وزارة التعليم العالي والبحث العلمي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
جامعة عبدالحميد ابن باديس مستغانم
Université Abdelhamid Ibn Badis de Mostaganem
كلية العلوم و التكنولوجيا
Faculté des Sciences et de la Technologie

N° d'ordre : M……/GE/2020

MEMOIRE DE FIN D'ETUDE DE MASTER ACADEMIQUE

Filière : Génie électrique
Spécialité : Télécommunication

Thème

Instalation et mise en oeuvre d'une Infrastructure à base des VLANs pour l'optimisation des sécurités réseaux

Présenté par :

Mr : HAKKOUMI MOUSSA

Mme : MEKRI KHEIRA

Soutenu le 09 / 09 / 2020 devant le jury composé de :

Président de jury : MR Benabdellah Yagoubi

Examinateur 1 : MR Henni Sid Ahmed

L'encadreur : MR Resfa Abbes

Année Universitaire : 2019 / 2020

Remerciement :

Au terme de ce travail, nous adressons nos vifs remerciements à notre encadreur, Mr Resfa Abbes Pour sa patience, sa disponibilité et surtout ses judicieux conseils, qui ont contribué à alimenter notre réflexion.

Nous tenons particulièrement à remercier vivement :
Les membres de jury pour avoir accepter d'évaluer notre travail.

Nous remercions tout le corps professoral, pour le travail énorme qu'il effectue afin de créer des conditions favorables pour le déroulement de nos études.

Enfin, nous tenons à témoigner nos sincères remerciements à toutes les personnes qui ont contribués de près ou de loin à l'élaboration de ce modeste travail.

Dédicace :

A l'Eternel Dieu pour sa protection continue dans ma vie.

A l' âme de ma trop chère Mére Qui me manque tant,maintenant elle apprécie cet humble geste comme preuve de reconnaissance de la part d'une fille qui a toujours prié pour le salut de son ame.

Que dieu la protège du fond de sa miséricorde.

A mon cher père pour sa tendresse et son soutien.

A mes fils Abdelkrim et Anes qui me donne de l'amour et la volonté.

A mes frères et mes sœurs pour leur appui et leur encouragement.

J'espére qu'ils trouveront dans ce travail toutes mes reconnaissances.

Kheira

Dédicaces :

Je dédie ce travail :

A ma famille, elle qui m'a doté d'une éducation digne, son amour afait de moi ce que je suis aujourd'hui

Particulièrement à mon Père pour le gout à l'effort qu'il a suscité en moi…

A vous mes frères Badr et Youcef qui m'avez toujours soutenu et encouragé durant ces années d'études.

A tous ceux que j'aime et ceux qui m'aiment.

Moussa

Table des matières :

Chapitre 02 : Les réseaux VLANs

Chapitre 03: La mise en place des VLANs

Chapitre 04:résultats de Simulation et discussion

Liste des figures :

Liste des Tableaux :

Liste des abréviations:

CLI : Command Line Interface.

DHC : Dynamic Host Configuration Protocol.

BID : Bridged Identity.

BPDU : Bridge Protocol Data Unit.

EIGRP : Extended Interior Gateway Routing Protocol.

HSRP : Hot Standby Routing Protocol.

HTTP : Hypertext Transfer Protocol.

IGRP : Intenior Gateway Routing Protocol.

IP : Internet Protocol.

ISO : Organisation Internationale de normalisation.

JPEG : Joint Photographic Experts Group.

LAN : Local Area Network.

MAC : Media Access Control.

MAN : Metropolitan Area Network.

OSI : Open System Interconnection.

OSPF : Open Shortest Path First. PC : Personel Computer.

RFC : Request For Comments (Ensemble de documents qui font référence auprés de la communité internet).

RIP : Routing Information Protocol.

STP : Spanning-Tree Protocol.

TCP : Transmission Control Protocol.

USB : Universal Serial Bus

VLAN : Virtual Local Area Network.

VTP : VLAN Trunking Protocol.

WAN : Wide Area Network

Introduction générale :

Ces dernières années, l'évolution des services et du trafic a suscité un développement technologique permettant d'augmenter la capacité et les fonctionnalités des ressources.

Au sein d'une organisation, un réseau informatique est peut être vu comme le cœur de la majeure partie de son activité. Il met en relation des équipements terminaux (ordinateurs, imprimantes, stations de travail, terminaux passifs), et des serveurs. Tous ces éléments sont entièrement sous la responsabilité de l'entreprise.

En effet, l'utilisation d'un réseau local est primordiale au bon fonctionnement d'une entreprise car il facilite la transmission, la duplication, le partage des dossiers et des périphériques. Il permet aussi le traitement et la consultation des bases de données et une transmission rapide et fiable des données.

Cependant, l'évolution des réseaux locaux a vu l'introduction d'un concept appelé **VLAN**, réseau local virtuel, afin de s'affranchir des limitations de l'architecture physique (contraintes géographiques, contraintes d'adressage, ...) en définissant une segmentation logique basée sur un regroupement de machines grâce à des critères (adresses MAC, numéros de port, protocole, etc.).

Dans le présent mémoire, nous présenterons en détail les étapes que nous allons suivre afin de réaliser notre projet, structuré en quatre chapitres organisés comme suit :

- Le premier chapitre s'intitulant « Généralités sur les différents réseaux », définit quelques notions théoriques de base, qui aideront et seront utiles pour la compréhension de la problématique posée, à savoir la définition d'un réseau, les topologies, les types, etc.
- D'autre part, le second chapitre nommé « les réseaux Vlans », où nous allons faire le point sur le concept des VLANs, leurs types, leurs utilités et quelques protocoles permettant leurs gestions.

- Le troisième chapitre «la mise en place des Vlans », est basée sur la, stucturation et addressage et configuration des équipements de notre modèle type en général dans le but de détecter les problèmes qu'il rencontre, puis proposer une solution à adopter.

Le dernier chapitre « résultats de simulation et discussion », basé sur la conception du modèle type, La simulation ainsi que toutes les configurations appliquées des solutions et des tests de validation.

chapitre 01 :

Généralité sur les différents réseaux

1.1 Introduction:

Un réseau désigne un ensemble d'équipements interconnectés pour permettre la communication de données entre applications, quelles que soient les distances qui les séparent.

Un réseau informatique est un ensemble des ressources de communication (matérielles et logicielles) reliés entre eux pour échanger des informations.

Un réseau s'appuie sur deux notions fondamentales :

- L'interconnexion qui assure la transmission des données d'un nœud à un autre.
- La communication qui permet l'échange des données entre processus.

L'objectif de ce chapitre est de présenter quelques concepts de basessur les réseaux informatiques, pour bien aider à mieux assimiler le fonctionnement des réseaux. Donc, toutes les notions nécessaires seront présentées, tirant exemple de la classification des réseaux, la topologie, le modèle OSI et TCP/IP ainsi les périphériques réseauxp

1.2 Classification et topologie des réseaux:

Il existe de trois types de réseaux : MAN .LAN . WAN. [1]

1.2.1 Par portée :

1) Les réseaux locaux ou LAN (Local Area Network) correspondent aux réseaux intra-entreprise (quelques centaines de mètres et n'excèdent pas quelques kilomètres), généralement réseaux dits "privés". Le réseau de votre établissement est un réseau de type LAN.

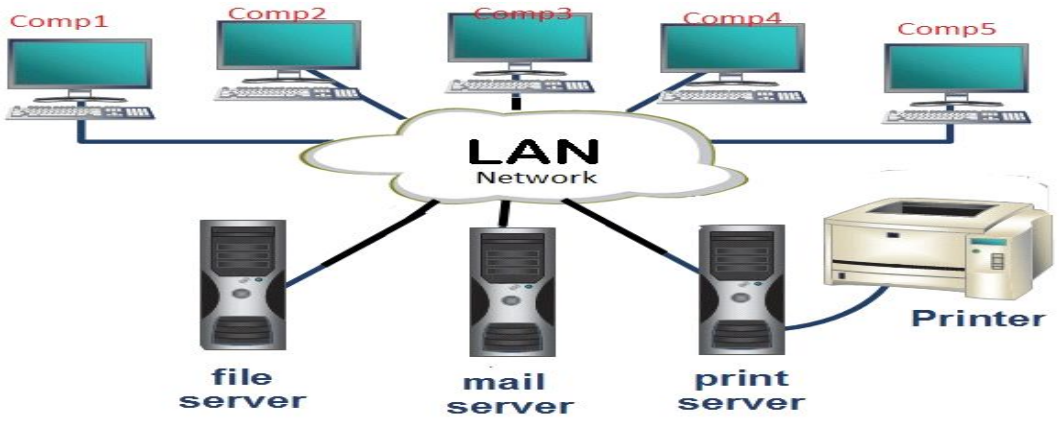


Fig 1.1 : Les réseaux locaux ou LAN (Local Area Network)

2) Les réseaux grands distances ou WAN (Wide Area Network) sont des réseaux étendus, généralement réseaux dits "publics" (gérés par des opérateurs publics ou privés), et qui assurent la transmission des données sur des longues distances à l'échelle d'un pays ou de la planète. Internet est un réseau de type WAN.

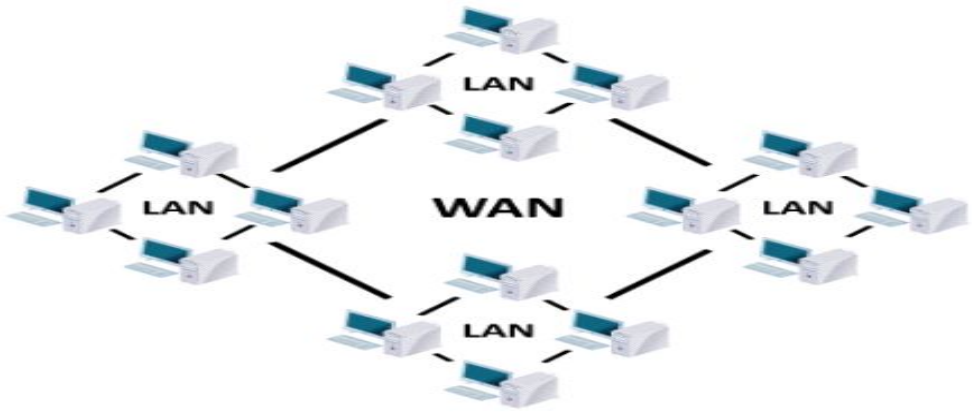


Fig 1.2 : Les réseaux grands distances ou WAN (Wide Area Network)

3) MAN (Métropolitain Area Network) Ce type de réseaux est récent et garde les avantages des LAN sur de plus longues distances de l'ordre de la ville.

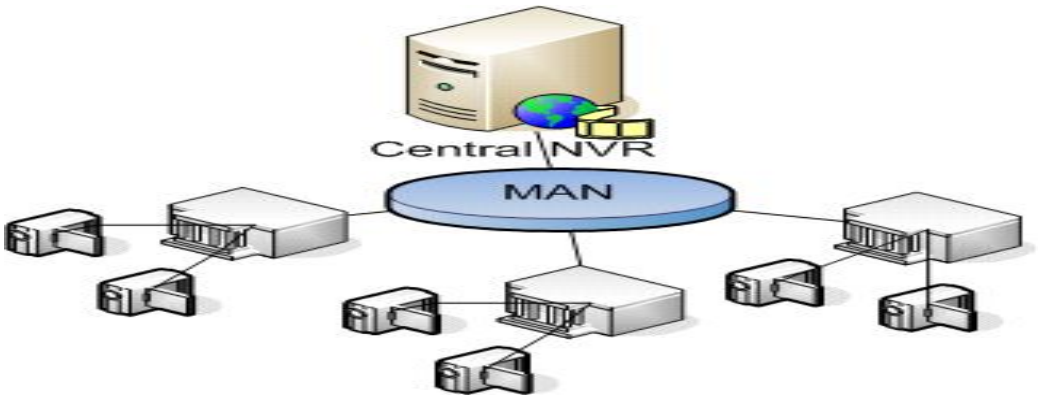


Fig 1.3 : Les réseaux MAN (Métropolitain Area Network)

1.2.2 Par utilisation:

Les réseaux informatiques utilisant la famille des protocoles TCP/IP, on distingue :

- ✓ Intranet : le réseau interne d'une entité organisationnelle
- ✓ Extranet : le réseau externe d'une entité organisationnelle
- ✓ Internet : le réseau des réseaux interconnectés à l'échelle de la planète

1.2.3 Par topologie d'un réseau:

Il existe deux types de topologies : topologie logique et topologie physique

1.2.3.1 La topologie logique :

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

1.2.3.2 La topologie physique :

1.2.3.2.1 **Réseau en étoile :**

les équipements du réseau sont reliés à un équipement central. dans une topologie en étoile les ordinateurs du réseau sont reliés à un système matériel appelé HUB.

1.2.3.2.2 **Réseau en bus :**

l'interconnexion est assurée par un média partagé entre tous les équipements raccordés dans cette topologies les ordinateurs sont reliés a un même câble.

1.2.3.2.3 **Réseau en anneau :**

les câbles de liaison entre les ordinateurs forment une boucle (cercle fermé) ou un anneau de communication.

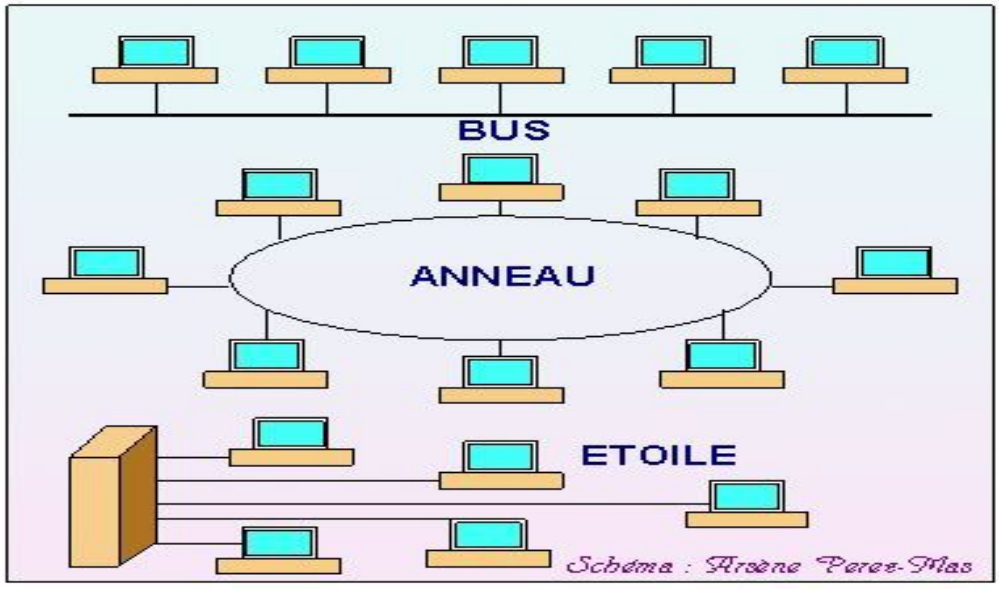


Fig 1.4 : Topologie physique d'un réseau

1.3 Principes de fonctionnement :

1.3.1 Maille:

Ce type de câblage n'est plus utilisé car il nécessite beaucoup de câbles. Avec n machines il faut : n (n -1) /2 câbles.

1.3.2 Bus :

Sur un câble de type bus, on utilise souvent un système CSMA/CD (Carriere Sense Multiple Acces / Collision Detection) Accès multiple avec détection de porteuse et détection des collisions.

1.4 Caractéristiques:

Les caractéristiques de base d'un réseau sont :

- La topologie qui définit l'architecture d'un réseau : on distinguera la topologie physique qui définit la manière dont les équipements sont interconnectés entre eux, de la topologie logique qui précise la manière dont les équipements communiquent entre eux.
- Le débit exprimé en bits/s (ou bps) qui mesure une quantité de données numériques (bits) transmises par seconde (s).
- La distance maximale (ou portée) qui dépend de la technologie mise en œuvre.
- Le nombre de nœuds maximum que l'on peut interconnecter.

1.5 Les composantes physiques des reseaux locaux:

- ✓ **Le Média :**

Il correspond au moyen de transporter l'information, en général il s'agit du câblage ou support 3 types de câblage sont utilisés en réseau local :

1.5.1 le câble coaxial :

Le câble coaxial ou ligne coaxiale est une ligne de transmission ou liaison asymétrique, utilisée en hautes fréquences, composée d'un câble à deux conducteurs.

Fig 1.5 : ligne de transmission ou liaison asymétrique (câble coaxial)

1.5.2 la paire torsadée :

Une paire torsadée est une ligne symétrique formée de deux fils conducteurs enroulés en hélice l'un autour de l'autre. Cette configuration a pour but principal de limiter la sensibilité aux interférences et la diaphonie dans les câbles multi paires.

Il existe (généralement) deux types de câbles à paires torsadées :

-Paire torsadée non blindée (UTP:Unshielded Twisted Pair)

-Paire torsadée blindée (STP:Shielded Twisted Paire)

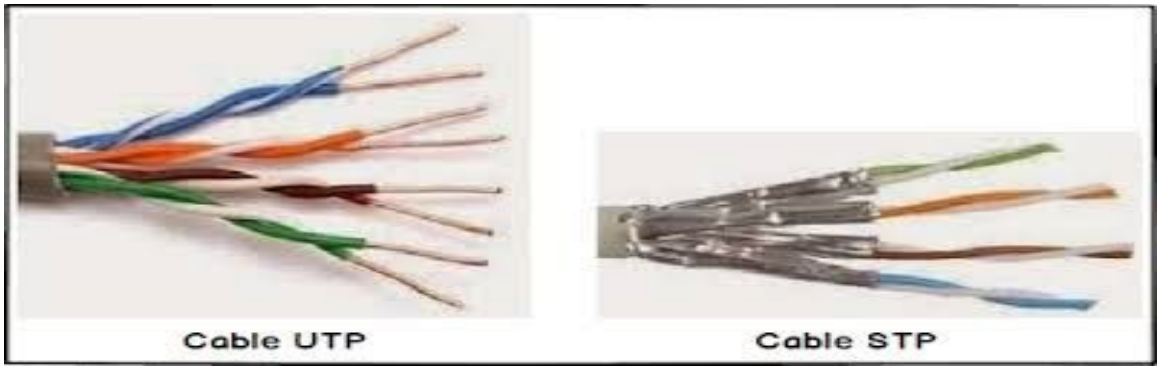


Fig 1.6 : La paire torsadée (une ligne symétrique)

1.5.3 La fibre optique :

une fibre optique est un fil dont l'âme, très fine, en verre ou en plastique, a la propriété de conduire la lumière et sert pour la fibroscopie, l'éclairage ou la transmission de données numériques. Elle offre un débit d'information nettement supérieur à celui des câbles coaxiaux et peut servir de support à un réseau « large bande » par lequel transitent aussi bien la télévision, le téléphone, la visioconférence ou les données informatiques. Le principe de la fibre optique date du début du xxe siècle mais ce n'est qu'en 1970 qu'est développée une fibre utilisable pour les télécommunications, dans les laboratoires de l'entreprise américaine Corning Glass Works (actuelle Corning Incorporated).

Elle est constituée en fibre de verre, l'information circule sous forme lumineuse.

- **Avantage :**

- Les fibres optiques sont aussi plus minces et plus légères. Ainsi, cela leur permet d'offrir un meilleur ajustement, là où l'espace est un problème.
- très grande fiabilité,
- débit élevé,
- isolation galvanique
- poids moindre
- utilisation sur de grandes distances (jusqu'à 50 km)

- **Inconvénient :**

- coût élevé.

- prix de composants
- prix des outils de connexions

✓ **Distance :**

La distance entre l'émetteur et le récepteur doit rester courte ; ou alors des répéteurs sont nécessaires pour amplifier le signal.

-Les sources d'émission de faible puissance-lumière sont limitées à une faible puissance. Bien que des émetteurs de forte puissance soient disponibles pour améliorer l'alimentation électrique ; mais cela implique aussi un coût supplémentaire.

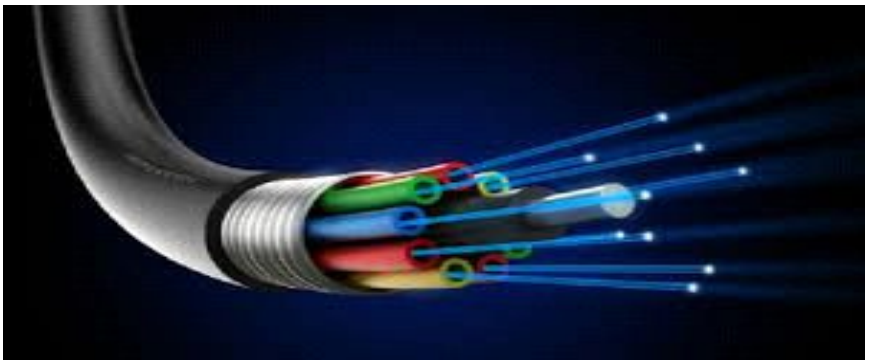


Fig 1.7 : Sources d'émission de faible puissance-lumière

1.5.4 Les différents types de câbles optiques :

Pour être complet, passons maintenant en revue les différents types de câbles à fibres optiques les plus courants. De façon synthétique, il existe trois types de câbles à fibres optiques. Il y a d'abord le câble à fibre optique monomode. Ensuite, nous avons la fibre optique multimode. Enfin, nous avons la fibre optique plastique (POF).

1.5.4.1 Fibre optique monomode :

Le « mode » dans le câble de fibre optique se rapporte au chemin dans lequel la lumière voyage. La fibre monomode a un diamètre de noyau plus petit de 9 microns ; 8,3 microns pour être exact. Elle ne laisse passer qu'une seule longueur d'onde, et ne dispose que d'une seule voie pour la lumière. Ainsi, cela diminue considérablement les réflexions lumineuses et diminue l'atténuation. Le câble de fibre optique monomode est légèrement plus cher que ses homologues multimodes ; qui sont souvent utilisés dans les connexions réseau sur de grandes distances.

1.5.4.2 Fibre optique multimode :

Ensuite, la fibre optique multimode a un diamètre de noyau plus grand que celui du câble de fibre optique monomode. Cela lui permet de transmettre de multiples voies et plusieurs longueurs

d'onde de lumière. La fibre optique multimode est disponible en deux tailles : 50 microns et 62,5 microns. Ce câble est couramment utilisé pour de courtes distances. Y compris des câbles de raccordement, et notamment ceux de la FTTO. On l'utilise aussi pour les connexions vers un équipement, les données et les applications audio / vidéo dans les réseaux locaux.

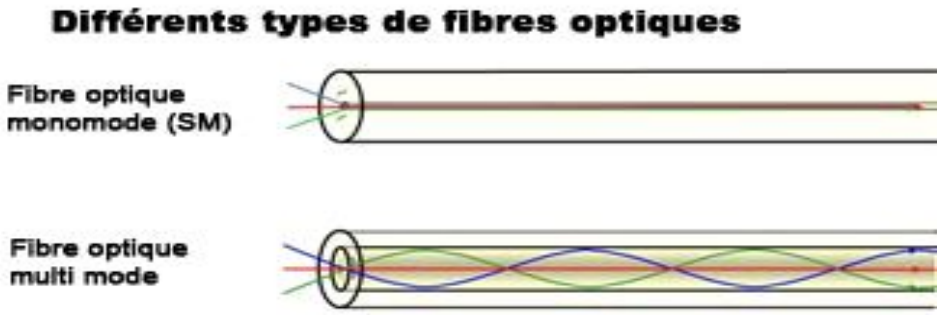


Fig 1.8 : La fibre optique multimode

1.5.4.3 Fibre optique en plastique (POF) :

Enfin, la POF est une fibre optique avec un diamètre typique de 1 mm. Sa « grande taille » lui permet de coupler facilement beaucoup de lumière provenant de sources et de connecteurs qui n'ont pas besoin d'être très précis. Étant en plastique, ce type de câble de fibre optique est plus durable. Il peut être installé en quelques minutes avec un minimum d'outils et de formation. Le prix du câble optique en plastique est plus compétitif, ce qui en fait une option intéressante pour les connexions LAN de bureau et les liaisons courtes à basse vitesse.

1.5.5 La carte réseau (carte LAN – Carte Ethernet):

Une carte réseau est matérialisée par un ensemble de composants électroniques soudés sur un circuit imprimé. L'ensemble constitué par le circuit imprimé et les composants soudés s'appelle une carte électronique, d'où le nom de carte réseau.

La carte réseau se présente sous la forme d'une carte d'extension connectée à un bus (généralement PCI) et comportant un connecteur RJ45 ou BNC ou fibre. Certaines cartes réseaux (voir photo) sont polyvalentes (combo), elles comportent alors un connecteur BNC permettant de relier le poste à un réseau en bus et un connecteur RJ45 permettant de relier le poste à un réseau en étoile.

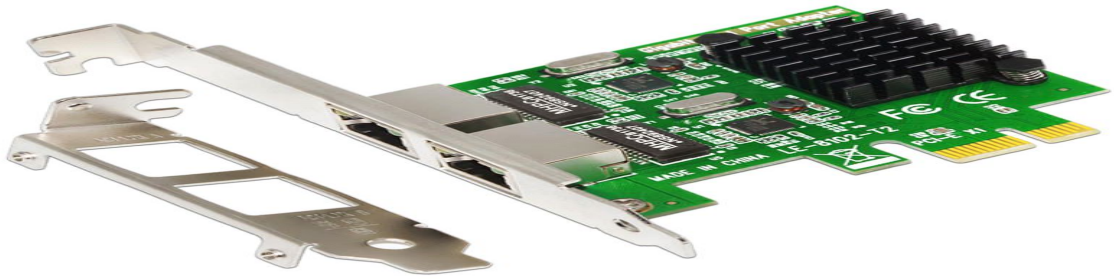


Fig 1.9 : La carte réseau (carte LAN – Carte Ethernet)

1.6 Modèles de référence

Un modèle de référence est utilisé pour décrire la structure et le fonctionnement des communications réseaux. On connaît deux modèles :

- Le modèle OSI (Open Systems Interconnect) qui correspond à une approche plus théorique en décomposant le fonctionnement en une pile de 7 couches.
- Le modèle DoD (Department Of Defense) qui répond à un problème pratique comprenant une pile de 4 couches pour décrire le réseau Internet (la famille des protocoles TCP/IP).

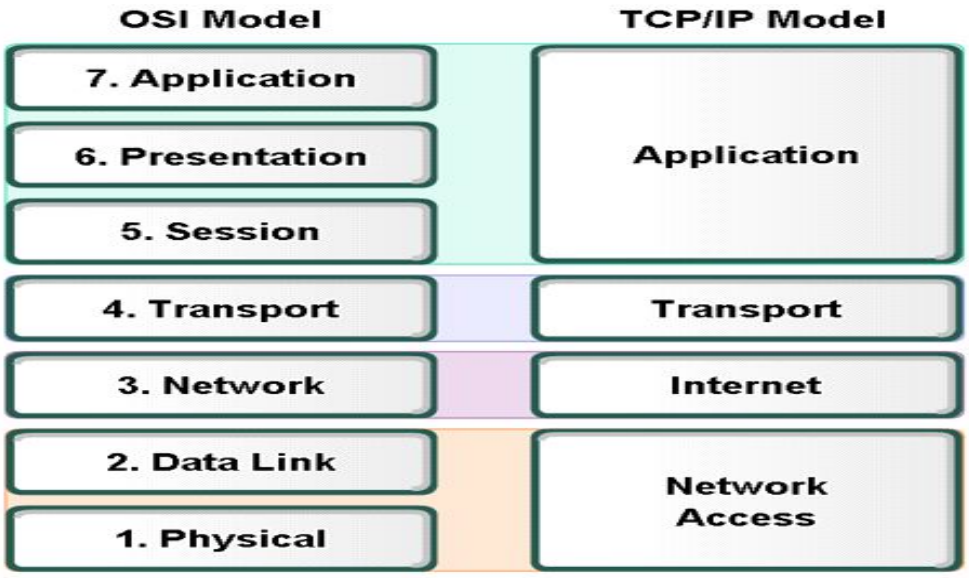


Fig 1.10 : Modèles OSI et DoD

1.6.1 Les couches basses :

Dans le modèle OSI, les trois couches basses assurent des fonctions orientées ”transmission“ :

1.6.1.1 La couche physique :

Cette couche physique s'occupe de la transmission physique des données entre deux équipements réseaux. Elle s'occupe de tout ce qui a trait au bas-niveau, au matériel : la transmission des bits, leur encodage, la +synchronisation entre deux cartes réseau, etc. Elle définit les standards des câbles réseaux, des fils de cuivre, du WIFI, de la fibre optique, ou de tout autre support électronique de transmission.

1.6.1.2 La couche de liaison de données :

Spécifie comment les paquets de la couche supérieure seront transportés. Elle assure la mise en trames, leurs acheminements sans erreurs et la méthode d'accès au réseau physique.

1.6.1.3 La couche réseau :

Est la troisième couche du modèle OSI La couche réseau construit une voie de communication de bout à bout à partir de voies de communication avec ses voisins directs. Ses apports fonctionnels principaux sont donc :

- **Le routage :**

Détermination d'un chemin permettant de relier les 2 machines distantes.

- **Le relayage :**

Retransmission d'un PDU (Protocol Data Unit ou Unité de données de protocole) dont la destination n'est pas locale pour le rapprocher de sa destination finale. [2]

1.6.2 Les couches hautes :

1.6.2.1 La couche transport :

Elle segmente les données de la couche session, prépare et contrôle les taches de la couche réseau, est responsable du transport des données de bout en bout au travers du réseau.

1.6.2.2 La couche session :

Établit une communication entre émetteur et récepteur en assurant l'ouverture et la fermeture des sessions.

1.6.2.3 La couche présentation :

Elle convertit les données en informations compréhensibles par les applications et les utilisateurs. Elle peut comporter des fonctions de traduction, de compression, d'encryptage.[3]

1.6.2.4 La couche application :

C'est l'interface entre l'utilisateur ou les applications et le réseau. Elle concerne la messagerie, les transferts et partages de fichiers, l'´émulation de terminaux.

1.7 L'interconnexion d'un réseau local :

Les équipements d'interconnexion de réseaux permettent :

- de relier des réseaux hétérogènes (couches et protocoles différents) d'organiser au mieux le réseau pour une exploitation optimale (adressage des réseaux et sous-réseaux, VLAN, proxy, ...)
- de contourner les limites techniques des architectures des réseaux

(Augmentation des distances des segments physiques, changement de support physique, ...)

- d'offrir une sécurité maximale (pare-feu ou firewall, VLAN, proxy,..)

1.7.1 Répéteur:

dispositif permettant d'´étendre la distance de câblage d'un réseau local. Il amplifie et répète les signaux qui lui parviennent.

1.7.2 Pont:

Un pont (bridge) est un dispositif permettant de relier des réseaux de même nature.

1.7.3 Routeur:

Un routeur (router) est un dispositif permettant de relier des réseaux locaux de telle façon `à permettre la circulation de données d'un réseau`à un autre de façon optimale.

1.7.4 Passerelle :

Une passerelle (gateway) est un dispositif permettant d'interconnecter des architectures de réseaux différentes .Elle assure la traduction d'un protocole d'un haut niveau vers un autre.

1.7.5 Concentrateur :

Un concentrateur (hub) est un dispositif permettant de connecter divers élément de réseau

1.7.6 Commutateur :

Un commutateur réseau (en anglais switch), est un équipement qui relie plusieurs segments (câbles ou fibres) dans un réseau informatique et de télécommunication et qui permet de créer des circuits virtuels.

1.7.7 Adaptateurs :

les adaptateurs (adapter) sont destinés à être insérés dans un poste de travail ou un serveur afin de les connecter `à un système de câblage.

Note : Les échanges de données entre équipements sont basés sur une communication logique qui se définit par les principes généraux suivants :

- L'architecture qui définit les rôles endossés par les équipements.
- Les protocoles qui assurent l'échange des données.
- L'adressage qui permet d'identifier de manière unique les équipements en communication.

1.8 Catégorie:

Les réseaux informatiques peuvent aussi être catégorisés par la relation fonctionnelle (le rôle) entre les équipements. On distingue par exemple :

- L'architecture client/serveur qui centralise des ressources sur un serveur qui offre des services pour des clients. Le réseau Internet, basé sur cette architecture, peut être vu comme un réseau de services composés exclusivement de serveurs.
- L'architecture poste à poste ou pair-à-pair (peer-to-peer) qui permet de partager simplement des fichiers le plus souvent, mais aussi des flux multimédia continus (streaming) ou du calcul réparti. Les systèmes peer-to-peer permettent une décentralisation des systèmes, en permettant à tous les ordinateurs de jouer le rôle de client et de serveur.
- Les protocoles rendent possible le dialogue entre des machines différentes en définissant les règles pour réaliser une communication. Cela comprend :
- Le dictionnaire : la liste des primitives (comme demande connexion, acquittement, ...)
- Le scénario du dialogue : l'enchaînement des primitives (représentable par un diagramme de l'échange)
- Les modalités : la taille et la représentation des informations, temps d'attente, etc ...
- Les messages échangés : les différents champs composant le bloc d'informations (taille et contenu).
- Le protocole TCP/IP, adressage IP et routage : [4]
- TCP/IP est actuellement le protocole de communication le plus utilisé dans les réseaux locaux. C'est aussi le protocole de transport utilisé par le réseau Internet..

1.9 L'addresse IP:

Chaque machine d'un réseau TCP/IP possède une adresse IP (Internet Protocol). Une adresse IP est constituée d'un groupe de 4 octets soit 4 fois 8 bits, les octets les plus à gauche déterminent l'adresse du réseau et le ou les octets de droite déterminent l'adresse de la machine.

Exemple : 192.168.1.5

192.168.1.0 correspond à l'adresse réseau alors que 5 représente l'adresse de l'ordinateur dans le réseau. Le nombre de machines maximum pouvant être connectés sur ce type de réseau est de 254 (i1 comporte 256 possibilités de 0 à 255 mais les octets 0 et 255 sont réservés).

1.9.1 Les classes d'adresses :

Les adresses IP sont regroupées en 3 classes principales. Ce sont les bits de poids forts (bits à gauche de l'adresse IP) qui déterminent la classe d'adresse :

Classe	1er octet	Etendue	Etendue en nombre décimal	Nbre de machines possibles
A	**0**	De 00000001 à **0**1111110	De 1 à 126	256^3-2=**16 777 214**
B	**10**	De **10**000000 A **10**111111	De 128 à 191	256^2-2=**65 534**
C	**110**	De **110**00000 à **110**11111	De 192 à 223	256-2=**254**
D	**1110**	De **1110**0000 à **1110**1111	De 224 à 239	Réservé (multicast)
E	**1111**	De **1111**0000 à **1111**1110	De 240 à 254	Réservé à un usage futur

Tab 1.1 : Les classes d'adresses IP

1.9.2 Le masque de sous-réseau :

Le masque de sous-réseau permet de différencier l'adresse IP du réseau de l'adresse IP de la machine. Comme l'adresse IP, le masque de sous-réseau se compose d'un groupe de 4 octets. Chaque classe d'adresse comporte un masque par défaut (qui peut être personnalisé pour créer des sous-réseaux mais c'est une affaire de spécialiste).

Masques de sous-réseau par défaut : [5]

Classes	Masque de sous-réseau par défaut	Nombre de machines maximum
A	255. 0. 0. 0	256^3-2=**16 777 214**
B	255.255. 0. 0	256^2-2=**65 534**
C	255.255.255.0	256-2=**254**

Tab 1.2 : Masques de sous-réseau des différents classes

Les octets ayant la valeur 0 déterminent la plage d'adresses utilisable pour les machines.

Exemple : Adresse IP : 172. 16.12.21 / Masque de sous-réseau : 255.255. 0. 0

On en déduit :

- Que cette machine est dans un réseau de classe B (172 est compris entre 127 et 191)
- Que l'adresse du réseau est : 172.16.0.0 (l'adresse de réseau est codée sur les 2 premiers octets car les deux premiers octets du masque de réseau sont égaux à 255)

➢ Les deux derniers octets servent à identifier de manière unique chaque machine du réseau 172.16.0.0 (car les deux derniers octets du masque de réseau sont égaux à 0)

➢ Que l'adresse IP de la machine est : 172.16.12.21. En fait, sur le réseau 172.16.0.0 on peut avoir potentiellement 65534 machines connectées. Si on ajoute d'autres machines sur ce réseau, leur adresse IP commencera alors par 172.16 et les deux derniers octets seront librement choisis de 172.16.0.1 à 172.16.255.254

1.9.3 Le choix d'une adresse IP :

Le choix de l'adresse IP n'est pas libre :

1) En cas d'ajout d'un nouvel ordinateur à un réseau local, il faut tenir compte de l'adresse réseau et vérifier que l'adresse IP n'est pas déjà prise par un autre ordinateur

2) La majorité des adresses IP sont réservées pour l'Internet et pour en bénéficier il faut les acquérir auprès de l'Internet. En effet Internet utilise l'adressage IP pour identifier de manière unique les postes qui lui sont reliés.

Classe A : 10.0.0.0

Classe B : de 172.16.0.0 à 172.31.0.0

Classe C : de 192.168.0.0 à 192.168.255.0

1.9.4 Adressage IP statique – adressage IP dynamique :

L'adressage IP statique consiste à attribuer à chaque ordinateur (serveur, station,…) une adresse IP fixe. Sous Windows 2003, effectuez un clic droit sur l'icône Favoris réseau puis cliquez sur Propriétés

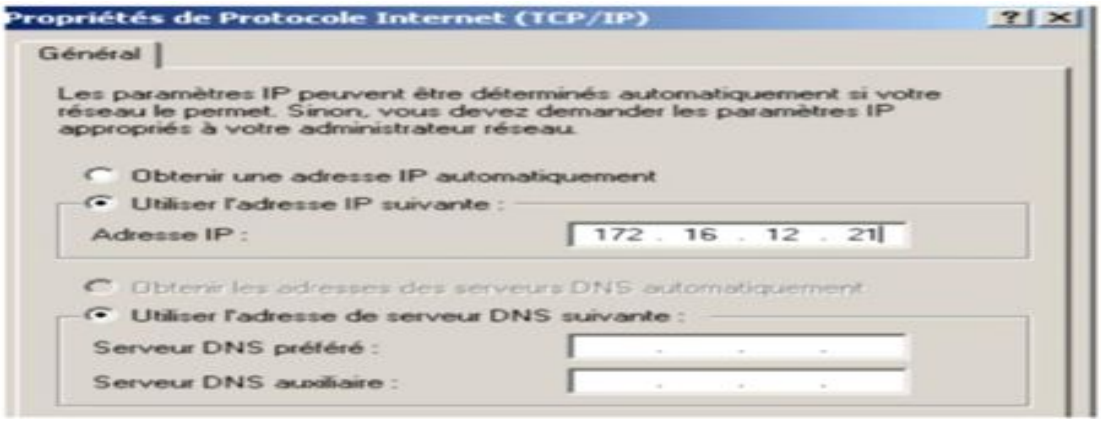


Fig 1.11 : L'adressage IP statique

1.10 Les protocoles réseaux (LAN) :

1.10.1 Les Virtual LAN (VLAN) :

Un réseau local virtuel (ou VLAN) est un groupe d'unités réseau ou d'utilisateurs qui ne sont pas limités à un segment de commutation physique. Les unités ou les utilisateurs d'un VLAN peuvent être regroupés par fonction, service, application, etc., et ce, quel que soit le segment physique où ils se trouvent. Un VLAN crée un domaine de broadcast unique qui n'est pas limité à un segment physique et qui est traité comme un sous-réseau. La configuration d'un VLAN est effectuée, par logiciel, dans le commutateur. Les VLAN ont été uniformisés conformément à la spécification IEEE 802.1Q. Il subsiste cependant des variantes d'implémentation d'un constructeur à l'autre.

1.10.2 Le protocole VTP :

Le VTP (VLAN Trunking Protocol) est un protocole de niveau 2 utilisé pour configurer et administer les VLAN sur les périphériques Cisco. Le VTP permet d'ajouter, renommer ou supprimer un ou plusieurs Vlans sur un seul switch (serveur) qui propagera cette nouvelle configuration à l'ensemble des autres switchs du réseau (clients). VTP permet ainsi d'éviter toute incohérence de configuration des Vlans sur l'ensemble d'un réseau local.

1.10.3 Protocole Spanning-Tree :

Le protocole Spanning-Tree (STP) est un protocole de couche 2 (liaison de données) conçu pour les switchs et les bridges. La spécification de STP est définie dans le document IEEE 802.1d. Sa principale fonction est de s'assurer qu'il n'y a pas de boucles dans un contexte de liaisons redondantes entre des matériels de couche 2. STP détecte et désactive des boucles de réseau et fournit un mécanisme de liens de backup. Il permet de faire en sorte que des matériels compatibles avec le standard ne fournissent qu'un seul chemin entre deux stations d'extrémité. Le protocole RSTP (Rapid Spanning-Tree Protocol) est défini par le standard IEEE 802.1w. Il diffère principalement de STP de par sa convergence plus rapide. En effet, RSTP offre une convergence au minimum 5 fois plus rapide que STP. RSTP prend moins de 10 secondes pour converger.

1.10.4 Le protocole ARP (protocole de niveau 3):

L'Address Resolution Protocol (ARP, protocole de résolution d'adresse) est un protocole effectuant la traduction d'une adresse de protocole de couche réseau (typiquement une adresse IPv4) en une adresse MAC (typiquement une adresse Ethernets), ou même de tout matériel de couche Il se situe à l'interface entre la couche réseau (couche 3 du modèle OSI) et la couche de liaison (couche 2 du modèle OSI).

1.10.5 Le protocole ICMP:

Le protocole ICMP (Internet Control Message Protocol) est un protocole qui permet de gérer les informations relatives aux erreurs aux machines connectées. Etant donné le peu de contrôles que le protocole IP réalise, il permet non pas de corriger ces erreurs mais de faire part de ces erreurs aux protocoles des couches voisines. Ainsi, le protocole ICMP est utilisé par tous les routeurs, qui l'utilisent pour signaler une erreur (appelé Delivery Problème).

1.10.6 Le protocole OSPF:

L'Open Shortest Path First (OSPF) est un protocole de routage IP interne de type protocole à état de liens (Link-state Protocol). Ce protocole n'envoie pas aux routeurs adjacents le nombre de sauts qui les sépare, mais l'état de la liaison qui les sépare. De cette façon, chaque routeur est capable de dresser une carte de l'état du réseau et peut par conséquent choisir à tout moment la route la plus appropriée pour un message donné. De plus, ce protocole évite aux routeurs intermédiaires d'avoir à incrémenter le nombre de sauts, ce qui se traduit par une information beaucoup moins abondante, ce qui permet d'avoir une meilleure bande passante utile qu'avec le protocole RIP.

1.10.7 ACL:

Une ACL (Access Control List) est une liste séquentielle de critères utilisée pour du filtrage des paquets. Les ACLs sont capables d'autoriser ou d'interdire des paquets, que ce soit en entrée ou en sortie.

1.10.8 Les protocoles de réseau étendu Technologie Frame Relay:

Le relayage de trames (ou FR, pour l'anglais Frame Relay) est un protocole à commutation de paquets situé au niveau de la couche de liaison (niveau 2) du modèle OSI, utilisé pour les échanges intersites (WAN) il a été inventé par Eric Scace, ingénieur chez Sprint International. Les PVC (Circuit virtuel permanent) s'identifient au niveau des interfaces des DTE et DCE grâce à des DLCI (Data Link Connection Identifiers) afin de pouvoir distinguer les flux provenant des différents PVC. Les DLCI sont généralement des numéros d'identification à valeur uniquement locale (à une interface) qu'on assimile à une sous-interface dans certains contextes : sur un routeur par exemple, chaque PVC d'une interface pourra ainsi avoir sa propre adresse IP associée.

1.10.9 Technologie Ligne spécialisée :

Une ligne spécialisée (LS) ou ligne louée correspond en informatique ou en télécommunications, à une liaison entre deux points, connectés en permanence ensemble. Elle s'oppose à un partage de ressources comme dans un réseau de type VPN (X25, Frame Relay, ATM, MPLS...). La ligne spécialisée n'est souvent dédié qu'entre le client et le point d'accès au réseau de l'opérateur, après les données sont transportés soit sur un réseau TDM, ATM ou MPLS où la bande passante est dédiée.

1.10.10 NAT et PAT:

Le NAT et le PAT sont deux protocoles qui permettent aux machines d'un réseau interne/locale d'accéder à Internet avec leur adresses IP "non publiques", ils consistent donc a translater ces adresses en adresse IP publiques qui sont limités, d'où la nécessite de cette translation.

1.11 Conclusion:

Au cours de ce chapitre, nous avons défini les réseaux informatiques, leurs différents types et leurs topologies, ensuite nous avons donné une description globale du modèle OSI et TCP/IP et cité les équipements d'interconnexion dans un réseau local afin de bien aborder le chapitre suivant qui sera consacré aux réseaux virtuels (VLANs).

chapitre 02

Les réseaux VLANs

2.1 Introduction:

Les réseaux locaux virtuels (Virtual LAN) sont apparus comme une nouvelle fonctionnalité dans l'administration réseau avec le développement des commutateurs.

En effet, dans un réseau local, la communication entre les différentes machines est régie par l'architecture physique. Grâce aux réseaux virtuels (Vlans), il est possible de s'affranchir des limitations de l'architecture physique (contraintes géographiques, contraintes d'adressage,...).

En définissant une segmentation logique (logicielle) basée sur un regroupement de machines grace à des critères (adresses M AC, numéros de port, protocole, etc.).

Dans ce chapitre, nous allons présenter les principales notions d'un réseau local virtuel

2.2 Les VLANs:

Un VLAN (Virtual Local Area Network) Ethernet est un réseau local virtuel (logique) utilisant la technologie Ethernet :

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

Les VLAN permettent à un manager de réseau pour segmenter logiquement un LAN en différents domaines de diffusion, Les VLAN permettent également de définir des domaines de diffusion sans utiliser de routeurs.

Les utilisateurs situés à différents étages d'un même bâtiment ou même dans des bâtiments différents peuvent désormais appartenir au même réseau local.

Les routeurs ne devraient être utilisés que pour communiquer entre deux VLAN.

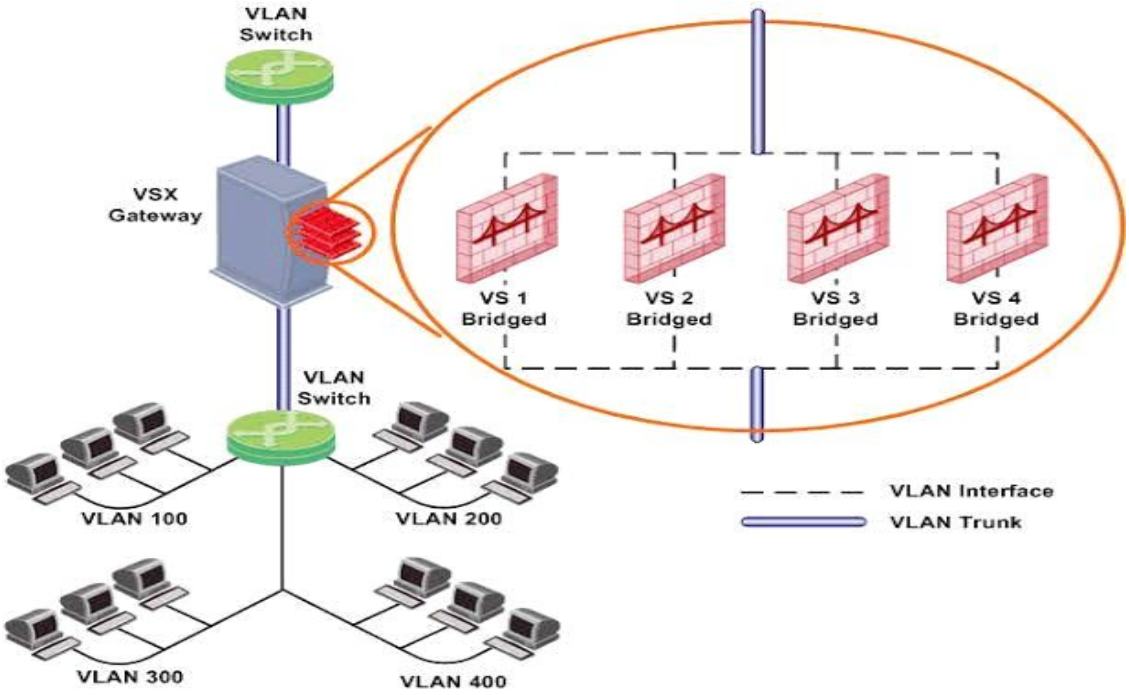


Fig II .1 : Un VLAN avec des domaines de diffusion (sans routeurs).

2.2.1 L'intérêt d'avoir des VLANs:

Les VLAN offrent un certain nombre d'avantages par rapport aux LAN traditionnels. Elles sont:

1) Meilleures performances :

Dans les réseaux où le trafic consiste en un pourcentage élevé d'émissions et de multidiffusions, Les VLAN peuvent réduire la nécessité d'envoyer un tel trafic vers des destinations inutiles. Par exemple, dans un domaine de diffusion composé de 10 utilisateurs, si le trafic de diffusion n'est destiné qu'à 5 des utilisateurs, le fait de placer ces 5 utilisateurs sur un VLAN distinct peut réduire le trafic

-Par rapport aux switches, les routeurs nécessitent davantage de traitement du trafic entrant, À mesure que le volume de trafic passant par les routeurs augmente, la latence des routeurs augmente également.

2) Formation de groupes de travail virtuels :

Actuellement, il est courant de trouver des équipes de développement de produits inter fonctionnelles avec des membres de différents départements tels que le marketing, Ventes, comptabilité et recherche. Ces groupes de travail sont généralement formés pour une courte période de temps. Pendant cette période, la communication entre les membres du groupe de travail sera

élevée. Pour contenir des diffusions et des multidiffusions au sein du groupe de travail, un VLAN peut être configuré pour eux. Avec les VLAN, il est plus facile de regrouper les membres d'un groupe de travail. Sans VLAN.

Un autre problème lié à la configuration de groupes de travail virtuels est la mise en œuvre de batteries de serveurs centralisées, qui sont essentiellement des collections de serveurs et des ressources majeures pour faire fonctionner un réseau à un emplacement central.
Les avantages ici sont nombreux puisque il est plus efficace et plus rentable de fournir une meilleure sécurité.

3) Administration simplifiée :

70% des coûts du réseau sont le résultat d'ajouts et de mouvements, et les changements d'utilisateurs dans le réseau. Chaque fois qu'un utilisateur est déplacé dans un LAN, recâblage, nouvel adressage de station, et la reconfiguration des concentrateurs et des routeurs deviennent nécessaire. Certaines de ces tâches peuvent être simplifiées grâce à l'utilisation de VLAN.

4) Réduction des coûts :

Les VLAN peuvent être utilisés pour créer des domaines de diffusion qui éliminent le besoin de routeurs coûteux, Des économies sont réalisées grâce à l'utilisation plus efficace de la bande passante et des liaisons ascendantes existante.

5) Sécurité :

Périodiquement, des données sensibles peuvent être diffusées sur un réseau. Dans de tels cas, placer uniquement les utilisateurs qui peuvent avoir accès à ces données sur un VLAN peut réduire les chances d'un outsider accèdent aux données.

2.2.2 Les propriétés offertes par les VLAN:

- Support des transferts de données allant jusqu'à 1Gb/s.
- Peut couvrir un bâtiment, relier plusieurs bâtiments ou encore.
- S'étendre au niveau d'un réseau plus large.
- Une station peut appartenir plusieurs VLAN simultanément. C'est un sous réseau de niveau 2 construit à partir d'une technologie permettant de cloisonner des réseaux par usage de filtres de sécurité. Cette technologie balise le domaine de broadcast auquel ces machines.

2.2.3 Les avantages et les inconvénients des VLANs :

Ce mode de segmentation des réseaux locaux modifie entièrement la manière dont les réseaux sont conçus, administrés et maintenus.

✓ **Les avantages :**

- Augmentation des performances : La segmentation créée par les VLAN réduit la taille des domaines de broadcast et de ce fait le nombre de collisions sur ces domaines. De plus, les VLAN se basent sur la commutation (et non le routage) pour segmenter les domaines de diffusion ce qui permet un traitement bien plus rapide.

- Réduction des coûts : L'utilisation de VLAN permet de simplifier l'administration du réseau. A chaque fois qu'un utilisateur change de LAN, il faut modifier l'adresse du poste et certains paramètres des routeurs. Tandis que si un utilisateur change de lieu physique mais pas de VLAN, il peut ne pas y avoir de modifications à faire (sous réserve de disposer de bons outils de gestion des VLAN).De plus, l'utilisation des VLAN entraîne souvent la réduction du nombre de routeurs nécessaires, or les routeurs sont plus onéreux que les switches.

- Formation de groupes virtuels : Il est courant de retrouver, dans les entreprises, des groupes de développement, de travail sur un projet spécifique, composés de membres qui viennent de différents départements (production, vente, etc.).Ces groupes sont souvent formés pour un temps défini et à courte durée. Dans ce cas de figure, un VLAN pourrait être implémenté (sans avoir à déplacer les individus) pour les besoins ponctuels de ce groupe et ce pour plusieurs groupes différents dans l'entreprise. Ce qui permet de créer des groupes de travail de manière transparente vis-à-vis de l'architecture physique du réseau.

- Gain de sécurité : Périodiquement, des données sensibles sont envoyées en broadcast sur le réseau par les machines (et plus particulièrement les serveurs). Les VLAN permettent d'isoler les serveurs dans un même domaine de broadcast et de les isoler par service. Les VLAN apportent donc une grande flexibilité dans la gestion des réseaux ; les utilisateurs pourront être regroupés selon leur centre d'intérêt.

Les VLAN sont réalisés sur une architecture commutée et le concept de VLAN est applicable dans un même bâtiment, entre plusieurs bâtiments ou sur un réseau WAN.

✓ **Inconvénients :**

- L'utilisation de VLAN engendre malgré une certaine complexité dans la configuration des routeurs et de commutateurs et dans la gestion d'ensemble du LAN .Il faut parfaitement connaitre les normes et le matériel, c'est donc un important effort de formation.

- Les échanges administratifs sur les réseaux locaux ne sont pas négligeables, au déterminent du débit utile : il faut en effet que les informations de VLAN soient échangées entre commutateurs et vers les routeurs pour diffuser régulièrement les adresses MAC....
- Délais : lorsqu'une station est connectée à un commutateur, ce dernier peut mettre un peu de temps avant de trouver à quel VLAN elle appartient de même lorsqu'une station est déplacée d'un commutateur à un autre, il peut y avoir des problèmes dans la reconfiguration.

- Les normes de routage cohabitent toujours avec des solutions propriétaires, ce qui peut causer des problèmes d'interopérabilité si le matériel utilisé n'est pas homogène. Il faut donc bien souvent changer tout le matériel actif déjà en place le remplacer par des commutateurs dont le cout ne cesse d'augmenter avec l'arrivée de toutes ces fonctionnalités nouvelle. [6]

2.3 La technique des VLANs :

Pour réaliser des VLANs, il faut tout d'abord des commutateurs spéciaux de niveau 2 du modèle OSI qui supportent le VLAN.

Ces produits combinent tous les avantages des solutions précédentes : i' Partitionnement en plusieurs domaines de broadcast i' Affectation d'un ou plusieurs ports à un VLAN depuis une console centrale (Amélioration de la bande passante par la fonction de commutation i' Adaptation de la vitesse du Switch à la capacité du réseau i' Regroupement des VLAN sur un même segment backbone (réseaux distants avec des Vlan commun de bout en bout) Gestion d'une bonne étanchéité entre VLAN

2.4 Méthodes d'implantation des VLANs :

On distingue généralement trois techniques pour construire des VLAN, en fonction de leurs méthodes de travail, nous pouvons les associer à une couche particulière du modèle OSI

2.5 Les différents types de VLAN:

Plusieurs types de VLAN sont définis, selon le critère de commutation et le niveau auquel il s'effectue :

2.5.1 VLAN de niveau 1 ou VLAN par port:

On affecte chaque port des commutateurs à un VLAN. L'appartenance d'une carte réseau à un VLAN est déterminée par sa connexion à un port du commutateur. Les ports sont donc affectés

statiquement à un VLAN. Ce type de réseaux virtuels n'a rien de bien innovant. Lorsque les équipements réseau étaient simples et fiables, on faisait déjà des

VLAN par port tout simplement en construisant des réseaux physiquement séparés, Les ports des Switch sont associés à des VLANs (Figure 2) i' Ports 1,2 et 3 appartiennent au VLAN i' Ports 4,5 et 6 au VLAN 2 i' Ports 7 et 8 au VLAN 3

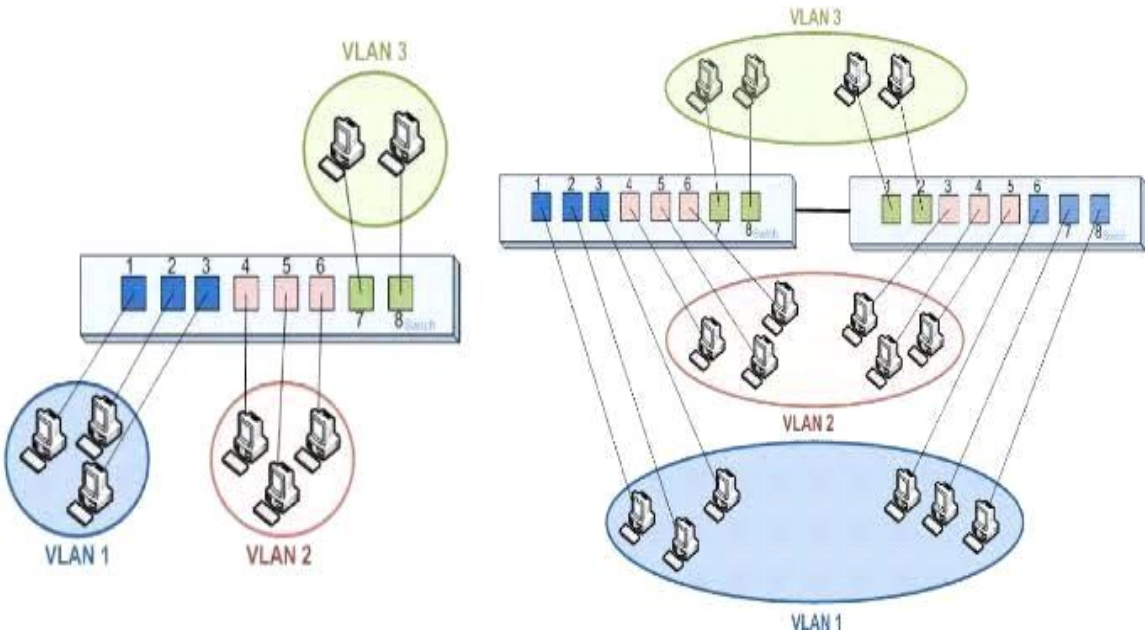


Fig II .2 : VLAN de niveau 1 ou VLAN par port

2.5.2 VLAN de niveau 2 ou VLAN MAC:

On affecte chaque adresse MAC à un VLAN. L'appartenance d'une carte réseau à un VLAN est déterminé par son adresse MAC. En fait il s'agit à partir de l'association Mac/VLAN d'affecter dynamiquement les ports des commutateurs à chacun des VLAN, Une station peut théoriquement être membre de plusieurs VLANs différents. Le principal inconvénient de ce modèle est la mise à jour des correspondances entre les VLANs et les adresses MAC, qui peut être ardue dans des réseaux de grande taille.

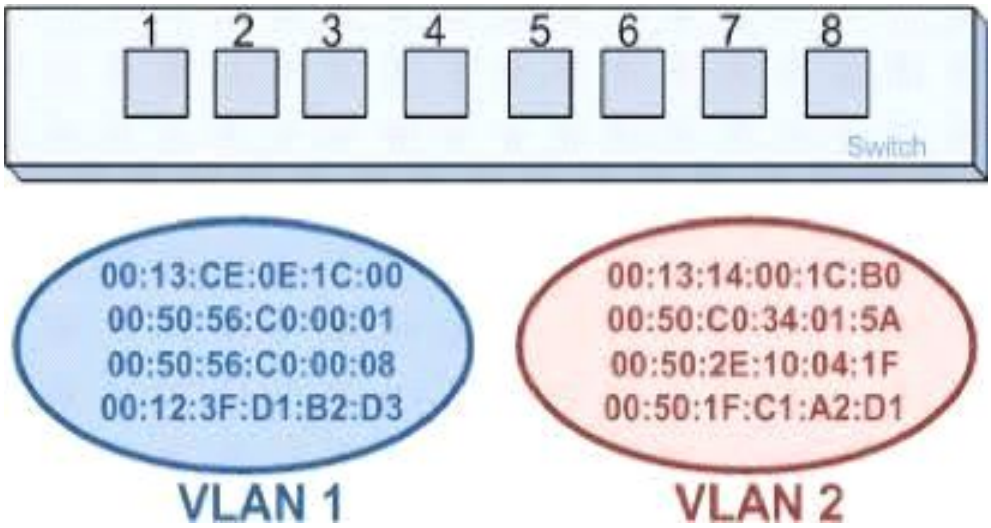


Fig II .3 : VLAN de niveau 3 ou VLAN d'adresses réseaux

On affecte un protocole de niveau 3 ou de niveau supérieur à un VLAN. L'appartenance d'une carte réseau à un VLAN est déterminée par le protocole de niveau 3 ou supérieur qu'elle utilise. En fait il s'agit à partir de l'association protocole/VLAN d'affecter dynamiquement les ports des commutateurs a chacun des VLAN.

2.6 Principe de fonctionnement des VLANs :

Comment transporter et reconnaitre à l'arrivée sur un même segment physique, des trames issues de plusieurs VLANs.

2.6.1 l'étiquetage :

L'étiquetage consiste à marquer toutes les trames sortantes du commutateur avec le n° du VLAN d'appartenance.

Le commutateur suivant peut alors repérer les trames et les diriger vers le VLAN correspondant [7]

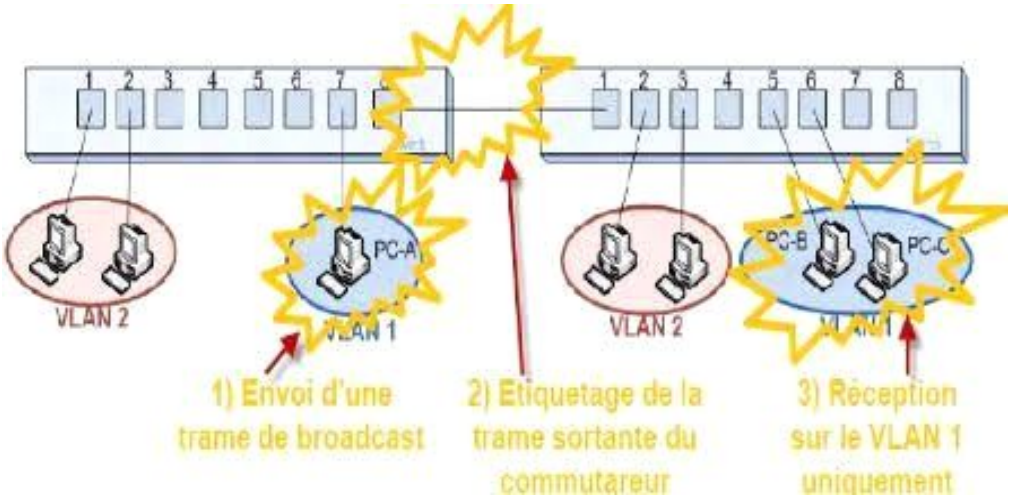


Fig II.4: L'étiquetage et les trames sortantes du commutateur avec le n° du VLAN

=

2.6.2 La trame Ethernet classique :

Cette figure nous montre une trame Ethernet classique sans VLANs

- TPID: type du tag,ox8100pour 802.1Q
- Priorité: niveaux de priorité définis par l'IEEE 802.1P
- CFI: Ethernet ou token-ring
- VID: VLAN identifier,jusqu a 4096 vlans

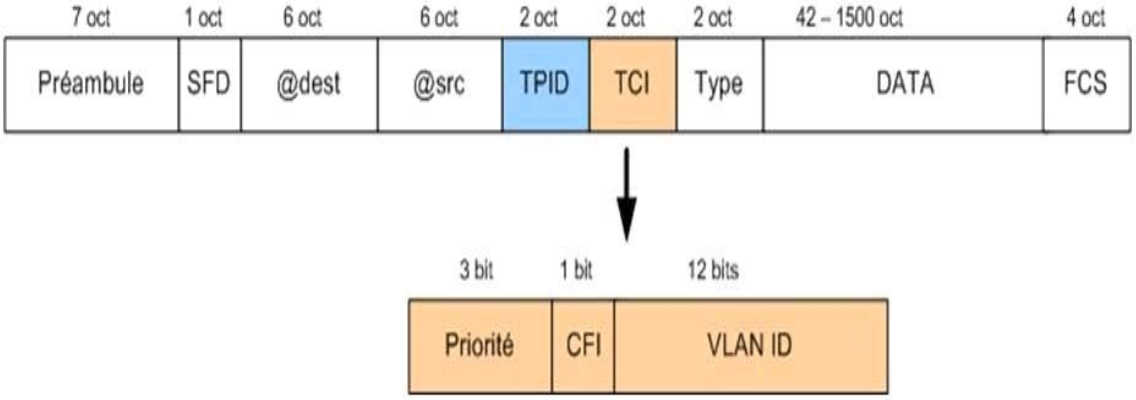


Fig II .5 : Trame Ethernet classique sans VLANs

2.6.3 La trame Ethernet 802.1q :

L'étiquetage se fait grâce à la norme 802.1q (dot1.q) et Les trames ont un champ supplémentaire, Le principe consiste à ajouter dans l'en-tête de la trame Ethernet un marqueur qui

va identifier le VLAN. Il existe quelques solutions propriétaires pour réaliser ceci, mais le système s'est avéré tellement intéressant qu'une norme a été définie, il s'agit de la norme 802.1q.

2.6.3.1 Description de la norme :

La figure suivante illustre la modification de la trame Ethernet et l'ajout d'un champ sur 4 octets par la norme 802.1Q :

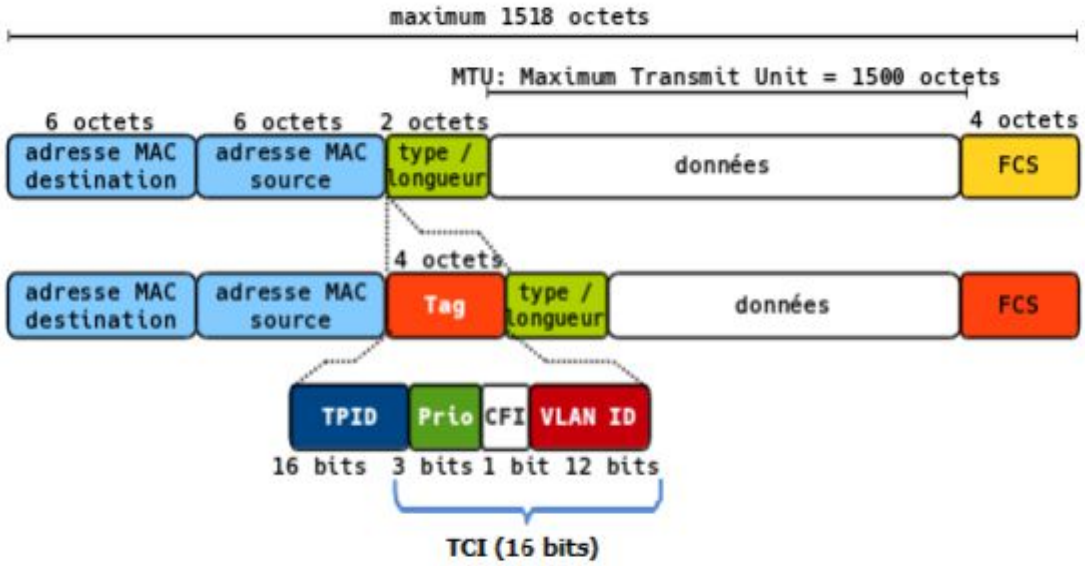


Fig II .5.1 : Extension de la trame Ethernet modifiée par la norme 802.1Q [14].

- ✓ **Tag Protocol Identifier (TPID) :**

C'est la partie qui définit le protocole de tag utilisé. Dans le cas du 802.1Q on trouvera comme valeur (en notation hexadécimale) : 0x8100.

- ✓ **3.3 Tag Control Information (TCI) :**

Cette partie se compose de trois champs :

a) User Priority :

3 bits utilisés pour coder 8 niveaux de priorité (de 0 à 7). On se sert de ces 8 niveaux pour fixer la priorité des trames d'un VLAN par rapport à d'autres

Exemple d'utilisation : on favorise un VLAN sur lequel on utilise la visioconférence (nécessitant beaucoup de bande passante) par rapport à un VLAN où l'on ne fait qu'envoyer et recevoir des mails.

b) Canonical Format Identifier(CFI) : Ce champ d'un bit assure la compatibilité entre adresses MAC Ethernet et Token Ring. Un commutateur Ethernet fixe cette valeur à 0

c) VLAN ID (VID) : C'est le champ d'identification du VLAN auquel appartient la trame par l'intermédiaire de ce champ de 12 bits, on peut coder 4094 VLAN (les valeurs 0 et FFF sont réservées). La valeur par défaut est 1.

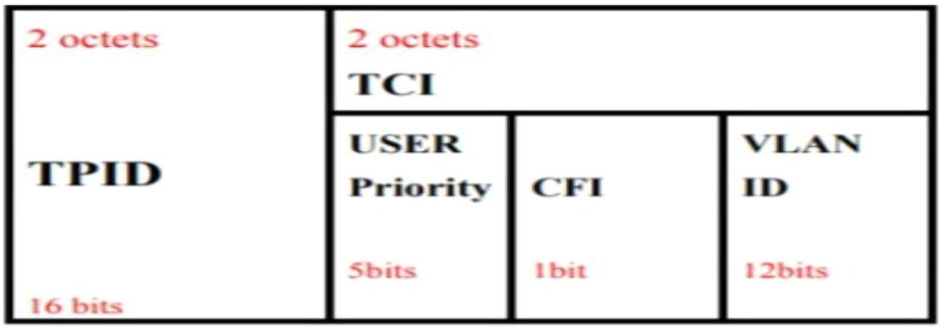


Fig II .6 : VLAN ID (VID)

2.7 Le Protocol ISL (Inter Switch Link Protocol) :

Pour étendre les réseaux virtuels sur plus d'un commutateur, CISCO a mis au point son propre protocole ISL. Ce protocole achemine les informations d'appartenance aux réseaux virtuels. ISL représente en fait une structure de trame et un protocole qui, en plus de transport des informations d'appartenance aux réseaux virtuels, permet à ces réseaux d'échanger des trames.

a) Présentation générale :

Pour identifier les réseaux virtuels, **ISL** utilise un mécanisme de marquage explicite des paquets. Un commutateur qui utilise ce marquage encapsule la trame reçue dans un paquet dont l'en-tête contient un champ d'appartenance aux VLAN et l'adresse MAC de la trame, permettant d'acheminer le paquet vers le routeur et les commutateurs appropries. Lorsqu'elle atteint le réseau destination, on supprime l'en-tête, et la trame est acheminée vers l'équipement récepteur.

b) Structure des trames ISL :

- Les trames ISL comprennent trois champs principaux :
- Un en-tête qui est constitué de plusieurs champs.
- Trame encapsulée dont la longueur est comprise entre 1 et 24575 octets.
- Champ CRC, ce champ qui est ajouté à la fin du paquet ISL, porte sur l'intégrité du paquet.

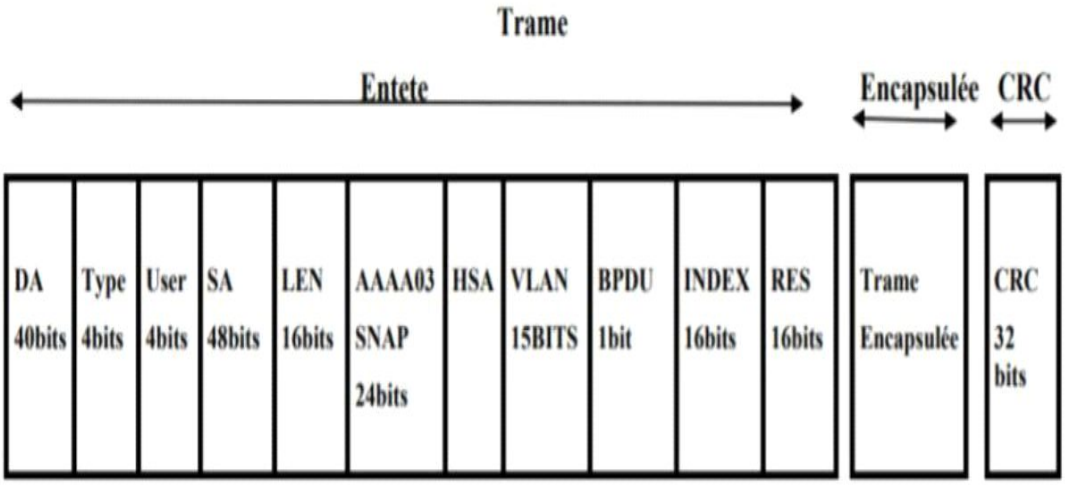


Fig II .7 : Trames ISL

2.8 La notion des trunks :

Un lien TRUNK est un lien qui permet de faire transiter plusieurs VLANs sur un seul lien physique (Une "sorte" d'agrégation de plusieurs lignes de télécommunication ou de VLAN afin d'augmenter la bande passante...)

Sur un LAN avec plusieurs VLAN sur plusieurs commutateurs on peut donc faire circuler ces VLANs sur tous les commutateurs avec un seul lien entre deux commutateurs (sinon il faut un lien par VLAN).

Il ne faut pas oublier que les VLANs transitant sur un même trunk se partagent la bande passante, c'est pourquoi il est recommandé d'utiliser des connexions à débit important, comme du Gigabit Ethernet ou de la fibre optique dans le meilleur des cas.

Ce schéma ci-dessous (Figure 4) nous illustre la liaison de trunk entre deux commutateurs

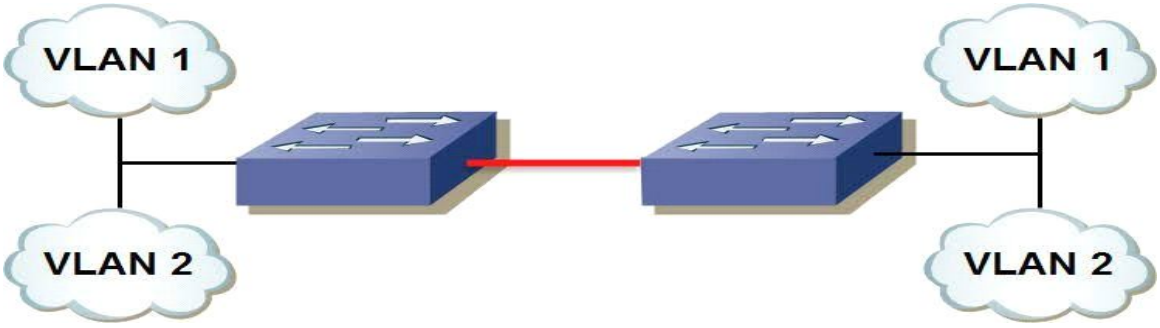


Fig II .8 : Les VLANs transitant sur un même trunk

2.8.1 Rappel sur la notion de VLAN (Virtual Local Area Network):

L'objectif d'une configuration de vlan est de permettre la configuration de réseaux différents sur un même switch.

Il existe plusieurs façons de configurer les vlans. Cette page traitera uniquement du vlan par port. La norme utilisée ici porte l'identifiant 802.1q.

Les avantages principaux de la segmentation par vlan sont la réduction des domaines de broadcast et l'accroissement de la sécurité (si des filtres sont mis en place pour la communication entre les réseaux). [8]

2.8.2 Principe de fonctionnement du vlan par port :

Un tag de 4 octet est ajouté à la trame ethernet. Ce tag comprend entre autre l'identifiant de VLAN. Ainsi, la trame sera transmise uniquement aux ports appartenant au vlan identifié dans la trame.

Type de configuration des ports des switchs Cisco Le port est configuré en mode Access ou en mode trunk.

Le mode Access est utilisé pour la connexion terminale d'un périphérique (pc, imprimante, serveur, ...) appartenant à un seul vlan. Le mode trunk est utilisé dans le cas ou plusieurs vlans doivent circuler sur un même lien. C'est par exemple le cas de la liaison entre deux switchs ou bien le cas d'un serveur ayant une interface appartenant à plusieurs vlans.

VLAN non affecté à un port et présent sur le switch

Des vlans peuvent être créés sur un switch et n'être affectés à aucun port. C'est le cas du vlan de management (une adresse IP sera configurée sur ce vlan).

Un switch qui sert de liaison aura également les vlans qui doivent le traverser déclaré dans sa configuration.

2.8.3 Communication entre les vlans :

La communication entre les vlans est possible en passant par un routeur ou un switch de niveau 3 (switch-routeur).

Selon l'utilisation, il peut être conseillé de filtrer les réseaux au minimum au moyen d'ACLs (access control list).

- **VLAN natif:** Le vlan appelé "natif" est le vlan par défaut du switch (en général le vlan 1). Sans configuration, tous les ports du switch sont placés dans ce VLAN. Ce vlan n'est pas marqué même si il passe sur une liaison trunk.

2.8.4 Configuration type d'un switch:

- La liaison entre les switchs est en mode trunk.
- Les autres ports des switchs sont en mode access.
- Le vlan dédié aux téléphones sera également configuré sur tous les ports en plus de leur vlan data respectif.

Un vlan dédié à l'administration et à la supervision du switch sera créé. L'adresse IP de supervision du switch sera associée à ce vlan.

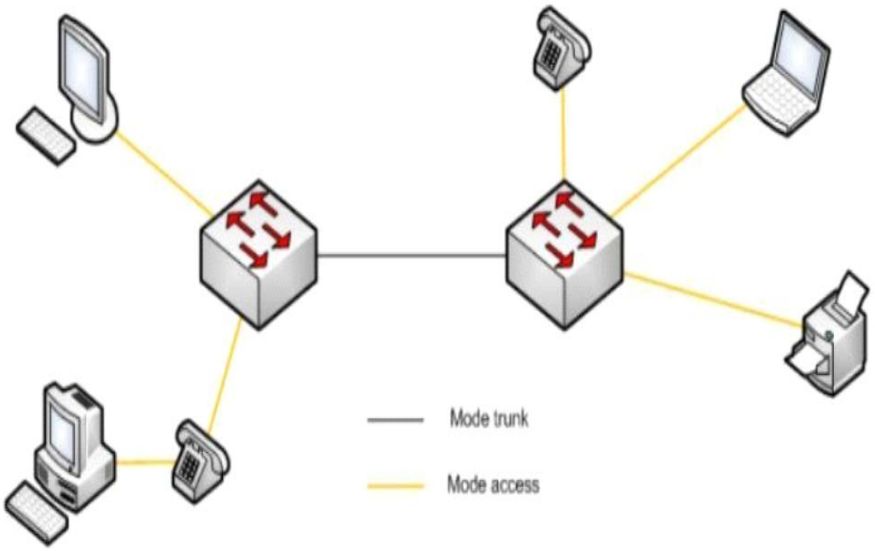


Fig II .9: Liaison mode trunk et mode access

2.9 Principe du routage INTER-VLAN :

Quand un hôte d'un VLAN veut communiquer avec un hôte d'un autre VLAN, un routeur est nécessaire ou un commutateur de couche 3.

La connectivité entre les VLANs peut être établie par le biais d'une connectivité physique ou logique. Une connectivité logique implique une connexion unique, ou agrégation, du commutateur au routeur. Cette agrégation peut accepter plusieurs VLAN. Cette topologie est appelée «router-on-a stick » car il n'existe qu'une seule connexion physique avec le routeur.

En revanche, il existe plusieurs connexions logiques entre le routeur et le commutateur.
Une connectivité physique implique une connexion physique séparée pour chaque VLAN.

Cela signifie une interface physique distincte pour chaque VLAN.
LespremièresconfigurationsdeVLANreposaientsurdesrouteursexternesconnectésà des commutateurs compatibles VLAN.

Pour permettre aux hôtes de VLANs de communiquer entre eux, il faut utiliser un routeur ou commutateur de couche 3. Le terme commutateur de couche 3 désigne un commutateur capable d'assurer une fonction de routage en plus de ses fonctions habituelles. Ainsi, au lieu d'un routeur externe, on aura un routeur interne au commutateur. [9]

2.10 Conclusion:

Dans ce chapitre, nous avons défini en premier lieu le réseau local virtuel. Puis, nous avons cité les différents avantages des VLANs, leurs différents types. Ensuite, nous avons présenté les méthodes d'implémentation des VLANs. Enfin, nous avons cité quelques protocoles d'administration et de gestion des VLANs ainsi que les listes de contrôle d'accès.

Chapitre 03:

La mise en place des Vlans

3.1 Introduction:

Un VLAN est en quelque sorte un sous-réseau virtuel, généralement associé à une adresse sous-réseau propre.

Cela implique donc que les vlans ne peuvent pas communiquer entre eux à moins que l'on utilise un routeur…

Que faut-il configurer?

1. Avoir une liaison fonctionnelle entre le switch et le routeur.
2. Définir la liaison entre le switch et le routeur comme un « trunk »
3. Créer les vlans sur le switch
4. Attribuer les interfaces désirées dans les différents vlans (uniquement utiles pour l'administration du switch).
5. Pour chaque VLAN sur le switch, créer une sous interface (sur celle utilisée par le trunk).

Remarque : Les switchs d'ancienne génération n'acceptent pas plus d'une interface de type vlan ».

- Les **VLANS** isolent correctement les groupes de postes/d'utilisateur mais bloquent complètement la communication entres elles.
- C'est justement la problématique qu'on va discuter dans ce chapitre.

Notre chapitre est devisé en deux parties :

- **Partie 1 : Structure et adressage du réseau.**

- **Partie 2 : Configuration des équipements.**

3.2 Partie 01: Structure et adressage du réseau :

3.2.1 Présentation:

Dans ce tutoriel, on va voir comment mettre en place un réseau simple, pour bien expliquer les détailles et aborder tous les aspects techniques de la mise en œuvre des VLANs.

Note :

Dans le chapitre 04 : simulation et discussion des résultats nous allons discuter plusieurs schémas en montrons les avantages et les inconvénients de chacun.

On discutera plus tard tout ce qui concerne la **capacité** du réseau et **ses méthodes de distributions**.

Dans ce chapitre on simplifie notre réseau qui est constitué de **04 postes** de travails **02 switchs** et **01 routeur** on se basant sur les techniques de déploiement et d'implantation des vlans.

Les deux switchs partageront des VLANS et le routeur se chargera des tâches de routage inter-VLANs. Nous aborderons divers fonction et manipulation sous des éléments de marques **Cisco.** [10]

3.2.2 Architecture scenario de déploiement :

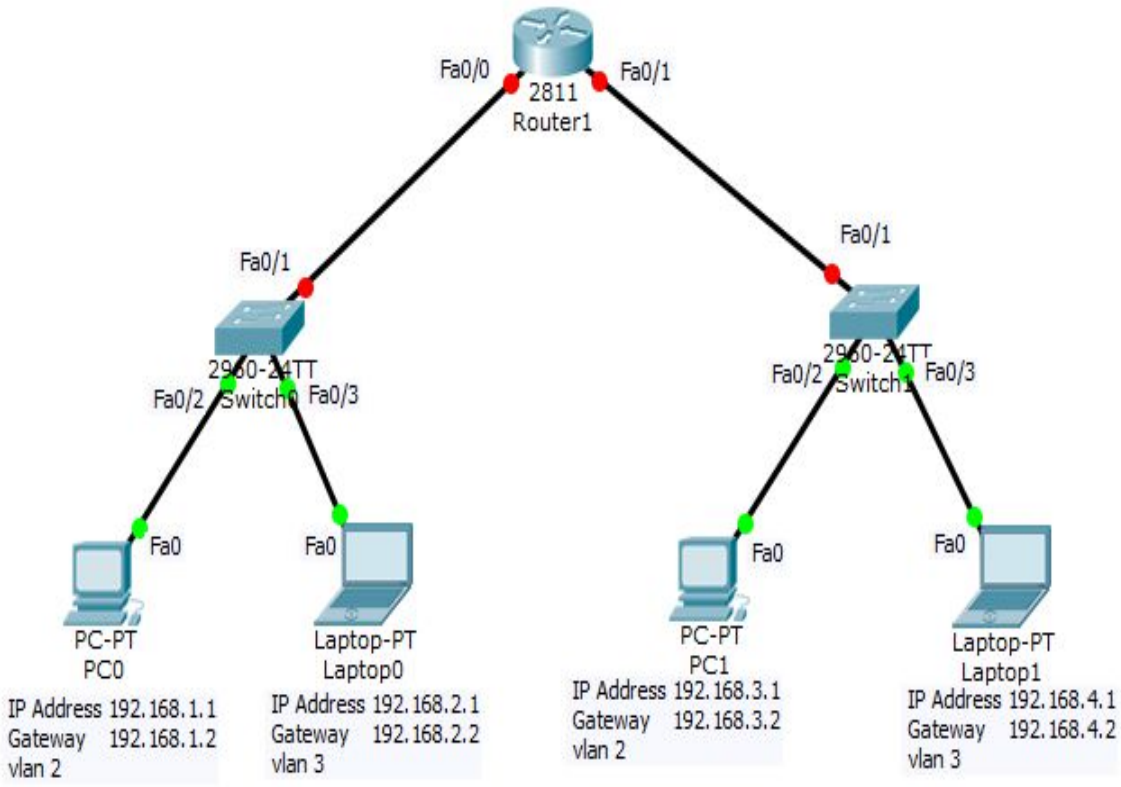


Figure III.1 Architecture déploiement

3.2.3 Présentation du simulateur « Cisco Packet Tracer »:

Dans cette configuration on essaye de configurer notre modèle type en utilisant le simulateur **« Cisco Packet Tracer »** faire aussi les différents tests et la validation de la configuration.

Le **« Cisco Packet Tracer »**est un programme puissant de simulation qui permet aux étudiants d'expérimenter le comportement du réseau, en effet il fournit la simulation, la visualisation, la création, évaluation et les capacités de collaboration et facilite l'enseignement et l'apprentissage des technologies complexes.

A travers le simulateur **« Cisco Packet Tracer »**nous avions reproduit notre environnement de travail pour nous permettre d'aboutir à une bonne configuration de notre solution VLAN.

La Figure suivante : est une image montrant l'interface principale du simulateur Cisco Packet Tracer :

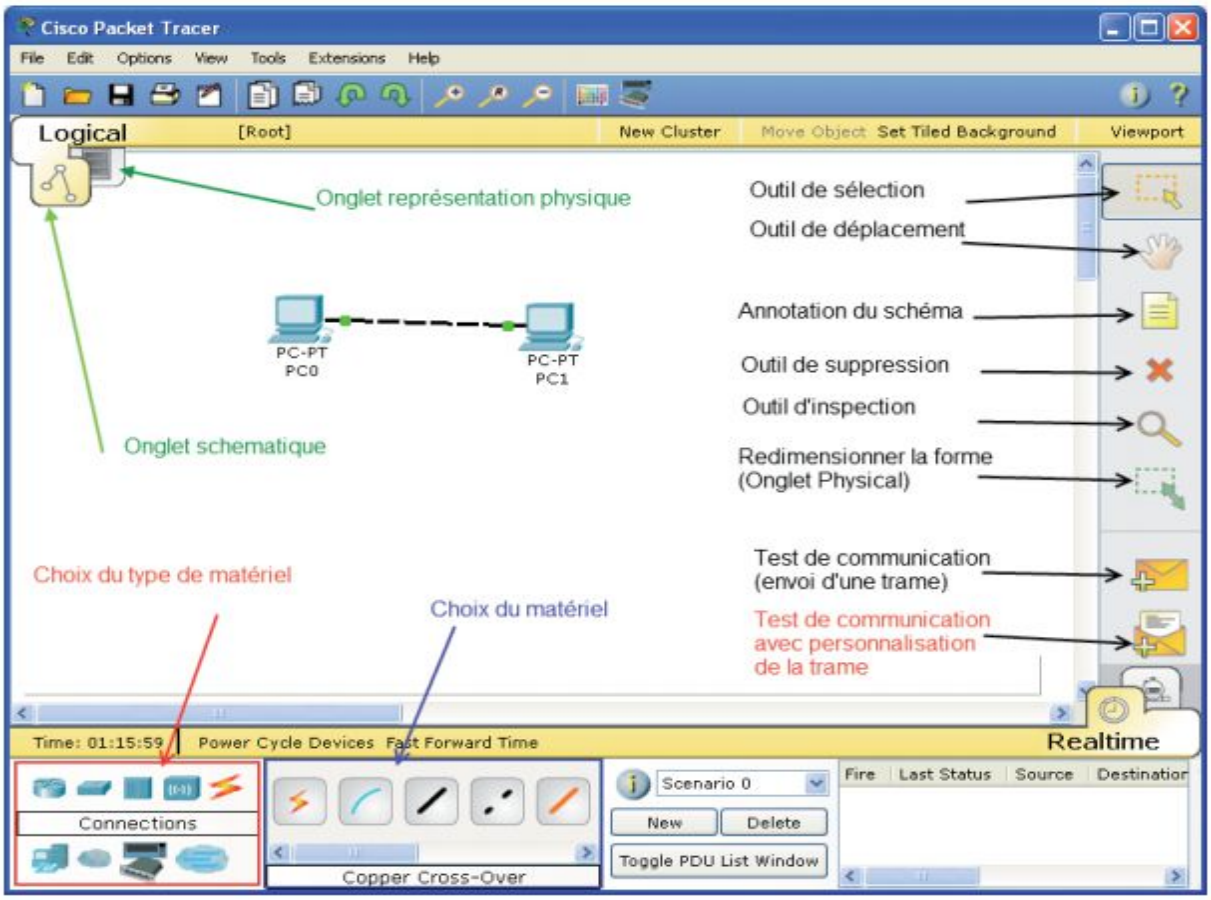


Figure III.2 : L'interface de simulateur « Cisco Packet Tracer ».

3.2.4 Interface commande de Packet Tracer:

Toutes les configurations des équipements du réseau, c'est au niveau de CLI (Command Language Interface) quelles seront réalisées. CLI est une interface de simulateur Packet Tracer qui permet la configuration des équipements du réseau à l'aide d'un langage de commandes, c'est-à-dire qu'à partir des commandes introduites par l'utilisateur du logiciel, que la configuration est faite [11].

La Figure suivante est l'interface CLI du Packet Tracer:

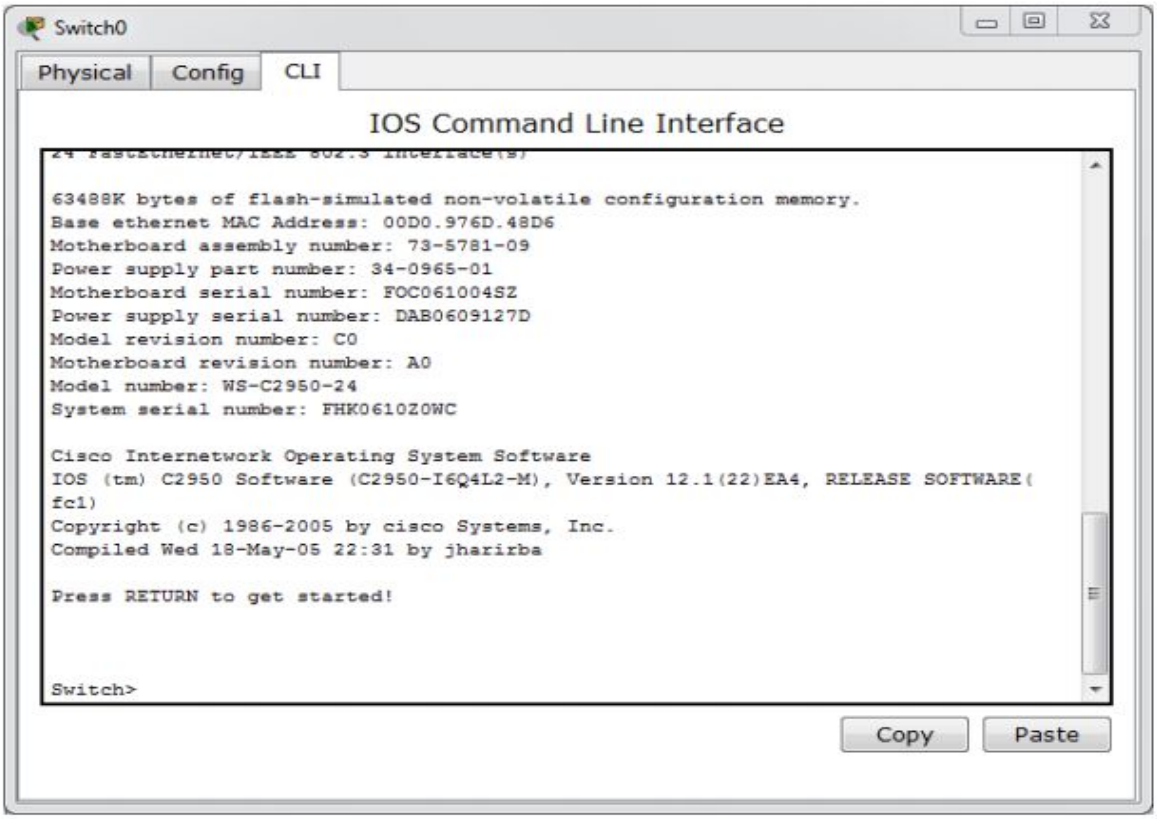


Figure III.3: Interface CLI

3.2.5 L'adressage des différents VLANs :

VLAN	IP Adresse	Gateway
VLAN 2	PC0 :192.168.1.1 PC1 :192.168.3.1	PC0 :192.168.1.2 PC1 :192.168.3.2
VLAN 3	Laptop0 :192.168.2.1 Laptop1 :192.168.4.1	Laptop0 :192.168.2.2 Laptop1 :192.168.4.2

Tableau III.1 le dimensionnement de notre réseau au niveau des VLAN

A chaque VLAN sera affecté une adresse IP afin d'effectuer le routage inter VLAN.

Cette répartition permettra d'une part à l'administrateur d'être plus à l'aise dans la gestion de son parc informatique et d'autre part de bien dimensionner notre bande passante par priorité de segment.

3.3 Eléments fonctionnels du VLAN:

3.3.1 Les normes :

Les VLANs seront mis en oeuvre via ces deux normes :

· 802.1q (Etiquetage de trames)
· ISL (Encapsulation de trames)

La norme ISL est une Technologie propriétaire CISCO.

Grâce à cette norme nous pourrions :

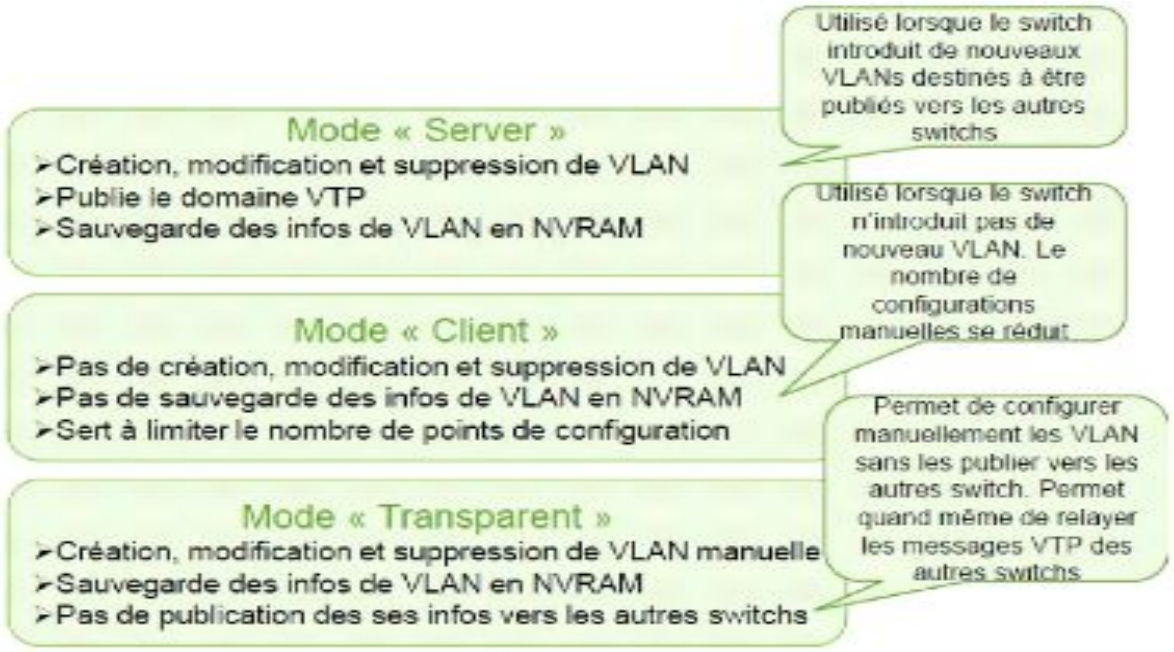
· Créer un lien «Trunk» qui véhicule le trafic entre les différents VLANs
· Associer un port à un ou plusieurs Vlans
· Choisir les Vlans à véhiculer avec le «pruning»

3.3.2 Les protocoles :

Protocole VTP

Les Switchs vont SW1, SW2 vont s'échanger les informations sur les VLANs grâce au protocole VTP : Vlan Trunking Protocol.

Les Switchs peuvent se situer dans plusieurs modes VTP :



Commande VTP ;

Pour configurer un VTP, il faut :

- Définir le mode (vtp server)
- Le domaine et éventuellement un mot de passe (vtp domain) ==== **NB : voir annexe 1**

Commande vérification VTP (show vtp status) ======**NB** : **voir annexe 2**

3.3.3 le protocole IEEE 802.3ad

L'agrégation de liens est définie dans la norme IEEE 802.3ad ; elle permet d'augmenter la bande passante disponible entre deux stations Ethernet en autorisant l'utilisation de -+plusieurs liens physiques comme un lien logique unique. Ces liens peuvent exister entre 2 commutateurs ou entre un commutateur et une station. Avant cette norme, il était impossible d'avoir plusieurs liens Ethernet sur une même station, sauf si ces liens étaient reliés à des réseaux ou des VLANs différents. L'agrégation de liens (appelé également link aggregation ou port trunking) apporte les avantages suivants :

- La bande passante peut être augmentée à volonté, par pallier. Par exemple, des liens Fast Ethernet additionnels peuvent augmenter une bande passante entre deux stations sans obliger le réseau à passer à la technologie Gigabit pour évoluer ;
- La fonction de « load balancing » (équilibrage de charge) peut permettre de distribuer le trafic entre les différents liens ou au contraire de dédier une partie de ces liens (et donc de la bande passante) à un trafic particulier ;

- La redondance est assurée automatiquement : le trafic sur une liaison coupée est redirigé automatiquement sur un autre lien. [12]

3.4 Le routage inter-vlan:

Le trafic entre les VLANs est assuré par un équipement de niveau 3 (Fig) :

- Un routeur
- Un commutateur de niveau 3

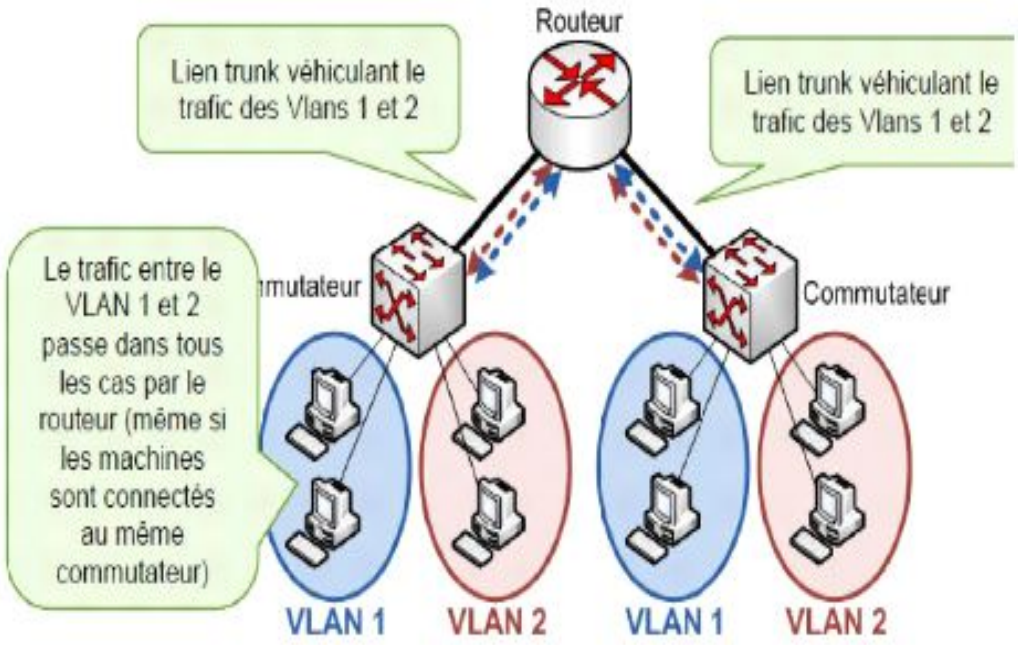


Figure III.4 Routage Inter-Vlan

Figure III.5 sous réseaux Vlan

Pour faire du routage entre vlan (Figure 3.3), il faudrait d'abord réunir les conditions suivantes :

- Attribuer à chaque VLAN des plages d'adresses IP n'appartenant pas au même réseau (Figure 3.4)
- Configurer un routeur capable de comprendre l'étiquetage 802.1q
- Créer un lien spécial entre le Switch et le routeur avec des trames étiquetées 802.1q

3.4.1 Le lien Trunk

L'implémentation du lien Trunk va nous permettre de véhiculer le trafic venant des différents VLANs du réseau.

Les trames des VLANs sont étiquetées lorsqu'elles sont envoyées par un lien Trunk. Cela permet d'acheminer directement l'information à son destinataire précis.

Le lien trunk peut être défini au niveau d'un commutateur

· Soit vers un routeur

· Soit vers un autre commutateur

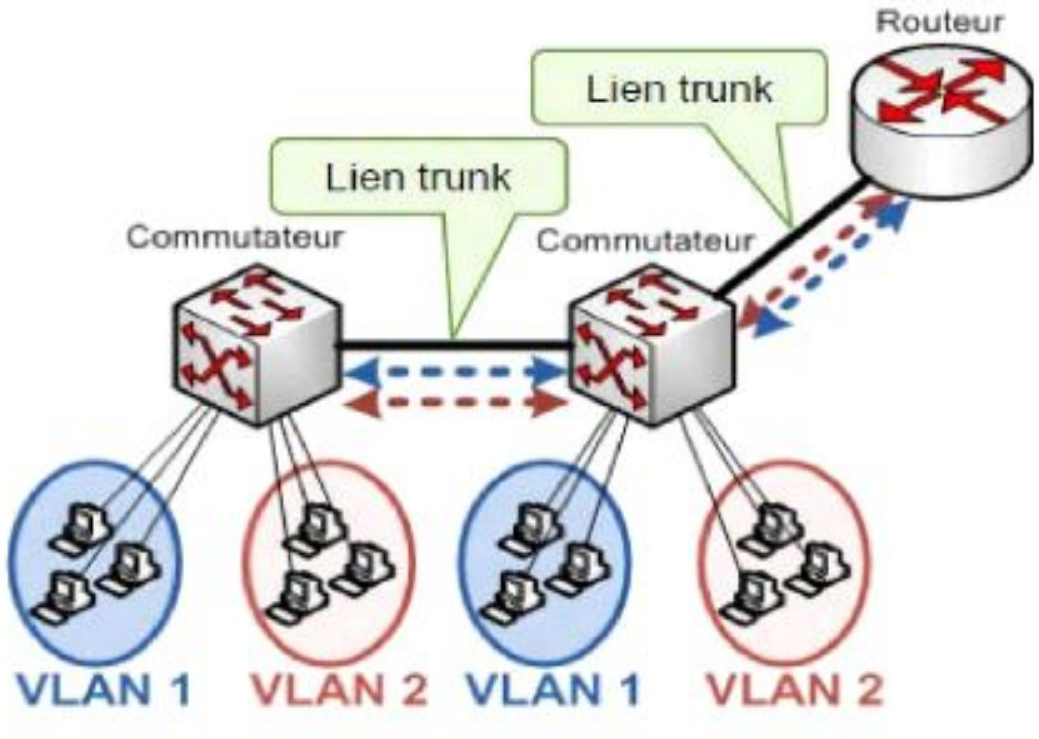


Figure III.6 Le lien Trunk

3.4.2 . Commande lien trunk

La commande **switchport** permet de définir un lien trunk ========**NB : Voir annexe 3**

Commande pour associé le port d'un Switch à un vlan Toujours avec la commande **switchport**, mais cette fois ci en précisant le N° de Vlan. ===== **NB : Voir annexe 4**

Selon la version de l'IOS (12.0 ou 12.1 T), nous pouvions agir sur plusieurs ports à la fois

Exemple : toutes les interfaces de 1 à 15

Cisco Internetwork Operating System Software

IOS (tm) 950 Software (950-I6Q4L2-M), Version 12.1(22)EA4, RELEASE SOFTWARE(fc1)

Copyright (c) 1986-2005 by cisco Systems, Inc. Compiled Wed 18-May-05 22:31 by jharirba

Press RETURN to get started!

Switch>en
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#inter
Switch(config)#interface fast
Switch(config)#**interface fastEthernet 0/1 – 15**

3.5 Partie 02 : Configuration des équipements:

3.5.1 Configuration des Vlans ;

La première étape à suivre une fois que le câblage est en place est de créer les deux VLANS sur nos deux Switchs. Pour faire simple, nous allons supposer que nous aurons deux VLANS (2 et 3) avec une liaison par port trunk entre le Switch 0 et le Switch 1. Le reste de la configuration sera détaillée et expliquée plus tard.

```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#ho
Switch(config)#hostname SW0
SW0(config)#
```

Nous allons ensuite créer les VLANS et les nommer :

```
SW0(config)#vlan 2
SW0(config-vlan)#name vlan-2
SW0(config-vlan)#vlan 3
SW0(config-vlan)#name vlan-3
SW0(config-vlan)#exit
```

Nous allons configurer les interfaces pour chaque Vlan :

```
SW0(config)#interface f0/2
SW0(config-if)#switchport mode access
SW0(config-if)#switchport access vlan 2
SW0(config-if)#exit
SW0(config)#interface f0/3
SW0(config-if)#switchport mode access
SW0(config-if)#switchport access vlan 3
SW0(config-if)#exit
```

On spécifie également les VLANS que nous souhaitons laisser passer sur notre trunk à savoir les trames étiquetées sur les VLAN 2,3. Par défaut, toutes les VLANS peuvent passer sur un port trunk. Si nous spécifions l'autorisation de certaines VLANs, les autres ne seront pas acceptés à transiter. Nous allons maintenant affecter les ports voulus à nos différentes VLANS.

On exécute donc ces commandes sur nos deux switchs :

```
SW0(config)#interface f0/1
SW0(config-if)#switchport mode trunk
SW0(config-if)#switchport trunk allowed vlan 2,3
SW0(config-if)#exit
```

3.5.2 TEST VLANs :

Nous allons maintenant tester la connectivité des postes situées sur le même VLAN.

On prend pas exemple le poste "PC0" sur le VLAN 2 et avec l'IP 192.168.1.1 pour pinger le poste **"PC1"** située sur le VLAN 2 de l'autre switch et avec l'IP 192.168.3.1 :

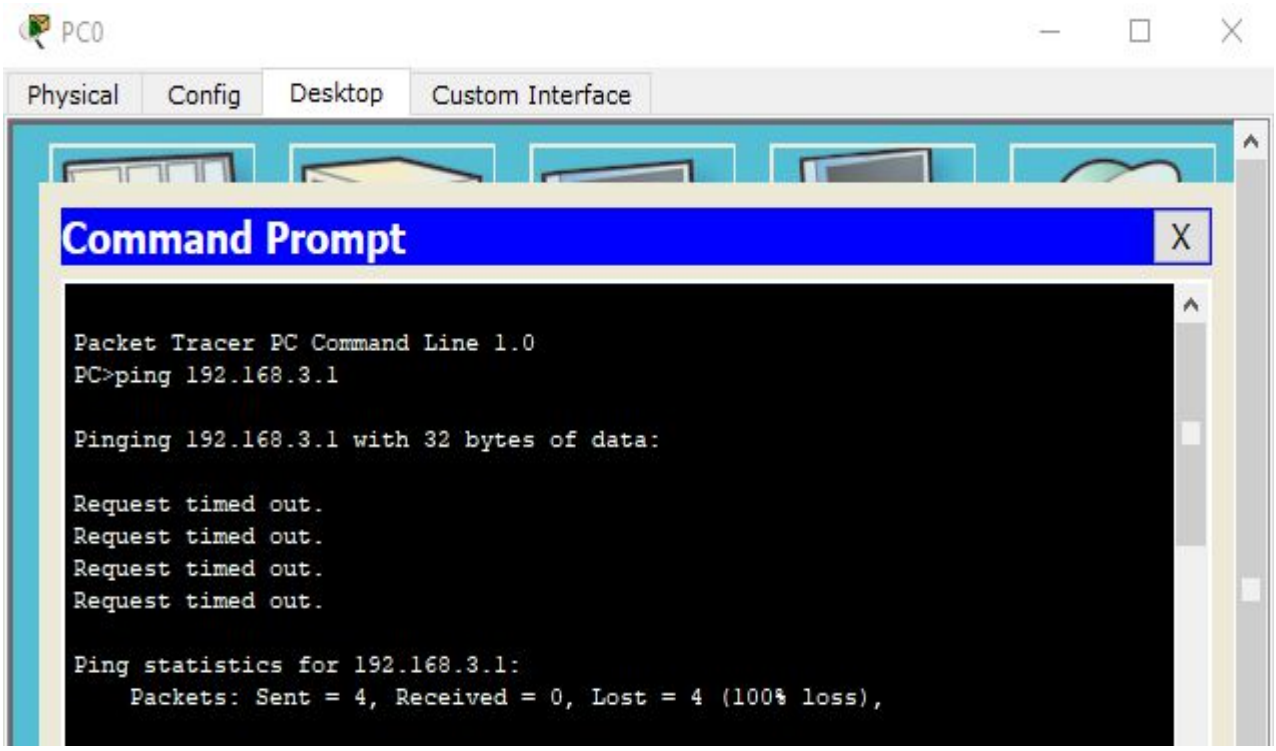


Figure III.7 Test vlan

On peut faire la même chose en pingant du poste **"Laptop0"** au poste **" Laptop1"** qui sont également tout deux sur le même **VLAN** (3 cette fois ci).

Les plus curieux aurons remarqué que le **"PC0"** ou "PC1" ne peuvent pinger **"Laptop0"** et "Laptop1" qui sont sur des **VLANS** différentes (2 et 3). C'est justement la problématique que nous

venons de nous créer est que les VLANS isolent correctement les groupes de postes/d'utilisateur mais bloquent complétement la communication entres elles.

Pourquoi ?

Les VLANs sont des LAN virtuelle (d'où leur nom) et comme chaque LAN, nous ne pouvons les interconnectés que par l'intermédiaire de routeur (d'élément gérant la couche 3 - réseau plus spécifiquement). Nous avons maintenant besoin de router nos différentes VLANS entre elles pour qu'elles puissent communiquer.

Nous abordons donc la deuxième partie du tutoriel qui est donc le routage inter-vlan.

3.5.3 Routage inter-vlan

Il se peut qu'un besoin de communication se fasse entre les deux groupes de travail. Il est alors possible de faire communiquer deux Vlans sans pour autant compromettre leur sécurité.

Pour cela nous utilisons un routeur relié à un des deux switchs. Nous appelons ce type de routage inter-vlan un Router-on-stick. Cela signifie que le router va, par intermédiaire d'un seul lien physique router et faire transiter un ensemble de VLAN. On aurait également pu mettre en place un switch de niveau trois qui aurai été capable d'effectuer les tâches de routage inter-vlan.

Plusieurs Vlans peuvent avoir pour passerelle un même port physique du routeur qui sera "découpé" en plusieurs interfaces virtuelles.

Nous pouvons en effet diviser un port du routeur selon les Vlans à router et ainsi créer une multitude de passerelles virtuelles avec des adresses IP différentes. [13]

3.5.4 Configuration du routeur

Nous allons donc créer notre interface virtuelle sur le port Fa0/0 de notre routeur.

Il faut tout d'abord absolument activer l'interface physique pour que les interfaces virtuelles soient opérationnelles :

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R0
R0(config)#
```

```
R0(config)#interface f0/0
R0(config-if)#no sh

R0(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to
up

R0(config-if)#ex
R0(config)#
```

Nous allons ensuite créer l'interface **fa0/0.1** (interface virtuelle 1 de l'interface physique fa0/0),nous dirons que ce port virtuel sur la passerelle des postes du VLAN 2 :

```
R0(config)#interface f0/0.1
R0(config-subif)#encapsulation dot1Q 2
R0(config-subif)#ip address 192.168.1.2 255.255.255.0
R0(config-subif)#no sh
R0(config-subif)#ex
```

Nous faisons pareil pour l'interface fa0/0.2 et les postes du réseau du vlan 3 :

```
R0(config-subif)#interface f0/0.2
R0(config-subif)#encapsulation dot1Q 3
R0(config-subif)#ip address 192.168.2.2 255.255.255.0
R0(config-subif)#no sh
R0(config-subif)#ex
R0(config)#
```

Un petit mot de la commande "encapsulation dot1q" :

La norme de trame **802.1q** indique que les trames sont étiquetées pour contenir le numéro de vlan à laquelle elles sont destinées/attribuées.

La commande "**encapsulation dot1q 2**" permet donc d'encapsuler une trame pour transiter sur le vlan 2 si elle est destinée à celui ci.

Le routeur a besoin de cette information par exemple quand il voit une trame venant du vlan 2 (étiquetée vlan 2) qui souhaite se diriger sur le vlan 3. Il change donc à ce moment là son étiquetage 802.1q pour que les switchs puissent correctement acheminé la trame vers le ou les postes du vlan 3.

Même travaille pour l'interface F0/1 de notre routeur :

-Activer l'interface

-ainsi que créer les sous interfaces(virtuels) pour les autres vlans de notre deuxième switch

Voici finalement notre réseau :

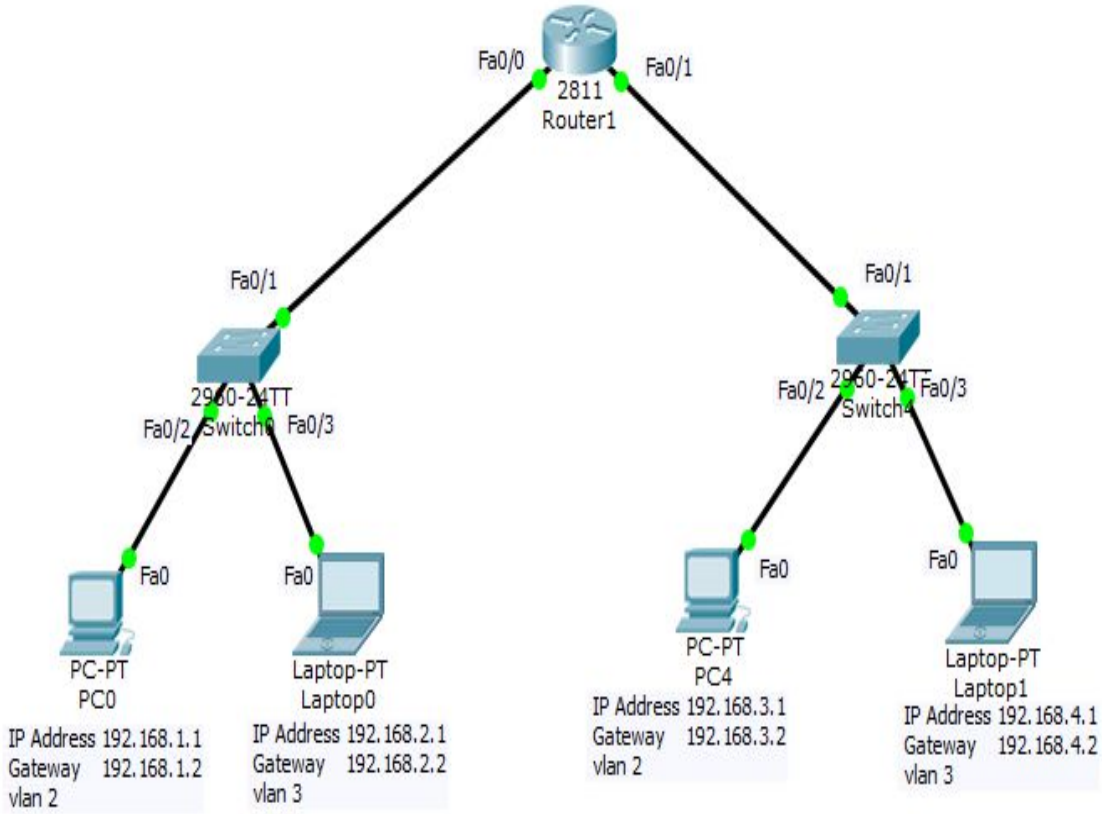


Figure III.8 schéma final du scénario

3.5.5 Test Routage Vlan

Une fois que nous avons mis les bonnes passerelles à nos postes, nous pouvons tester la communication inter-VLAN par l'intermédiaire d'un simple **ping** par exemple du poste 192.168.1.1 vers 192.168.3.1

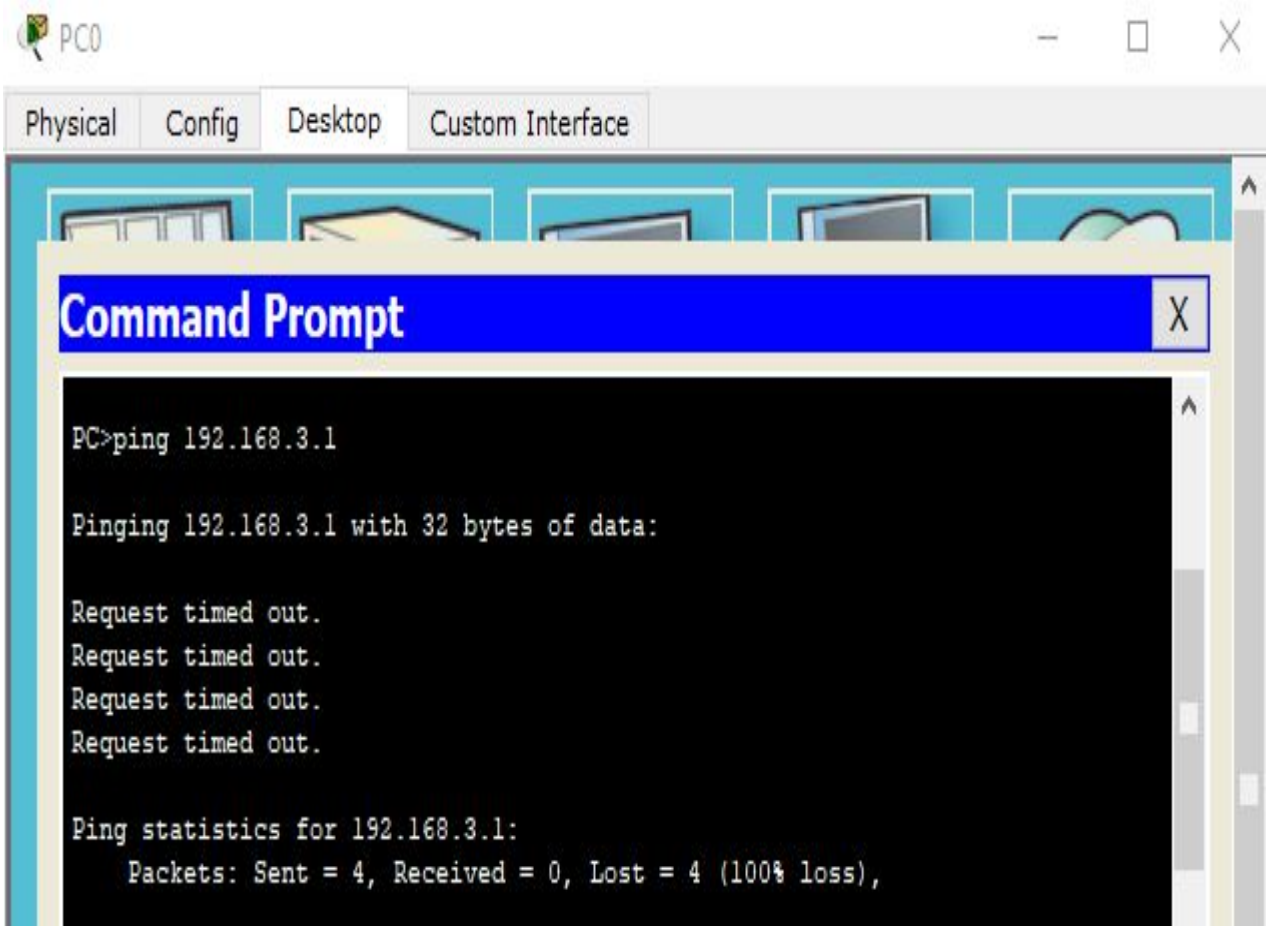


Figure III.9 Test Routage Vlan

3.6 La Sécurité réseau:

3.6.1 La sécurité contre court-circuit:

Les locaux seront protégés par des fusibles ; en cas de court-circuit, les fusibles se déclenchent.

3.6.2 La sécurité contre surtension :

Les équipements du réseau doivent être protégés par des régulateurs de tensions et des stabilisateurs.

3.6.3 . La sécurité contre l'incendie :

Nous devrons prévoir des extincteurs pour nous protégés contre l'incendie.

3.6.4 La sécurité contre le virus:

Nous allons sécuriser notre réseau et nos machines en installant un anti-virus, plus que nécessaire nous allons être reliés à l'internet ; et notre anti-virus sera mise à

jour régulièrement pour prévenir les attaques des virus.

3.6.5 La sécurité contre l'espionnage:

Pour lutter contre l'espionnage nous allons mettre en place un pare feu et une clé cryptage qui sera affichée automatique dans notre outil de communication réseau

3.7 Conclusion:

La technologie VLAN offre de nombreux avantages aux administrateurs réseau. Les VLAN permettent notamment de contrôler les broadcasts de couche 3 ; ils améliorent la sécurité du réseau et facilitent le regroupement logique des utilisateurs du réseau.

Toutefois, les VLAN ont une limite importante. Ils fonctionnent au niveau de la couche 2, ce qui signifie que les unités d'un VLAN ne peuvent pas communiquer avec les utilisateurs d'un autre VLAN sans utiliser des routeurs et des adresses de couche réseau.

Chapitre 04:

Résultat de Simulation et Discussion

4.1 Introduction :

Après avoir bien étudié les solutions proposées du coté théorique, vient le tou de la conception de l'architecture technique.

Cette partie consiste à organiser notre réseau sur les différents plans (nommage, adressage et routage) et déployer les protocoles nécessaires.

Pour cela on a proposé 04 scénario en discutant les résultat de chacun pour bien justifier les avantages et inconvénients ainsi illustrer notre solution retenue.

4.2 Les protocoles de routage :

Les protocoles de routages permettent l'échange des informations à l'intérieur d'un système autonome. On retient les protocoles suivants couramment utilisés :

- États de lien, ils s'appuient sur la qualité et les performances du média de communication qui les séparent. Ainsi chaque routeur est capable de dresser une carte de l'état duré seau pour utiliser la meilleure route : OSPF
- Vecteur de distance, chaque routeur communique aux autres routeurs la distance qui les sépare .Ils élaborent intelligemment une cartographie de leurs voisins sur le réseau : RIP
- Hybride des deux premiers, comme EIGRP

4.3 SIMULATION (scenario01) :

4.3.1 Tableau Récapitulatif (4.1) du réseau (Routeur / Switch / 8 Stations):

Stations	Adresse IP	Masque Réseau	Ports	Vlans	Switch	Routeur
Station 01	192.168.10.2	255.255.255.0	F0/1	Vlan 10	2960-24TT	2811
Station 02	192.168.20.2	255.255.255.0	F0/2	Vlan 20	2960-24TT	2811
Station 03	192.168.30.2	255.255.255.0	F0/3	Vlan 30	2960-24TT	2811
Station 04	192.168.40.2	255.255.255.0	F0/4	Vlan 40	2960-24TT	2811
Station 05	192.168.50.2	255.255.255.0	F0/5	Vlan 50	2960-24TT	2811
Station 06	192.168.60.2	255.255.255.0	F0/6	Vlan 60	2960-24TT	2811
Station 07	192.168.70.2	255.255.255.0	F0/7	Vlan 70	2960-24TT	2811
Station 08	192.168.80.2	255.255.255.0	F0/8	Vlan 70	2960-24TT	2811

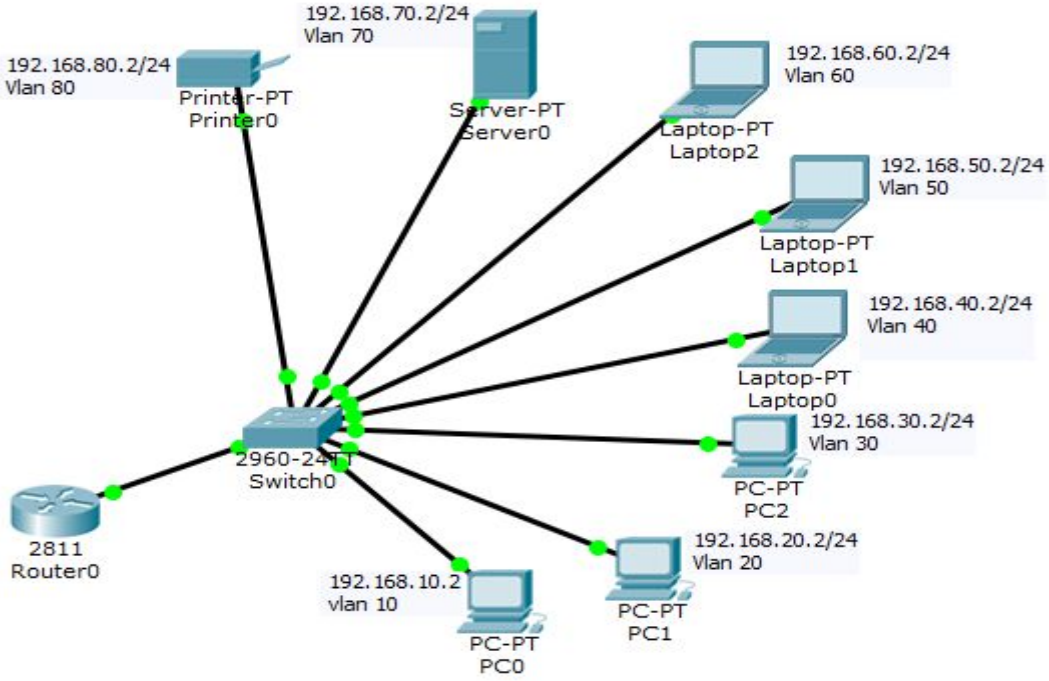


Fig.4.1 schéma scenario 01 (Routeur / Switch / 8 Stations)

4.3.2 Configuration ET discussion des résultats scenario 01:

1) **Création des Vlans dans le Switch 2960-24TT par la console CLI (Command Line Interface):**

Switch0 > enable

Switch# configure terminal

Switch (config)#hostname SW1

-1-SW1(config)#vlan 10**-2-** SW1(config)# name A

-3-SW1(config)#vlan 20**-4-** SW1(config)# name B

-5-SW1(config)#vlan 30**-6-** SW1(config)# name C

-7-SW1(config)#vlan 40**-8-** SW1(config)# name D

-9-SW1(config)#vlan 50**-10-** SW1(config)# name E

-11-SW1(config)#vlan 60**-12-** SW1(config)# name F

-13-SW1(config)#vlan 70 **-14-** SW1(config)# name I

-15-SW1(config)#vlan 80**-16-** SW1(config)# name J

2) Affectation des Vlans pour chaque port :

```
Switch(config)#hostname SW1

SW1(config)#interface FastEthernet0/1
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 10
SW1(config-if)#exit
SW1(config)#

SW1(config)#interface FastEthernet0/2
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 20
SW1(config-if)#exit
SW1(config)#

SW1(config)#interface FastEthernet0/3
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 30
SW1(config-if)#exit
SW1(config)#

SW1(config)#interface FastEthernet0/4
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 40
SW1(config-if)#exit
SW1(config)#

SW1(config)#interface FastEthernet0/5
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 50
SW1(config-if)#exit
SW1(config)#
SW1(config)#interface FastEthernet0/6
```

```
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 60
SW1(config-if)#exit
SW1(config)#

SW1(config)#interface FastEthernet0/7
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 70
SW1(config-if)#exit
SW1(config)#

SW1(config)#interface FastEthernet0/8
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 80
SW1(config-if)#exit
SW1(config)#
```

3) Création du port Trunk pour l'ensemble des Vlans dans le Switch SW1 et le routeur :

3.1)Agrégation de liens :

L'agrégation de liens est définie dans la norme IEEE 802.3ad ; elle permet d'augmenter labande passante disponible entre deux stations Ethernet en autorisant l'utilisation de plusieursliens physiques comme un lien logique unique. Ces liens peuvent exister entre 2commutateurs ou entre un commutateur et une station. Avant cette norme, il était impossibled'avoir plusieurs liens Ethernet sur une même station, sauf si ces liens étaient reliés à desréseaux ou des VLANs différents. L'agrégation de liens (appelé également *link aggregation* ou *port trunking*) apporte lesavantages suivants :

- ✓ La bande passante peut être augmentée à volonté, par pallier. Par exemple, des liensFast Ethernet additionnels peuvent augmenter une bande passante entre deux stationssans obliger le réseau à passer à la technologie Gigabit pour évoluer ;- La fonction de « load balancing » (équilibrage de charge) peut permettre de distribuerle trafic entre les différents liens ou au contraire de dédier une partie de ces liens (etdonc de la bande passante) à un trafic particulier.

- ✓ La redondance est assurée automatiquement : le trafic sur une liaison coupée estredirigé automatiquement sur un autre lien.

3.2) La répartition du trafic :

Les interfaces Ethernet sont considérées comme une interface unique (une seule adresse MAC) avec tous ces liens physiques, la fonction d'agrégation de liens est donc totalement transparente pour les couches de haut niveau comme pour les protocoles de routage. Par contre, pour conserver l'ordre d'arrivée des trames à leur destinataire, les algorithmes chargés de l'agrégation créent des sessions appelées « conversations » qui regroupent les trames Ethernet ayant les mêmes adresses sources et destinations (couple **S**ender **A**ddress/**D**estination **A**ddress). Les trames d'une même conversation sont alors limitées à un seul lien physique. En d'autres termes, les données d'une même adresse source vers une même adresse destination se feront à travers le même lien.
L'émission vers une autre destination se fera via un autre lien. Il est donc possible qu'un seul des liens soit utilisé complètement et que les autres ne le soient pas du tout. Nous pouvons également préciser que tous les liens physiques d'un même groupe doivent opérer en point à point, entre deux stations full-duplex et que tous les liens doivent fonctionner avec le même débit.

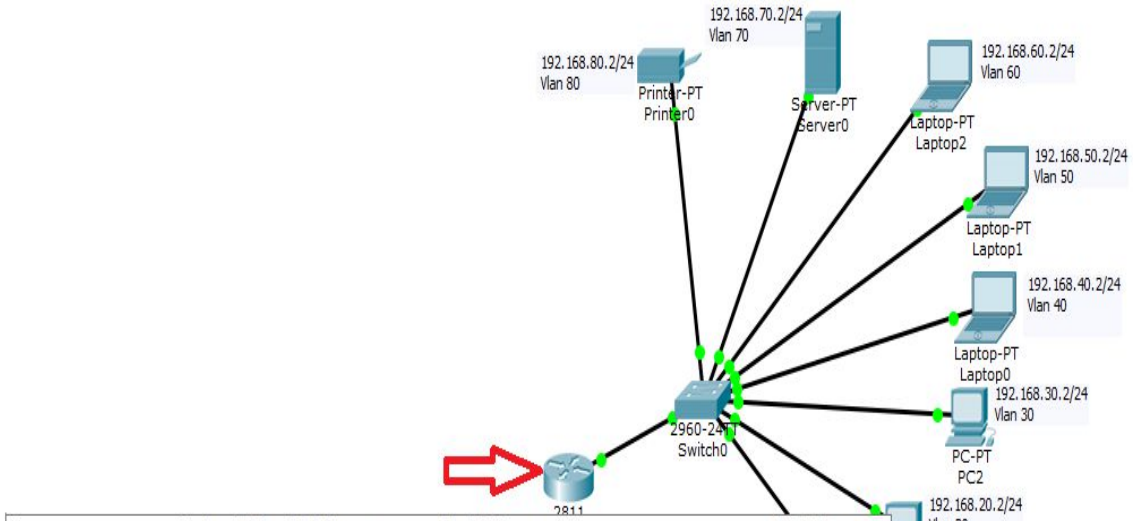
- A partir du port FastEthernet0/9 qui y est entre le Switch et le routeur on peut créer le le port Trunk qui donne la permission aux différents machines pour se communiquent entre eux avec les lignes commandes Ci-dessous :

```
SW1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW1(config)#interface FastEthernet0/9
SW1(config-if)#switchport mode trunk
SW1(config-if)#switchport trunk allowed vlan 10,20,30,40,50,60,70,80
SW1(config-if)#exit
SW1(config)#
```

4) Affectation des Sub-adresses IP pour chaque station dans le routeur RT1 pour l'adresse du port FastEthernet0/ :

On diffuse les Sub-adresses IP de chaque station dans le routeur pour le port FastEthernet0/, pour que les différentes machines peuvent se communiquent entre eux avec cette méthode et via l'adresse IP de chaque machine dans le routeur (car elle seront identifiés par leurs adresses IP dans le routeur).

```
Router>ena
Router#configure terminal
Router(config)#hostname RT1
RT1(config)#interface FastEthernet0/0.10
RT1(config-subif)#encapsulation dot1Q 10
RT1(config-subif)#ip address 192.168.10.1 255.255.255.0

RT1(config)#interface FastEthernet0/0.20
RT1(config-subif)#encapsulation dot1Q 20
RT1(config-subif)#ip address 192.168.20.1 255.255.255.0

RT1(config)#interface FastEthernet0/0.30
RT1(config-subif)#encapsulation dot1Q 30
RT1(config-subif)#ip address 192.168.30.1 255.255.255.0

RT1(config)#interface FastEthernet0/0.40
RT1(config-subif)#encapsulation dot1Q 40
RT1(config-subif)#ip address 192.168.40.1 255.255.255.0

RT1(config)#interface FastEthernet0/0.50
RT1(config-subif)#encapsulation dot1Q 50
RT1(config-subif)#ip address 192.168.50.1 255.255.255.0

RT1(config)#interface FastEthernet0/0.60
RT1(config-subif)#encapsulation dot1Q 60
RT1(config-subif)#ip address 192.168.60.1 255.255.255.0

RT1(config)#interface FastEthernet0/0.70
RT1(config-subif)#encapsulation dot1Q 70
RT1(config-subif)#ip address 192.168.70.1 255.255.255.0

RT1(config)#interface FastEthernet0/0.80
RT1(config-subif)#encapsulation dot1Q 80
RT1(config-subif)#ip address 192.168.80.1 255.255.255.0
RT1(config-subif)#exit
RT1(config)#
```



Port	Link	VLAN	IP Address	IPv6 Address	MAC Address
FastEthernet0/0	Up	--	<not set>	<not set>	0001.425A.EA01
FastEthernet0/0.10	Up	--	192.168.10.1/24	<not set>	0001.425A.EA01
FastEthernet0/0.20	Up	--	192.168.20.1/24	<not set>	0001.425A.EA01
FastEthernet0/0.30	Up	--	192.168.30.1/24	<not set>	0001.425A.EA01
FastEthernet0/0.40	Up	--	192.168.40.1/24	<not set>	0001.425A.EA01
FastEthernet0/0.50	Up	--	192.168.50.1/24	<not set>	0001.425A.EA01
FastEthernet0/0.60	Up	--	192.168.60.1/24	<not set>	0001.425A.EA01
FastEthernet0/0.70	Up	--	192.168.70.1/24	<not set>	0001.425A.EA01
FastEthernet0/0.80	Up	--	192.168.80.1/24	<not set>	0001.425A.EA01
FastEthernet0/1	Down	--	<not set>	<not set>	0001.425A.EA02
Vlan1	Down	1	<not set>	<not set>	0060.7055.538B

Hostname: RT1

Physical Location: Intercity, Home City, Corporate Office, Main Wiring Closet

Fig.4.2 schéma descriptif du routeur scenario 01

Port	Link	VLAN	IP Address	MAC Address
FastEthernet0/1	Up	10	--	0007.EC49.1701
FastEthernet0/2	Up	20	--	0007.EC49.1702
FastEthernet0/3	Up	30	--	0007.EC49.1703
FastEthernet0/4	Up	40	--	0007.EC49.1704
FastEthernet0/5	Up	50	--	0007.EC49.1705
FastEthernet0/6	Up	60	--	0007.EC49.1706
FastEthernet0/7	Up	70	--	0007.EC49.1707
FastEthernet0/8	Up	80	--	0007.EC49.1708
FastEthernet0/9	Up	--	--	0007.EC49.1709
FastEthernet0/10	Down	1	--	0007.EC49.170A
FastEthernet0/11	Down	1	--	0007.EC49.170B
FastEthernet0/12	Down	1	--	0007.EC49.170C
FastEthernet0/13	Down	1	--	0007.EC49.170D
FastEthernet0/14	Down	1	--	0007.EC49.170E
FastEthernet0/15	Down	1	--	0007.EC49.170F
FastEthernet0/16	Down	1	--	0007.EC49.1710
FastEthernet0/17	Down	1	--	0007.EC49.1711
FastEthernet0/18	Down	1	--	0007.EC49.1712
FastEthernet0/19	Down	1	--	0007.EC49.1713
FastEthernet0/20	Down	1	--	0007.EC49.1714
FastEthernet0/21	Down	1	--	0007.EC49.1715
FastEthernet0/22	Down	1	--	0007.EC49.1716
FastEthernet0/23	Down	1	--	0007.EC49.1717
FastEthernet0/24	Down	1	--	0007.EC49.1718
GigabitEthernet0/1	Down	1	--	0007.EC49.1719
GigabitEthernet0/2	Down	1	--	0007.EC49.171A
Vlan1	Down	1	<not set>	00E0.F9E8.57B3

Hostname: RT1

Physical Location: Intercity, Home City, Corporate Office, Main Wiring Closet

Router0

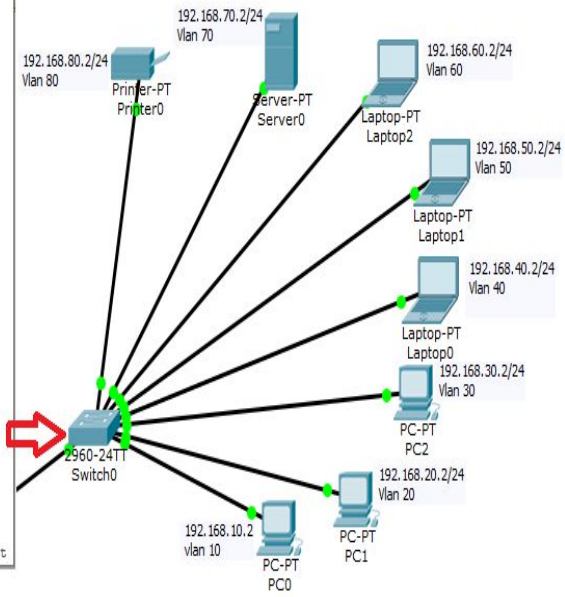


Fig.4.3 schéma descriptif du Switch scenario 01

4.4 SIMULATION (scenario 02):

4.4.1 Tableau Récapitulatif (4.2) du réseau (01 Routeur /03 Switch / 12 Stations)

Stations	Adresse IP	Masque Réseau	Ports	Vlans	Switch	Routeur
Station 01	192.168.10.2	255.255.255.0	F0/1	Vlan 10	2960-24TT	2811
Station 02	192.168.20.2	255.255.255.0	F0/2	Vlan 20	2960-24TT	2811
Station 03	192.168.30.2	255.255.255.0	F0/3	Vlan 30	2960-24TT	2811
Station 04	192.168.40.2	255.255.255.0	F0/4	Vlan 40	2960-24TT	2811
Station 05	192.168.50.2	255.255.255.0	F0/5	Vlan 50	2960-24TT	2811
Station 06	192.168.60.2	255.255.255.0	F0/6	Vlan 60	2960-24TT	2811
Station 07	192.168.70.2	255.255.255.0	F0/7	Vlan 70	2960-24TT	2811
Station 08	192.168.80.2	255.255.255.0	F0/8	Vlan 80	2960-24TT	2811
Station 09	192.168.90.2	255.255.255.0	F0/1	Vlan 90	2960-24TT	2811
Station 10	192.168.100.2	255.255.255.0	F0/2	Vlan 100	2960-24TT	2811
Station 11	192.168.110.2	255.255.255.0	F0/3	Vlan 110	2960-24TT	2811
Station 12	192.168.120.2	255.255.255.0	F0/4	Vlan 120	2960-24TT	2811

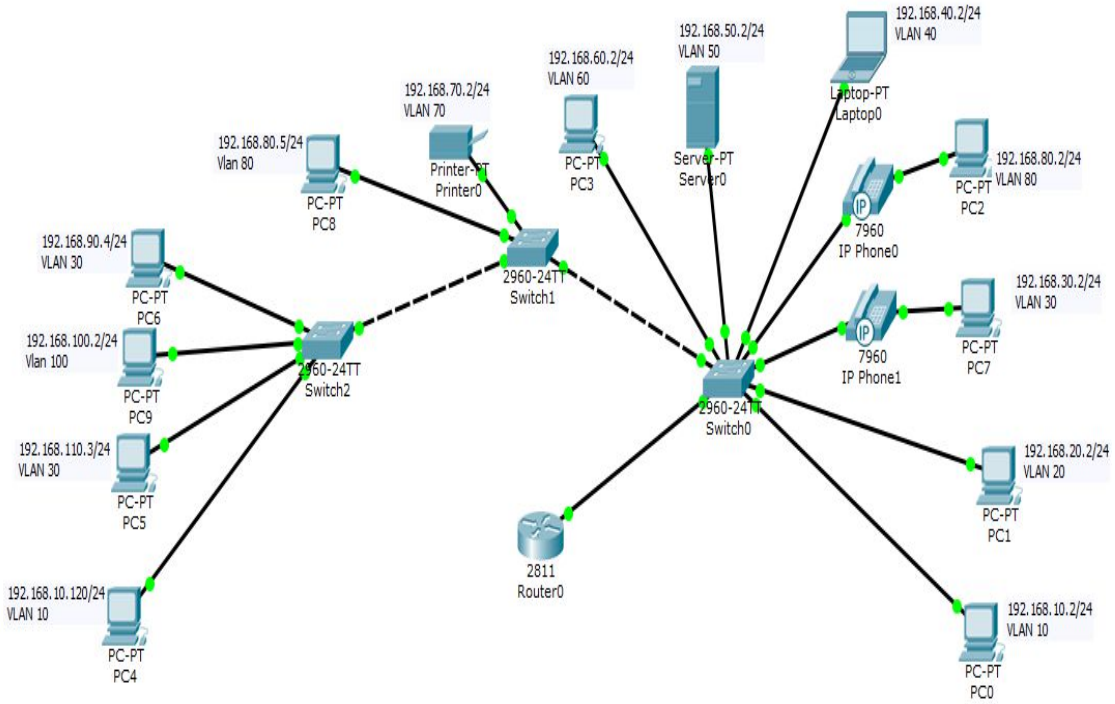


Fig.4.4 schéma scenario 02 (01 Routeur /03 Switch / 12 Stations)

4.4.2 Configuration ET discussion des résultat scenario 02:

1) Création des Vlans dans le Switch0 2960-24TT par la console CLI (Command Line Interface) :

Switch0 > enable

Switch # configure terminal

Switch (config)#hostname SW1

-1-SW1(config)#vlan 10 **-2-** SW1(config)# name DATA10

-3-SW1(config)#vlan 20 **-4-** SW1(config)# name DATA20

-5-SW1(config)#vlan 30 **-6-** SW1(config)# name DATA30

-7-SW1(config)#vlan 40 **-8-** SW1(config)# name DATA40

-9-SW1(config)#vlan 50 **-10-** SW1(config)# name DATA50

-11-SW1(config)#vlan 60 **-12-** SW1(config)# name DATA60

2) Configuration de deux PC connectés aux IP Phones.

Router0 (config)#ip dhcp pool data

Router0 (dhcp-config)#network 192.168.30.0 255.255.255.0

Router0 (dhcp-config)#default-router 192.168.30.1

Router0 (dhcp-config)#option 150 ip 192.168.30.1

Router0 (dhcp-config)#exit

Router0 (config)#

3) Configuration de deux IP Phones connectés aux deux PC.

Une fois cette étape terminée, le router et le switch devraient afficher une connexion verte.

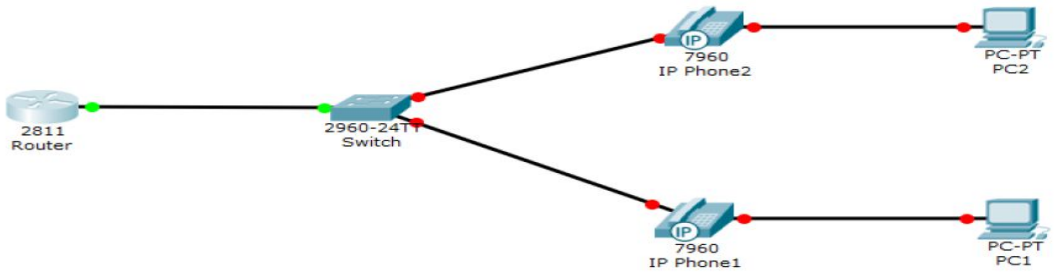


Fig.4.5 connexion 02 PC via 02 IP Phones

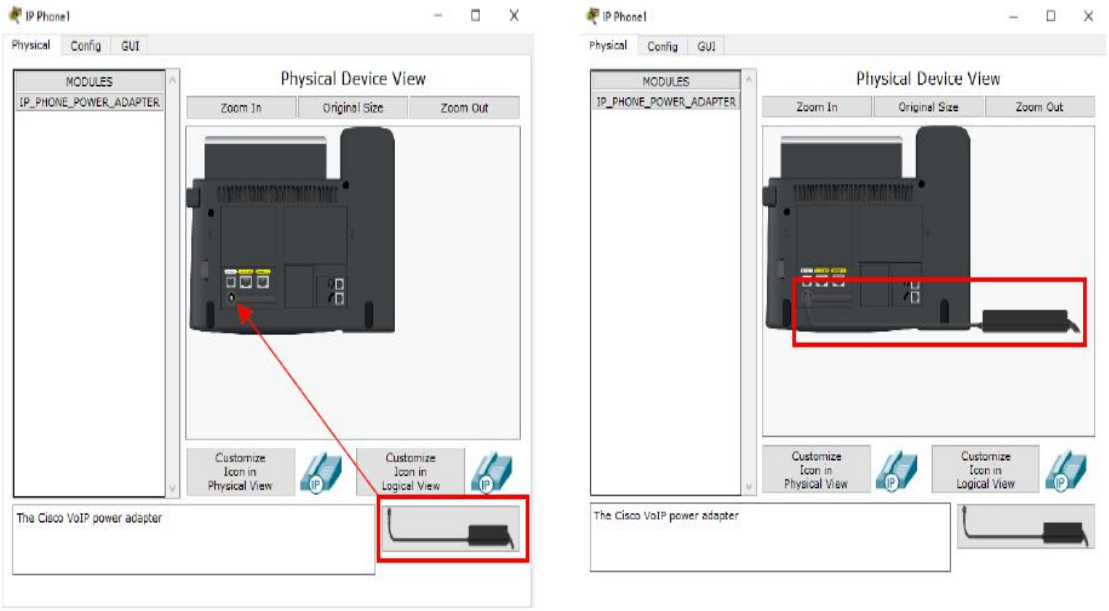


Fig.4.5.1 branchement des IP phones

Ensuite nous allons démarrer les IP Phones, en cliquant dessus nous allons brancher l'adaptateur secteur afin de l'alimenter (vous pouvez également utiliser des switchs POE Power Over Ethernet, afin de ne pas avoir à utiliser le secteur pour alimenter vos téléphones).

Normalement, toutes les connexions devraient être affichées en vertes :

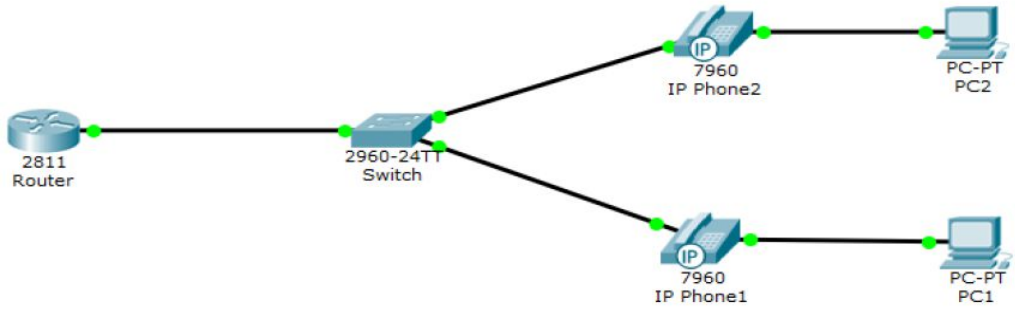


Fig.4.5.2 connexion 02 PC via 02 IP Phones

Router0(config)#ip dhcp pool voice
Router0(dhcp-config)#network 192.168.80.0 255.255.255.0
Router0 (dhcp-config)#default-router 192.168.80.1
Router0 (dhcp-config)#option 150 ip 192.168.80.1
Router0 (dhcp-config)#exit
Router0 (config)#telephony-service
Router0 (config-telephony)#max-dn 2
Router0 (config-telephony)#max-ephone 2
Router0 (config-telephony)#ip source-address 192.168.30.1 port 2000
Router0 (config-telephony)#auto assign 4 to 6
Router0 (config-telephony)#auto assign 1 to 5
Router0 (config-telephony)#exit

Switch0>enable
Switch0#configure terminal
Switch0(config)#interface range FastEthernet 0/2-3
Switch0(config-if-range)#switchport mode access
Switch0(config-if-range)#switchport voice vlan 1
Switch0(config-if-range)#exit
Switch0(config)#

4) Création des Vlans dans le Switch1 2960-24TT par la console CLI (Command Line Interface) :

Switch1> enable

Switch # configure terminal

Switch (config)#hostname SW2

-1-SW2(config)#vlan 70 **-2-** SW2(config)# name DATA70

-3-SW2(config)#vlan 80 **-4-** SW2(config)# name DATA80

5) Création des Vlans dans le Switch2 2960-24TT par la console CLI (Command Line Interface) :

Switch2> enable

Switch2 # configure terminal

Switch2 (config)#hostname SW3

-1-SW3(config)#vlan 90 **-2-** SW3(config)# name DATA90

-3-SW3(config)#vlan 100**-4-** SW3(config)# name DATA100

-5-SW3(config)#vlan 110 **-6-** SW3(config)# name DATA110

-7-SW3(config)#vlan 120 **-8-** SW3(config)# name DATA120

6) Affectation des Vlans pour chaque port dans le Switch SW1 :

Switch(config)#hostname SW1

SW1(config)#interface FastEthernet0/1
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 10
SW1(config-if)#exit
SW1(config)#

SW1(config)#interface FastEthernet0/2

SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 20
SW1(config-if)#exit

SW1(config)#interface FastEthernet0/3
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 30
SW1(config-if)#exit
SW1(config)#interface FastEthernet0/4
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 40
SW1(config-if)#exit

SW1(config)#interface FastEthernet0/5
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 50
SW1(config-if)#exit

SW1(config)#interface FastEthernet0/6
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 60
SW1(config-if)#exit

7) Affectation des Vlans pour chaque port dans le Switch SW2:

Switch(config)#hostname SW2
SW2(config)#interface FastEthernet0/1
SW2(config-if)#switchport mode access
SW2(config-if)#switchport access vlan 70
SW2(config-if)#exit

SW2(config)#interface FastEthernet0/2
SW2(config-if)#switchport mode access

SW2(config-if)#switchport access vlan 80
SW2(config-if)#exit

8) Affectation des Vlans pour chaque port dans le Switch SW3 :

Switch(config)#hostname SW2
SW2(config)#interface FastEthernet0/1
SW2(config-if)#switchport mode access
SW2(config-if)#switchport access vlan 90
SW2(config-if)#exit

SW2(config)#interface FastEthernet0/2
SW2(config-if)#switchport mode access
SW2(config-if)#switchport access vlan 100
SW2(config-if)#exit

Switch(config)#hostname SW2
SW2(config)#interface FastEthernet0/1
SW2(config-if)#switchport mode access
SW2(config-if)#switchport access vlan 110
SW2(config-if)#exit

SW2(config)#interface FastEthernet0/2
SW2(config-if)#switchport mode access
SW2(config-if)#switchport access vlan 0
SW2(config-if)#exit

9) Création du port Trunk pour l'ensemble des Vlans dans le Switch SW1 et le routeur :

Sélection des ports concernés par l'agrégation

Les ports utilisés pour le regroupement (*trunk*) ne sont pas forcément consécutifs. Nous rappelons qu'il est essentiel que les ports en question soient dans le même mode (même vitesse, full duplex). Tout comme nous pouvons souligner que tout port rajouté à un *trunk*perd ses configurations de «

port security ». Les ports sélectionnés pour l'agrégation sont les ports 5-7 (de 5 et 7) sur SW1 et SW2, 5-7 sur SW1 et SW2, le port 1 étant pris pour la connexion (la passerelle de sortie vers le réseau Internet). Les ports 5-7 sont pris sur SW1,SW2 pour l'agrégation avec PC0-PC1-PC7-PC2-Laptop0-Server0-PC3.Les ports 6-7 pour l'agrégation Printer0-PC8-PC6-PC9-PC5-PC4.

10) Configuration du port trunking

La première étape a donc consisté à mettre en place les *trunks* de façon statique, sans utiliser de protocole particulier. Le mot clé trunk qui indique qu'il s'agit d'un *trunk* statique sans protocole d'agrégation particulier. En effet il permet uniquement d'obtenir une redondance de liens (4 liens à 100 Mbps ne donne un débit que de 100 Mbps) et non un cumul Ce qui se fait comme suit :

- A partir du port FastEthernet0/7 qui y est entre le Switch et le routeur on peut créer le le port Trunk qui donne la permission aux différents machines pour se communiquent entre eux (Les ports sélectionnés pour l'agrégation)avec les lignes commandes Ci-dessous :

```
SW1#configure terminal
SW1(config)#interface FastEthernet0/7
SW1(config-if)#switchport mode trunk
SW1(config-if)#switchport trunk allowed vlan 10,20,30,40,50,60,70,80,90,100,110,120
SW1(config-if)#exit
SW1(config)#
```

11) Création du port Trunk pour l'ensemble des Vlans dans le Switch SW2 et le SW1 :

A partir du port FastEthernet0/5 qui y est entre le Switch et le routeur on peut créer le port Trunk qui donne la permission aux différents machines pour se communiquent entre eux(Les ports sélectionnés pour l'agrégation)avec les lignes commandes Ci-dessous :

```
SW2#configure terminal
SW2(config)#interface FastEthernet0/5
SW2(config-if)#switchport mode trunk
SW2(config-if)#switchport trunk allowed vlan 10,20,30,40,50,60,70,80,90,100,110,120
SW2(config-if)#exit
SW2(config)#
```

12) Création du port Trunk pour l'ensemble des Vlans dans le Switch SW2 et le SW3 :

A partir du port FastEthernet0/6 qui y est entre le Switch et le routeur on peut créer le port Trunk qui donne la permission aux différents machines pour se communiquent entre eux avec les lignes commandes Ci-dessous :

```
SW2#configure terminal
SW2(config)#interface FastEthernet0/6
SW2(config-if)#switchport mode trunk
SW2(config-if)#switchport trunk allowed vlan 10,20,30,40,50,60,70,80,90,100,110,120
SW2(config-if)#exit
SW2(config)#
```

13) Création du port Trunk pour l'ensemble des Vlans dans le Switch SW3 et le SW2 :

A partir du port FastEthernet0/5 qui y est entre le Switch et le routeur on peut créer le port Trunk qui donne la permission aux différents machines pour se communiquent entre eux avec les lignes commandes Ci-dessous :

```
SW2#configure terminal
SW2(config)#interface FastEthernet0/7
SW2(config-if)#switchport mode trunk
SW2(config-if)#switchport trunk allowed vlan 10,20,30,40,50,60,70,80,90,100,110,120
SW2(config-if)#exit
SW2(config)#
```

14) Affectation des Sub-adresses IP pour chaque station dans le routeur RT1 pour l'adresse du port FastEthernet0/ :

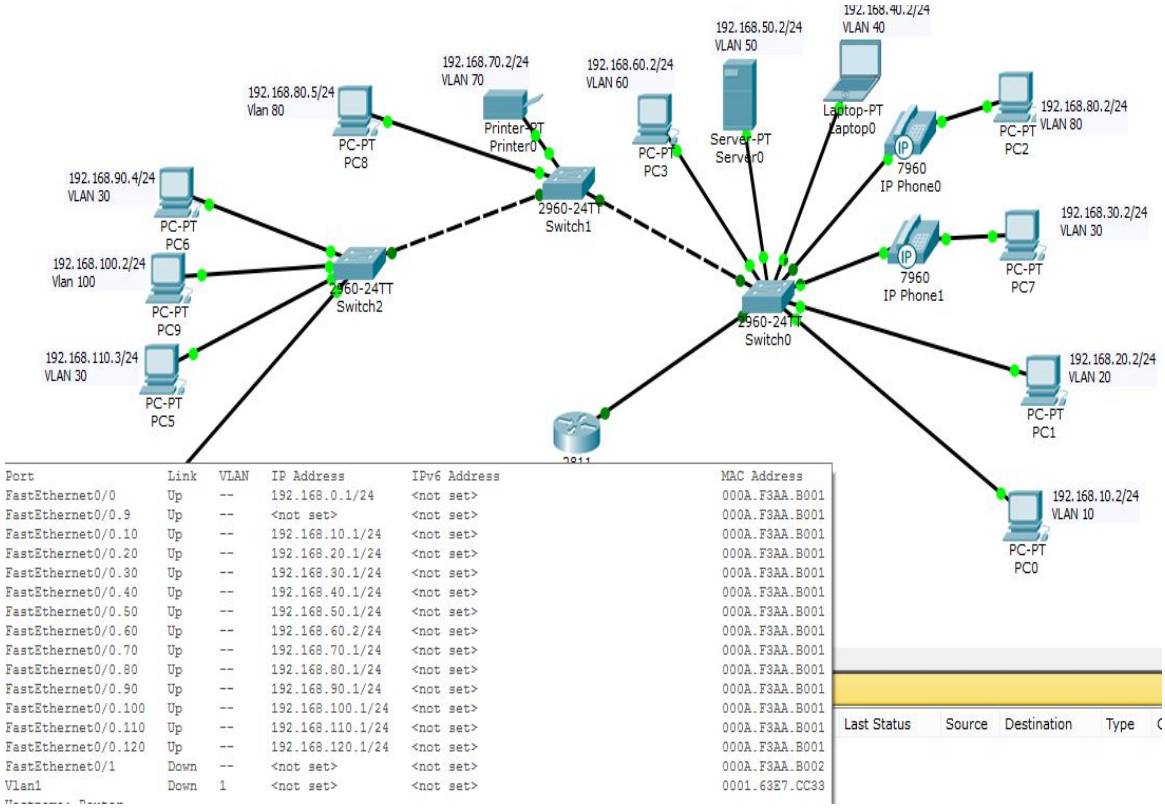
On diffuse les Sub-adresses IP de chaque station dans le routeur pour le port FastEthernet0/, pour que les différentes machines peuvent se communiquent entre eux avec cette méthode et via l'adresse IP de chaque machine dans le routeur (car elles seront identifiés par leurs adresses IP dans le routeur).

15) Identification et étiquetage du câblage et*Identification des machines :*

La première étape a été de repérer le câblage du réseau : Nous avons alors observé quel'étiquetage qui était en place ne correspondait plus à la réalité. Afin de pouvoir identifier plusfacilement les machines, nous avons défini une nouvelle nomenclature d'étiquetage puisreétiqueter tout le réseau. Pour nous permettre de réaliser ce qui nous était demandé, nousavons dû installer du câblage supplémentaire entre les commutateurs.

```
Router>ena
Router#configure terminal
Router(config)#hostname RT1
RT1(config)#interface FastEthernet0/0.10
RT1(config-subif)#encapsulation dot1Q 10
RT1(config-subif)#ip address 192.168.10.1 255.255.255.0

RT1(config)#interface FastEthernet0/0.20
RT1(config-subif)#encapsulation dot1Q 20
RT1(config-subif)#ip address 192.168.20.1 255.255.255.0

RT1(config)#interface FastEthernet0/0.30
RT1(config-subif)#encapsulation dot1Q 30
RT1(config-subif)#ip address 192.168.30.1 255.255.255.0

RT1(config)#interface FastEthernet0/0.40
RT1(config-subif)#encapsulation dot1Q 40
RT1(config-subif)#ip address 192.168.40.1 255.255.255.0


RT1(config)#interface FastEthernet0/0.50
RT1(config-subif)#encapsulation dot1Q 50
RT1(config-subif)#ip address 192.168.50.1 255.255.255.0

RT1(config)#interface FastEthernet0/0.60
RT1(config-subif)#encapsulation dot1Q 60
RT1(config-subif)#ip address 192.168.60.1 255.255.255.0

RT1(config)#interface FastEthernet0/0.70
RT1(config-subif)#encapsulation dot1Q 70
RT1(config-subif)#ip address 192.168.70.1 255.255.255.0
```

```
RT1(config)#interface FastEthernet0/0.80
RT1(config-subif)#encapsulation dot1Q 80
RT1(config-subif)#ip address 192.168.80.1 255.255.255.0

RT1(config)#interface FastEthernet0/0.90
RT1(config-subif)#encapsulation dot1Q 90
RT1(config-subif)#ip address 192.168.90.1 255.255.255.0

RT1(config)#interface FastEthernet0/0.100
RT1(config-subif)#encapsulation dot1Q 100
RT1(config-subif)#ip address 192.168.100.1 255.255.255.0

RT1(config)#interface FastEthernet0/0.110
RT1(config-subif)#encapsulation dot1Q 110
RT1(config-subif)#ip address 192.168.110.1 255.255.255.0

RT1(config)#interface FastEthernet0/0.120
RT1(config-subif)#encapsulation dot1Q 120
RT1(config-subif)#ip address 192.168.120.1 255.255.255.0
```



Port	Link	VLAN	IP Address	IPv6 Address	MAC Address
FastEthernet0/0	Up	--	192.168.0.1/24	<not set>	000A.F3AA.B001
FastEthernet0/0.9	Up	--	<not set>	<not set>	000A.F3AA.B001
FastEthernet0/0.10	Up	--	192.168.10.1/24	<not set>	000A.F3AA.B001
FastEthernet0/0.20	Up	--	192.168.20.1/24	<not set>	000A.F3AA.B001
FastEthernet0/0.30	Up	--	192.168.30.1/24	<not set>	000A.F3AA.B001
FastEthernet0/0.40	Up	--	192.168.40.1/24	<not set>	000A.F3AA.B001
FastEthernet0/0.50	Up	--	192.168.50.1/24	<not set>	000A.F3AA.B001
FastEthernet0/0.60	Up	--	192.168.60.2/24	<not set>	000A.F3AA.B001
FastEthernet0/0.70	Up	--	192.168.70.1/24	<not set>	000A.F3AA.B001
FastEthernet0/0.80	Up	--	192.168.80.1/24	<not set>	000A.F3AA.B001
FastEthernet0/0.90	Up	--	192.168.90.1/24	<not set>	000A.F3AA.B001
FastEthernet0/0.100	Up	--	192.168.100.1/24	<not set>	000A.F3AA.B001
FastEthernet0/0.110	Up	--	192.168.110.1/24	<not set>	000A.F3AA.B001
FastEthernet0/0.120	Up	--	192.168.120.1/24	<not set>	000A.F3AA.B001
FastEthernet0/1	Down	--	<not set>	<not set>	000A.F3AA.B002
Vlan1	Down	1	<not set>	<not set>	0001.63E7.CC33

Fig.4.6.1 schéma descriptif scénario 02

Port	Link	VLAN	IP Address	MAC Address
FastEthernet0/1	Up	10	--	0060.4755.2E01
FastEthernet0/2	Up	20	--	0060.4755.2E02
FastEthernet0/3	Up	30	--	0060.4755.2E03
FastEthernet0/4	Up	30	--	0060.4755.2E04
FastEthernet0/5	Up	--	--	0060.4755.2E05
FastEthernet0/6	Up	--	--	0060.4755.2E06
FastEthernet0/7	Up	40	--	0060.4755.2E07
FastEthernet0/8	Up	50	--	0060.4755.2E08
FastEthernet0/9	Up	60	--	0060.4755.2E09
FastEthernet0/10	Down	1	--	0060.4755.2E0A
FastEthernet0/11	Down	1	--	0060.4755.2E0B
FastEthernet0/12	Down	1	--	0060.4755.2E0C
FastEthernet0/13	Down	1	--	0060.4755.2E0D
FastEthernet0/14	Down	1	--	0060.4755.2E0E
FastEthernet0/15	Down	1	--	0060.4755.2E0F
FastEthernet0/16	Down	1	--	0060.4755.2E10
FastEthernet0/17	Down	1	--	0060.4755.2E11
FastEthernet0/18	Down	1	--	0060.4755.2E12
FastEthernet0/19	Down	1	--	0060.4755.2E13
FastEthernet0/20	Down	1	--	0060.4755.2E14
FastEthernet0/21	Down	1	--	0060.4755.2E15
FastEthernet0/22	Down	1	--	0060.4755.2E16
FastEthernet0/23	Down	1	--	0060.4755.2E17
FastEthernet0/24	Down	1	--	0060.4755.2E18
GigabitEthernet0/1	Down	1	--	0060.4755.2E19
GigabitEthernet0/2	Down	1	--	0060.4755.2E1A
Vlan1	Down	1	<not set>	000A.F3EC.6E79

VLANs
SWITCH0

Hostname: Switch

Physical Location: Intercity, Home City, Corporate Office, Main Wiring Closet

Fig.4.6.2 schéma descriptif du switch scénario 02

4.5 SIMULATION (scenario 03):

4.5.1 Tableau Récapitulatif (4.3) du réseau

(03 Routeurs / 03 Switch / 08 Stations X 3 ➔ 24 Stations)

Stations	Adresse IP	Masque Réseau	Ports	Vlans	Switch	Routeur
Station 01	192.168.10.2	255.255.255.0	F0/1	Vlan 10	2960-24TT	2811
Station 02	192.168.20.2	255.255.255.0	F0/2	Vlan 20	2960-24TT	2811
Station 03	192.168.30.2	255.255.255.0	F0/3	Vlan 30	2960-24TT	2811
Station 04	192.168.40.2	255.255.255.0	F0/4	Vlan 40	2960-24TT	2811
Station 05	192.168.50.2	255.255.255.0	F0/5	Vlan 50	2960-24TT	2811
Station 06	192.168.60.2	255.255.255.0	F0/6	Vlan 60	2960-24TT	2811
Station 07	192.168.70.2	255.255.255.0	F0/7	Vlan 70	2960-24TT	2811
Station 08	192.168.80.2	255.255.255.0	F0/8	Vlan 70	2960-24TT	2811

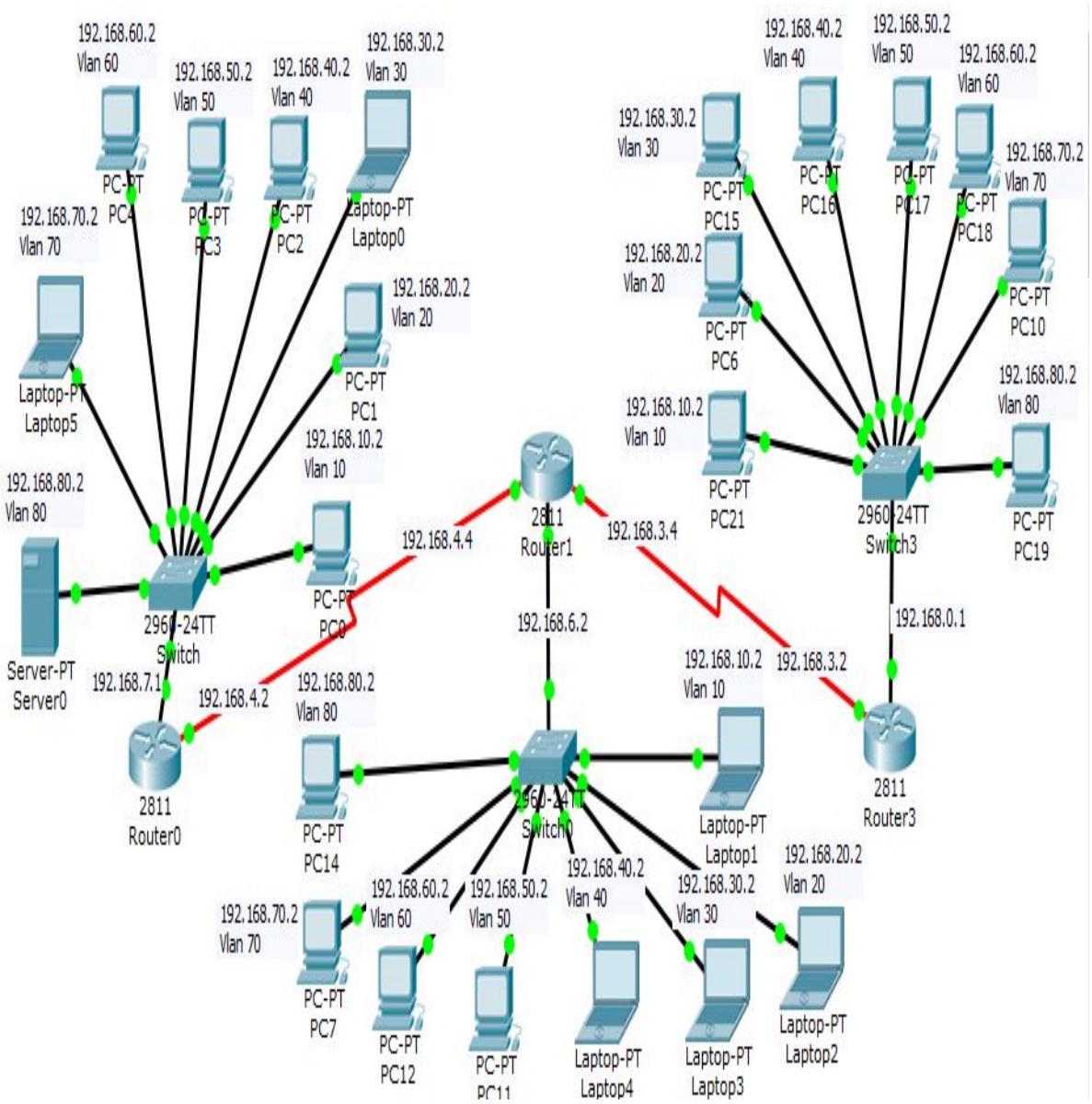


Fig.4.7 schema scenario 03

(03 Routeurs / 03 Switch / 08 Stations X 3 ➔ 24 Stations)

4.5.2 Configuration ET discussion des résultat scenario 03:

1. Configuration Switch 3(Switch Droite)

==========Création des différents Vlans ==========

```
Switch>ena
Switch#conf t
Switch(config)#vlan 10
```

Switch(config-vlan)#name a

Switch(config-vlan)#vlan 20

Switch(config-vlan)#name b

Switch(config-vlan)#vlan 30

Switch(config-vlan)#name c

Switch(config-vlan)#vlan 40

Switch(config-vlan)#name d

Switch(config-vlan)#vlan 50

Switch(config-vlan)#name e

Switch(config-vlan)#vlan 60

Switch(config-vlan)#name f

Switch(config-vlan)#vlan 70

Switch(config-vlan)#name i

Switch(config-vlan)#vlan 80

Switch(config-vlan)#name j

==========Affectation des Vlans aux différent Ports==========

Switch(config-vlan)#int f0/1

Switch(config-if)#switchport mode acc

Switch(config-if)#switchport acc vlan 10

Switch(config-if)#int f0/2

Switch(config-if)#switchport mode acc

Switch(config-if)#switchport acc vlan 20

Switch(config-if)#int f0/3

Switch(config-if)#switchport mode acc

Switch(config-if)#switchport acc vlan 30

Switch(config-if)#int f0/4

Switch(config-if)#switchport mode acc

Switch(config-if)#switchport acc vlan 40

Switch(config-if)#int f0/5

Switch(config-if)#switchport mode acc

Switch(config-if)#switchport acc vlan 50

Switch(config-if)#int f0/6

Switch(config-if)#switchport mode acc

Switch(config-if)#switchport acc vlan 60
Switch(config-if)#int f0/7
Switch(config-if)#switchport mode acc
Switch(config-if)#switchport acc vlan 70
Switch(config-if)#int f0/8
Switch(config-if)#switchport mode acc
Switch(config-if)#switchport acc vlan 80

2) **Création du port Trunk pour l'ensemble des Vlans dans le Switch SW3 :**

A partir du port FastEthernet0/9 qui y est entre le Switch et le routeur on peut créer le port Trunk qui donne la permission aux différents machines pour se communiquent entre eux (Les ports sélectionnés pour l'agrégation)avec les lignes commandes Ci-dessous :

SW3#configure terminal
SW3(config)#interface FastEthernet0/9
SW3(config-if)#switchport mode trunk
SW3(config-if)#switchport trunk allowed vlan 10,20,30,40,50,60,70,80
SW3(config-if)#exit
SW3(config)#

3) **Configuration Switch 2(Switch Milieu)**

==========Création des différents Vlans ==========

Switch>ena
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#name a
Switch(config-vlan)#vlan 20
Switch(config-vlan)#name b
Switch(config-vlan)#vlan 30
Switch(config-vlan)#name c
Switch(config-vlan)#vlan 40

Switch(config-vlan)#name d

Switch(config-vlan)#vlan 50

Switch(config-vlan)#name e

Switch(config-vlan)#vlan 60

Switch(config-vlan)#name f

Switch(config-vlan)#vlan 70

Switch(config-vlan)#name i

Switch(config-vlan)#vlan 80

Switch(config-vlan)#name j

==========Affectation des Vlans aux différent Ports==========

Switch(config-vlan)#interface fastEthernet0/1

Switch(config-if)#switchport mode access

Switch(config-if)#switchport access vlan 10

Switch(config-if)#interface fastEthernet0/2

Switch(config-if)#switchport mode access

Switch(config-if)#switchport access vlan 20

Switch(config-if)#interface fastEthernet0/3

Switch(config-if)#switchport mode access

Switch(config-if)#switchport access vlan 30

Switch(config-if)#interface fastEthernet0/4

Switch(config-if)#switchport mode access

Switch(config-if)#switchport access vlan 40

Switch(config-if)#interface fastEthernet0/5

Switch(config-if)#switchport mode access

Switch(config-if)#switchport access vlan 50

Switch(config-if)#interface fastEthernet0/6

Switch(config-if)#switchport mode access

Switch(config-if)#switchport access vlan 60

Switch(config-if)#interface fastEthernet0/7

Switch(config-if)#switchport mode access

Switch(config-if)#switchport access vlan 70

Switch(config-if)#interface fastEthernet0/8

Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 8

4) Création du port Trunk pour l'ensemble des Vlans dans le Switch SW2 (Switch Milieu) :

A partir du port FastEthernet0/9 qui y est entre le Switch et le routeur on peut créer le port Trunk qui donne la permission aux différents machines pour se communiquent entre eux (Les ports sélectionnés pour l'agrégation)avec les lignes commandes Ci-dessous :

SW2#configure terminal
SW2(config)#interface FastEthernet0/9
SW2(config-if)#switchport mode trunk
SW2(config-if)#switchport trunk allowed vlan 10,20,30,40,50,60,70,80

5) Configuration Switch 1(Switch Gauche)

==========Création des différents Vlans ==========
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#name a
Switch(config-vlan)#vlan 20
Switch(config-vlan)#name b
Switch(config-vlan)#vlan 30
Switch(config-vlan)#name c
Switch(config-vlan)#vlan 40
Switch(config-vlan)#name d
Switch(config-vlan)#vlan 50
Switch(config-vlan)#name e
Switch(config-vlan)#vlan 60
Switch(config-vlan)#name f
Switch(config-vlan)#vlan 70
Switch(config-vlan)#name i

Switch(config-vlan)#vlan 80

Switch(config-vlan)#name j

==========Affectation des Vlans aux différent Ports==========

Switch(config-vlan)#interface fastEthernet0/1

Switch(config-if)#switchport mode access

Switch(config-if)#switchport access vlan 10

Switch(config-if)#interface fastEthernet0/2

Switch(config-if)#switchport mode access

Switch(config-if)#switchport access vlan 20

Switch(config-if)#interface fastEthernet0/3

Switch(config-if)#switchport mode access

Switch(config-if)#switchport access vlan 30

Switch(config-if)#interface fastEthernet0/4

Switch(config-if)#switchport mode access

Switch(config-if)#switchport access vlan 40

Switch(config-if)#interface fastEthernet0/5

Switch(config-if)#switchport mode access

Switch(config-if)#switchport access vlan 50

Switch(config-if)#interface fastEthernet0/6

Switch(config-if)#switchport mode access

Switch(config-if)#switchport access vlan 60

Switch(config-if)#interface fastEthernet0/7

Switch(config-if)#switchport mode access

Switch(config-if)#switchport access vlan 70

Switch(config-if)#interface fastEthernet0/8

Switch(config-if)#switchport mode access

Switch(config-if)#switchport access vlan 80

6) **Création du port Trunk pour l'ensemble des Vlans dans le Switch SW1 (Switch Gauche) :**

A partir du port FastEthernet0/9 qui y est entre le Switch et le routeur on peut créer le port Trunk qui donne la permission aux différents machines pour se communiquent entre eux (Les ports sélectionnés pour l'agrégation)avec les lignes commandes Ci-dessous :

SW1#configure terminal
SW1(config)#interface FastEthernet0/9
SW1(config-if)#switchport mode trunk
SW1(config-if)#switchport trunk allowed vlan 10,20,30,40,50,60,70,80

7) Configuration du protocole (RIP) Routing Information Protocol :

La configuration du protocole (RIP) couramment utilisépour donner la permission aux différentes stations pour qu'ils communiquent entre eux librement dans le réseau, comme nous pouvons interdire ou empêché un sous réseau qui y est constitués de (quelques stations) pour qu'ils restent en contacte bien sûr via des Vlans crées précédemment.

==========Router 3Droite ==========

il y a deux IP qui rentrent dans le router
-I- IP serial : 192.168.3.2
-2- IP qui vient de Switch : 192.168.0.1

Alors on configure le Router Gauche via le CLI (Command Line Interface)
On aura :

Router 0>
Router 0>enable
Router 0#configure terminal
Router 0(config)#router rip
Router 0(config-router)#network 192.168.3.2
Router 0(config-router)#network 192.168.0.1

8) Affectation des Sub-adresses IP pour chaque station dans le routeur RT1 pour l'adresse du port FastEthernet0/ :

On diffuse les Sub-adresses IP de chaque station dans le routeur pour le port FastEthernet0/, pour que les différentes machines peuvent se communiquent entre eux avec cette méthode et via l'adresse IP de chaque machine dans le routeur (car elle seront identifiés par leurs adresses IP dans le routeur).

```
Router>ena
Router#configure terminal
Router(config)#hostname RT1
RT1(config)#interface FastEthernet0/0.10
RT1(config-subif)#encapsulation dot1Q 10
RT1(config-subif)#ip address 192.168.10.1 255.255.255.0

RT1(config)#interface FastEthernet0/0.20
RT1(config-subif)#encapsulation dot1Q 20
RT1(config-subif)#ip address 192.168.20.1 255.255.255.0

RT1(config)#interface FastEthernet0/0.30
RT1(config-subif)#encapsulation dot1Q 30
RT1(config-subif)#ip address 192.168.30.1 255.255.255.0

RT1(config)#interface FastEthernet0/0.40
RT1(config-subif)#encapsulation dot1Q 40
RT1(config-subif)#ip address 192.168.40.1 255.255.255.0


RT1(config)#interface FastEthernet0/0.50
RT1(config-subif)#encapsulation dot1Q 50
RT1(config-subif)#ip address 192.168.50.1 255.255.255.0

RT1(config)#interface FastEthernet0/0.60
RT1(config-subif)#encapsulation dot1Q 60
RT1(config-subif)#ip address 192.168.60.1 255.255.255.0

RT1(config)#interface FastEthernet0/0.70
RT1(config-subif)#encapsulation dot1Q 70
RT1(config-subif)#ip address 192.168.70.1 255.255.255.0
```

RT1(config)#interface FastEthernet0/0.80

RT1(config-subif)#encapsulation dot1Q 80

RT1(config-subif)#ip address 192.168.80.1 255.255.255.0

==========Router 1Milieu ==========

il y a deux IP qui rentrent dans le router

-I- IP serial 1: 192.168.3.4

-2- IP serial 2 : 192.168.4.4

-3- IP Switch : 192.168.6.2

Alors on configure le Router Gauche via le CLI (Command Line Interface)

On aura :

Router 0>

Router 0> enable

Router 0#configure terminal

Router 0(config)#router rip

Router 0(config-router)#network 192.168.3.4

Router 0(config-router)#network 192.168.4.4

Router 0(config-router)#network 192.168.6.2

---

9) Affectation des Sub-adresses IP pour chaque station dans le routeur RT1 pour l'adresse du port FastEthernet0/ :

On diffuse les Sub-adresses IP de chaque station dans le routeur pour le port FastEthernet0/, pour que les différentes machines peuvent se communiquent entre eux avec cette méthode et via l'adresse IP de chaque machine dans le routeur (car elle seront identifiés par leurs adresses IP dans le routeur).

Router>ena

Router#configure terminal

Router(config)#hostname RT1

RT1(config)#interface FastEthernet0/0.10

RT1(config-subif)#encapsulation dot1Q 10
RT1(config-subif)#ip address 192.168.10.1 255.255.255.0

RT1(config)#interface FastEthernet0/0.20
RT1(config-subif)#encapsulation dot1Q 20
RT1(config-subif)#ip address 192.168.20.1 255.255.255.0

RT1(config)#interface FastEthernet0/0.30
RT1(config-subif)#encapsulation dot1Q 30
RT1(config-subif)#ip address 192.168.30.1 255.255.255.0

RT1(config)#interface FastEthernet0/0.40
RT1(config-subif)#encapsulation dot1Q 40
RT1(config-subif)#ip address 192.168.40.1 255.255.255.0

RT1(config)#interface FastEthernet0/0.50
RT1(config-subif)#encapsulation dot1Q 50
RT1(config-subif)#ip address 192.168.50.1 255.255.255.0

RT1(config)#interface FastEthernet0/0.60
RT1(config-subif)#encapsulation dot1Q 60
RT1(config-subif)#ip address 192.168.60.1 255.255.255.0

RT1(config)#interface FastEthernet0/0.70
RT1(config-subif)#encapsulation dot1Q 70
RT1(config-subif)#ip address 192.168.70.1 255.255.255.0

RT1(config)#interface FastEthernet0/0.80
RT1(config-subif)#encapsulation dot1Q 80
RT1(config-subif)#ip address 192.168.80.1 255.255.255.0

==========Router 0 Gauche==========

il y a deux IP qui rentrent dans le router

-I- IP serial : 192.168.4.2

-2- IP qui vient de Switch : 192.168.7.1

Alors on configure le Router Gauche via le CLI (Command Line Interface)

On aura :

Router 0>

Router 0> enable

Router 0#configure terminal

Router 0(config)#router rip

Router 0(config-router)#network 192.168.4.2

Router 0(config-router)#network 192.168.7.1

10) Affectation des Sub-adresses IP pour chaque station dans le routeur RT1 pour l'adresse du port FastEthernet0/ :

On diffuse les Sub-adresses IP de chaque station dans le routeur pour le port FastEthernet0/, pour que les différentes machines peuvent se communiquent entre eux avec cette méthode et via l'adresse IP de chaque machine dans le routeur (car elle seront identifiés par leurs adresses IP dans le routeur).

Router>ena

Router#configure terminal

Router(config)#hostname RT1

RT1(config)#interface FastEthernet0/0.10

RT1(config-subif)#encapsulation dot1Q 10

RT1(config-subif)#ip address 192.168.10.1 255.255.255.0

RT1(config)#interface FastEthernet0/0.20

RT1(config-subif)#encapsulation dot1Q 20

RT1(config-subif)#ip address 192.168.20.1 255.255.255.0

RT1(config)#interface FastEthernet0/0.30

RT1(config-subif)#encapsulation dot1Q 30

RT1(config-subif)#ip address 192.168.30.1 255.255.255.0

RT1(config)#interface FastEthernet0/0.40

RT1(config-subif)#encapsulation dot1Q 40

RT1(config-subif)#ip address 192.168.40.1 255.255.255.0

RT1(config)#interface FastEthernet0/0.50

RT1(config-subif)#encapsulation dot1Q 50

RT1(config-subif)#ip address 192.168.50.1 255.255.255.0

RT1(config)#interface FastEthernet0/0.60
RT1(config-subif)#encapsulation dot1Q 60
RT1(config-subif)#ip address 192.168.60.1 255.255.255.0

RT1(config)#interface FastEthernet0/0.70
RT1(config-subif)#encapsulation dot1Q 70
RT1(config-subif)#ip address 192.168.70.1 255.255.255.0

RT1(config)#interface FastEthernet0/0.80
RT1(config-subif)#encapsulation dot1Q 80
RT1(config-subif)#ip address 192.168.80.1 255.255.255.0

4.6 Avantages et inconvénients du réseau N° 01 (01 Router + 01 Switch) à base des Vlans:

- **L'avantage** de l'utilisation et l'application des Vlans dans un réseau constitué d'un seul Router et un seul Switch réside dans la capacité des PC connectés qui ne dépasse pas la capacité des ports constituant le switchet dans la facilité du control de ce réseauavec des adresses IP différentes et c'est robuste à contrôlésainsi rapide.

- **L'inconvénient**de l'utilisation et l'application des Vlans dans un réseau constitué d'un seul Router et un seul Switch est lié avec le nombre de PC connectés aux différents ports de switch est bien sûr qui ne dépasse pas 24 PC, pour la simple raison qui sont égale aux nombres de ports de ce switch

4.7 Avantages et inconvénients du réseau N° 02 (01 Router + 03 Switch) à base des Vlans:

- **L'avantage** de l'utilisation et l'application des Vlans dans un réseau constitué d'un seul Router et trois (03) Switchvia des Vlans est basé réellement sur le nombre des Vlans crées

dans chaque Switch constituant ce réseau et quand il s'agit d'utilisé un nombre de PC supérieur à 24 dans un réseau, on ajoute plus de Switch pour augmenter la capacité de PC qui seront utile pour ce réseau.

- **L'inconvénient**de l'utilisation et l'application des Vlans dans un réseau constitué d'un seul Router et trois (03) Switch via des Vlans est lié sur la mal gérance ainsi la difficulté de contrôle de ce réseau avec des adresses IP différentes pour chaque sous réseau, est cela bien sûr est due aux autres Switch auxiliaire ajoutés au Switch de base qui y est relié directement au router pour la raison de faire augmenter le nombre de PC, et d'une autre coté grâce aux messages de broadcaste et bien sûr cela rendre la connexion entre les PC difficile à contrôler et lente.

4.8 Avantages et inconvénients du réseau N° 03 (03 Router + 03 Switch) à base des Vlans:

- **L'avantage** de l'utilisation et l'application des Vlans dans un réseau constitué d'un trois Router et trois (03) Switch via des Vlans est basé sur le bon fonctionnement de la connexion entre les différents PC avec des adresses IP différentes et leurs Vlans créent dans chaque Switch, ainsi le bon contrôle et la bonne gestion de la connexion entre les PC malgré le nombre supérieur utilisés dans chaque Switch constituant le réseau.

- **L'inconvénient**de l'utilisation et l'application des Vlans dans un réseau constitué de trois Router et trois (03) Switch via des Vlans est basé seulement sur la sécurité du réseau qui n'est pas assuré jusqu'à l'instant…et ce qu'on va le prouvé dans le schéma qui suit cette partie.

4.9 Les solutions pour optimiser la sécurité du réseau :

- **Contrôle des points d'accèsInternet :**
  Les points d'accès Internet constituent un passage potentiel pour les pirates informatiques pour accéder au système informatique d'unréseau. Ainsi, pour renforcer la sécurité informatique du site notamment sur un réseau multi sites, il est fortement recommandé de limiter au maximum le nombre d'utilisateurs. Effectivement, actuellement, il est difficile, voire impossible, d'interdire d'autre PC à l'accès à Internet. Toutefois, des

limitations peuvent être installées notamment grâce à des solutions de pare-feu. Cette solution permet de filtrer le contenu échangé sur Internet et bloquer ainsi les contenus ainsi que les serveurs douteux en se fondant sur une liste de sites régulièrement mis à jour.

- **Sauvegarde des données :**

  Les données stockées sur des serveurs extérieurs doivent être synchronisées au moins une fois par jour. Le plus souvent, les professionnels optent pour une délocalisation des données en les stockant à distance via une liaison par fibre directe vers un hébergeur. Pour cela, il faut les compétences d'un intégrateur d'infrastructure informatique IT. Ce dernier apporte à l'entreprise les solutions nécessaires afin d'assurer la protection de ses données stockées, et afin d'améliorer la performance de son infrastructure informatique. Faire appel à un professionnel lui permet de se prémunir des défaillances de son système d'information. Ainsi, en cas de souci, le professionnel peut facilement procéder à une restauration des données de réseau afin de préserver son activité et sa productivité.

- **Installation d'outils de surveillance :**

  Pour se prémunir d'une intrusion dans l'enceinte de réseau, la surveillance de l'accès doit être suivie en continu. C'est aussi valable pour le point d'accès au réseau. L'installation d'un antivirus apte à analyser les supports amovibles ainsi que les ordinateurs portables figure parmi les solutions les plus classiques. Nombreuses sont aussi les sociétés qui optent pour la tenue d'un journal de connexion. Mais, il est aussi possible de miser sur un anti-spywares et d'un anti-spam afin de filtrer les courriels en réseau. Enfin, l'installation d'un Réseau Privé Virtuel permet aussi aux professionnels de ne pas laisser sur le web des informations cruciales sur le réseau.

4.10 SIMULATION (scenario 04):

4.10.1 Tableau Récapitulatif (4.4) du réseau:

(03 Routeur / 03 Switch / 06 Stations / 04 Laptop/Sever/Printer)

Stations	Adresse IP	Masque Réseau	Ports	Vlans	Switch	Routeur	Point D'accès
Laptop 0	192.168.20.2	255.255.255.0	F0/1	Vlan 20	2960-24TT	2811	Access Point 1
Laptop 01	192.168.120.2	255.255.255.0	F0/2	Vlan 120	2960-24TT	2811	Access Point 5
Laptop 02	192.168.30.2	255.255.255.0	F0/3	Vlan 30	2960-24TT	2811	Access Point 0
Laptop 03	192.168.130.2	255.255.255.0	F0/4	Vlan 130	2960-24TT	2811	Access Point 6
Server PT 0	192.168.40.2	255.255.255.0	F0/5	Vlan 40	2960-24TT	2811	--
Printer PT 0	192.168.50.2	255.255.255.0	F0/6	Vlan 50	2960-24TT	2811	--
PC 0	192.168.60.2	255.255.255.0	F0/8	Vlan 60	2960-24TT	2811	--
PC 01	192.168.70.2	255.255.255.0	F0/9	Vlan 70	2960-24TT	2811	--
PC 02	192.168.80.2	255.255.255.0	F0/10	Vlan 80	2960-24TT	2811	--
PC 03	192.168.90.2	255.255.255.0	F0/11	Vlan 90	2960-24TT	2811	--
PC 04	192.168.100.2	255.255.255.0	F0/12	Vlan 100	2960-24TT	2811	--
PC 05	192.168.110.2	255.255.255.0	F0/13	Vlan 110	2960-24TT	2811	--

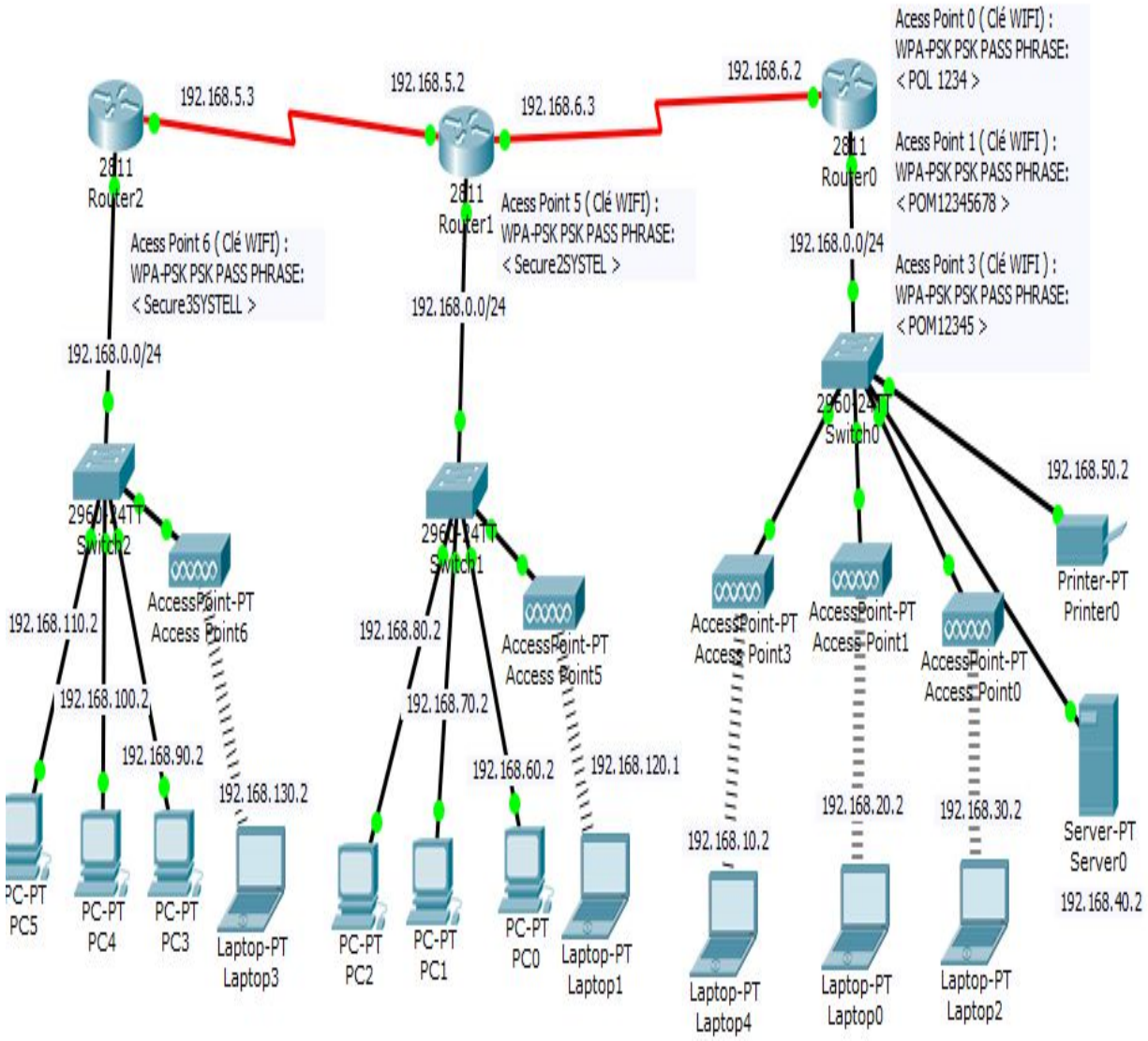


Fig.4.8 schéma scenario 04

(03 Routeur / 03 Switch / 06 Stations / 04 Laptop/Sever/Printer)

4.10.2 Configuration ET discussion des résultat scenario 04:

1) Configuration Switch 3 (Switch Droite)

==========Création des différents Vlans ==========

Switch>ena

Switch#conf t

Switch(config)#vlan 10

Switch(config-vlan)#name a

Switch(config-vlan)#vlan 20

Switch(config-vlan)#name b
Switch(config-vlan)#vlan 30
Switch(config-vlan)#name c
Switch(config-vlan)#vlan 40
Switch(config-vlan)#name d
Switch(config-vlan)#vlan 50
Switch(config-vlan)#name e

==========Affectation des Vlans aux différent Ports==========

Switch(config-vlan)#int f0/1
Switch(config-if)#switchport mode acc
Switch(config-if)#switchport acc vlan 10
Switch(config-if)#int f0/2
Switch(config-if)#switchport mode acc
Switch(config-if)#switchport acc vlan 20
Switch(config-if)#int f0/3
Switch(config-if)#switchport mode acc
Switch(config-if)#switchport acc vlan 30
Switch(config-if)#int f0/4
Switch(config-if)#switchport mode acc
Switch(config-if)#switchport acc vlan 40
Switch(config-if)#int f0/5
Switch(config-if)#switchport mode acc
Switch(config-if)#switchport acc vlan 50

2) **Création du port Trunk pour l'ensemble des Vlans dans le Switch SW0 :**

A partir du port FastEthernet0/9 qui y est entre le Switch et le routeur on peut créer le port Trunk qui donne la permission aux différents machines pour se communiquent entre eux (Les ports sélectionnés pour l'agrégation)avec les lignes commandes Ci-dessous :

SW0#configure terminal
SW0(config)#interface FastEthernet0/9
SW0(config-if)#switchport mode trunk

SW0(config-if)#switchport trunk allowed vlan 10,20,30,40,50

SW0(config-if)#exit

SW0(config)#

3) Configuration Switch 2(Switch Milieu)

==========Création des différents Vlans ==========

Switch>ena

Switch#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)#vlan 60

Switch(config-vlan)#name a

Switch(config-vlan)#vlan 70

Switch(config-vlan)#name b

Switch(config-vlan)#vlan 80

Switch(config-vlan)#name c

Switch(config-vlan)#vlan 120

Switch(config-vlan)#name e

==========Affectation des Vlans aux différent Ports==========

Switch(config-vlan)#interface fastEthernet0/1

Switch(config-if)#switchport mode access

Switch(config-if)#switchport access vlan 60

Switch(config-if)#interface fastEthernet0/2

Switch(config-if)#switchport mode access

Switch(config-if)#switchport access vlan 70

Switch(config-if)#interface fastEthernet0/3

Switch(config-if)#switchport mode access

Switch(config-if)#switchport access vlan 80

Switch(config-if)#interface fastEthernet0/4

Switch(config-if)#switchport mode access

Switch(config-if)#switchport access vlan 120

4) Création du port Trunk pour l'ensemble des Vlans dans le Switch SW1 (Switch Milieu) :

A partir du port FastEthernet0/9 qui y est entre le Switch et le routeur on peut créer le port Trunk qui donne la permission aux différents machines pour se communiquent entre eux (Les ports sélectionnés pour l'agrégation)avec les lignes commandes Ci-dessous :

```
SW1#configure terminal
SW1(config)#interface FastEthernet0/9
SW1(config-if)#switchport mode trunk
SW1(config-if)#switchport trunk allowed vlan 60,70,80,120
```

5) Configuration Switch 1 (Switch Gauche)

```
==============Création des différents Vlans ============================
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 90
Switch(config-vlan)#name a
Switch(config-vlan)#vlan 100
Switch(config-vlan)#name b
Switch(config-vlan)#vlan 110
Switch(config-vlan)#name c
Switch(config-vlan)#vlan 130
Switch(config-vlan)#name d
==========================Affectation des Vlans aux différent
Ports================
Switch(config-vlan)#interface fastEthernet0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 90
Switch(config-if)#interface fastEthernet0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 100
Switch(config-if)#interface fastEthernet0/3
Switch(config-if)#switchport mode access
```

Switch(config-if)#switchport access vlan 110
Switch(config-if)#interface fastEthernet0/4
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 130

6) **Création du port Trunk pour l'ensemble des Vlans dans le Switch SW2 (Switch Gauche) :**

A partir du port FastEthernet0/9 qui y est entre le Switch et le routeur on peut créer le port Trunk qui donne la permission aux différents machines pour se communiquent entre eux (Les ports sélectionnés pour l'agrégation)avec les lignes commandes Ci-dessous :

SW2#configure terminal
SW2(config)#interface FastEthernet0/9
SW2(config-if)#switchport mode trunk
SW2(config-if)#switchport trunk allowed vlan 90,100,110,130

7) **Configuration du protocole (RIP) Routing Information Protocol :**

La configuration du protocole (RIP) couramment utilisépour donner la permission aux différentes stations pour qu'ils communiquent entre eux librement dans le réseau, comme nous pouvons interdire ou empêché un sous réseau qui y est constitués de (quelques stations) pour qu'ils restent en contacte bien sûr via des Vlans crées précédemment.

==========Router 3Droite ==========

il y a deux IP qui rentrent dans le router
-I- IP serial : 192.168.6.2
-2- IP qui vient de Switch : 192.168.0.1
Alors on configure le Router Gauche via le CLI (Command Line Interface)
On aura :
Router 0>
Router 0>enable
Router 0#configure terminal
Router 0(config)#router rip
Router 0(config-router)#network 192.168.6.2

Router 0(config-router)#network 192.168.0.1

Router 0(config-router)#network 192.168.10.2

Router 0(config-router)#network 192.168.20.1

Router 0(config-router)#network 192.168.30.1

Router 0(config-router)#network 192.168.40.1

Router 0(config-router)#network 192.168.50.1

Router 0(config-router)#network 192.168.0.1

8) Affectation des Sub-adresses IP pour chaque station dans le routeur RT0 pour l'adresse du port FastEthernet0/ :

On diffuse les Sub-adresses IP de chaque station dans le routeur pour le port FastEthernet0/, pour que les différentes machines peuvent se communiquent entre eux avec cette méthode et via l'adresse IP de chaque machine dans le routeur (car elle seront identifiés par leurs adresses IP dans le routeur).

Router>ena

Router#configure terminal

Router(config)#hostname RT1

RT1(config)#interface FastEthernet0/0.10

RT1(config-subif)#encapsulation dot1Q 10

RT1(config-subif)#ip address 192.168.10.2 255.255.255.0

RT1(config)#interface FastEthernet0/0.20

RT1(config-subif)#encapsulation dot1Q 20

RT1(config-subif)#ip address 192.168.20.2 255.255.255.0

RT1(config)#interface FastEthernet0/0.30

RT1(config-subif)#encapsulation dot1Q 30

RT1(config-subif)#ip address 192.168.30.2 255.255.255.0

RT1(config)#interface FastEthernet0/0.40

RT1(config-subif)#encapsulation dot1Q 40

RT1(config-subif)#ip address 192.168.40.2 255.255.255.0

RT1(config)#interface FastEthernet0/0.50

RT1(config-subif)#encapsulation dot1Q 50

RT1(config-subif)#ip address 192.168.50.2 255.255.255.0

==========Router 1Milieu ==========

il y a deux IP qui rentrent dans le router

-I- IP serial 1: 192.168.6.3

-2- IP serial 2 : 192.168.5.2

-3- IP Switch : 192.168.0.1

Alors on configure le Router Gauche via le CLI (Command Line Interface)

On aura :

Router 0> jj

Router 0> enable

Router 0#configure terminal

Router 0(config)#router rip

Router 0(config-router)#network 192.168.6.3

Router 0(config-router)#network 192.168.5.2

Router 0(config-router)#network 192.168.0.1

Router 0(config-router)#network 192.168.60.2

Router 0(config-router)#network 192.168.70.2

Router 0(config-router)#network 192.168.80.2

Router 0(config-router)#network 192.168.120.2

---

9) Affectation des Sub-adresses IP pour chaque station dans le routeur RT1 pour l'adresse du port FastEthernet0/ :

On diffuse les Sub-adresses IP de chaque station dans le routeur pour le port FastEthernet0/, pour que les différentes machines peuvent se communiquent entre eux avec cette méthode et via l'adresse IP de chaque machine dans le routeur (car elle seront identifiés par leurs adresses IP dans le routeur).

Router>ena

Router#configure terminal

Router(config)#hostname RT2

RT2(config)#interface FastEthernet0/0.60

RT2(config-subif)#encapsulation dot1Q 60
RT2(config-subif)#ip address 192.168.60.2 255.255.255.0

RT2(config)#interface FastEthernet0/0.70
RT2(config-subif)#encapsulation dot1Q 70
RT2(config-subif)#ip address 192.168.70.2 255.255.255.0

RT2(config)#interface FastEthernet0/0.80
RT2(config-subif)#encapsulation dot1Q 80
RT2(config-subif)#ip address 192.168.80.2 255.255.255.0

RT2(config)#interface FastEthernet0/0.120
RT2(config-subif)#encapsulation dot1Q 120
RT2(config-subif)#ip address 192.168.120.2 255.255.255.0

==========Router 0 Gauche ==========

il y a deux IP qui rentrent dans le router

-I- IP serial : 192.168.5.3
-2- IP qui vient de Switch : 192.168.0.1

Alors on configure le Router Gauche via le CLI (Command Line Interface)
On aura :

Router 0>
Router 0> enable
Router 0#configure terminal
Router 0(config)#router rip
Router 0(config-router)#network 192.168.5.3
Router 0(config-router)#network 192.168.0.1
Router 0(config-router)#network 192.168.90.2
Router 0(config-router)#network 192.168.100.2
Router 0(config-router)#network 192.168.110.2
Router 0(config-router)#network 192.168.130.2

10) Affectation des Sub-adresses IP pour chaque station dans le routeur RT2 pour l'adresse du port FastEthernet0/ :

On diffuse les Sub-adresses IP de chaque station dans le routeur pour le port FastEthernet0/, pour que les différentes machines peuvent se communiquent entre eux avec cette méthode et via l'adresse IP de chaque machine dans le routeur (car elle seront identifiés par leurs adresses IP dans le routeur).

```
Router>ena
Router#configure terminal
Router(config)#hostname RT3
RT3(config)#interface FastEthernet0/0.90
RT3(config-subif)#encapsulation dot1Q 90
RT3(config-subif)#ip address 192.168.90.2 255.255.255.0

RT3(config)#interface FastEthernet0/0.100
RT3(config-subif)#encapsulation dot1Q 100
RT3(config-subif)#ip address 192.168.100.2 255.255.255.0

RT3(config)#interface FastEthernet0/0.110
RT3(config-subif)#encapsulation dot1Q 110
RT3(config-subif)#ip address 192.168.110.2 255.255.255.0

RT3(config)#interface FastEthernet0/0.130
RT3(config-subif)#encapsulation dot1Q 130
RT3(config-subif)#ip address 192.168.130.2 255.255.255.0
```

4.11 Conclusion :

À travers ce chapitre nous avons illustrer notre solution retenue que nous l'avons justifier après discussion de 03 différents scénario.

Nous avons configuré les équipements utilisés avec le du simulateur « Cisco Packet Tracer » et nous avons avons effectué un ensemble de tests, de validation et vérification pour chaque scénario afin de prouver l'efficacité de notre solution retenue.

Conclusion générale :

Dans notre travail, nous avons abordé les généralités sur les réseaux locaux virtuels notamment, leurs différents types et leurs utilités, ainsi quelques protocoles d'administration et de gestion qu'on a implémentée sur notre architecture réseau.

En effet, nous avons constaté l'intérêt majeur que joue les VLANs, dans l'amélioration de la qualité de transmission d'information et plus de souplesse dans l'administration d'un réseau local.

Ce travail a fait l'objet d'une expérience intéressante, et a eu énormément d'apport sur nos connaissances et nos compétences en terme de configuration dans un environnement ***Cisco***.

De Plus, nous avons enrichi nos connaissances déjà acquises dans la segmentation des réseaux locaux d'entreprises en VLANs. Enfin, pour augmenter la disponibilité et la fiabilité du réseau, Il est nécessaire, pour l'entreprise de prendre en compte notre solution retenue.

Bliographie :

[1] Ecole Informatique, et al. “Articles - Étudiants SUPINFO.” Classification Des Réseaux Informatiques | SUPINFO, École Supérieure D'Informatique, www.supinfo.com/articles/single/5709-classification-reseaux-informatiques

[2] “What Is a Protocol Data Unit (PDU) - May 19, 2020. https://fr.scribd.com/document/396336983/Chap-7-La-Couche-Transport-Du-Modele-OSI-Copie

[3] pro, TECHNOLOGUE. “Le Modele De Reference OSI.” Le Modele De Reference OSI : LA COUCHE APPLICATION : NIVEAU 7 https://tvaira.free.fr/btssn/reseaux/cours/courreseauxenerlites.pdf

[4] “Articles.” Gralon, www.gralon.net/articles/internet-et-webmaster/logiciel/article-le-protocole-tcp-ip---presentation-et-fonctionnement-1597.htm

[5] Hersent, Olivier, et al. IP Telephony Deploying Voice-over-IP Protocols. J. Wiley, 200

[6] Les Avantages Et Les Inconvénients Des VLANs. shmsprod.s3.amazonaws.com/media/editor/143832/Advantages_and_Disadvantages_of_VLANs.pdf

[7] “VLAN - Réseaux Virtuels.” CommentCaMarche, www.commentcamarche.net/contents/543-vlan-reseaux-virtuels

[8] Goffinet, François. “Configuration Des VLANs Sous Cisco IOS.” Cisco.goffin et.org, 21 Feb. 2020, https://www.clemanet.com/switch-vlan-cisco.php

[9] “Configurer Le Routage InterVLAN Sur Des Commutateurs De Niveau 3.” Cisco, Cisco, 31 Jan. 2020, https://fr.scribd.com/document/92077642/Routage-InterVLAN

[10] Dorigny, Mickael, Sawssen, Abdoulaye Bah, Geckoh, and Thibault. “Mise En Place De VLANs Et De Routage Inter-VLANs: Cisco: IT-Connect.” IT, March 25, 2014

https://www.it-connect.fr/mise-en-place-de-vlans-et-de-routage-inter-vlans/

[11] “Configuration Du Protocole VTP (VLAN Trunk Protocol).” Cisco, Cisco, 31 Jan. 2020,

https://www.memoireonline.com/04/10/3431/m_Etude-et-optimisation-du-reseau-local-de-inova-si7.html

[12] “Configurez Le Port Aux Configurations D'interface VLAN Sur Un Commutateur Par Le CLI.” Cisco. Cisco, February 26, 2020

https://www.it-connect.fr/mise-en-place-de-vlans-et-de-routage-inter-vlans/

[13]. “Configure InterVLAN Routing on Layer 3 Switches.”

Cisco. Cisco, April 21, 2020.

https://www.it-connect.fr/mise-en-place-de-vlans-et-de-routage-inter-vlans/

Annex :

ANNEXE 1

1 **Commande VTP**

Copyright (c) 1986-2005 by cisco Systems, Inc. Compiled Wed 18-May-05 22:31 by jharirba

Press RETURN to get started!

Switch>en

Switch#conf t

Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#host

Switch(config)#hostname SWITCH1

SWITCH1(config)#enable password password

SWITCH1(config)#exit

%SYS-5-CONFIG_I: Configured from console by console

SWITCH1#vlan database

% Warning: It is recommended to configure VLAN from config mode, as VLAN database mode is being deprecated. Please consult user documentation for configuring VTP/VLAN in config mode.

SWITCH1(vlan)#vtp server

Device mode already VTP SERVER.

SWITCH1(vlan)#vtp domain INOVA

Changing VTP domain name from NULL to INOVA SWITCH1(vlan)#vtp password

% Incomplete command.

SWITCH1(vlan)#vtp password password

Setting device VLAN database password to password SWITCH1(vlan

Annex 02

Commande vérification VTP (show vtp status**)**

```
WITCH1>en

Password:

SWITCH1#sh

SWITCH1#show vtp st

SWITCH1#show vtp status

VTP Version : 2

Configuration Revision : 0

Maximum VLANs supported locally : 255 Number of existing VLANs : 5

VTP Operating Mode : Server

VTP Domain Name : INOVA

VTP Pruning Mode : Disabled

VTP V2 Mode : Disabled

VTP Traps Generation : Disabled

MD5 digest : 0x88 0x17 0xD7 0xB4 0x58 0x41 0x97 0xB2

Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00

Local updater ID is 0.0.0.0 (no valid interface found)

SWITCH1#
```

Annex 03

Commande lien trunk

Press RETURN to get started!

Switch>en

Switch>enable

Switch#conf t

Switch#conf terminal

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)#int Switch(config)#interface fast

Switch(config)#interface fastEthernet 0/20

Switch(config-if)#swi Switch(config-if)#**switchport mode trunk**

Annex04

Commande pour associé le port d'un Switch à un vlan

Cisco Internetwork Operating System Software

IOS (tm) 950 Software (950-I6Q4L2-M), Version 12.1(22)EA4, RELEASE SOFTWARE(fc1)

Copyright (c) 1986-2005 by cisco Systems, Inc. Compiled Wed 18-May-05 22:31 by jharirba

Press RETURN to get started!

Switch>en

Switch#conf t

Switch#conf terminal

Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#inter

Switch(config)#interface fast

Switch(config)#interface fastEthernet 0/2

Switch(config-if)#swit

Switch(config-if)#**switchport mode access vlan**

Résumé :

Le dévellopement rapide de la technologie expose les professionnels à des risques de sécurité importante.

Ainsi, afin de protéger leurs données et leur réseau, les réseaux doivent déployer des solutions de sécurité afin de garantir leur intégrité. Différentes solutions peuvent actuellement être mises en place.

En effet dans un réseau local la communication entre les différentes machines est régie par l'architecture physique.

Grâce aux réseaux virtuels (VLANs) il est possible de s'affranchir des limitations de l'architecture physique (contraintes géographiques, contraintes d'adressage, ...) en définissant une segmentation logique (logicielle) basée sur un regroupement de machines grâce à des critères (adresses MAC, numéros de port, protocole, etc.).

Celle-ci nous permettra de définir à travers ces fonctionnalités, une meilleure planification du déploiement future.

Abstract :

The rapid development of technology exposes Professionals to significant security risks.

Thus, in order to protect their data and their network , networks must deploy security solutions to guarantee their integrity.

Different solutions can currently be implemented. In fact, in a local network, communication between the different machines is governed by the physical architecture.

Thanks to virtual networks (VLANs) it is possible to overcome the limitations of the physical architecture (geographic constraints, addressing constraints, etc.) by defining a logical (software) segmentation based on a grouping of machines thanks to criteria (MAC addresses, port numbers, protocol, etc.).

This will allow us to define, through these functionalities, a better planning of the future deployment

ملخص :

يؤدي التطور السريع للتكنولوجيا إلى تعريض المحترفين لمخاطر أمنية كبيرة.
وبالتالي ، من أجل حماية بياناتهم وشبكاتهم، يجب على الشبكات نشر حلول أمنية لضمان سلامتها. يمكن حاليا تنفيذ حلول مختلفة.

في الواقع ، في الشبكة المحلية ، يخضع الاتصال بين الأجهزة المختلفة للبنية المادية بفضل الشبكات الافتراضية (VLANs), من الممكن التغلب على قيود البنية المادية (القيود الجغرافية، وقيود المعالجة، وما إلى ذلك) من خلال تحديد تجزئة منطقية (برمجية) استنادًا إلى مجموعة من الأجهزة بفضل المعايير (عناوين MAC ، أرقام المنافذ ،البروتوكول ، إلخ).
سيتيح لنا ذلك تحديد - من خلال هذه الوظائف- تخطيطًا أفضل للانتشار المستقبلي.