour la navigation web entre un serveur HTTP et un butineur. Le protocole assure (normalement) qu'un client comme Internet Explorer ou Netscape Communicator peut envoyer des requêtes et recevoir les réponses de serveurs HTTP comme APACHE ou Internet Information Server sans problèmes particuliers.

  Les ennuis viennent du fait que les clients supportent bien souvent des extensions "propriétaires" du protocole. Ces extensions sont dans la plupart du temps entérinées dans les versions successives du protocole, c'est ainsi que tout évolue.
- POP3 (Post Office Protocol version 3) : Le protocole qui permet au client de relever à distance le courrier classé dans sa boîte aux lettres.
- IMAP4 (Interactive Mail Access Protocol version 4) : Normalement, ce protocole devrait prendre la place de POP3. Certains fournisseurs sérieux, comme FREE l'implémentent déjà. Contrairement à POP3 qui ne permet une gestion des messages qu'une fois qu'ils sont rapatriés localement, IMAP propose des fonctionnalités plus fines.
- NNTP (Network News Transfert Protocol) : Très proche de SMTP, ce protocole est employé par les forums usenet. Bien que l'usage des forums NNTP n'entre que tardivement dans les moeurs des internautes "débutants", ce moyen de communication offre des avantages incomparables par rapport aux listes de diffusion par exemple.

Chaque application se compose en principe de deux programmes distincts : un client et un serveur que l’on nomme souvent Démon.

3-2- La couche transport de Bout en Bout :

a- Définition :

La couche transport est responsable des traitements de paquets entre la couche Internet et une application. Elle est donc chargée des questions de qualité de service touchant la fiabilité, le contrôle de flux et la correction des erreurs.

Le concept de numéro de port ou numéro de socket est prépondérant dans ce monde des communications TCP/IP : à chaque application qui s’exécute sur l’ordinateur, correspond un numéro de port unique au niveau transport.

b- Les deux modes de transfert :

Il y a deux modes de transfert accompagnés chacun de son type de protocole dans la couche transport :

i- Le mode connecté : avec son protocole le TCP (Transmission Control Protocol)

Dans ce mode, il se met en place un processus de "handshake" (poignée de main) entre le client et le serveur. Ce processus permet d'établir un dialogue à propos du transfert de données. Il assure le contrôle de flux au moyen de fenêtres glissantes et fournit des numéros de séquence, des accusés de réception et des demandes d'émission etc. Il retransmet toute information non reçue et fournit un circuit virtuel entre les applications des utilisateurs finaux. Ce protocole présente l'avantage de permettre aux applications de savoir exactement où en est le processus de transfert de données et donc de garantir la transmission des segments.

Pour arriver à cette fonctionnalité, TCP définit un certain nombre de caractéristiques :

— flot d'octets : les données échangées sont vues comme un flot de bits, divisé en octets et les octets sont reçus dans l'ordre où ils ont été envoyés ;

— circuit virtuel en mode connecté : le transfert des données ne peut commencer qu'après l'établissement d'une connexion entre les deux machines. Durant le transfert, les deux machines continuent à vérifier que les données sont transmises correctement.

Le terme de circuit virtuel est employé, car les deux programmes d'application voient la connexion comme un circuit physique, la fiabilité de la transmission étant une illusion créée par le service de transport

— transfert par paquet : les programmes d'application envoient leurs données sur le circuit virtuel en les passant régulièrement au système d'exploitation de la machine. Chaque application choisit la taille de données qui lui convient, exprimée en nombre d'octets. Le protocole TCP est libre de découper les données en paquets de tailles différentes de ce qu'il a reçu de l'application. Pour rendre le transfert plus performant, le protocole TCP attend d'avoir suffisamment de données pour remplir un datagramme avant de l'envoyer sur le sous-réseau.

— flot de données non structurées : le service de transport ne prend pas en compte les données structurées (cela est du ressort de l'application).

— connexion duplex : la connexion permet un transfert de données bidirectionnel. Ce sont deux flots de données inverses, sans interaction apparente. Il est possible de déterminer l'envoi dans un sens, sans arrêter l'autre sens. Ce principe permet de renvoyer des acquittements d'un sens de transmission, en même temps que les données de l'autre sens.

Le protocole TCP définit la structure des données et des acquittements échangés, et les mécanismes permettant de rendre le transport fiable. Il spécifie comment distinguer plusieurs connexions sur une même machine, et comment faire la détection et la correction, lors de la perte ou duplication de paquets. Il définit comment établir une connexion et comment la terminer.

Le protocole TCP permet à plusieurs programmes d'établir une connexion en même temps et démultiplexe les données reçues, provenant d'applications différentes. TCP utilise la notion abstraite de port qui identifie la destination ultime dans la machine.

TCP est donc un protocole en mode connecté qui n'a de sens qu'entre deux points d'extrémité de connexion. Pour cela, le programme d'une extrémité effectue une ouverture de connexion « passive » qui permet d'accepter une connexion entrante en lui affectant un numéro de port. L'autre programme d'application exécute une ouverture de connexion « active ». Une fois la connexion établie, le transfert de données peut commencer.

Le protocole TCP voit un flot de données comme un suite d'octets qu'il divise en segments. Généralement, chaque segment est transmis dans un seul datagramme IP.

TCP utilise un mécanisme de fenêtre pour réaliser une transmission performante par un contrôle de flux adapté aux caractéristiques de l'application et du réseau. Le mécanisme de fenêtre permet l'anticipation, c'est-à-dire l'envoi de plusieurs messages sans attendre d'acquittement. Cela permet d'éviter les congestions, si les fenêtres sont bien adaptées. La fenêtre permet également de réaliser un contrôle au niveau de la machine terminale, en autorisant le récepteur à limiter l'envoi des données s'il n'a pas la place nécessaire pour les recevoir dans ses mémoires. Le mécanisme de fenêtre opère au niveau de l'octet et non pas du message. Les octets à transmettre sont numérotés séquentiellement, et l'émetteur gère trois pointeurs pour chaque fenêtre. De la même façon, le récepteur doit tenir à jour une fenêtre en réception. Pour une connexion, il est possible d'échanger des données indépendamment dans chaque sens, et chaque extrémité de connexion doit ainsi maintenir deux fenêtres, l'une en émission et l'autre en réception.

Une différence importante entre un mécanisme de fenêtre classique et celui employé par TCP provient de la taille de la fenêtre qui peut varier dans le temps. Chaque acquittement, spécifiant combien d'octets ont été reçus, contient une information de taille de fenêtre qui indique combien d'octets supplémentaires le récepteur est en mesure d'accepter. La taille de fenêtre peut être vue comme la taille libre des mémoires. Le récepteur ne peut réduire la fenêtre en deçà d'une valeur qu'il a déjà acceptée précédemment. En revanche, une taille de fenêtre plus petite peut accompagner un acquittement, de façon à ce qu'elle diminue en même temps qu'elle se déplace.

L'unité de protocole de TCP est appelée un segment. Ces segments sont échangés pour établir la connexion, pour transférer des données, pour les acquittements, pour modifier la taille de la fenêtre et enfin pour fermer une connexion. Les informations de contrôle de flux peuvent être transportées dans le flot de données inverses. Chaque segment est composé de deux parties : l'en-tête suivi des données.

Le format d'un segment est représente par la figure1.4 ci-dessous.

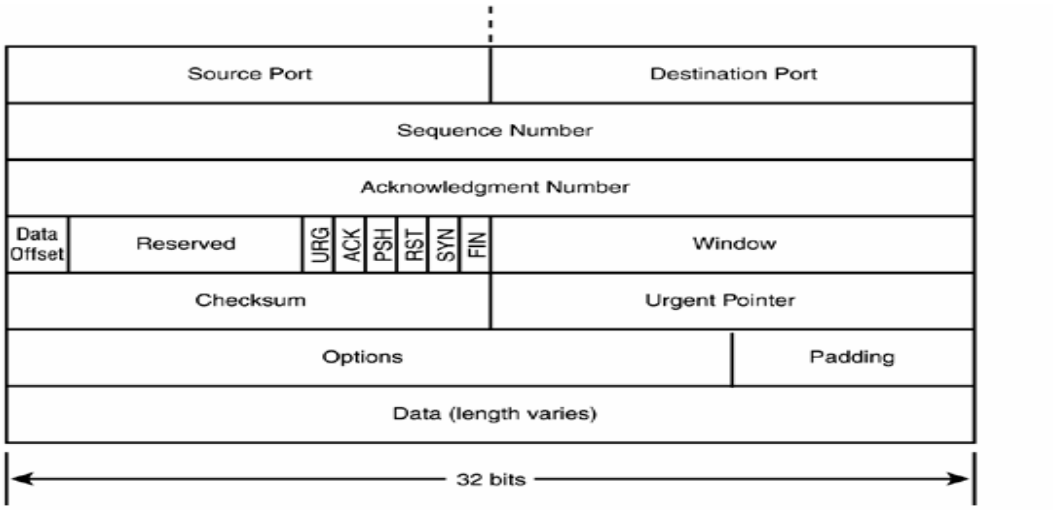


Figure 1.4: format du segment TCP

Dans le segment, on trouve les zones suivantes :

1 – Source port sur 16 bits. Ce champ contient l'adresse du port d'entrée. Associée avec l'adresse IP, cette valeur donne un identificateur unique appelé socket ;

2 – Destination port sur 16 bits. Même chose que le précédent mais pour l'adresse destination ;

3 – Séquence number (SEQ) sur 32 bits. Ce champ indique le numéro du premier octet porté par le segment ;

4 – Acknowledgement number (ACK) sur 32 bits. Cette valeur indique le numéro « sequence number » du prochain segment attendu. En d'autres termes, c'est un acquittement de tous les octets qui ont été reçus auparavant ;

5 – Data offset sur 4 bits. Cette valeur indique la longueur de l'en-tête par un multiple de 32 bits. Si la valeur 8 se trouve dans ce champ, la longueur totale de l'en-tête est de 8 × 32 bits. Cette valeur est nécessaire parce que la zone d'option est de longueur variable ;

6 – La zone suivante est réservée pour une utilisation ultérieure.

Ce champ doit être rempli de 0 ;

7 – Urgent Pointer (URG) sur 1 bit. Si ce bit est positionné à 1, cela indique que le champ Urgent Pointer dans la suite est utilisé ;

8 –Synchronisation (SYN) sur 1 bit. Si SYN = 1, cela indique une demande d'ouverture de connexion ;

9 –Acknowledgement (ACK) sur 1 bit. Si ACK = 1, cela indique que le champ Acknowledgement number est utilisé ;

10 –Reset (RST) sur 1 bit. Si RST = 1, cela signifie que l'émetteur demande que la connexion TCP soit redémarrée ;

11 –Push function (PSH) sur 1 bit. Si PSH = 1, cela indique que l'émetteur souhaite que les données de ce segment soient délivrées le plus tôt possible au destinataire ;

12 –Terminale (FIN) sur 1 bit. Si FIN = 1, cela signifie que l'émetteur souhaite fermer la connexion ;

13 – Window (WNDW) sur 16 bits. La valeur indiquée dans ce champ donne le nombre d'octets que le récepteur accepte de recevoir. Plus exactement, la valeur de WNDW contient le numéro du dernier octet que l'émetteur du segment peut prendre en compte. En retranchant le numéro indiqué dans Acknowledgement number, on obtient le nombre d'octets que le récepteur accepte de recevoir ;

14 – Checksum sur 16 bits. Les deux octets permettent de détecter les erreurs dans l'en-tête et le corps du segment ;

15 – Urgent Pointer (URGPTR) sur 16 bits. Ce champ spécifie le dernier octet d'un message urgent ;

16 – Options (OPT). Cette zone contient les différentes options du protocole TCP. On y trouve principalement des options de routage.

Le segment se termine par les données transportées.

ii- Le mode non connecté : avec son protocole le UDP (User Datagram protocol)

Le protocole UDP (User Datagram Protocol) permet aux applications d'échanger des datagrammes. Ce protocole UDP utilise la notion de « port » qui permet de distinguer les différentes applications qui s'exécutent sur une machine. En plus du datagramme et de ses données, un message UDP contient, à la fois, un numéro de port source et un numéro de port destination, comme le montre la figure1.5.

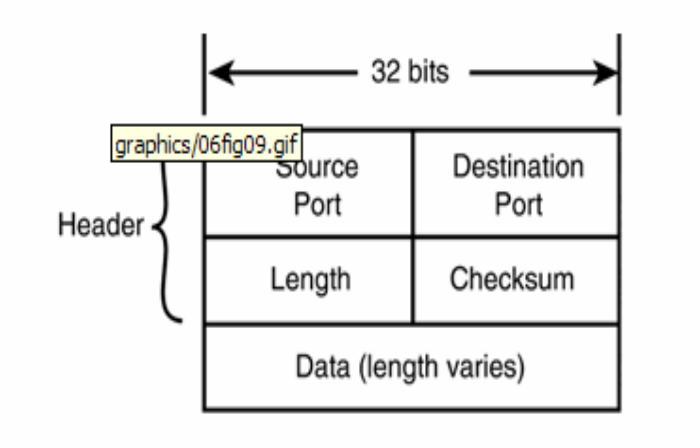


Figure 1.5: format du segment UDP

Le protocole UDP n'exécute aucune vérification logicielle sur l'acheminement des segments au niveau de la couche transport. Il n'utilise aucun acquittement, ne reséquence pas les messages et ne met en place aucun contrôle de flux.

Avantage :

L'avantage de ce protocole est sa vitesse. Comme il ne fournit pas d'accusés de réception, le trafic sur le réseau est plus faible, ce qui accélère les transferts.

Inconvénient :

Les messages UDP peuvent être perdus, dupliqués, remis hors séquence ou arriver trop tard pour être traités en réception donc ce protocole n'est pas fiable.

3-3- La couche internet :

La couche Internet de la pile TCP/IP correspond à la couche réseau du modèle OSI. Elle est chargée de transporter des paquets sur un réseau au moyen un adressage logiciel.

Plusieurs protocoles sont exécutés dans la couche Internet TCP/IP tel que :

a- Le protocole IP (Internet Protocol) :

Le protocole IP est un protocole très simple qui a pour but de transporter des paquets, que l'on appelle datagrammes, d'une porte d'entrée du réseau à une porte de sortie. C'est une couche dans un mode sans connexion, c'est-à-dire qu'un émetteur peut envoyer des datagrammes sans au préalable avertir l'entité correspondante de l'autre côté du réseau. Il ne se préoccupe pas du contenu des datagrammes ; il recherche uniquement un moyen de les acheminer à destination. La version actuelle, celle utilisée dans le réseau Internet, est IPv4 (IP version 4). Une nouvelle version, IPv6, prendra bientôt sa place.

i- IPv4 Internet Protocol version 4:

- Le datagramme IPv4 :

Le service rendu par le protocole IPv4 est déterminé par un système de remise de paquets, non fiable, « au mieux » et sans connexion. Le service est dit non fiable car la remise n'est pas garantie. Un paquet peut être perdu, dupliqué, ou remis hors séquence, mais le protocole IP ne détectera rien et n'en informera ni l'émetteur, ni le récepteur. Il est dit sans connexion car chaque paquet est traité indépendamment des autres. Les paquets d'un même message, transitant d'une machine à une autre, peuvent utiliser des routes différentes et certains peuvent être perdus, les autres arrivant à leur destination.

Il y a une analogie entre un réseau physique et un réseau TCP/IP. Dans un réseau, l'unité transférée entre deux noeuds est la trame qui contient un en-tête et des données. L'en-tête contient des informations comme l'adresse source et destinataire. Dans un réseau TCP/IP, l'unité de base à transférer est le datagramme Internet, souvent appelé datagramme IP, ou paquet IP, ou simplement datagramme. Le datagramme est également divisé en un en-tête et une partie donnée. La structure du datagramme IPV4 est décrite dans la figure 1.6 :

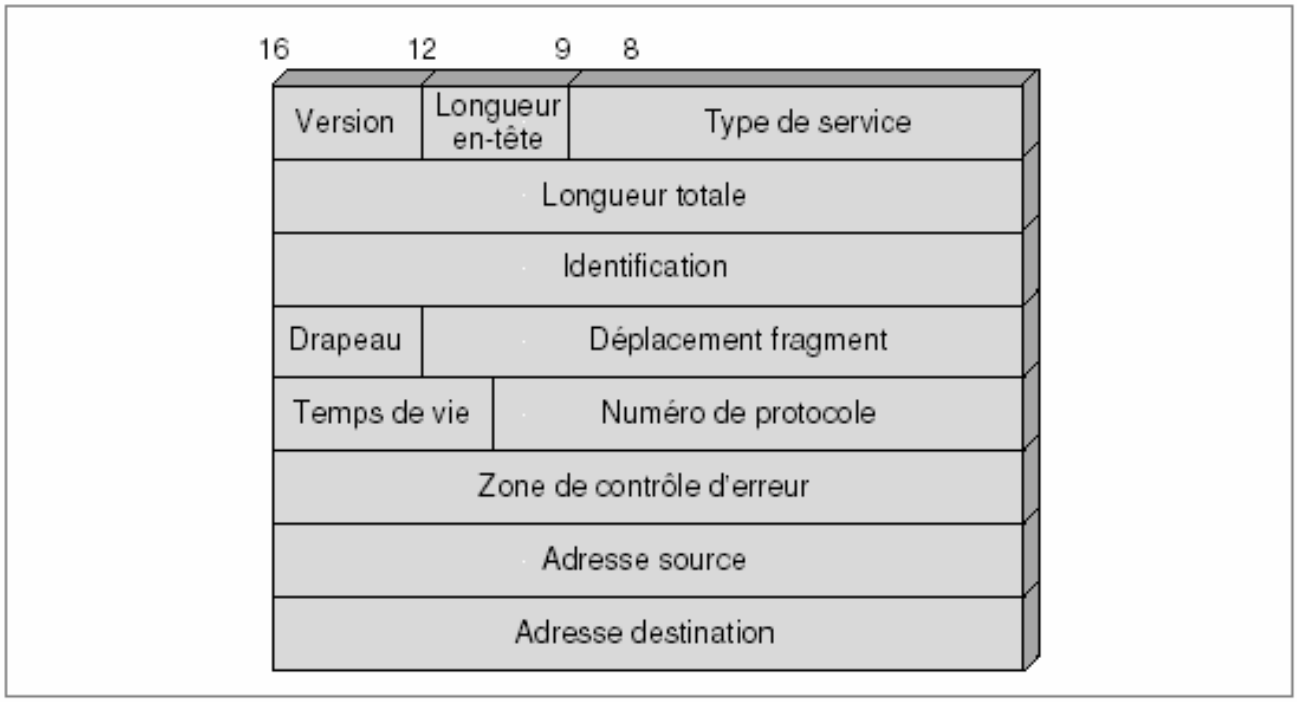


Figure 1.6: Datagramme IPv4

VERSION : numéro de version

Longueur en-tête : longueur de l'en-tête, en mots de 32 bits

Type de service : mode de traitement du datagramme

Longueur totale : longueur totale (en-tête + données)

Identification, Drapeau, Déplacement de fragmentation : fragmentation des datagrammes autorisant divers types de MTU sur l'interréseau

TTL : Time To Live : durée de vie

Numéro protocole : Numéro de protocole de couche supérieure (couche 4) qui envoie le datagramme

Zone de contrôle d'erreur: contrôle d'intégrité de l'en-tête

Adresse IP d'origine et adresse IP de destination : adresses IP de 32 bits

- L'encapsulation et décapsulation des paquets IPv4 :

Contrairement aux trames, les datagrammes sont manipulés par le logiciel. Ils peuvent être de longueur quelconque. Cependant, comme ils doivent transiter de machine en machine, ils sont toujours transportés dans des trames physiques.

Ce concept est appelé l'encapsulation. Pour le sous-réseau, un datagramme est une entité comme une autre. Dans le meilleur des cas, le datagramme est contenu dans une seule trame, ce qui rend la transmission plus performante.

Le processus d'encapsulation et de décapsulation est décrit dans la figure1.7 :

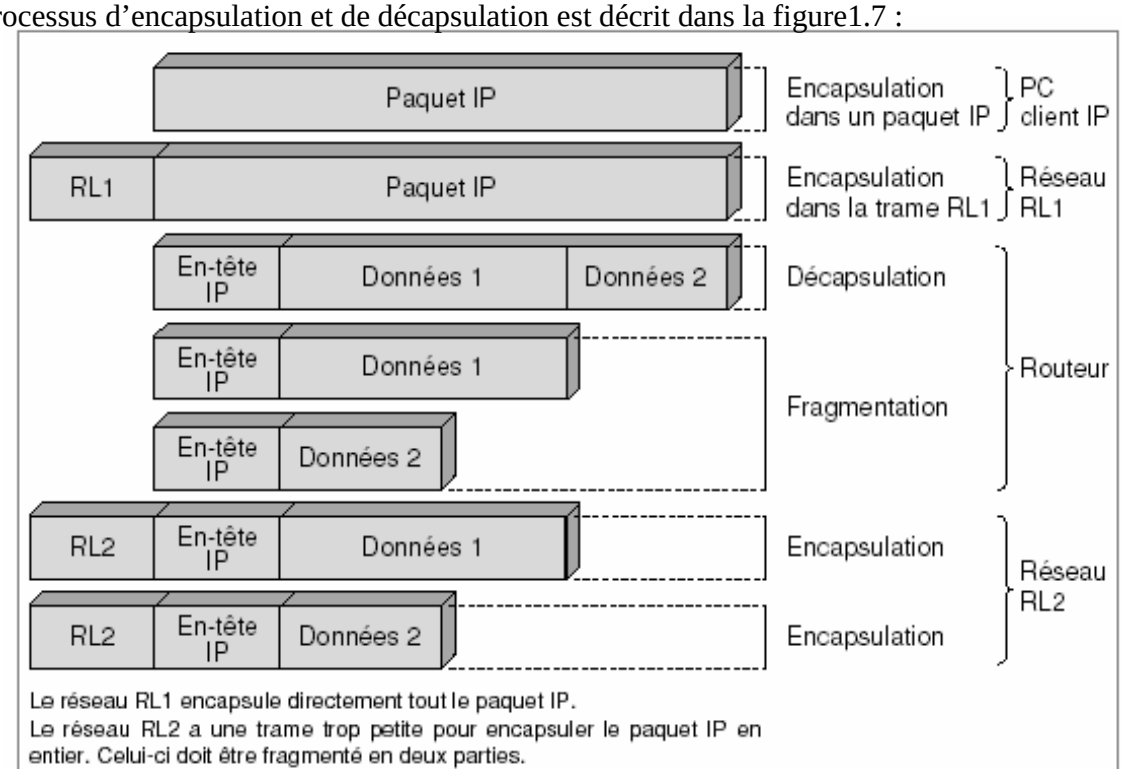


Figure 1.7: Encapsulation et décapsulation des paquets IPv4

- L’adressage IPv4:

Avant de commencer, Il est faut qu’il existe deux systèmes d'adressage dans les réseaux :

- adressage physique : L’adresse physique ou plus connue sous le nom d’adresse MAC (Medium Access Control) est une adresse écrite en dur dans la ROM (Read Only Memorie) d'un équipement réseau, le plus souvent une interface réseau. Cette adresse est réputée unique et décidée par le constructeur de la carte.

Il faut bien comprendre que cette adresse est indispensable, parce qu'elle est la seule qui soit définie à la mise en route d'un système, puisqu'elle réside dans une ROM. D'ailleurs, certains protocoles réseaux simples se contentent de cette adresse pour fonctionner. Comme exemple NetBEUI.

Cette adresse est définie sur 6 octets.

• Les trois premiers (les plus à gauche) sont attribués au constructeur.

• Les trois derniers sont spécifiques à un équipement matériel donné.

-Avantages et inconvénients :

Nous l'avons vu, le principal avantage est que cette adresse unique est disponible immédiatement lors de la procédure de "boot" et qu'elle est alors la seule disponible, de plus, c'est la seule qui soit utilisable dans les couches basses du réseau.

Son principal inconvénient est qu'elle est physiquement attachée à un hôte. Pour en changer, il faut changer d'interface. De plus, la répartition de ces adresses sur un réseau est faite de manière quasi aléatoire, il n'y a que le constructeur de l'interface qui maîtrise cette adresse. Il est donc impossible d'organiser cet adressage de manière logique.

Cette méthode ne permettant pas l'interconnexion de réseaux, il va être nécessaire d'ajouter dans la couche supérieure (niveau 3), une adresse logique qui sera attribuée par l'administrateur du réseau, en coordination avec les organismes chargés de gérer l'attribution de ces adresses. Dans le cas ici, il s'agit de la fameuse adresse IP.

- Adressage logique : Les machines travaillant sous le protocole IP possèdent une adresse tenant sur 32 bits c'est-à-dire sur 4 octets.

Cette adresse est souvent représentée par une suite de quatre nombres séparés par des points ; par exemple 191.92.34.223.

L’adresse est constituée de deux parties : un identificateur de réseau (le NetID) et un identificateur de la machine à l’intérieur de ce réseau (le HostID).

Il existe quatre classes d'adresses, chacune permettant de coder un nombre différent de réseaux et de machines décrites par la figure 1.8 ci-dessous :

— classe A – 128 réseaux (codés sur 7 bits) et 16 777 216 hôtes (codés sur 24 bits)
Adresse de départ Début-fin : 0-127;

— classe B – 16 384 réseaux (codés sur 14 bits) et 65 535 hôtes (codés sur 16 bits)
Adresse de départ Début-fin : 128-191;

— classe C – 2 097 152 réseaux (codés sur 21 bits) et 256 hôtes (codés sur 8 bits)
Adresse de départ Début-fin :192-223;

— classe D – adresses de groupe (codés sur 28 bits) Adresse de départ Début-fin : 224-255.

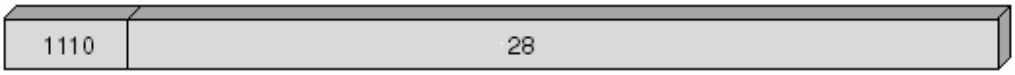


Figure 1.8: Classes d'adresse IPv4

- Faiblesses d'IPv4

Les faiblesses d'IPv4 concernent d'abord l'adressage qui est limité par les quatre octets disponibles. En fait, la distribution des adresses n'a pas été faite avec suffisamment de soin et de nombreuses adresses de classe A et surtout B sont excessivement mal utilisées.

Le second problème concerne l'arrivée d'applications multimédias qui contiennent des synchronismes forts comme celui de la parole. Dans la version IPv4, il est impossible de discerner, dans la zone d'information du paquet, une application qui possède des contraintes par rapport à une application qui n'a pas de contraintes particulières. Il n'y a pas non plus de possibilité de faire transiter de la signalisation ou de l'information de gestion.

ii- IPv6 Internet Protocol version 6 :

Le protocole IPv6 représente la nouvelle génération du protocole IP. Les fonctionnalités ont été entièrement repensées et le protocole IPv6 forme réellement une nouvelle génération, d'où le nom IPng (next generation) qu'on lui donne également.

Le format du paquet IPv6 est décrit dans la figure 1.9 ci après.

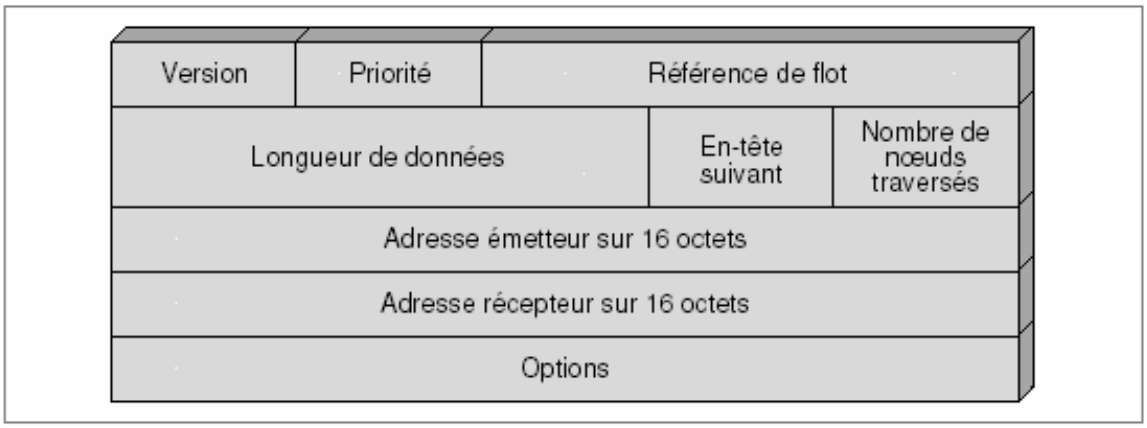


Figure 1.9 : Datagramme IPv6

Version : champ qui porte le numéro de version (6 pour IPv6).

Priorité : champ qui indique un niveau de priorité permettant un traitement plus ou moins prioritaire dans les noeuds du réseau. Les principales valeurs sont les suivantes :

0 pas de priorité particulière ;

1 trafic de base (news) ;

2 transfert de données sans contrainte temporelle (email) ;

3 réservé pour le futur ;

4 transfert en blocs avec attente du récepteur (transfert de fichiers) ;

5 réservé pour le futur ;

6 traficinteractif (login, terminal virtuel) ;

7 trafic pour le contrôle (routage, contrôle de flux).

Référence de flot : champ qui permet d'indiquer la qualité de service (QoS) des informations transportées dans le paquet IPv6. Cette indication permet aux routeurs de prendre des décisions adaptées aux données transportées ; des algorithmes d'ordonnancement des trames pourront être implantés dans les routeurs.

Longueur de données : champ indiquant la longueur des données précise la longueur totale du datagramme en octets (sans tenir compte de l'en-tête). Ce champ étant de 2 octets, la longueur maximale est de 64 Ko.

En-tete suivant : champ qui identifie le protocole qui sera utilisé à l'intérieur du champ de données.

Les options sont les suivantes :

0 Hop-by-Hop Option Header ;
4 IP ;
6 TCP ;
17 UDP ;
43 Routing Header ;
44 Fragment Header ;
45 Interdomain Routing Protocol ;
46 Resource Reservation Protocol (RSVP);
50 Encapsulating Security Payload;
51 Authentification Header;
58 ICMP;
59 No Next Header;
60 Destination Options Header.

Nombre de nœud traversés : indique le nombre maximal de noeuds traversés par le paquet avant que celui-ci soit détruit

- Adressage IPv6 :

L'adresse IPv6 tient sur 16 octets au lieu des 4 pour la première génération. La difficulté réside dans la représentation et l'utilisation rationnelle de ces 128 bits. La représentation s'effectue par groupe de 16 bits sous la forme :

123 : FCBA : 1 024 : AB23 : 0 : 0 : 24 : FEDC

Une série d'adresses égales à 0 peut être abrégée par le signe « :: » qui ne peut apparaître qu'une seule fois dans l'adresse. En effet, il faut pouvoir en déduire le nombre d'adresses 0 en série et si deux séries de 0 existaient, il ne serait plus possible d'en déduire la longueur de chacune.

- Avantage de IPv6 :

L'adressage IPv6 constitue un adressage hiérarchique avec beaucoup plus de niveaux que les trois disponibles dans IPv4.

Un avantage immédiat sera de réduire la taille des tables de routage des routeurs et donc d'augmenter le temps de recherche des informations pour effectuer la procédure de routage.

- Le champ d'extension:

Les informations facultatives de la couche réseau ne sont pas incluses dans l'en-tête IPv6. Elles sont incluses dans le champ d'extension illustré dans la figure 1.10. Elles sont chiffrés et sont placés entre l'en-tête IPv6 et l'en-tête de la couche supérieure. Les en-têtes de l'extension ne sont pas traités par chaque noeud le long de l'acheminement du paquet. Ils sont examinés seulement par le noeud (ou noeuds dans le cas de destinations multicast) qui est identifié dans le champ de l'Adresse de Destination de l'en-tête de l' IP. Cela améliore l'efficacité du réseau en n'exigeant pas que chaque routeur traite l'information qui est prévue seulement pour le noeud de destination. La seule exception est l'option HOP-BY-HOP. L'option HOP-BY-HOP contient de l'information qui est prévue pour chaque routeur le long du parcours du paquet.

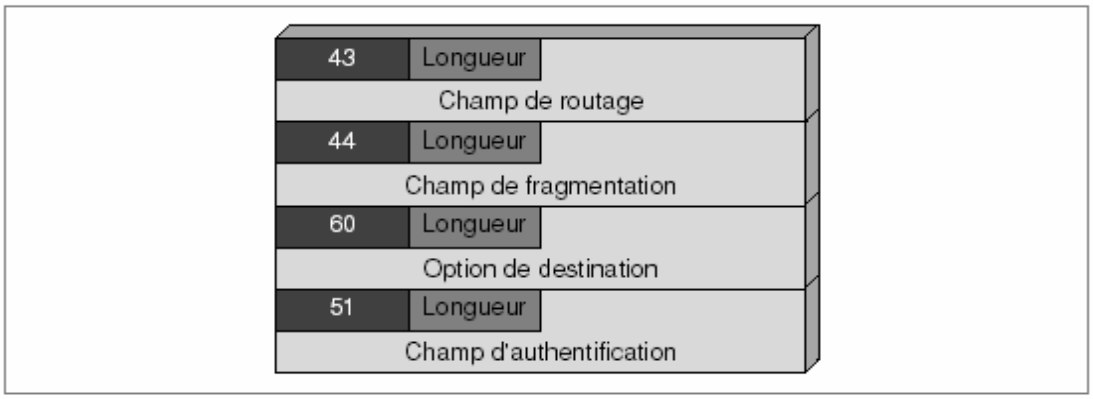


Figure 1.10: champs d'extension de l'adressage IPv6

Chaque zone d'extension commence par un champ indiquant, par un numéro, le type d'extension. On a les options suivantes, qui ont déjà pu être utilisées dans la partie « en-tête suivante » :

0 Hop-by-Hop Option Header;

43 Routing Header;

44 Fragment Header;

51 Authentification Header;

59 No Next Header;

60 Destination Options Header.

b- Le protocole ICMP (Internet Control Message Protocol)

La gestion et le contrôle sont des processus fortement imbriqués dans les nouvelles générations de réseaux IP. La différence entre les deux processus s'estompe de fait par l'accroissement de la vitesse de réaction des composants, de telle sorte qu'un contrôle, qui demande une réaction en temps réel, n'est plus très loin d'un processus de gestion.

Dans le système en mode sans connexion, chaque passerelle et chaque machine fonctionnent de façon autonome. De même, le routage et l'envoi des datagrammes se font sans coordination avec le récepteur. Ce système marche bien tant que les machines ne rencontrent pas de problème et que le routage est correct, mais cela n'est pas toujours le cas.

Outre les pannes matérielles et logicielles du réseau et des machines qui y sont connectées, des problèmes surviennent lorsqu'une station est déconnectée du réseau, que ce soit temporairement ou de façon permanente, ou lorsque la durée de vie du datagramme expire, ou enfin lorsque la congestion d'une passerelle devient trop importante.

Pour permettre aux machines de rendre compte de ces anomalies de fonctionnement, on a ajouté à Internet un protocole d'envoi de messages de contrôle, appelé ICMP *(Internet Control Message Protocol).*

Le destinataire d'un message ICMP n'est pas un processus application mais le logiciel Internet de la machine. Ce logiciel IP traite le problème porté par le message ICMP à chaque message reçu.

Les messages ICMP ne proviennent pas uniquement des passerelles. N'importe quelle machine du réseau peut envoyer des messages à n'importe quelle autre machine. Les messages permettent de rendre compte de l'erreur en remontant jusqu'à l'émetteur d'origine. Les messages ICMP prennent place dans la partie donnée des datagrammes IP. Comme n'importe quels autres datagrammes, ils peuvent être perdus. En cas d'erreur d'un datagramme contenant un message de contrôle, aucun message de rapport de l'erreur n'est transmis.

Comme pour le protocole IP, deux versions du protocole ICMP sont disponibles, la version associée à IPv4 et celle associée à IPv6. La version ICMPv6 est particulièrement importante, car elle regroupe tous les messages de contrôle et d'information des différents protocoles de la première génération.

3-4- La couche d'accès au réseau :

Le nom de cette couche a un sens très large et peut parfois prêter à confusion. On lui donne également le nom de couche hôte-réseau. Cette couche se charge de tout ce dont un paquet IP a besoin pour établir une liaison physique, puis une autre liaison physique. Cela comprend les détails sur les technologies LAN et WAN, ainsi que tous les détails dans les couches physiques et liaison de données du modèle OSI.

a- Le protocole ARP (Address resolution protocol)

Le protocole ARP (Address Resolution Protocol) détermine l'adresse de couche liaison de données pour les adresses IP connues.

Pour envoyer un datagramme sur Internet, le logiciel réseau convertit l'adresse IP en une adresse physique, utilisée pour transmettre la trame. La traduction de l'adresse IP en une adresse physique est effectuée par le réseau sans que l'utilisateur s'en aperçoive.

Le protocole ARP effectue cette traduction en s'appuyant sur le réseau physique. ARP permet aux machines de *résoudre* les adresses sans utiliser de *table statique.* Une machine utilise ARP pour déterminer l'adresse physique du destinataire. Elle diffuse pour cela sur le sous réseau une requête ARP qui contient l'adresse IP à traduire. La machine possédant l'adresse IP concernée répond en renvoyant son adresse physique. Pour rendre ARP plus performant, chaque machine tient à jour, en mémoire, une table des adresses résolues et réduit ainsi le nombre d'émissions en mode diffusion.

Résolution d'adresse–Détermination de l'adresse d'un équipement à partir de l'adresse de ce même équipement à un autre niveau protocolaire. On résout, par exemple, une adresse IP en une adresse physique ou en une adresse ATM.

Table statique–Table de correspondance qui n'est pas modifiée automatiquement par le réseau lorsque interviennent des changements dans la configuration.

b-Le protocole RARP (Reverse ARP)

Le protocole RARP (Reverse Address Resolution Protocol) détermine les adresses réseau, lorsque les adresses de couche liaison de données sont connues.

De façon inverse, une station qui se connecte au réseau peut connaître sa propre adresse physique sans avoir d'adresse IP. Au moment de son initialisation, cette machine doit contacter son serveur afin de déterminer son adresse IP et ainsi de pouvoir utiliser les services TCP/IP. Dans ce cas, le protocole RARP permet à la machine d'utiliser son adresse physique pour déterminer son *adresse logique* sur Internet. Par le biais du mécanisme RARP, une station peut se faire identifier comme cible en diffusant sur le réseau une requête RARP. Les serveurs recevant le message examinent leur table et répondent au client. Une fois l'adresse IP obtenue, la machine la stocke en mémoire vive et n'utilise plus RARP jusqu'à ce qu'elle soit réinitialisée.

Dans la version IPv6, les protocoles ARP et RARP ne sont plus utilisés et sont remplacés par un protocole de découverte des voisins, appelé ND *(Neighbor Discovery)*, qui est un sous-ensemble du protocole de contrôle ICMP.

4- Les types de réseaux :

Les réseaux peuvent être classés en fonction des distances couvertes c'est-à-dire leur étendue géographique.

4-1- Les WAN (Wide Area Network) :

Les WAN, appelés aussi réseaux publics, sont des réseaux qui peuvent couvrir un pays ou un continent, voire toute la planète. Bien sûr, il existe des opérateurs qui gèrent ces réseaux. Ils ne sont chargés que de véhiculer les données. La facturation peut être forfaitaire, mais est le plus souvent fonction de la distance, de la durée, du volume de données échangés ou d'un mélange de ces trois paramètres. Les réseaux WAN seront plus détaillés dans un chapitre plus loin.

4-2- Les MAN (Metropolitan Area Network):

Les MAN ou réseaux métropolitains couvrent une superficie moins importante limitée généralement à environ 200 km. Ils peuvent, par exemple, servir pour relier les différents bâtiments d'une entreprise. La portée est plus réduite que pour les réseaux publics, donc les débits doivent être plus importants. Ces réseaux doivent aussi être tolérants aux pannes car, vu les étendues couvertes, la coupure d'un câble ne doit pas paralyser les entreprises. La facturation liée à l'utilisation du réseau est forfaitaire et par conséquent indépendante des volumes de données transférées.

4-3- Les LAN (Local Area Network):

Les LAN ou réseaux locaux sont des réseaux de plus faible étendue, allant de quelques mètres à quelques kilomètres. En général, ils servent à interconnecter les équipements d'une même entreprise, d'un même étage d'un bâtiment, ou voire simplement les équipements se trouvant dans un bureau. Leur raison est non seulement le partage de ressources qui peuvent être chères (disques, moyens d'impression) mais il constituent aussi l'épine dorsale de l'activité informatique et du système d'information de l'entreprise. Les réseaux locaux feront l'objet d'une étude plus approfondie dans le chapitre suivant

CHAPITRE II: LOCAL AREA NETWORK (LAN)
RESEAU LOCAL

1-Définition :

Les LAN sont des réseaux à haut débit et à faible pourcentage d'erreur, couvrant une région géographique relativement peu étendue (jusqu'à quelques milliers de mètres). Les LAN relient des stations de travail, des périphériques, des terminaux et d'autres unités à l'intérieur d'un bâtiment ou d'autres zones géographiques limitées[2].

2-La topologie des réseaux :

La *topologie* définit la structure du réseau. La définition de la topologie comprend deux parties :

- la topologie physique, représentant la disposition effective des fils (média), et
- la topologie logique, précisant la façon dont les hôtes accèdent au média.

La topologie physique :

Les topologies physiques couramment utilisées sont la topologie

- en bus :

  Dans une topologie en bus, tous les hôtes sont directement connectés à un seul segment de backbone (une longueur de câble).

- en anneau :

  Dans une topologie en anneau, chaque hôte est connecté à son voisin. Le dernier hôte se connecte au premier. Cette topologie crée un anneau physique de câble.

- en étoile, (étoile étendue) :

  Dans une topologie en étoile, tous les câbles sont raccordés à un point central. Ce point est habituellement un concentrateur ou un commutateur.

  Une topologie en étoile étendue repose sur la topologie en étoile. Elle relie les étoiles individuelles entre elles en reliant les concentrateurs/commutateurs. Cette topologie, comme on peut le deviner étend la portée et l'importance du réseau.

- hiérarchique :

  Une topologie hiérarchique est créée de la même façon qu'une topologie en étoile étendue. Toutefois, au lieu de relier les concentrateurs/commutateurs

ensemble, le système est relié à un ordinateur qui contrôle le trafic dans la topologie.

- maillée **:**

Une topologie maillée est utilisée lorsqu'il ne faut absolument pas qu'il y ait de rupture de communication, par exemple dans le cas des systèmes de contrôle d'une centrale nucléaire. Chaque hôte possède ses propres connexions à tous les autres hôtes. Cela est aussi caractéristique de la conception du réseau Internet, qui possède de nombreux chemins vers un emplacement.

La topologie logique :

La topologie logique d'un réseau est la méthode qu'utilisent les hôtes pour communiquer par le média. Les deux types de topologie logique les plus courants sont le broadcast (diffusion) et le passage de jeton.

2-1- Le broadcast :

Le broadcast signifie simplement que chaque hôte envoie ses données à tous les autres hôtes sur le média du réseau, donc chaque message envoyé par un équipement sur le réseau est reçu par tous les autres. Les stations n'ont pas à respecter un certain ordre pour utiliser le réseau ; il s'agit d'une méthode de type " premier arrivé, premier servi ". L'Ethernet fonctionne de cette façon.

2-2- Le passage de jeton :

Selon cette méthode, l'accès au réseau est contrôlé en passant un jeton électronique de manière séquentielle à chaque hôte. Lorsqu'un hôte reçoit le jeton, cela signifie qu'il peut transmettre des données sur le réseau. Si l'hôte n'a pas de données à transmettre, il passe le jeton à l'hôte suivant et le processus est répété.

3-Modification du modèle de référence OSI :

3-1- Le modèle de référence IEEE 802 :

Les réseaux locaux fondent leur conception sur le modèle de référence à 7 couches OSI défini par l'ISO.

Il n'y a pas de difficulté pour appliquer les couches hautes de ce modèle de référence aux réseaux locaux. Par contre, les couches basses (la couche 2) posent problèmes. En effet le modèle de l'ISO a été conçu en ayant comme référence des réseaux publics maillés, c'est-à-dire, des réseaux construits sur des liaisons point à point, conduisant à des topologies (les graphes des connexions) irrégulières. Or les réseaux locaux ont des topologies régulières.

L'approche initiale prise dans le monde des réseaux locaux a été d'utiliser un support partagé. Chaque équipement peut entendre le trafic émis par les autres. Cela simplifie énormément l'architecture puisqu'il n'est pas nécessaire de configurer le réseau pour qu'un message arrive à sa destination (tous les équipements le reçoivent) et cela rend le système plus robuste puisqu'il ne nécessite pas d'équipement centralisé pour le gérer.

L'IEEE (Institute of Electrical and Electronical Engineers), par l'intermédiaire du comité 802, a défini les modifications qu'il fallait apporter au modèle de référence de l'ISO pour l'adapter à l'environnement des réseaux locaux. Certains des travaux de ce comité sont repris par l'ISO sous la référence 8802.

Le modèle de l'IEEE divise la couche liaison en deux sous-couches :

a- La sous-couche MAC *(Medium Access control) :*

Elle gère l'accès au support selon le principe CSMA/CD de la norme IEEE 802.3 et offre un ensemble de service à la sous-couche LLC. Trois fonctions peuvent être distinguées pour cette couche :

- les fonctions d'émission
- les fonctions de réception
- les traitements de collision

- les fonctions d'émission :

A la réception d'une demande d'émission, provenant de la sous-couche LLC, la sous-couche MAC doit

Lire un paquet de données

Lire l'adresse de destination transmise par la sous-couche LLC

Fabriquer la trame (Adresse, Longueur des données, données, CRC

Attendre l'indication d'absence de porteuse provenant de la sous-couche physique
Emettre la trame

Indiquer le succès de la transmission à la sous couche LLC ou le cas échéant traiter la collision signalée par la couche physique.

Ces séquences sont répétées jusqu'à ce que toutes les données soient transmises. Pour cela les paquets de données sont retirés de la file de la sous-couche LLC au fur et à mesure de la transmission des trames.

La fonction réception :

La lecture des trames passant par le support est effectuée en permanence. Lorsqu'une trame est lue, la fonction réception exécute les séquences suivantes :

- lecture de la trame
- décodage de l'adresse de destination
- comparaison de celle-ci et de l'adresse de la station

- si les deux adresses sont identiques :
  * vérification du CRC
  * vérification de la longueur de la trame
  * envoi d'un état de réception à la sous couche LLC
  * si le CRC et la longueur sont valides :
    - communication des données à la sous-couche LLC
    - communication de l'adresse source à la sous-couche LLC

***b- La sous-couche LLC** (Logical Link control) :*

Cette sous-couche, qui est définie dans la norme IEEE 802.2, a été créée afin de permettre à une partie de la couche liaison de données de fonctionner indépendamment des technologies existantes.

Elle assure la polyvalence des services fournis aux protocoles de couche réseau situés au-dessus d'elle tout en communiquant efficacement avec les diverses technologies sous-jacentes.

Elle gère les communications entre les dispositifs sur une seule liaison d'un réseau
En tant que sous-couche, LLC participe au processus d'encapsulation.

Elle supporte aussi bien les services non orientés connexion que les services orientés connexion qui sont utilisés par les protocoles de couche supérieure.

La norme IEEE 802.2 définit un certain nombre de champs dans les trames de couche liaison de données, lesquels permettent à plusieurs protocoles de couche supérieure de partager une liaison de données physiques.

Il en existe 3 versions présentant des différences de fiabilité, et qui s'interfacent à l'ensemble des couches physiques :

LLC1 : - service sans connexion
- pas d'acquittement sur erreur
- pas de contrôle de flux de données
- cette version implique qu'un contrôle d'intégrité de message soit fait dans l'une des couches supérieures (généralement en couche transport) Cette version est intéressante dans le cas où la transmission physique se fait avec un faible taux d'erreur. En effet l'élimination des erreurs par les couches supérieures, le renvoi des trames, consomme un temps important.

LLC2 : - service orienté connexion
- Acquittement des trames
- Reprise sur erreur
- contrôle de flux de données

C’est le service le plus complet offert par le standard 802.2. Un service orienté connexion exige la mise en place d’interface entre couches voisines et de protocole entre couches paires d’une assez grande complexité.

LLC3 : - Protocole plus simple que LLC2
- Met en place un service avec acquittement mais sans connexion

Elle est moins fiable que LLC2 mais moins coûteuse en temps

3-2- Les différents sous-comités des standards IEEE 802 :

Différents sous-comités travaillent sur des points particuliers liés aux réseaux locaux. Ces sous-comités sont désignés par un numéro. Pour référencer les différents documents produits par ces sous-comités, une lettre suit le nom de celui-ci.

- 802.1 est chargé de définir l’architecture générale liée à la famille des standards IEEE 802 et les relations avec le modèle de référence de l’ISO.

Des exemples de points spécifiques traités sont le format d’adresse, l’interconnexion par pont (IEEE 802.1D), la qualité de service (IEEE 802.1p), les réseaux virtuels (IEEE 802.1Q).

- 802.2 spécifie la sous-couche LLC. Trois types de fonctionnement sont définis par la norme.

Le type 1 spécifie un service datagramme. Ce type n’ajoute aucun contrôle supplémentaire par rapport à la sous-couche MAC, seule sa fonction d’aiguillage vers le niveau supérieur est utilisée. Dans les réseaux bureautiques, ce mode de fonctionnement est couramment utilisé.

Le type 2 est un mode connecté identique au protocole HDLC (High Level Data link Control) utilisé dans les réseaux publics X.25. Il est très peu utilisé dans les réseaux locaux.

Le type 3 définit des datagrammes acquittés utilisés dans les réseaux locaux industriels.

- 802.11 spécifie un mode d’accès pour les réseaux sans fils (wi-fi).

4-Domaine de broadcast ou domaine de diffusion :

4-1-Définition :

Les trames de diffusions sont des messages envoyés par un hôte et visible par tout les autres qui lui sont interconnectés.

Le domaine de diffusion est l’ensemble de tous les dispositifs qui recevront des trames de diffusion provenant de n'importe quel des dispositifs faisant partie de cet ensemble. Les domaines de broadcast sont généralement délimités par les routeurs parce que ces derniers ne réacheminent pas de trames de diffusion.

4-2- Fonctionnement :

Adresse de broadcast::

Pour pouvoir envoyer des messages de broadcast, il faut utiliser une adresse spécifique appelée Adresse de broadcast. La diffusion de ce genre de message est supportée par le protocole IP. Les messages sont destinés à être vus par tous les hôtes d'un réseau. Pour créer, cette adresse de broadcast on met des 1 sur toute la portion Hôte de l'adresse IP.

Le nœud source adresse les trames de diffusions au moyen de l'adresse de broadcast, laquelle précise que la trame doit être envoyée à tous les nœuds de destination possible. La trame est ensuite envoyée dans le réseau qui la copie et l'achemine à chacun des nœuds du réseau. Il est important de retenir que ce sont les ponts et les commutateurs qui transmettent le trafic de broadcast, ce que les routeurs ne font généralement pas.

5- Les outils d'interconnections :

5-1- Les répéteurs :

Un répéteur est un organe réseau qui a pour mission de répéter les éléments binaires pour que ces signaux reprennent la forme qui leur a été donnée par l'émetteur. Il n'est pas un organe intelligent capable d'apporter des fonctionnalités supplémentaires. Le répéteur ne fait qu'augmenter la longueur du support physique.

Les répéteurs sont des unités de couche 1 du modèle OSI, car ils agissent uniquement au niveau du bit et ne se soucient d'aucune autre information.

5-2- Les concentrateurs :

Le but du concentrateur est de régénérer et de resynchroniser les signaux réseau au niveau du bit. Il fait cela au niveau du bit pour un grand nombre d'hôtes (par exemple 4, 8 ou même 24) en utilisant un processus appelé concentration.

Le concentrateur est aussi connu sous le nom de répéteur multiport, car sa définition est très semblable à celle du répéteur. Donc, il est aussi un équipement de couche 1 du modèle OSI.

Le concentrateur récupère le trafic provenant de plusieurs machines qui lui sont connectées. Il est lui-même connecté sur un réseau plus puissant pour y faire transiter le trafic qu'il a concentré.

Classification des concentrateurs :

Les concentrateurs peuvent être soit :

- intelligents ou actifs : ces concentrateurs sont dotés de ports console, ce qui signifie qu'ils peuvent être programmés pour gérer le trafic réseau.

- non intelligents ou passifs : ces concentrateurs prennent simplement un signal de réseau entrant et le répètent à chaque port sans avoir la capacité d'effectuer des fonctions de gestion.

5-3- Les ponts :

Le pont est un répéteur intelligent capable de s'apercevoir que la trame qu'il reçoit n'a pas besoin d'être répétée parce que le récepteur est du même côté de la liaison. Les ponts permettent d'agrandir les réseaux en les tronçonnant en sous réseaux.

Une autre façon de voir les ponts est de noter que le pont est capable de détecter l'adresse qui se situe dans la trame et de déterminer s'il doit ou non le répéter vers une sortie (voire plusieurs sorties dans le cas d'adresse de destination en multipoint).

Un pont est un équipement de couche 2 du modèle OSI conçue pour connecter deux segments LAN. Bien que les routeurs et les commutateurs aient pris en charge beaucoup des fonctions des ponts, ceux-ci demeurent néanmoins importants dans de nombreux réseaux.

5-4- Les commutateurs (switches):

Un commutateur vise à concentrer la connectivité tout en accroissant l'efficacité de la transmission de données. Il travail comme un équipement combinant la connectivité d'un concentrateur et les capacités de régulation du trafic d'un pont sur chaque port. Le commutateur commute les trames des ports d'entrée (interfaces) aux ports de sortie, tout en fournissant à chaque port une pleine bande passante.

Le commutateur est aussi une unité de couche 2, il est également appelé pont multiport. Le commutateur est capable de prend des décisions en fonction des adresses MAC contrairement au concentrateur qui ne prend aucune décision. En raison des décisions qu'il prend, le commutateur rend le LAN beaucoup plus efficace. Il effectue cela en " commutant " les données uniquement au port auquel le bon hôte est connecté. Par contraste, un concentrateur achemine les données à tous les ports, de sorte que tous les hôtes doivent examiner et traiter (accepter ou rejeter) toutes les données.

Il y a deux types de commutateur ou switch :

a- Les switches simple :

Les switches simple sont ceux qu'on utilise dans un petit réseau et qui inondent le marché, pas besoin de grande formalité pour leur application, il faut brancher simplement et ça marche.

b- Les switches configurable :

Par contre, pour ce genre de matériel, ils sont équipés de processeur CPU, et de différent type de mémoire pour contenir les IOS et les configurations. Ces switches peuvent prendre des décisions en fonction des configurations faites par l'administrateur. Pour plus de détail voir annexe 1.

c- La segmentation des LAN

Un réseau peut être divisé en unités plus petites appelées segments. Chaque segment utilise le mode d'accès CSMA/CD et assure le trafic entre les utilisateurs sur le segment.

La segmentation permet d'isoler le trafic entre chaque segment, comme cela, la bande passante disponible augmente pour chaque utilisateur en créant des domaines de collisions plus petites.

Pour segmenter un réseau LAN on utilise soit un pont soit un commutateur soit un routeur.

5-5- Les routeurs :

Les routeurs sont utilisés pour interconnecter les réseaux LAN, et pour plus de précision voir la référence [19].

CHAPITRE III: VIRTUAL LOCAL AREA NETWORK (VLAN)

RESEAU LOCAL VIRTUEL

1- Généralités :

Pourquoi avoir introduit le concept de VLAN ?

Il y a trois nécessités pour la conception de VLAN :

- le besoin de limiter les domaines de broadcast ou diffusion :

Avec les concentrateurs et les commutateurs de première génération, la séparation des flux gérés par la couche 2 ne peut se faire qu'en regroupant géographiquement les groupes de travail. En effet, si le commutateur segmente les domaines de collision, il maintient cependant un seul domaine de diffusion.

- le besoin de garantir une sécurité :

Si l'interconnexion du réseau repose sur les commutateurs et non sur les routeurs (ce qui est de plus en plus le cas) cela pose deux problèmes :

Les trames de diffusion sont propagées sur tout le réseau, or ces trames sont nombreuses (ARP, DHCP, Netbios, .etc.). En mettant une carte réseau en mode 'promiscuous' on peut capturer ces trames.

La séparation et la sécurité des domaines de diffusion exigeaient, avant l'apparition des VLAN, une séparation géographique des domaines de diffusion et une interconnexion par routeur

- pour permettre la mobilité des utilisateurs:

Dans un réseau LAN un utilisateur défini dans un segment physique n'en sera plus membre s'il en change. Alors il ne pourra plus communiquer avec les membres de son ancien segment

2- Définition :

Une première définition[13][14] :

Un VLAN (Virtual Local Area Network) Ethernet est un réseau local virtuel (logique) utilisant la commutation s'appuyant sur Ethernet :

- pour regrouper les éléments du réseau (utilisateurs, périphériques, etc.) selon des critères logiques (fonction, partage de ressources, appartenance à un département, etc.),
- sans les contraintes physiques (câblage informatique inapproprié, etc.).

Une définition plus technique :

Un VLAN permet de créer des domaines de diffusion (domaines de *broadcast*) gérés par les commutateurs indépendamment de l'emplacement où se situent les noeuds, ce sont des domaines de diffusion gérés logiquement

3- Propriétés offertes par les VLAN :

- Les messages de diffusion émis par une station d'un VLAN ne sont reçus que par les stations de ce VLAN
- On obtient un cloisonnement virtuel similaire à l'utilisation d'un câblage multiple
- Augmentation du débits : support des transferts de données allant jusqu''a 1Gb/s ;
- peut couvrir un bâtiment, relier plusieurs bâtiments ou encore s'étendre au niveau d'un réseau plus large;
- une station peut appartenir à plusieurs VLAN simultanément.

4- Type de VLAN :

Les VLAN déployés sur plusieurs commutateurs sont classés suivant deux types :

- Les VLAN implicites : lorsqu'un message Ethernet passe d'un commutateur à un autre (switch). Tout élément connecté à un switch peut accéder à tout autre élément du même VLAN connecté sur le même switch. Le mode de transmission du switch permet de mettre directement en relation deux postes ;
- Les VLAN explicites : une étiquette (tag) d'appartenance à un VLAN est ajoutée à chaque Ethernet

Pour définir des VLAN, il faut que les commutateurs supportent l'extension de la technologie Ethernet (IEEE 802.1q).

5- Méthode d'implémentation des VLAN :

Les méthodes de construction d'un VLAN doivent déterminer la façon dont le commutateur va associer la trame à un VLAN. Usuellement on présente trois méthodes pour créer des VLAN :

- Les VLAN de niveau 1 : les VLAN par port,
- Les VLAN de niveau 2 : les VLAN par adresses MAC,
- Les VLAN de niveau 3 : les VLAN par adresses de niveau 3 ainsi que des méthodes dérivées telles que
  - Les VLAN par protocole et
  - Les VLAN par sous réseau IP

5-1- Les VLAN de niveau 1 : VLAN par port

Un VLAN par port est obtenu en associant chaque port du commutateur à un VLAN particulier. L'appartenance d'une trame à un VLAN est alors déterminée par la connexion de la carte réseau à un port du commutateur. Les ports sont donc affectés statiquement à un VLAN. La figure 3.1 illustre bien ce principe.

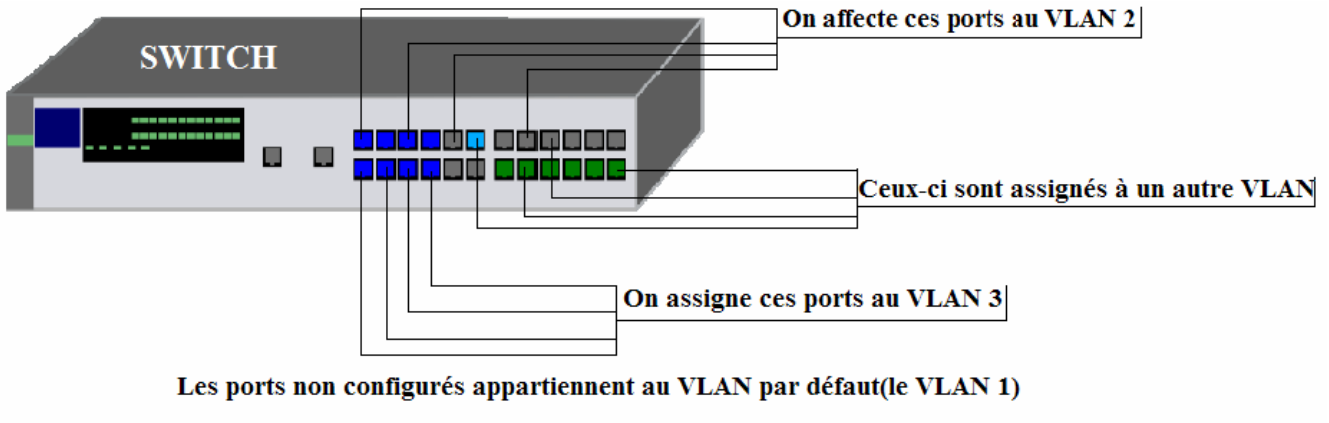


Figure 3.1: Principe du VLAN par port

- Particularité :

Toutes les stations reliées sur un port par l'intermédiaire d'un même concentrateur, appartiennent au même VLAN.

- Inconvénient :

Les VLAN par port manquent de souplesse, tout déplacement d'une station nécessite une reconfiguration des ports c'est-à-dire, si on déplace physiquement une station il faut désaffecter son port du VLAN puis affecter le nouveau port de connexion de la station au bon VLAN.

Si on déplace logiquement une station (on veut la changer de VLAN) il faut modifier l'affectation du port au VLAN.

5-2- Les VLAN de niveau 2 : les VLAN par adresses MAC :

Un VLAN par adresse physique est constitué en associant les adresses MAC des stations à chaque VLAN. L'appartenance d'une trame à un VLAN est déterminée par son adresse MAC. En fait il s'agit, à partir de l'association Mac/VLAN, d'affecter statiquement ou dynamiquement les ports des commutateurs à chacun des VLAN en fonction de l'adresse MAC de l'hôte qui émet sur ce port. Si on veut changer de VLAN il faut donc modifier l'association MAC/VLAN. Dans la figure 3.2, la configuration des VLAN est résumée dans le tableau 1 MAC/VLAN.

Tableau 1 : Association MAC/VLAN

MAC Address	VLAN ID
000e.78c2.636a	2
0c94f.843b.84f4	2
86ba.a89e.9fd3	10
6573.bdf7.a2c6	10
093c.2bdc.ffff	2
ff00.cc67.94ee	10

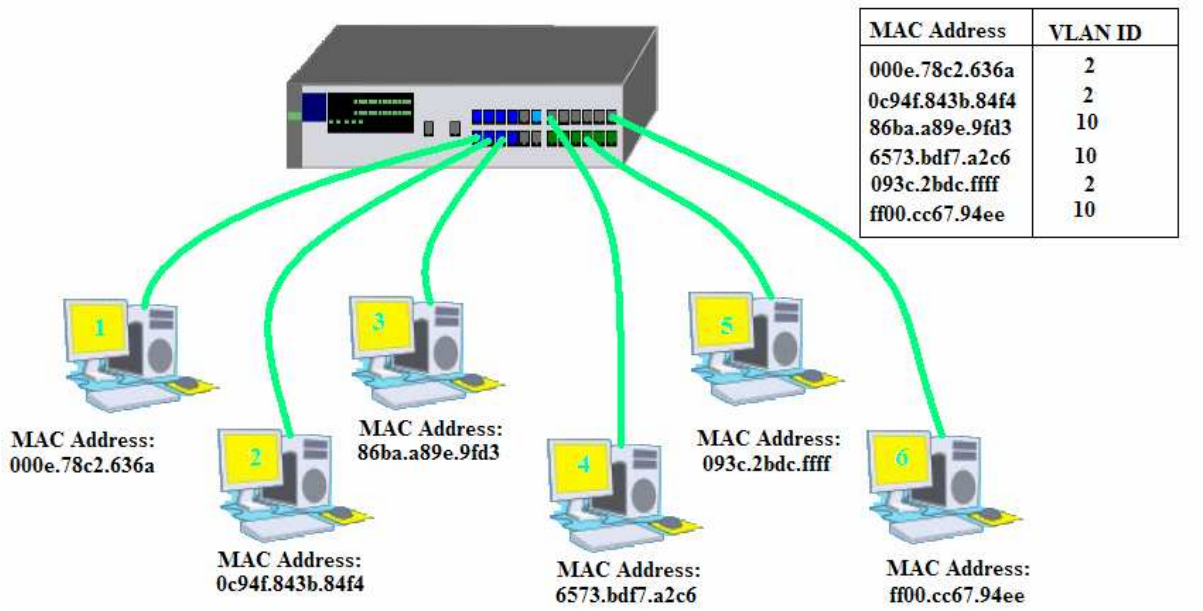


Figure 3.2 : Principe du VLAN par adresse MAC

- Avantage :

L'intérêt principal de ce type de VLAN est l'indépendance vis-à-vis de la localisation géographique. Si une station est déplacée sur le réseau physique, son adresse physique ne changeant pas, elle continue d'appartenir au même VLAN (ce fonctionnement est bien adapté à l'utilisation de machines portables).

- Inconvénient :

La configuration peut s'avérer fastidieuse : elle nécessite une table de correspondance VLAN, MAC contenant toutes les adresses MAC des machines de l'entreprise, depuis cette table, doit être partagée/propagée sur tous les commutateurs.

5-3- Les VLAN de niveau 3:

Un VLAN de niveau 3 peut être construit en utilisant une adresse ou un protocole de niveau 3 ou supérieur. On affecte à une adresse ou à un protocole un VLAN.

L'appartenance d'une trame à un VLAN est alors déterminée par l'adresse/Protocole de niveau 3 ou supérieur qu'elle contient. En effet, le commutateur doit donc accéder à ces informations. Pratiquement, il s'agit à partir de l'association adresse/Protocole niveau 3/VLAN d'affecter dynamiquement les ports des commutateurs à chacun des VLAN. L'exemple dans la figure 3.3 rend le concept plus clair.

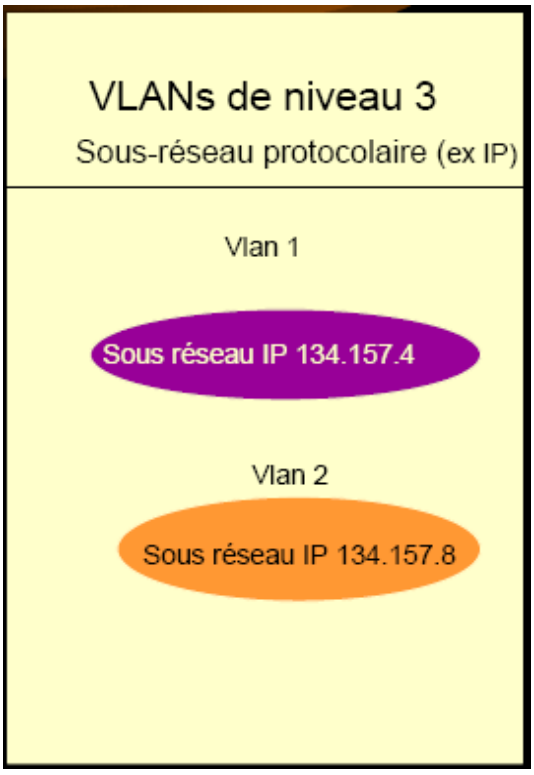


Figure 3.3: exemple de VLAN par sous réseau IP

- Inconvénient :

Dans ce cas ci, les commutateurs apprennent automatiquement la configuration des VLAN en accédant aux informations de couche 3. Ce qui entraîne un fonctionnement moins rapide que celui du VLAN de niveau 2.

a- Les VLAN par sous réseau IP :

On parle souvent de VLAN par sous réseau quand on utilise le protocole IP. Un VLAN est associé à chaque sous réseau IP. Les commutateurs apprennent la configuration et il est possible de changer une station de place sans reconfigurer le VLAN.

- Inconvénient :

Une petite dégradation des performances de la commutation due à l'analyse des informations.

b- Les VLAN par protocole :

Un VLAN de niveau 3 par protocole est obtenu en associant une trame à un VLAN en fonction du protocole qu'elle transporte. Par exemple, on peut constituer un VLAN avec un protocole de niveau 3 pour isoler les flux IP, IPX, Appletalk etc.…

- Inconvénient :

Cette méthode est très rare, elle est moins performante car les commutateurs doivent analyser les trames.

- Autre perspective :

On peut trouver aussi des VLAN construits à partir de protocole supérieur (notamment H320). On parle quelquefois de VLAN par règles ou par types de service.

Enfin l'apparition du Wi-fi pose des problèmes de sécurité que les VLAN peuvent résoudre. Ainsi une solution basée sur des VLAN par SSID est envisageable.

6- La norme 802.1q:

La norme 802.1q date de décembre 1998, c'est donc une norme récente. Elle reprend « l'étiquette » définit par la norme 802.3ac en spécifiant l'utilisation des champs. Les spécifications du groupe 802.1q de l'IEEE ont pour but d'assurer l'interopérabilité d'équipements d'origines hétérogènes offrant des services de type réseaux locaux virtuels

6-1-Typologies des trames

La norme définie trois types de trames :

- les trames non étiquetées (untagged frame)
- les trames étiquetées (tagged frame)
- les trames étiquetées par une priorité (priority-tagged frame)

Une trame étiquetées est une trame qui contient une entête supplémentaire. Cette entête modifie le format standard d'une trame, notamment de la trame 802.3.

Les trames sans étiquette et les trames étiquetées par une priorité ne comportent aucune information permettant d'identifier les VLAN auxquels ils appartiennent. Ces trames appartiennent à des VLAN spéciaux reliés à des ports physiques ou utilisant des extensions réservées à des équipementiers (3COM, CISCO..) dont la plupart ont participé à la rédaction du standard. Ces trames qui forment le VLAN natif qui permet d'assurer l'interopérabilité avec un switch qui ne supporterait pas le 802.1q.

6-2- Modèle architectural:

La norme présente un modèle à trois couches pour les VLAN selon la figure 3.4 :

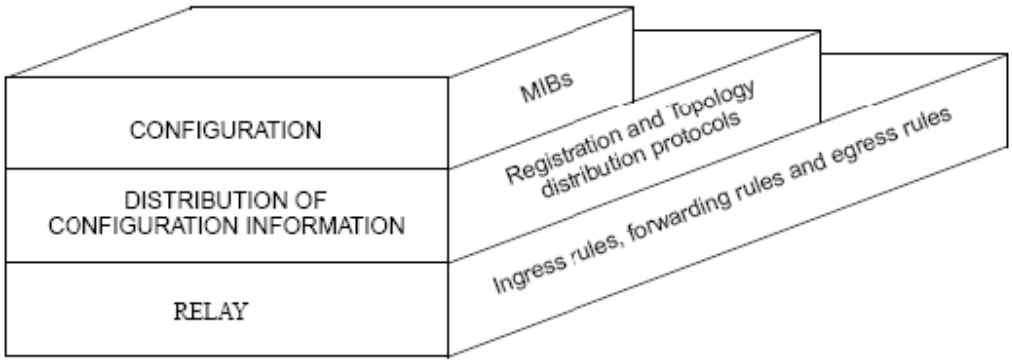


Figure 3.4 : Modèle architectural de la norme 802.1q

a- La couche configuration :

· La couche configuration permet d'indiquer comment sont associés les équipements aux différents réseaux VLAN. Cette configuration pouvant s'opérer à partir de MIBs (Management Information Base) par le protocole SNMP (Single Network Management Protocol) ou des fichiers de configuration. Elle définit aussi les commandes administratives nécessaires à la gestion des VLAN.

b- La couche distribution :

· La couche distribution/résolution permet aux switches la résolution de chaque paquet par rapport à son VLAN associé. C'est-à-dire qu'elle se préoccupe des éléments liés à la définition automatique des VLAN et leur propagation dans un réseau.

c- La couche relay :

· La couche correspondance « relay » définit le processus de traitement d'une trame par un commutateur « VLAN informé » et la commutation de trames dans un commutateur « VLAN informé ».

i- Principe de fonctionnement d'un switch 802.1q dans la couche relay :

Le principe de retransmission et de filtrage des trames est illustré selon le schéma de la figure 3.5 suivant.

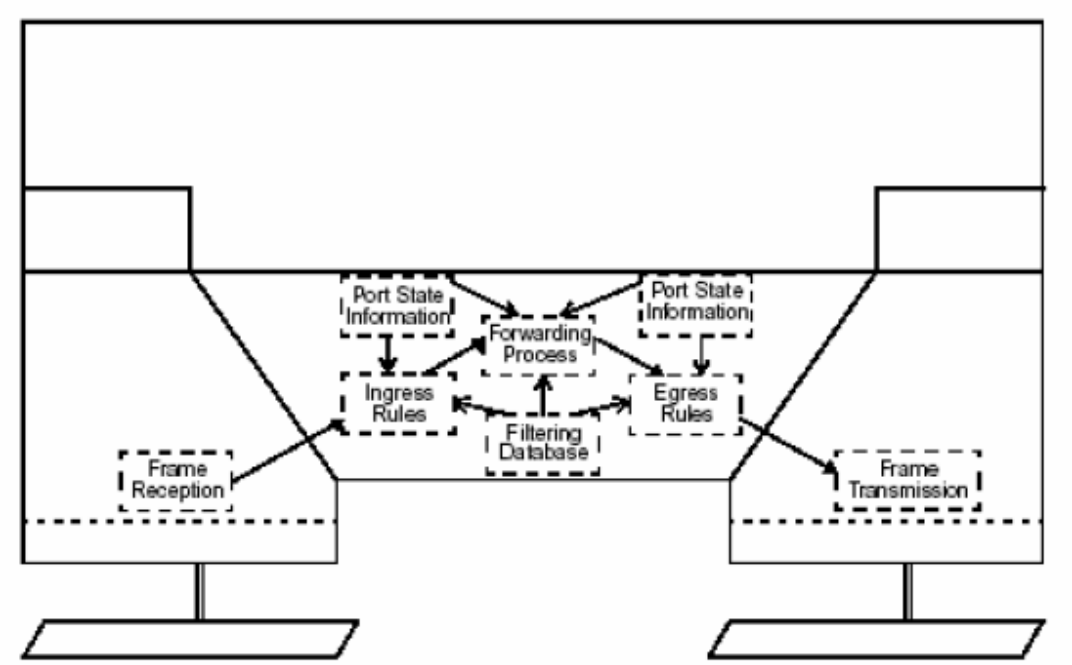


Figure 3.5: Retransmission et filtrage des trames

ii- Le processus de commutation et de traitement se décompose en trois opérations :

- Les opérations liées au traitement d'une trame en entrée d'un port « VLAN informé » : Elles sont contrôlées par des règles d'entrée (ingress rules). Ces règles s'appliquent à toutes les trames entrantes. La prise en compte de ces règles est spécifiée pour chaque port. Exemples de règles :
  - Rejet de trames non « taggés » lorsque les règles de filtrage établies n'acceptent que les trames taggés.

· Contrôle de l'appartenance à un VLAN d'une trame reçue par comparaison aux données MAC stockées dans la base de données de filtrage

- Les opérations liées à la décision de commutation (forwarding process) d'une trame prise par un commutateur « VLAN informé » c'est-à-dire déterminer sur quels ports du switch les trames doivent être transférées. Pour cela, le process forwarding analyse l'ensemble de ces paquets selon les données émanant de la base de données de filtrage, des états de port et des règles ingress et egress et leur réserve ensuite le traitement approprié.

  Ces opérations sont donc contrôlées par des tables de filtrage (filtering database) qui répertorient les associations entre ports et adresses Mac et entre port et VLAN. La base de données de filtrage permet aussi d'interpréter la sémantique de tous les paquets du réseau pour pallier au spoofing par exemple.

  On associe à ces opérations les opérations de gestion de priorité si celles-ci sont actives. Dans ce cas il y a une table des priorités qui associe une file d'attente à chaque niveau de priorité (8 maximums).

  Les « Port statement information » fournissent l'information sur la configuration de chaque port du switch.

- Les opérations liées au traitement d'une trame en sortie d'un port « VLAN informé ». Elles sont contrôlées par des règles de sorties (egress rules) qui sont les mêmes que dans ingress rules mais appliquées aux trames sortantes. Il peut aussi y avoir éventuellement ajout ou retirement d'une étiquette à la trame et recalcule du FCS (Frame Check sequence).

6-3- Structure des trames Ethernet étiquetées 802.1Q:

Les trames Ethernet étiquetées sont différentes des trames classiques car elles contiennent :

- une entête supplémentaire insérée immédiatement après les champs adresse source et destination.
- Un CRC en fin de trame, le FCS, après que le payload ait été rattaché à l'entête.

La figure 3.6 met en évidence l'entête supplémentaire des trames Ethernet étiquetées.

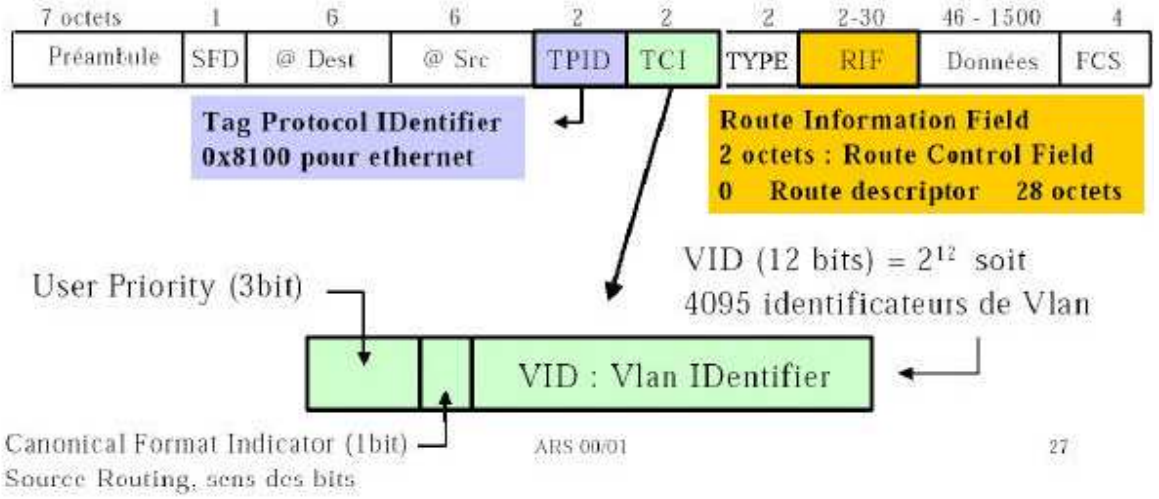
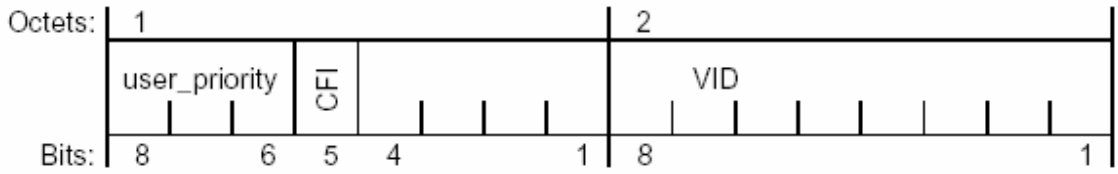


Figure 3.6 Structure des trames Ethernet étiquetées.

a- Le champ Tag Protocol Identifier (TPID) :

Parfois aussi designé sous l'acronyme VPID (VLAN Protocol Identifier), ces champs de deux (2) Octets désignent le type de tag. Attention il ne faut pas le confondre avec l'identifiant d'un VLAN. Il permet par exemple au switch d'identifier la trame comme comportant un tag 802.1Q pour celle ayant un format Ethernet II / 802.3. Dans ce cas, cette valeur est égale à la constante hexadécimale 0x8100.

b- Le champ Tag Control Information (TCI).



Ce champ a une longueur de 2 octets. Le premier champ de 3 bits, nommer user_priority, permet de définir huit niveaux de priorité. Il est utilisé par le protocole 802.1p.

Lorsqu'il est positionné à 1, le bit CFI (Canonical Format Indicator) indique que les adresses MAC sont bien au format standard. Il est utilisé par le routage par la source.

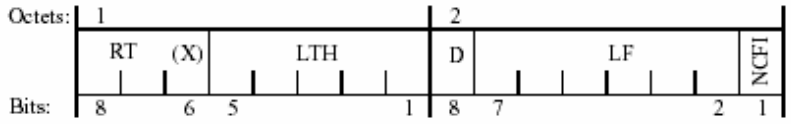
Le champ VID de 12 bits désigne le VID (VLAN identifier) auquel appartient la trame.

c- Le champ TYPE :

Longueur/type : 2 octets. En 802.3 donne la longueur de la trame. En Ethernet II ou DIX (Digital Intel Xerox) indique le type de données transporté.

d- Champ Embedded Source-Routing Information Field (E-RIF):

Ce champ spécifie notamment les informations de routage (champ RT), ainsi que la longueur maximale des trames (champ LF).



6-4- Les types de port dans un commutateur « VLAN informé » :

Les paramètres associés à un port (Port State Information) sont entre autres :

- son type (tagged, untagged, priority tagged) et
- les VLAN auxquels il participe (les PVID, Port VLAN Identifier).

Une trame en entrée ne comportant pas de VID ou bien un VID nul sera associée à un VLAN :

- soit en fonction des paramètres du port de réception
- soit en fonction d'extensions propriétaires non définies par le protocole 802.1Q.

Une trame en entrée doit toujours être associée à un VID. Un port peut admettre toutes les trames ou seulement les trames « étiquetées ». Si la trame n'est pas étiquetée et que le port n'est pas étiqueté, la trame sera associée au PVID du port (qui doit alors être unique) sinon elle est détruite.

Une trame en sortie dont l'association avec un VLAN ne correspond pas au(x) PVID du port en sortie sera détruite.

Un port « étiqueté » transmet des trames étiquetées mais peut traiter des trames non étiquetées.

Un port « non étiqueté » transmet des trames non étiquetées mais peut traiter des trames étiquetées (en enlevant notamment l'étiquette).

Enfin un port « étiqueté par une priorité » transmet des trames « étiqueté par une priorité » mais peut traiter les autres types de trames.

Un commutateur peut avoir des ports de différents types en même temps.

6-5- Notion de VLAN natif :

Les trafics de VLAN sont isolés de par les tags 802.1Q rajoutés aux trames Ethernet. La norme 802.1Q introduit des contraintes d'interopérabilité avec les VLAN natifs qui n'utilisent pas les tags Ethernet.

Ainsi un switch 802.1Q recevant ce type de trame non taggué va la traiter comme une trame du VLAN natif. Cela permet de dialoguer en « non taggué » avec des anciens switches non compatibles 802.1Q.

7- Inter-Switch Link (ISL) :

ISL est un protocole CISCO propriétaire pour interconnecter de multiples switches et échanger les informations des VLAN entre les switches. Il peut être utilisé pour maintenir des liens redondants et en équilibre de charge pour des liens utilisant le protocole spanning tree. Ce protocole ne sera pas pris en compte et nous n'entrerons pas trop dans les détails dans ce document pour des raisons de sécurité.

8-Méthode d'attribution des VLAN :

La méthode d'attribution des VLAN dépend de la façon par laquelle les ports du switch y sont assignés. On peut classer ces méthodes en deux :

- la méthode statique qui correspond au VLAN statique
- la méthode dynamique qui conduit au VLAN dynamique

La désignation statique vient du fait que l'appartenance d'un port à un VLAN a été introduite dans la configuration du switch par l'administrateur manuellement.

Le mot dynamique par contre est utilisé pour dire que le port est assigné à un VLAN automatiquement par le switch, cette décision est prise par le switch suivant une configuration bien précise donnée par l'administrateur.

8-1-méthode statique :

Il s'agit de fixer les ports du switch pour qu'ils fassent partie d'un VLAN. On remarque ici que cette action est une mise en œuvre du VLAN par port et du VLAN par adresse MAC introduit manuellement dans la configuration du switch par l'administrateur. Cette méthode est certes efficace mais pose le problème de l'administration qui devient très lourde à gérer notamment lors des déplacements de machines dans le réseau.

8-2- méthode dynamique :

Dans cette méthode, il est nécessaire de recourir à un système de connexion client/serveur. C'est-à-dire que dans le réseau on aura besoin d'un serveur, qui peut être un PC ou un switch pouvant effectuer le rôle, et des clients qui seront des switches compatible VLAN.

Si c'est un PC, on peut avoir un serveur d'AAA (Authentication-Authorization-Accounting) qui utilise les protocoles d'AAA que ce soit RADIUS (Remote Authentification Dial-in User Service) ou TACACS (Terminal Access Controler Access Control System)

Si c'est un switch, le VMPS (VLAN Membership Policy Server) est la fonction qui assure l'authentification des clients.

a-Fonctionnement du VMPS :

Un switch configuré comme un client du VMPS peut communiquer et interroger le serveur avec l'aide du protocole VQP (VLAN Query Protocol).

Lorsque le VMPS reçoit une requête VQP venant d'un switch client, il cherche dans sa base de données le tableau qui contient des informations sur les stations enregistrées et leur VLAN associé. La réponse du serveur se base sur les résultats d'une comparaison entre les valeurs dans le tableau avec celles envoyées par le switch client et la configuration du mode sécurité du serveur.

En réponse à une requête, le VMPS peut prendre une des actions suivantes :

- Si un groupe de port est par restriction assigné à un VLAN, le serveur vérifie la requête du port par rapport à ce groupe et répond suivant le cas comme suit :

- Si le VLAN est autorisé sur le port, le VMPS envoie le nom du VLAN au switch client.

- Si le VLAN n'est pas autorisé sur le port, et que le VMPS n'est pas configuré en mode sécurisé, il envoie un « access-denied » comme réponse.

- Si le VLAN n'est pas autorisé sur le port, et que le VMPS est configuré en mode sécurisé, il envoie un « port-shutdown » en guise de réponse.

- Si le VLAN dans la base de données ne correspond pas au VLAN courant sur le port et qu'un client actif existe sur le port, le serveur envoie un « Access denied ou un port-shutdown » dépendant du mode de sécurité du VMPS.

La figure 3.7 montre l'aspect de ce principe avec des switches catalyst 6500 pour serveur.

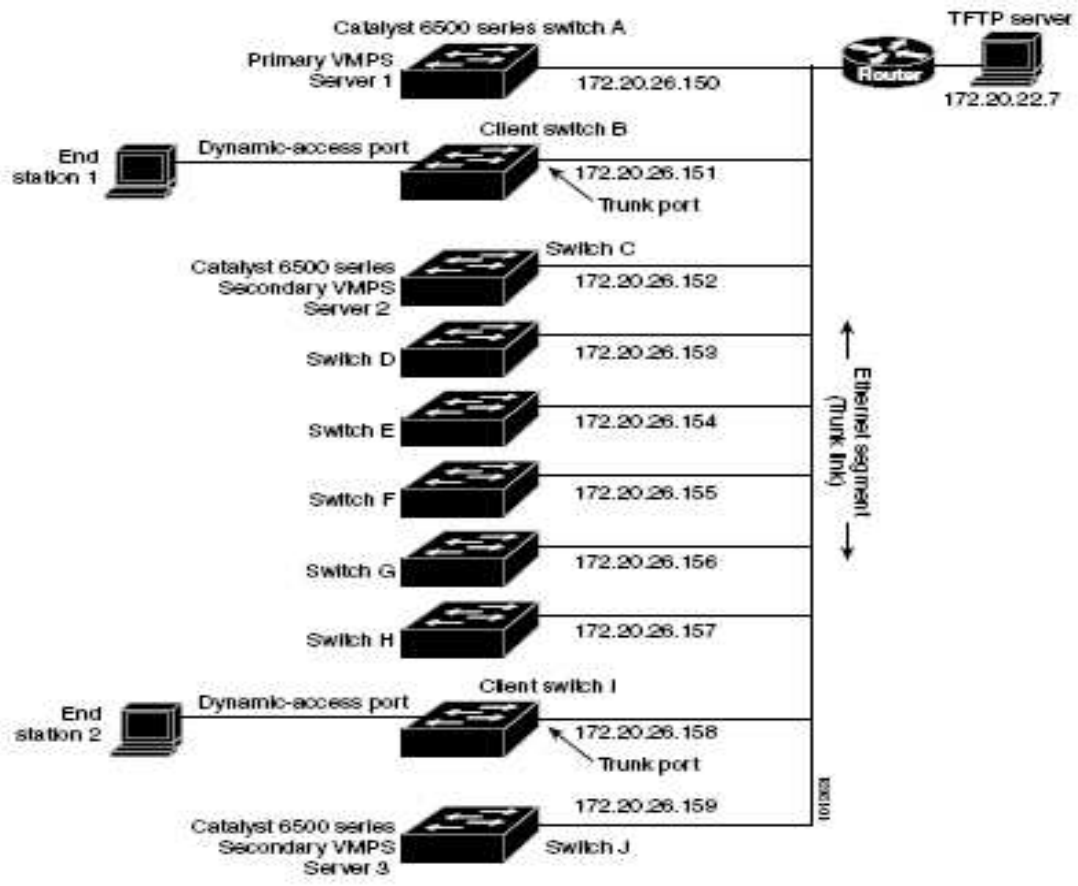


Figure 3.7 : réseau VLAN dynamique avec des switch catalyst 6500 en tant que serveur VMPS

b- Fonctionnement des serveurs utilisant RADIUS et TACACS:

i- généralités :

Les possibilités d'un serveur utilisant ces deux protocoles sont très nombreuses et très vastes mais pour simplifier, on se contentera ici de le mettre en œuvre dans le cas qui nous intéresse.

Ce service est capable :

- d'authentifier un utilisateur distant suivant de multiples modes plus ou moins sécurisés en s'appuyant sur une base de connaissance allant du simple fichier texte à l'annuaire LDAP, en passant par une base de données de type SQL
- d'enregistrer des informations sur chaque « LOGIN »
- de renvoyer au demandeur des paramètres variés pouvant, suivant le cas, être une configuration IP, ou dans le cas étudier ici un numéro de VLAN.

Dans le domaine VLAN, les deux cas qui nous intéressent sont :

-L'authentification depuis l'adresse MAC des stations connue sur un réseau filaire, en utilisant un système de « Login/password », avec le protocole CHAP(Challenge-Handshake

Authentication Protocole), éventuellement en assignant un numéro de VLAN suivant la machine.

- Et l'authentification avec certificat sur un réseau sans fil en utilisant le protocole EAP-TLS (Extensible Authentification Protocol-Transport Layer Security).

La norme utilisée dans ce mécanisme d'authentification est celle définie par L'IEEE 820.1x

ii- La norme 802.1x :

Le but de cette norme est d'offrir un mécanisme d'authentification des postes de travail. Elle a été initialement destinée au réseau filaire, étendu et au réseau sans-fil

La norme 802.1x a pour principe l'authentification d'un client sur un serveur d'authentification (radius) au travers d'un équipement réseau (switch, AP) qui reçoit du serveur l'autorisation de laisser le passage à un client. Le protocole utilisé est EAPOL (Extensible Authentification Protocol Over LAN).

La norme peut supporter deux topologies qui sont :

-Le point-à-point : dans une configuration point-à-point, seul un client peut se connecter au port du switch compatible 802.1x. Quand le client est remplacé par un autre, le port retourne à l'état bloqué. Il faut que le nouveau client soit authentifié à nouveau. La figure 3.8 montre ce genre de topologie.

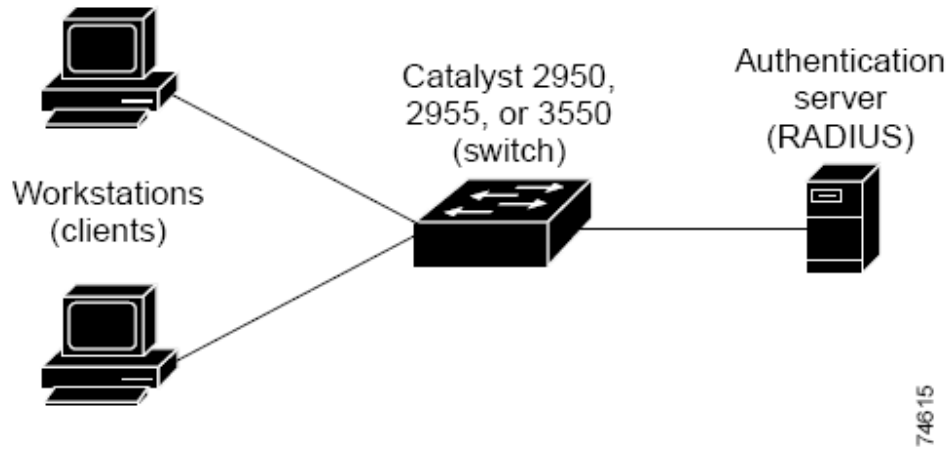


Figure 3.8 : topologie point-à-point supporter par 802.1x

- le wireless LAN : la figure 3.9 montre ce genre de topologie. Le port du switch est configuré pour accepter le mode Multiple-host et devient actif dès qu'un client est authentifié, alors tout autre client indirectement rattacher au port a accès au réseau. Si le port est bloqué, aucune machine ne peut accéder au réseau. Dans ce genre de topologie, il

revient au point d'accès d'authentifier les machines clients attaché à lui, et le point d'accès devient le client du switch.

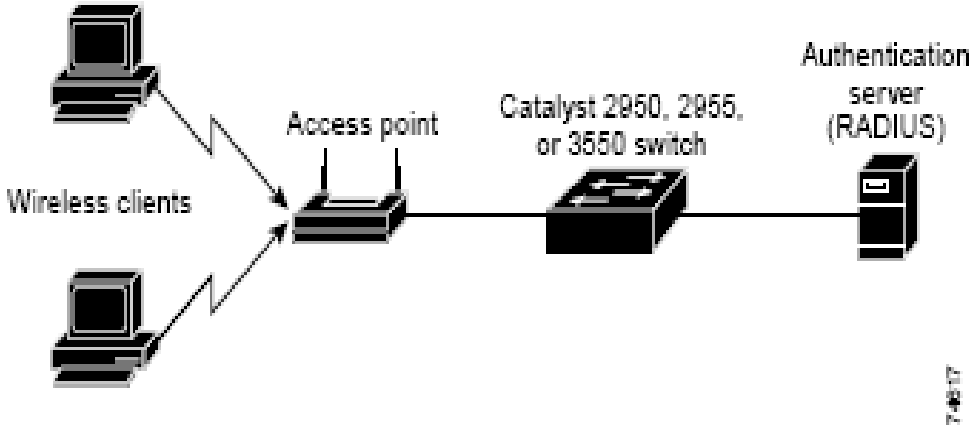


Figure 3.9 : topologie wireless LAN supporter par 802.1x

CHAPITRE IV : APPLICATION DES VLAN

1- Généralité :

Généralement, les entreprises ont des sites dans des régions différentes alors le problème pour la mise en place d'un réseau au sein de ces entreprises se divise en deux :

- La création du réseau interne à chaque site et
- L'interconnexion de ces différents sites

Le VLAN est une solution à la connexion interne dans un bâtiment. Et la liaison WAN fournit une alternative pour l'interconnexion des réseaux VLAN dans chaque site. Pour résumer, la figure 7.1 montre un bref aperçu des deux différentes solutions proposées.

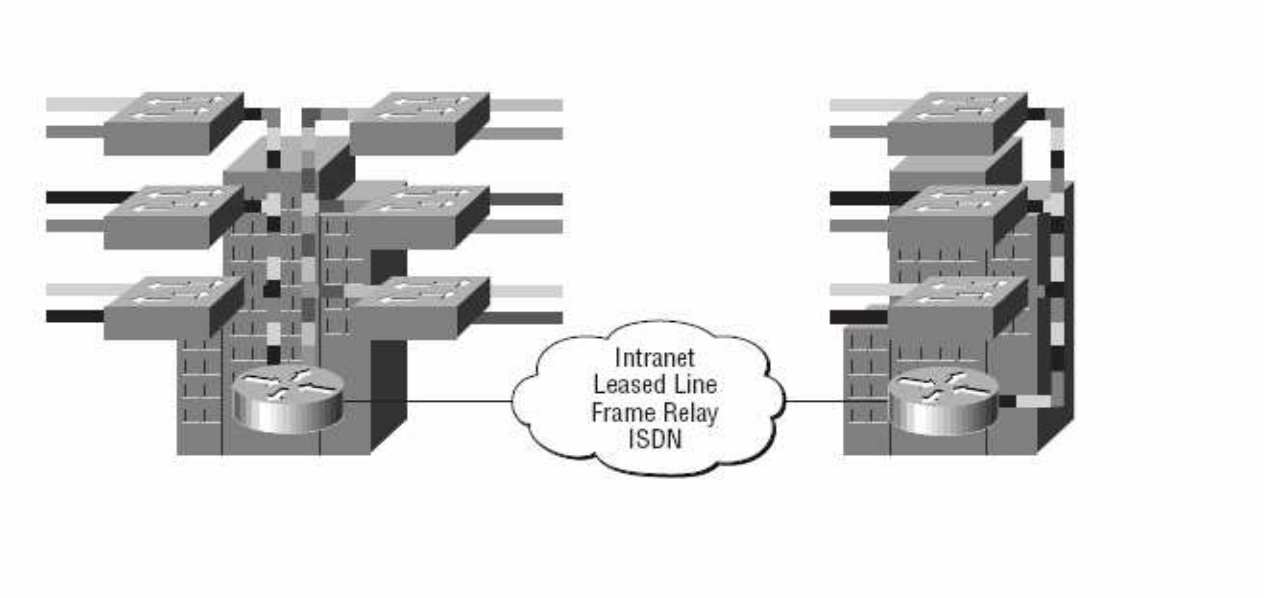


Figure 7.1 : Communication VLAN inter-site

2- Mise en place des VLAN :

2-1- Objectifs de conception du VLAN :

Les Objectifs prises durant la conception du réseau VLAN sont :

- Avoir une fonctionnalité du réseau : Le réseau doit fonctionner et doit permettre aux utilisateurs de répondre à leurs besoins professionnels. Il doit fournir une connectivité fiable entre les utilisateurs ainsi qu'entre les utilisateurs et les applications à un débit raisonnable.

- Permettre une Évolutivité : Le réseau doit avoir la possibilité de croître. La conception initiale doit pouvoir s'étendre sans qu'il soit nécessaire d'apporter des modifications importantes à la conception globale.

- Accorder une adaptabilité : Le réseau doit être conçu en tenant compte des technologies futures et ne doit pas comporter d'éléments susceptibles de limiter la mise en œuvre de ces nouvelles technologies à mesure qu'elles deviennent disponibles.

- et procurer une facilité de gestion - Le réseau doit être conçu pour faciliter la surveillance et la gestion des opérations afin de garantir en permanence sa stabilité.

2-2- Choix des Matériels :

Pour une plus grande interopérabilité avec d'autres constructeurs, et à cause de leur réputation en ce qui concerne la sécurité, nous avons choisi les célèbres produits de CISCO. Pour les routeurs la série 2600 permet une compatibilité VLAN et pour les switches, le modèle 2950 de la série 2900 catalyst est un « best seller » des produits CISCO en matière de VLAN.

Dans l'exemple pratique illustré par la figure 7.2, les commutateurs sont partagés sur trois VLAN dont le VLAN engineering, Marketing, et Accounting avec leur machine propre éparpillée dans les différents étages du bâtiment.

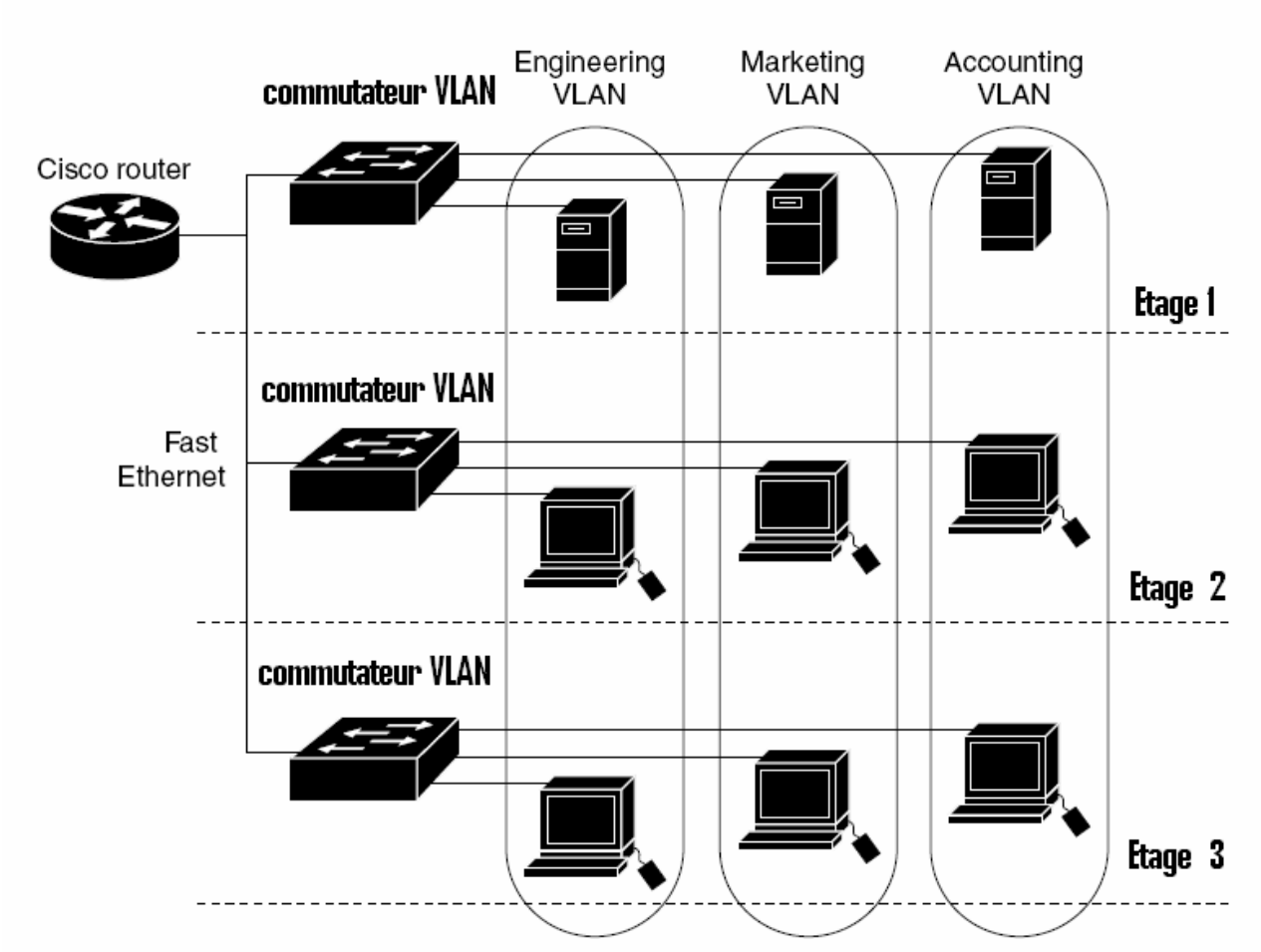


Figure 7.2 : Exemple pratique de mise en place de VLAN dans un immeuble

2-3- Simulation :

La simulation a été réalisée avec le logiciel BOSON NETSIM, et pour une bonne présentation, la figure 7.2 ci-dessus a été transformée selon la figure 7.3 :

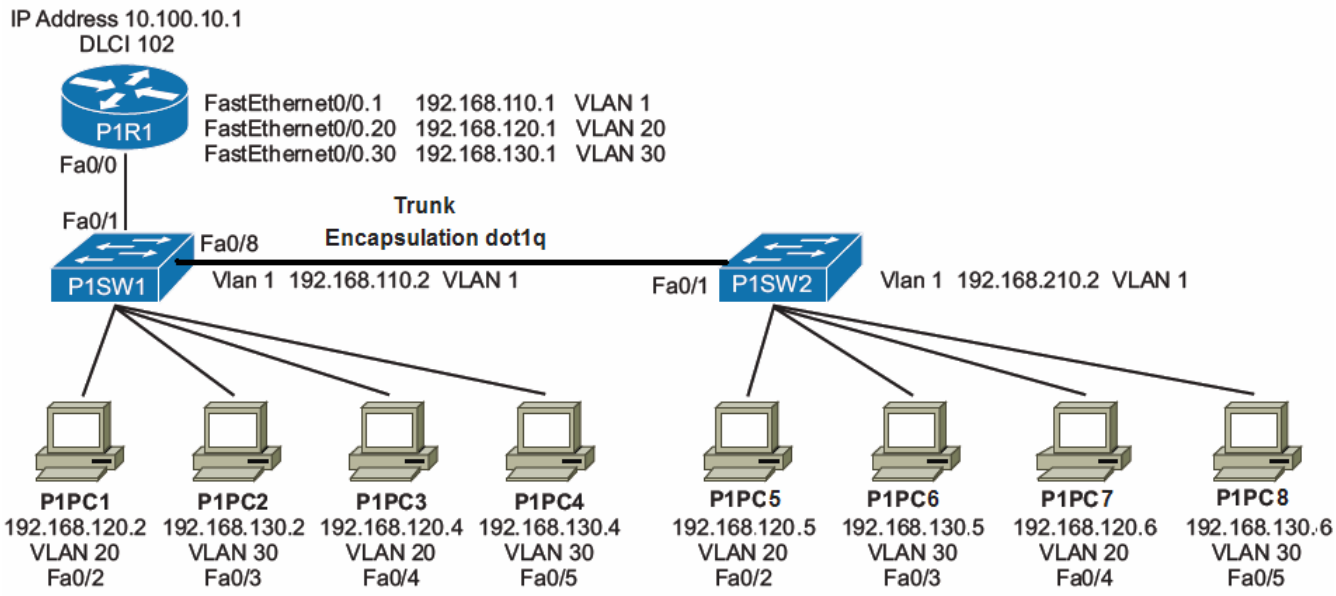


Figure 7.3 : montage pour la simulation VLAN

- description du montage :

On a créé un réseau avec un routeur, deux switches et huit PC dont quatre reliés à chaque switch. Les PC connectés à un switch sont configuré deux à deux sur des VLAN différents, le VLAN 20 ; le VLAN 30 donc au niveau de chaque switch on a deux PC sur un même VLAN, et en tout quatre PC pour un VLAN.

Pendant la simulation les VLAN statiques seront utilisés, chaque port de chaque commutateur va donc être attribué à un VLAN. Une telle disposition a été prise pour mettre en évidence les deux trunk entre les deux switches P1SW1 et P1SW2, entre le switch P1SW1 et le routeur P1R1, et le routage entre VLAN.

- configuration :

-Configuration du switch P1SW1

Création des VLAN

P1SW1# **VLAN database**

P1SW1 (VLAN)# **VLAN 20 name VLAN_20**

P1SW1 (VLAN)# **VLAN 30 name VLAN_30**

P1SW1 (VLAN)# **vtp domain bigdomain**

P1SW1 (VLAN)# **vtp server**

P1SW1 (VLAN)# **exit**

Création des trunk

P1SW1 (config)# **interface fastEthernet 0/1**

P1SW1 (config-if)# **switchport mode trunk**

P1SW1 (config-if)# **switchport trunk encapsulation dot1q**

P1SW1 (config-if)# **exit**

P1SW1 (config)# **interface fastEthernet 0/8**

P1SW1 (config-if)# **switchport mode trunk**

P1SW1 (config-if)# **switchport trunk encapsulation dot1q**

P1SW1 (config-if)# **exit**

Attribution des VLAN aux ports

P1SW1 (config)# **interface fastEthernet 0/2**

P1SW1 (config-if)# **switchport mode access**

P1SW1 (config-if)# **switchport access VLAN 20**

P1SW1 (config-if)# **exit**

P1SW1 (config)# **interface fastEthernet 0/3**

P1SW1 (config-if)# **switchport mode access**

P1SW1 (config-if)# **switchport access VLAN 30**

P1SW1 (config-if)# **exit**

P1SW1 (config)# **interface fastEthernet 0/4**

P1SW1 (config-if)# **switchport mode access**

P1SW1 (config-if)# **switchport access VLAN 20**

P1SW1 (config-if)# **exit**

P1SW1 (config)# **interface fastEthernet 0/5**

P1SW1 (config-if)# **switchport mode access**

P1SW1 (config-if)# **switchport access VLAN 30**

P1SW1 (config-if)# **exit**

- **Configuration du switch P1SW2**

Adhésion au domaine CISCO

P1SW2 # **VLAN database**
P1SW2 (VLAN)# **vtp domain CISCO**
P1SW2 (VLAN)# **vtp client**
P1SW2 (VLAN)# **exit**

Création du trunk

P1SW2 (config)# **interface fastEthernet 0/1**
P1SW2 (config-if)# **switchport mode trunk**
P1SW2 (config-if)# **switchport trunk encapsulation dot1q**
P1SW2 (config-if)# **exit**

Attribution des VLAN aux ports

P1SW2 (config)# **interface fastEthernet 0/2**
P1SW2 (config-if)# **switchport mode access**
P1SW2 (config-if)# **switchport access VLAN 20**
P1SW2 (config-if)# **exit**
P1SW2 (config)# **interface fastEthernet 0/3**
P1SW2 (config-if)# **switchport mode access**
P1SW2 (config-if)# **switchport access VLAN 30**
P1SW2 (config-if)# **exit**
P1SW2 (config)# **interface fastEthernet 0/4**
P1SW2 (config-if)# **switchport mode access**
P1SW2 (config-if)# **switchport access VLAN 20**
P1SW2 (config-if)# **exit**
P1SW2 (config)# **interface fastEthernet 0/5**
P1SW2 (config-if)# **switchport mode access**
P1SW2 (config-if)# **switchport access VLAN 30**
P1SW2 (config-if)# **exit**

iii- Configuration du Routeur P1R1

```
P1R1(config)# interface fastEthernet 0/0.1
P1R1(config-subif)# encapsulation dot1q 1
P1R1(config-subif)# ip address 192.168.110.1 255.255.255.0
P1R1(config-subif)# exit

P1R1(config)# interface fastEthernet 0/0.20
P1R1(config-subif)# encapsulation dot1q 20
P1R1(config-subif)# ip address 192.168.120.1 255.255.255.0
P1R1(config-subif)# exit

P1R1(config)# interface fastEthernet 0/0.30
P1R1(config-subif)# encapsulation dot1q 30
P1R1(config-subif)# ip address 192.168.130.1 255.255.255.0
P1R1(config-subif)# exit
```

3- Mise en place du réseau WAN:

3-1-Description :

Le choix du réseau WAN dépend des liaisons existant offertes par l'opérateur télécom dans le pays ou se trouve l'entreprise. Pour simplifier la topologie de la figure 7.3 du réseau, le deuxième switch P1SW2 a été enlevé.

On a créé un réseau qui relie deux sites séparés géographiquement, avec un routeur ; un switch et quatre PC dans chaque site. Dans chaque site, deux des PC sont connectés à un VLAN et les deux autres sont assignés à un autre VLAN.

Chaque routeur possède un sub-interface pour chaque VLAN, et un trunk 802.1q est utilisé pour connecter chaque sub-interface à son VLAN approprié sur le switch. Les routeurs dans chaque site sont connectés entre eux par un lien WAN Frame Relay point-à-point. Comme le montre la figure 7.4.

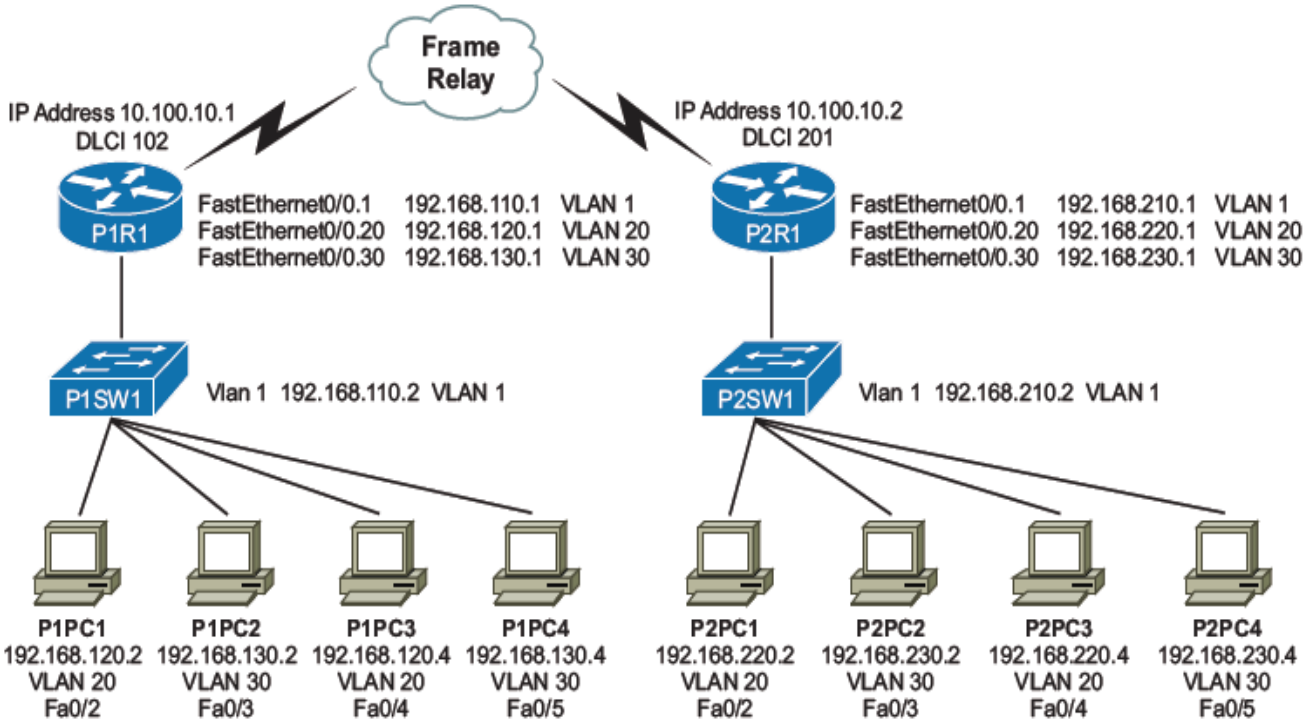


Figure 7.4 : interconnections entre deux sites géographiquement éloignés.

3-2-Simulation :

a- Configuration de l'interface série pour FRAME RELAY :

i- Configuration de l'encapsulation Frame Relay sur l'interface : pour designer des configuration valable sur les deux routeurs on utilisera PxR1 où x =[1-2] :

PxR1 #conf t

PxR1(config)# **interface serial 0**

PxR1(config-if)#**no shutdown**

PxR1(config-if)#**encapsulation frame-relay**

ii- Configuration du sub-interface en frame-relay point-à-point dans chaque routeur:

Pour P1R1:

P1R1#conf t

P1R1(config)# interface serial 0.1 point-to-point
P1R1(config-subif)# ip address 10.100.10.1 255.255.255.0
P1R1(config-subif)# frame-relay interface-dlci 102

Pour P2R1 :

P2R1#conf t

P2R1(config)# interface serial 0.1 point-to-point
P2R1(config-subif)# ip address 10.100.10.2 255.255.255.0
P2R1(config-subif)# frame-relay interface-dlci 202

iii- Configuration du routage dynamique :

Pour P1R1 :

P1R1#conf t

P1R1(config)# **router rip**

P1R1(config-router)# **network 10.0.0.0**

P1R1(config-router)# **network 192.168.110.0**

P1R1(config-router)# **network 192.168.120.0**

P1R1(config-router)# **network 192.168.130.0**

Pour P2R1 :

P2R1#conf t

P2R1(config)# **router rip**

P2R1(config-router)# **network 10.0.0.0**

P2R1(config-router)# **network 192.168.210.0**

P2R1(config-router)# **network 192.168.220.0**

P2R1(config-router)# **network 192.168.230.0**

4- Configuration des PC et vérification de la connectivité du réseau:

Les PC sont configurés avec leur adresse respective par la commande **winipcfg.** Lorsque la configuration de chaque matériel est terminée, pour vérifier la connectivité dans tout le réseau, on utilise la commande **ping.**

Durant la simulation comme dans la pratique, les tests de connectivité entre les PC se sont révélés positifs, ce qui prouve que le réseau fonctionne.

CONCLUSION

Actuellement, les réseaux informatiques ne cessent de s'élargir et mettent la pression au constructeur pour trouver de nouvelle solution adaptée au nouveau besoin des utilisateurs. Les VLAN ont vu le jour en conséquence des interminables demandes d'augmentation de bande passante et de stabilités dans les réseaux. Le travail que nous avons fait durant l'élaboration de ce document montre les nouveaux concepts introduits dans les routeurs, et les switches depuis le début de l'entreprise pour des améliorations de la communication. Les recherches étaient destinés essentiellement au moyen de configurations des routeurs et switches du constructeur CISCO, au mode d'implémentation des VLAN, et à la façon de les utilisés efficacement dans un réseau.

D'abord, notre étude consistait à apprendre à configurer les routeurs et switches CISCO au moyen du logiciel de simulation Boson netsim. Ensuite, la mise en pratique a été effectuée sur des routeurs et switches réels avec la mise à jour de l'IOS de certains matériels.

Finalement, en prenant du recul pour visualiser tout ce qui a été réalisé durant cette étude, il est évident que les connaissances en matière de configuration des routeurs et des switches resteront des atouts pour le futur. Malgré les difficultés, les obstacles ont tous été surmontés et l'objectif de l'étude a été atteint.

Certes, les VLAN ont apporté des solutions plus ou moins efficaces pour résoudre certain problème dans les réseaux locaux mais beaucoup de questions restent encore sans réponse et demandent des études plus approfondies, surtout pour les réseaux sans fil qui restent encore et toujours difficile à sécuriser. Puisque les réseaux sans fil sont en pleins essors, par suite à notre travail, l'étude de la configuration d'une topologie utilisant un réseau WIFI peut solutionner les problèmes de sécurisation.

ANNEXE 1
LES SWITCHES CISCO

1-Présentation Hardware

1-1- Structure interne

L'architecture interne d'un switch configurable CISCO se présente exactement comme celui d'un routeur CISCO. C'est-à-dire qu'il possède une Unité centrale (CPU), les différents types de mémoires qui ont exactement les mêmes rôles que dans un routeur.

1-2- structure externe

Par contre, la différence se trouve au niveau des ports d'entré/sortie qui ne sont que composés que de port Ethernet et/ou fastEthernet RJ45 pour le switch dont le nombre différencie les modèles, et un port console pour la configuration.

2- Software :

Evidement, puisque l'utilisation d'un routeur diffère de celui d'un switch, le logiciel IOS est d'un tout autre type sur le commutateur. Des évolutions sont possibles par des mises à jours pour s'adapter à de fonction future.

2-1- Mode de configuration :

Pour configurer des switch CISCO, on peut accéder directement à l'interface utilisateur du switch via un terminal ou accéder à distance au switch par une session TELNET. Mais quelle que soit la méthode utilisée pour accéder à un switch, celui-ci peut fonctionner dans différents modes. Chaque mode offre des fonctions différentes et pour des raisons de sécurité, il y a deux niveaux d'accès aux commandes :

- Mode utilisateur - Les tâches typiques comprennent, notamment, la vérification du fonctionnement du switch. Ce mode ne permet pas de modifier la configuration du switch.

L'invite de commande se présente comme suit :

Nom-switch>_

- Mode privilégié - Les tâches typiques comprennent, notamment, les changements de configuration du switch. Pour entrer en mode privilégié, on tape la commande *enable* dans le mode utilisateur. Et l'invite de commande devient :

Nom-switch>**enable**
Nom-switch#_

- Mode de configuration globale -- Mode offrant d'efficaces commandes monolignes pour l'exécution de tâches de configuration simple. Pour pouvoir configurer en mode de configuration globale, on tape la commande *configure terminal* dans le mode privilégié. Et l'invite de commande devient :

```
Nom-switch#configure terminal
                    Nom-switch(config)#_
```

-Autres modes de configuration -- Modes permettant de créer des configurations multilignes détaillées. Cette partie dépend des intentions de l'administrateur et des fonctions qu'il veut configurer.

Le switch CISCO peut supporter des protocoles propres à lui ou partager ceux des routeurs.

2-2- Les protocoles dans les switch :

a-Notion de CDP (CISCO Descovery Protocol)

Ce protocole a été développé par CISCO pour faciliter la découverte d'équipements du réseau et d'échanger des informations exhaustives sur la configuration de ceux-ci :

- Nom et adresse IP de l'équipement
- Version de CatOS/CatIOS/IOS installée
- Plate-forme matérielle et modules installés
- Fonctionnalités de l'équipement
- VLAN natif de l'équipement
- …

Les messages CDP sont envoyés en multicast. En dehors de divulguer des informations sur les équipements, ce protocole est très sensible aux « denials of services ». En effet les informations échangées par CDP ne sont jamais mises à jour ou remplacées, ainsi il est facile d'envoyer un grand nombre de messages pour saturer la mémoire de l'équipement.

b-La notion de trunk, et Dynamic Trunk Protocol

La fonction d'un trunk est de transporter des VLAN entre plusieurs commutateurs interconnectés et donc d'étendre la portée des VLAN à un ensemble de commutateurs. Il peut fonctionner aussi entre un commutateur et un routeur pour sortir vers le réseau WAN. Chaque VLAN est distingué de par ses tags 802.1q ou ICL (protocole CISCO).

Le Dynamic Trunk Protocol (DTP) autorise la configuration automatique de certains ports en mode trunk. Le Switch acceptera donc les trafics « taggés et non taggés ».

c- La notion de Spanning Tree Protocol

Le spanning tree protocol (STP) permet de manager les connexions Ethernet commutées (exemple par des VLAN). Il fournit des chemins redondants dans un réseau niveau 2 tout en évitant les boucles de routage. Il existe plusieurs types de protocole STP et tous ces types utilisent un algorithme qui calcule le meilleur chemin sans boucle à travers le réseau.

Dans les réseaux Ethernet, un seul chemin actif peut exister entre deux stations. En effet, plusieurs chemins actifs entre des stations causent inévitablement des boucles dans le réseau.

L'algorithme spanning tree fournit des chemins redondants en définissant un arbre qui recense tous les commutateurs dans un réseau étendu et force ensuite certains chemins de données à être à l'état « bloqué ». À intervalles réguliers, les commutateurs dans le réseau émettent et reçoivent des paquets spanning tree qu'ils emploient pour identifier le chemin. Si un segment de réseau devient inaccessible ou si les coûts spanning tree changent, l'algorithme spanning tree reconfigure la topologie spanning tree et rétablit la liaison en activant le chemin de réserve.

ANNEXE 2

Les commandes CISCO

« enable » ou « ena » ou « en » pour passer en mode administrateur sur l'équipement réseau.
Toutes les commandes indiquées ci-dessous sont à effectuer en mode administrateur.
Pour obtenir de l'aide sur une commande faite nom de la commande suivie d'un point d'interrogation :
ex : show ?

Commandes	Descriptions
configure terminal ou conf t ou conf term	Entre dans le mode de configuration globale
CTRL-Z	Permet de retourner à la racine du menu
exit	Sort et remonte d'un cran dans la hiérarchie des menus
hostname ou host <hostname>	Permet de modifier le nom de l'équipement réseau
enable secret <password>	Assigne un mot de passe encrypté à enable
interface ethernet | fastethernet | Serial | loopback <interface> ou int e | fa | s | lo	Entre dans le mode de configuration de l'interface
ip address <address> <mask> ou ip add	Configure l'interface avec l'ip et le masque de réseau
bandwidth ou band	Indique une bande passante
encapsulation <encap> [<type]> ou encap	Fournit l'encapsulation de l'interface
no shutdown ou no shut	Active ou Désactive l'interface
Les commandes de sauvegarde :	
copy running-config startup-config ou copy run star ou write mem	Sauvegarde la configuration courante en NVRAM
copy running-config tftp ou copy run tftp	Sauvegarde la configuration courante vers un serveur TFTP
copy startup-config tftp ou copy star tftp NVRAM	Sauvegarde la configuration situé en vers un serveur TFTP
copy tftp startup-config ou copy tftp star	Charge un fichier de configuration d'un serveur TFTP en NVRAM
copy tftp running-config ou copy tftp run	Charge un fichier de configuration d'un serveur TFTP dans la configuration Courante
erase startup-config ou erase star	Efface la configuration de la NVRAM

Configuration d'une connexion en telnet:	
router# conf t router(config)# line console 0 router(config)# login router(config)# password xyz	
Les commandes de configurations du routage :	
router <xxx> [<process-id>,<autonomous system>] rip,ospf,bgp,igrp,eigrp,is-is,...	Configure le protocole de routage d'un routeur
exemple de configuration du routage RIP: router# conf t router(config)# router rip *router(config-router)# version 1-2* router(config-router)# network *networknumber* ***exemple de configuration du routage OSPF:*** router# conf t router(config)# router ospf 10 *router(config-router)# network networknumber* ***exemple de configuration du routage IGRP:*** *router# conf t* *router(config)# router igrp autonomoussystem* router(config-router)# network *networknumber* ***exemple de configuration du routage EIGRP:*** *router# conf t* *router(config)# router eigrp autonomoussystem* router(config-router)# network *networknumber* ***exemple de configuration du routage BGP:*** *router# conf t* *router(config)#* router bgp *autonomoussystem* router(config-router)# network *networknumber* [mask *network-mask*] [route-map *route-map-name*]	
D'autres commandes de routage	
ip multicast-routing Permet de faire du routage multicast ip rsvp bandwidth [*interface-kbps*] [*singleflow-*	Active la réservation RSVP sur une interface

kbps]	
Les commandes sur un switch :	
vlan database vlan 1 name <vlan name>	Accès à la database et écriture dans le fichier vlan.dat
Exemple de configuration d'un vlan : switch# vlan database switch(vlan)# vlan <number> <name> switch(vlan)# exit	
switch(config)#interface fa<iface-number>	affectation sur un port
>switch(config)#interface range fa...	affectation sur un ensemble de ports
switch(config-if)#switchport mode access	Pour passer au mode de configuration de l'interface
switch(config-if)# switchport access vlan <number-name>	on active le vlan sur le ou les interfaces
Activation du trunking sur l'interface	Le truncking sert dans l'extension d'un domaine VLAN sur d'autre switch, pour ce faire CISCO utilise le protocole VTP VLAN Trunking Protocol
switchport trunk encap dot1q	Il y a 2 protocoles utilisés dans l'étiquetage: le protocole ISL (CISCO) et le protocole 802.1q (IEEE)
switchport mode trunk	active le mode trunk sur le port du commutateur serveur et client, le reste des ports est en mode access
vlan database vtp domain <domain-name> vtp server	Création d'un serveur VTP
vlan database vtp domain <domain-name> vtp client	Création d'un client VTP
ip default-gateway <ip-gateway>	On peut définir une passerelle par défaut pour communiquer entre VLAN, pour se faire on utilise un routeur
encapsulation ISL | dot1q <vlan-number>	en mode interface on peut spécifier le type d'encapsulation sur le routeur
D'autres commandes communes :	

reload	Redémarre l'équipement réseau
setup	Passe en mode de configuration assisté
ping [<address>]	ping seul, permet de faire un ping étendu de spécifier une interface particulière..., ping + address IP ping l'interface avec l'interface directement connecté.
Les commandes show :	
show interfaces ou sh int	Donne une description détaillé sur les interfaces
show running-config ou sh run	affiche la configuration courante
show startup-config ou sh star	affiche la configuration en NVRAM
show ip route ou sh ip route	affiche la table de routage
show ip <routing-protocol> [<options>]	affiche les informations sur le protocole de routage défini
show ip protocols	affiche les informations sur les protocoles utilisés

REFERENCE

[1] Cours E551IA, « Téléinformatique », Département Electronique, ESPA, Année 2007

[2] Cours E510, *« Réseau local »*, Département Electronique, ESPA, Année 2007

[3] Cours E520IA, *« Administration système »*, Département Electronique, ESPA, Année 2007

[4] Cours E558IA, *« Cryptographie »*, Département Electronique, ESPA, Année 2007

[5] Gary A. Donahue, « *Network Warrior* », O'Reilly, June 01, 2007.

[6] James Boney, « *Cisco IOS in a Nutshell* », O'Reilly, August 2007.

[7] Craig Hunt, « *TCP/IP Network Administration* », O'Reilly, April 2002.

[8] Ravi Malhotra, « *IP Routing* », O'Reilly, January 2002.

[9] «http://www.cisco.com »

[10] Jeff Doyle, « *Routing TCP/IP Volume 1/2* »,Ciscopress, 1998.

[11] David Barnes, Basir Sakandar, « *Cisco LAN switching Fundamentals* », O'Reilly, july 15, 2004.

[12] *Sylvain Eche, Constantin Yamkoudougou,* « *Etudes d'attaques sur les VLAN* », 2003.

[13] «http://www.supinfo-projects.com »

[14] « http://www.labo-cisco.com »

[15] Jürgen Ehrensberger, « LABORATOIRE RÉSEAUX LOCAUX VIRTUELS VLAN », support de cours Institut IICT / HEIG-VD format pdf

[16] « http://www.reseaucerta.org »

[17] « http://christian.caleca.free.fr »

[18] « http://www.boson.com »

[19] ANDRIAMANANJATOVO Mandaniaina Malala, « APPLICATION DES ROUTEURS CISCO DANS UN INTER RESEAU VLAN (VIRTUAL AREA NETWORK) », mémoire de fin d'études en vue de l'obtention du diplôme d'ingénieur.

Auteur : ANDRINIAINA Jimmy Rodin Adresse : ITZ 67 BEHENJY ITAOSY

Titre : **APPLICATION DES SWITCHES CISCO DANS UN RESEAU VLAN (VIRTUAL LOCAL AREA NETWORK)**

Nombre de pages : 64
Nombre de figures : 26
Nombre de tableaux : 2

Résumé :

Les administrateurs réseau étaient toujours confrontés aux problèmes de bande passante et de restriction géographique lors de l'application des réseaux traditionnels dans une quelconque situation. Alors pour solutionner ces problèmes et maintenir l'évolutivité d'un réseau local, tout en introduisant de nouveaux concept de sécurité, les constructeurs de matériels réseau comme CISCO ont créé le réseau virtuel ou VLAN (Virtual Local Area Network).

Le présent rapport a été axé principalement sur l'utilisation des switches configurables CISCO dans le domaine de la mise en place d'un réseau VLAN (Virtual Local Area Network).

Mots clés : VLAN, Routage, Routeur, Switch, CISCO, LAN, WAN

Rapporteur : Monsieur RAKOTONDRASOA Justin