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/2021

MEMOIRE DE FIN D'ETUDE DE MASTER ACADEMIQUE

Filière : Génie électrique
Spécialité : Télécommunication

Thème

Étude et simulation d'une architecture réseau mixte à base de la Solution Vlan et le protocole DHCP d'une plateforme VoIP

Présenté par :

Melle :Kheira BENAOUDA

Melle : Rachida BELGHOUL

Soutenu le -- / -- / 2021 devant le jury composé de :

Président de jury :	Mme MIMI MALIKA	Grade Pr	Université Abdelhamid Ibn Badis
Examinateur :	OULD MAMAR MADANI	Grade MCA	Université Abdelhamid Ibn Badis
L'encadreur :	RESFA ABBES	Grade MCB	Université Abdelhamid Ibn Badis

Année Universitaire : 2020 /2021

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 accepté 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 :

Je rends grâce à Dieu de m'avoir donné le courage et la volonté. Ainsi que la conscience d'avoir pu terminer mes études.

Je dédie ce modeste travail :

À mes très chères :

À celui qui m'a toujours appris comment réfléchir avant d'agir, à celui qui m'a soutenu tout au long de ma vie scolaire, à celui qui n'a jamais épargné un effort pour mon bien, mon cher père.

À celle qui est toujours à côté de mon cœur, à celle qui m'appris le vrai Sens de la vie, à celle qui n'a hésité aucun moment à m'encouragé Ma Chère mère.

A mes frères et ma sœur pour leur appui et leur encouragement.

A tous ma famille BENAOUDA et GOURINE ainsi qu'à mes amis ;

J'espère qu'ils trouveront dans ce travail toutes mes reconnaissances

Kheira

Dédicace

Je rends grâce à Dieu de m'avoir donné le courage et la volonté. Ainsi que la conscience d'avoir pu terminer mes études.

Je dédie ce modeste travail :

À mes très chères :

À celui qui m'a toujours appris comment réfléchir avant d'agir, à celui qui m'a soutenu tout au long de ma vie scolaire, à celui qui n'a jamais épargné un effort pour mon bien, mon cher père.

À celle qui est toujours à côté de mon cœur, à celle qui m'appris le vrai Sens de la vie, à celle qui n'a hésité aucun moment à m'encouragé Ma Chère mère.

A mes sœurs et mon frère : Naima, Fatima, Fadila; Touatia ;Houssin et mon petite cher Iyad

À ma grand-mère

A mon encadreur directeur de mémoire Docteur RESFA ABBES pour toutes ses conseils

et son aide jusqu'à la dernière minute, que Dieu la garde en bonne Santé ;

A touts mes amies les plus sincères surtout Fatima qui ma très aider à réaliser ce travaille et ma chère Ikram.

A mon binôme et cher amie Melle BENAOUDA Kheira ainsi que sa famille ;

A tous les enseignants et étudiants.

Atout mes collègues Et bien sûr à toute la famille "BELGHOUL " et à tous ceux que me connaît.

« RACHIDA »

Le sommaire

Liste des abréviations i
Liste des figures iii
Liste des tableaux iv

chapitre 01: Généralités sur les réseaux informatiques

1.1 Introduction 1
1.2 Types de réseaux 1
1.2.1 Réseaux locaux (LANs) 1
1.2.2 Réseaux étendus (WANs) 1
1.2.3 Réseaux métropolitains (MANs) 2
1.2.4 Personale Area Network (PAN) 3
1.3 Modèles de réseaux 3
1.3.1 Modèle OSI (Open System Interconnection) 3
1.3.2 Le modèle TCP/IP 4
1.4 L'adressage IP 5
1.4.1 Le protocole IP 5
1.4.2 Le format des adresses IP 5
1.4.3 Le format IPV4 5
1.4.4 Le masque réseau 5
1.4.5 Les classes des adresses IP 6
1.4.6 Adresses Spécifiques 6
1.4.7 Adresse privée 6
1.4.8 Adresse de diffusion 6
1.5 Les composantes physiques des réseaux locaux 7
1.5.1. La paire téléphonique torsadée 7
1.5.2. Les Types de blindages 7
1.5.2 Le câble coaxial 8
1.5.3 La fibre optique 8
1.5.3.1 Monomode 8
1.5.3.2 Multimode 8
1.6 Les connecteur 9
1.6.1. Les connecteurs BNC 9
1.6.2. Les connecteurs optiques 9
1.6.2.1 Connecteur SC 9

1.6.2.2. Connecteur LC 9
1.6.2.3. Connecteur FC 10
1.6.2.4. Connecteur ST 10
1.6.3. Les connecteurs RJ45 10
1.7.Les matériel d'interconnexions d'un réseau local 10
1.7.1. Les répéteurs 10
1.7.2. Les ponts 10
1.7.3. Les routeurs 11
1.7.4. Les passerelles 11
1.7.5. Les concentrateurs 11
1.7.6. Les autocommutateurs (PABX) 11
1.7.7. Adaptateur 11
1.8. Les topologies de base utilisées dans les réseaux 12
1.8.1. Topologie en bus 12
1.8.2. Topologie en étoile 12
1.8.3. Topologies en arbre 12
1.8.5. Topologie en anneau 13
1.8.6. Topologies maillée 13
1.9. conclusion 13

Chapitre 02 : Les réseaux VLANs

2.1 Introduction 15
2.2 Concepts VLAN 15
2.3 Intérêt à avoir des VLAN 16
2.4 Les propriétés offertes par les VLAN sont 16
2.5 Les avantages et les inconvénients des VLANs 16
2.6.La technique des VLANs 18
2.7.Méthodes d'implantation des VLANs 18
2.7.1. VLAN de niveau 1 ou VLAN par port 18
2.7.2. VLAN de niveau 2 ou VLAN MAC 18
2.7.3 VLAN de niveau 3 ou VLAN d'adresses réseaux 19
2.8 Principe de fonctionnement de VLANs 19
2.8.1 L'étiquetage 19
2.8.2 La trame Ethernet classique 20
2.8.3 La trame Ethernet 802.1q 20
2.9 Le Protocol ISL (Inter Switch Link Protocol) 20
2.10 La notion des trunks 22
2.11. Types de VLAN 22

2.11.1VLAN de données 22
2.11.2. VLAN par défaut 22
2.11.4. VLAN de gestion 23
2.12 Protocoles de transport des VLANs 23
2.12.1 VTP (Virtual Trunking Protocol) 23
2.12.2 Fonctionnement 24
2.13 Rappel sur la notion de VLAN (Vertual Local Area Network) 24
2.13.1Type de configuration des ports des switchs Cisco. 25
2.13.2 VLAN non affecté à un port et présent sur le switch 25
2.13.3 Communication entre les VLAN. 25
2.13.4 Configuration type d'un switch 25
2.14 Principe du routage INTER-VLAN 26
2.15 Conclusion 27

Chapitre 03 : La mise en place de VLANs

3.1 Introduction 29
3.2 Présentation 29
3.3 Architecture scenario de déploiement 29
3.4 Présentation de simulateur « Cisco Packet Tracer » 29
3.4.1 Définition 29
3.4.2 Présentation de l'écran 30
3.4.3 Spécification des connexions possibles 31
3.4.4 Affichage physique du matériel 32
3.4.5 Paramétrage des appareils 32
3.4.6 Les principales commandes CISCO (CLI) 35
3.5 Interface commande de Packet Tracer 36
3.6 L'adressage de différents VLANs 36
3.7 Les éléments fonctionnels de VLAN 36
3.7.1 Les normes 36
3.7.1.1 La norme 802.1q (etiquetage de trames) 36
3.7.1.2 ISL (Encapsulation de trames) 37
3.7.1.3 Lien des Trunks 37
3.7.1.4 Le routage inter-vlan 37
3.7.2 Les protocoles 38
3.7.2.1 Protocole VTP (VLAN Trunking Protocol) 38
3.7.2.2 Protocol DHCP 38
3.7.2.3 Protocole IEEE802.3ad 38
3.8 Configuration des équipements 38

3.8.1 Configuration du commutateur 39
3.8.1.1 Crée 2 vlans (vlan 10 et vlan 20) 39
3.8.1.2 Attribuer des ports au vlan de données 39
3.8.1.3 Attribuer des ports au vlan vocal 39
3.8.1.4 Configurer le port connecté au routeur en tant que junction 40
3.8.2 Configuration du routeur 40
3.8.2.1 pool DHCP pour telephones IP 40
3.8.2.2 pool DHCP pour pc IP 40
3.8.3 Routeur sur une configuration de baton 40
3.8.3.1 créer les sous-interfaces et les associer au vlan 40
3.8.4 Configuration du gestionnaire d'appels 40
3.8.4.1 Difinition de nombre maximmun de téléphones IP et de numéro d'annuaire 40
3.8.5 Configuration du telephone 41
3.8.5.1 Définition des numéros du telephone 41
3.8.5.2 Configuration du bouton telephone 41
3.8.6 Attribution d'adresse IP pour PCs à partir de DHCP 42
3.9 Test et validation de configuration 42
3.9.1 Test entre les équipements 43
3.9.2 Test inter-Vlan 44
3.9.3 Test entre Vlan 45
3.10 La sécurité réseau 45
3.6.1 La sécurité contre court-circuit 45
3.6.2 La sécurité contre surtension 45
3.6.3 . La sécurité contre l'incendie 45
3.6.4 La sécurité contre le virus 45
3.6.5 La sécurité contre l'espionnage 45
3.11 Conclusion 46

Chapitre 04 : Résultat de Simulation et Discussion

4.1 Introduction 48
4.2 Simulation résaux01 (Scénarion 01) 48
4.2.1 Tableau Récapitulatif du réseau (Routeur / Switch / 4 Stations) 48
4.2.2 Configuration ET discussion des résultats réseau 01 49
4.2.2.1Configuration du commutateur : 49
4.2.2.2Configuration du routeur 49
4.3 SIMULATION (résau02)(Scénario 02) 53
4.3.1 Tableau Récapitulatif du réseau (01 Routeur /03 Switch / 6 Stations) 53
Tab.4.2 53

4.3.2 Configuration ET discussion des résultats réseau 02 53
4.3.2.1Configuration du commutateur 54
4.3.2.2Configuration du routeur 55
4.4 SIMULATION (résau03) 57
4.4.1 Tableau Récapitulatif du réseau (03 Routeur /03 Switch / 6 Stations) 57
4.4.2 Configuration ET discussion des résultats réseau 03 58
4.4.3 Configuration des interfaces du routeurs (routeur0-routeur1- routeur2) 63
4.5 Avantages et inconvénients du réseau N° 01 (01 Router + 01 Switch) à base des Vlans 66
4.6.Avantages et inconvénients du réseau N° 02 (01 Router + 03 Switch) à base des Vlans 66
4.8 Avantages et inconvénients du réseau N° 03 (03 Router + 03 Switch) à base des Vlans 67
4.9.Les avantages et inconvénients du voip 68
4.10.conclusion 68
Conclusion générale 69
Résumé 70
Abstract: 70
Bibliographie 72

Liste des abréviations

ACL : Access Control List

ARP: Adress Resolution Protocol

BID: Bridged Identity.

ATM: Asynchronous Transfer Mode

BNC: Bayonet Neill–Concelman Connector

BPDU: Bridge Protocol Data Unit

CDM: Code Division Multiple.

CISCO: Société de matériel informatique

CLI: Command Line Interface.

DHCP: Dynamics Host Configuration Protocole.

EIGRP: Extended Interior Gateway Routing Protocol.

FC: Ferrule Connector

FDDI: Fiber Distributed Data Interface

FO: Fibre Optique**.**

HTTP: Hypertext Transfer Protocol.

HUB: Concentrateur réseau

IP: Internet Protocole.

ISO : Organisation Internationale de normalisation.

JPEG : Joint Photographic Experts Group.

LAN: Local Area Network.

LC: Lucent Connector

LLC: contrôle de liaison logique

MAC: Media Access Control

MAN: Metropolitan Area Network.

ISL: Inter-Switch Link

OSI: Open Systems Interconnections

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

PABX: Private Automatic Branch eXchange

PAN: Personal Area Network

PDU : Protocol Data Unit

PING: Packet Internet Groper**.**

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

RIP : Routing Information Protocol.

SNAP: protocole d'accès au sous-réseau

SC: Standard Connector

ST: Straight Tip

STB: Set-top box.

STP : Spanning-Tree Protocol

TCP: Transmission Control Protocol.

TRUNK: plate-forme de transport ferroviaire destiné pour les objets lourds ou encombrants.

UDP: User Detagram Protocol.

USB: Universal Serial Bus

UTP: Unshielded Twisted Pair

VLAN: Réseau Local Virtuel**.**

VOIP: Voice over IP.

VTP: VLAN Trunking Protocol**.**

WAN: Wide Area Network

WIFI: Wireless Fidehty (ensemble des protocoles de communication sans fil)

Liste des figures

Fig. 1.1 : Les réseaux locaux ou LAN (Local Area Network) **1**

Fig. 1.2 : Les réseaux grands distances ou WAN (Wide Area Network) **2**

Fig. 1.3 : Les réseaux MAN (Métropolitain Area Network) **2**

Fig.1.4 : Les réseaux PAN **3**

Fig.1.5 : Les Types de blindages **7**

Fig.1.6 FO monomode **8**

Fig.1.7 FO multimode à saut d'indice **8**

Fig.1.8 FO multimode à gradient d'indice **8**

Fig.1.9 connecteur BNC **9**

Fig.1.10 Les connecteurs optique **9**

Fig.1.11 connecteur RJ45 **10**

Fig.1.12 routeur **11**

Fig.1.13 passerelle **11**

Fig.1.14 Les concentrateurs **11**

Fig.1.15 Topologie en bus **12**

Fig.1.16 Topologie en étoile **12**

Fig.1.17 Topologies en arbre **12**

Fig.1.18 Topologie en anneau **13**

Fig.2.1 Segmentation avec vlan **15**

Fig.2.2 VLAN de niveau 1 **18**

Fig.2.3 VLAN de niveau 2 **19**

Fig.2.4 L'étiquetage **19**

Fig.2.5 La trame Ethernet classique **20**

Fig.2.6 La trame Ethernet 802.1q **20**

Fig2.7 Le protocole ISL **21**

Fig.2.8 La notion des trunk **22**

Fig.2.9 Le protocole VTP **23**

Fig.2.10 Rappel sur la notion de VLAN **25**

Fig.2.11 Configuration type d'un switch **26**

Fig.2.12 Routage inter-VLAN **26**

Fig.3.1 Architecture scenario de déploiement **29**

Fig.3.2 Présentation de l'écran **30**

Fig.3.3 Présentation de l'écran **30**

Fig3.4 Interface commande de Packet Tracer **36**

Fig.3.5 Lien des Trunks **37**

Fig.3.6 Commande lien trunk **37**

Fig.3.7 Attribution d'adresse IP pour PCs à partir de DHCP **42**

Fig.3.8 Test entre les équipements **43**

Fig.3.9 Test inter-VLAN **44**

Fig.3.10 Test entre Vlan **45**

Fig.4.1 scénario 01 **48**

Fig.4.2 scénario 02 **53**

Fig.4.3 scénario 03 **57**

Liste des tableaux

Tab.1.1 Comparaison entre les couches du modèle OSI et TCP/IP **3**

Tab.1.2 Masques de réseau de différentes classes **6**

Tab.1.3 Caractéristiques des classes des adresses IP **6**

Tab.2.1 Fonctionnement de VTP **24**

Tab.3.1 Les principales commandes CISCO (CLI) **35**

Tab.3.2 L'adressage de différents VLANs **36**

Tab.4.1 Scénario 01 **48**

Tap.4.2 Scénario 02 **53**

Tap.4.3 Scénario 03 **57**

1. 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 coeur 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

Ce chapitre a pour objectif de comprendre les notions de bases sur les réseaux informatiques, et de bien maitriser notre sujet.

Un réseau informatique *(network)* est un regroupement d'ordinateurs et d'équipements interconnectés entre eux, permettant la communication et le partage de différents éléments (des fichiers, des imprimantes...) entre différents stations relies, comme il permet aussi l'accès à distance aux bases de données.

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.

1.2 Types de réseaux

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

1.2.1 Réseaux locaux (LANs)

Un réseau local *(Local Area Network)* est une infrastructure de communication, reliant des équipements informatiques et permettant de partager des ressources communes dans une aire géographique limitée à quelques centaines de mètres à l'aide d'un support de transmission. L'objectif d'un réseau local dans une entreprise est de répondre à certain nombre de questions spécifiques aux équipements à interconnecter et aux applications à supporter.

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

Les inconvénients :

- cout d'installation élevé.
- Violations de vie privée.
- Travail de maintenance du réseau local.
- Couvre une zone limitée.

Les avantages :

- Partage de ressources et d'applications logicielles.
- Communication facile et économique.
- Sécurité des données.
- Partage internet.

1.2.2 Réseaux étendus (WANs)

Les réseaux étendus (*Wide Area Network*) interconnectent des réseaux locaux, qui à leur tour, donnent accès aux ordinateurs ou aux serveurs de fichiers situés en d'autres lieux. Comme les réseaux étendus relient des réseaux utilisateurs géographiquement dispersés, ils permettent aux entreprises de communiquer entre elles sur de grandes distances. Les réseaux étendus permettent le partage d'ordinateurs, imprimantes et autres équipements raccordés à un LAN situé sur un lieu distant.

Les réseaux étendus fournissent des communications instantanées à l'intérieur de grandes zones géographiques.

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

Les inconvénients :

- Cout d'installation élevé.
- Possibilité de lacunes en matière de sécurité.
- Nécessite un logiciel antivirus et des pare-feu.

Les avantages :

- peut couvrir une large zone géographique.
- Une infrastructure centralisée.
- Sécurité.
- Augmentation de la largeur de bande grâce à l'utilisation de lignes louées par opposition aux connexions à large bande.

1.2.3 Réseaux métropolitains (MANs)

Un réseau MAN *(Métropolitain Area Network)* est un réseau qui s'étend à une zone métropolitaine telle qu'une ville. Un réseau MAN comprend habituellement au moins deux réseaux LAN situés dans une zone géographique commune. Par exemple, une banque possédant plusieurs agences peut utiliser ce type de réseau.

Fig 1.3 : Les réseaux MAN (Métropolitain Area Network)

Les inconvénients :

- Le grand réseau devient difficile à gérer.
- Difficile de sécuriser le système contre les pirates et les espionnages industriels.

Les avantages :

- Haute sécurité.
- Facile d'implémenter des liens.
- Augmentez la vitesse de transfert des données.
- Flexibilité du service propos.

1.2.4 Personale Area Network (PAN)

Pour permettre l'échange de données des appareils modernes comme notamment les Smartphones, tablettes, ordinateurs portables ou les ordinateurs de bureau, ces derniers peuvent être connectés à un réseau adapté. Celui-ci peut être relié sous la forme d'un réseau personnel ou PAN (*Personnel Area Network*), on parle aussi de réseau domestique. Les techniques de transmission courantes sont l'**USB** ou le **FireWire**.

Fig1.4 :les réseaux PAN

1.3 Modèles de réseaux

Il existe deux types de modèle de réseau de base : le modèle de référence et le modèle d'applications**.**

OSI		TCP/IP
7	Couche application	Couche Application Applications réseau (FTP, SMTP, Http, DNS, Telnet ...)
6	Couche Présentation	
5	Couche Session	
4	Couche Transport	Couche Transport TCP ou UDP
3	Couche Réseau	Couche Internet IP, ARP
2	Couche Liaison données	Couche Accès réseau Ethernet, Token ring, Token Bus ...
1	Couche Physique	

Tab.1.1 Comparaison entre les couches du modèle OSI et TCP/IP.

1.3.1 Modèle OSI (Open System Interconnection)

Le modèle OSI est un modèle conceptuel. Il a pour but d'analyser la communication en découpant les différentes étapes en 7 couches, chacune de ces couches remplissant une tâche bien spécifique. An de connaitre les services de chaque couches on va les présenter ci-dessous l'une après l'autre :

1. Couche Physique :
Fournit les moyens mécaniques, optiques, électroniques, fonctionnels et procéduraux nécessaires à l'activation, au maintien et à la désactivation des connexions physiques nécessaires à la transmission des bits. Les systèmes sont interconnectés réellement au moyen de supports physiques de communication. Ces derniers ne font pas partie de la couche Physique

2. Couche Liaison de données :
Assure la transmission d'informations entre deux ou plusieurs systèmes immédiatement adjacents. Détecte et corrige, dans la mesure du possible, les erreurs issues de la couche inférieure. Les objets échangés sont souvent appelés trames.

3. Couche Réseau :
Achemine les informations à travers un réseau pouvant être constitué de systèmes intermédiaires (routeurs). Les objets échangés sont souvent appelés paquets.

4. Couche Transport :
Assure une transmission de bout en bout des données. Maintient une certaine qualité de la transmission, notamment vis-à-vis de la fiabilité et de l'optimisation de l'utilisation des ressources. Les objets échangés sont souvent appelés messages.

5. Couche Session :
Fournit aux entités coopérantes les moyens nécessaires pour synchroniser leurs dialogues, les interrompre ou les reprendre tout en assurant la cohérence des données échangées.

6. Couche Présentation
Spécifie les formats des données des applications (compression, encryptions,etc).

7. Couche Application :
Donne aux processus d'application les moyens d'accéder à l'environnement de communication de l'OSI. Comporte de nombreux protocoles adaptés aux différentes classes d'application.

1.3.2 Le modèle TCP/IP

Contrairement au modèle OSI, le modèle TCP/IP est né d'une implémentation mais il est inspiré du modèle OSI. Il reprend l'approche modulaire (utilisation de modules ou couches) mais en contient uniquement quatre. Les trois couches supérieures du modèle OSI sont souvent utilisées par une même application. Afin de connaitre les services de chaque couches on va les présenter brièvement ci-dessous l'une après l'autre :

1. Couche application
Le modèle TCP/IP regroupe en une seule couche tous les aspects liés aux applications et suppose que les données sont préparées de manière adéquate pour la couche suivante.

2. Couche transport

La couche transport est chargée des questions de qualité de service touchant la fiabilité, le contrôle de flux et la correction des erreurs. L'un de ses protocoles TCP, fournit d'excellents moyens de créer avec souplesse, des communications réseau fiables.

3. Couche Internet :

Le rôle de la couche Internet consiste à envoyer des paquets source à partir d'un réseau quelconque de l'inter réseau et à les faire parvenir à destination, indépendamment du trajet et des réseaux traversés pour y arriver. Le protocole qui régit cette couche est appelé protocole IP (Internet Protocol). L'identification du meilleur chemin et la commutation de paquets ont lieu au niveau de cette couche.

4. Accès Réseau

C'est la couche la plus basse de la pile TCP/IP. Elle contient toutes les spécificités concernant la transmission des données sur un réseau physique, elle spécifie la forme sous laquelle les données doivent être acheminées quel que soit le type de réseau utilisé et elle permet la Conversion des signaux analogiques/numériques. Elle est composée par deux niveaux MAC, LLC.

1.4 L'adressage IP

1.4.1 Le protocole IP

Le protocole IP (*Internet Protocol*) s'agit d'un protocole réseau de niveau trois, ce protocole permet d'émettre des paquets d'informations à travers le réseau, il est utilisé pour dialoguer les machines entre elles. Ainsi, il offre un service d'adressage unique pour l'ensemble des machines. Il n'est pas orienté connexion, c'est à dire qu'il n'est pas fiable Cela ne signifie pas qu'ils n'envoient pas correctement les données sur le réseau, mais qu'ils n'offrent aucune garantie pour les paquets envoyés sur l'ordre d'arrivée et la perte ou la destruction des paquets, cette fiabilité dépend de la couche de transport.

1.4.2 Le format des adresses IP

Il existe deux formats d'adresse IP : Le format IPV4 et le format IPV6

1.4.3 Le format IPV4

C'est une adresse de 32 bits, répartie en 4 fois 8 bits (octet). Cette adresse est un identifiant réseau qu'on peut diviser en 2 portions : la portion du réseau et la portion hôte. La première identifie le réseau sur lequel est la machine et la deuxième identifie les machines en elles-mêmes. Pour identifier ces deux parties chaque adresse est liée à un masque de sous-réseau ce qui permet de définir sur quel réseau elle se trouve. Le format binaire d'une adresse IP est comme suit : xxxxxxxx . xxxxxxxx .xxxxxxxx. xxxxxxxx (tel que x=0 ou x=1).

1.4.4 Le masque réseau

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

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 réseau de différentes classes

1.4.5 Les classes des adresses IP

Le but de la division des adresses IP en classes, est de facilité la recherche d'un ordinateur sur le réseau. En effet, avec cette notation il est possible de rechercher dans un premier temps le réseau à atteindre puis de chercher un ordinateur sur celui-ci. Ainsi, l'attribution des adresses IP se fait selon la taille du réseau. En effet, il existe 5 classes des adresses IP, à savoir : classe A, classe B, classe C, classe D et classe E, telle que, chaque classe a un format spécial de son adresse IP. « Adresse réseau et Adresse machine ».

Classes	0 1	2 3	4 5	6 7	8 9	10 11	12 13	14 15	16 17	18 19	20 21	22 23	24 25	26 27	28 29	30 31
A	0	réseau			hôte											
B	1 0	réseau							hôte							
C	1 1	0	réseau										hôte			
D	1 1	1 0	adresse multi-destinataire													
E	1 1	1 1	0	réservé												

Tab.1.3 Caractéristiques des classes des adresses IP.

1.4.6 Adresses Spécifiques

Dans l'ensemble des adresses IP, il existe certaines adresses qui sont spécifiques, c'est- à-dire, qu'elles ont un usage particulier. Parmi ces adresses, citant : Les adresses privées et les adresses de diffusion.

1.4.7 Adresse privée

Il existe des adresses privées, dans chaque classe :

A > =10.0.0.0 à 10.255.255.255

B > =172.16.0.0 à 172.31.255.255

C >= 192.168.0.0 à 192.168.255.255

Une adresse IP privée n'est pas visible sur internet, au contraire d'une IP publique. On emploie les adresses privées à l'intérieur du réseau et les adresses publiques sont des adresses internet.

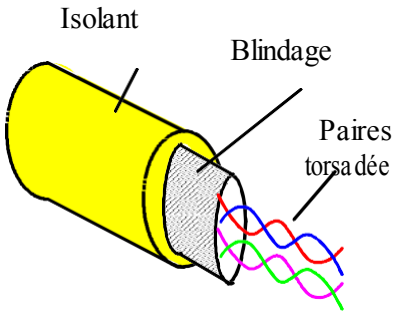
1.4.8 Adresse de diffusion

L'adresse de diffusion est utilisée pour envoyer un message à toutes les machines d'un réseau. Elle est obtenue en mettant tous les bits de l'host-id à 1. Il existe aussi l'adresse de Broadcast " générale ", cette

adresse permet l'envoi d'un message vers toutes les machines de tous les réseaux connectés. Le routeur quand il reçoit une adresse de Broadcast, va envoyer le message dans tous les périphériques du réseau concerné.

1.5 Les composantes physiques des réseaux locaux

1.5.1. La paire téléphonique torsadée



La paire téléphonique torsadée peut être:
- simple
- double,
- blindée.

Son débit est de 10 Mégabits / s.
Sa bande passante est de 4 MHz.
La distance maximum sans répéteur est de plus de 1 kilomètre.

1.5.2. Les Types de blindages

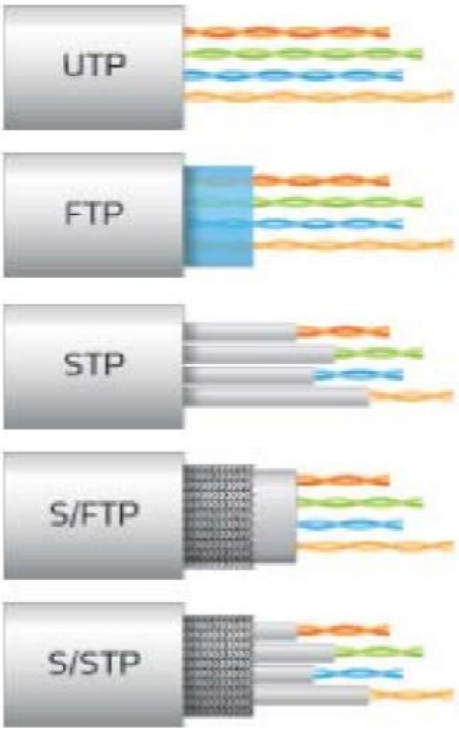
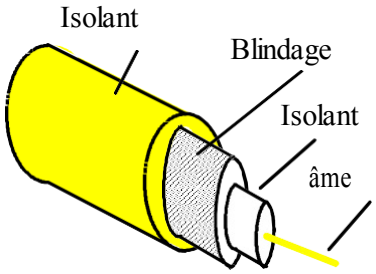


Fig.1.5

1.5.2 Le câble coaxial



Le câble coaxial a un blindage qui permet de l'isoler des perturbations extérieures.
Son débit est de 10 à 50 Mégabits/s.
Sa bande passante est de 50 à 400 Mégahertz et son impédance est de 50 ou 75 Ohms.
La distance maximum sans répéteur est de plus de 10 kilomètres.

1.5.3 La fibre optique

Est un file en verre ou plastique particulièrement fin qui a la propriété de conduire la lumière et sert dans les transmissions terrestres et océaniques de données. Il existe 2 grands types de fibres:

1.5.3.1 Monomode

Dans lequel il existe un seul mode de propagation de la lumière, le mode en ligne droite.

Débit: environ 100 Gbit/s
Portée maximale: environ 100 Km
Affaiblissement: 0,5 dB/Km

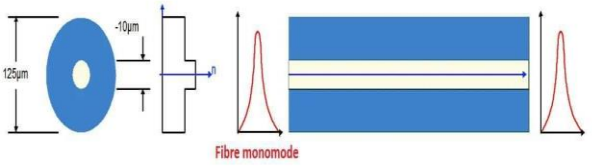


Fig.1.6

1.5.3.2 Multimode

Dans lequel il existe différents modes de propagation de la lumière au sein du cœur de la fibre.

Multimode à saut d'indice

Débit: environ 100 Mbit/s
Portée maximale: environ 2 Km
Affaiblissement: 10 dB/Km

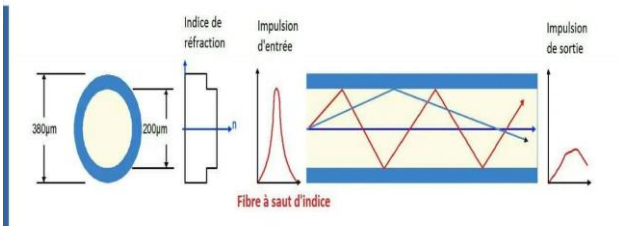


Fig.1.7

Multimode à gradient d'indice

Débit: environ 1 Gbit/s
Portée maximale: environ 2 Km
Affaiblissement: 10 dB/Km

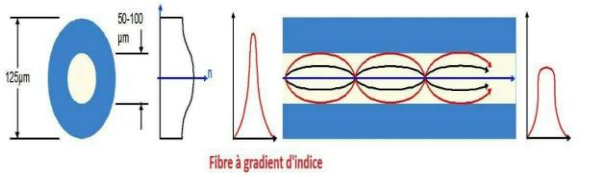


Fig.1.8

1.6 Les connecteur

1.6.1. Les connecteurs BNC

Le connecteur BNC (connecteur Bayonet-Neill–Concelman) est un connecteur RF utilisé en terminaison de câble coaxial, en particulier dans le domaine radiofréquence. Le connecteur BNC est généralement utilisé dans les applications nécessitant une fréquence inférieure à 4 GHz et moins de 500 V, et correspond à l'impédance caractéristique d'un câble 50 ohms ou 75 ohms.

Fig.1.9

1.6.2. Les connecteurs optiques

Fig.1.10

1.6.2.1 Connecteur SC

Le connecteur SC (Subscriber Connector) ou connecteur carré est doté d'un diamètre de férule 2,5mm et fonctionne par encliquetage (couplage push-pull). De profil carré, il offre des densités de connexion plus nombreuses dans les instruments et panneaux de brassage. Son faible coût et sa facilité d'utilisation en font un connecteur très réputé sur le marché.

1.6.2.2. Connecteur LC

Le connecteur LC (Lucent Connector) possède un diamètre de férule deux fois plus petit que celui des connecteurs SC. Il comprend les mêmes propriétés que le connecteur SC tout en étant plus petit. Il peut donc être utilisé dans des endroits plus difficiles d'accès.

1.6.2.3. Connecteur FC

Le connecteur FC (Ferrule Connector) est utilisé pour les jarretières optiques monomodes. Ce connecteur avec férule 2,5mm possède un embout céramique haut pression. Il tend à être remplacé par des connecteurs SC et LC à cause de la perte de ses vibrations et de sa perte d'insertion.

1.6.2.4. Connecteur ST

Le connecteur ST (Straight Tip) est utilisé pour les jarretières optiques multimodes. Il comprend une férule 2,5mm, est doté d'un embout céramique et possède un système de verrouillage à baïonnette qui permet d'éviter un serrage excessif du connecteur qui pourrait endommager la fibre.

1.6.3. Les connecteurs RJ45

Le connecteur RJ45 (Registered Jack) sert normalement à connecter les ordinateurs par l'intermédiaire d'un Hub (concentrateur) ou d'un commutateur (Switch). **[5]**

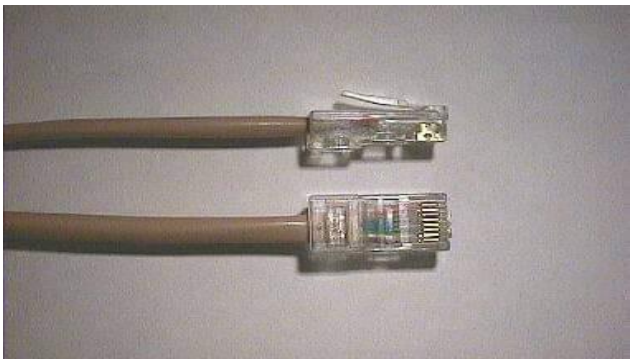


Fig.1.11

1.7.Les matériel d'interconnexions d'un réseau local

1.7.1. Les répéteurs

Ils permettent de raccorder deux réseaux identiques ou deux stations de travail ou une station et un serveur, lorsque la liaison ne peut pas être effectuée, en raison de la distance, par un seul câble. Ils n'ont aucune fonction de routage, de traitement des données, et d'accès au support.

1.7.2. Les ponts

Ils permettent d'interconnecter des réseaux ayant la couche 1 et 2 du modèle OSI (couche liaison) différentes, mais les couches supérieures à la 2 identiques. Les ponts, pour interconnecter des réseaux, décodent les en-têtes des trames du premier réseau, puis les modifient afin de les rendre compatible avec le deuxième réseau

- Fonction des ponts simples:
  - assurer la conversion du format des trames,
  - filtrer les trames en fonction de l'adresse du destinataire, passage ou pas par le pont,
  - positionner certains bits (tel que les bits A et C de la trame Token Ring).
- Fonction des ponts routeurs
  - établir la table de routage (adresse des éléments du réseau),
  - filtrage des trames,
  - contrôle de flux lorsque les débits des réseaux sont différents.

1.7.3. Les routeurs

Ils permettent l'interconnexion de réseaux présentant des différences physiques des bits et de la composition des trames, couche 1 et 2 du modèle OSI. Ils gèrent les en-têtes des trames et des
Paquets jusqu'à la couche 3 (couche réseau).

Fig.1.12

1.7.4. Les passerelles

Elles permettent l'interconnexion de réseau en adaptant l'ensemble des couches du modèle OSI afin de les rendre compatible l'autre réseau.

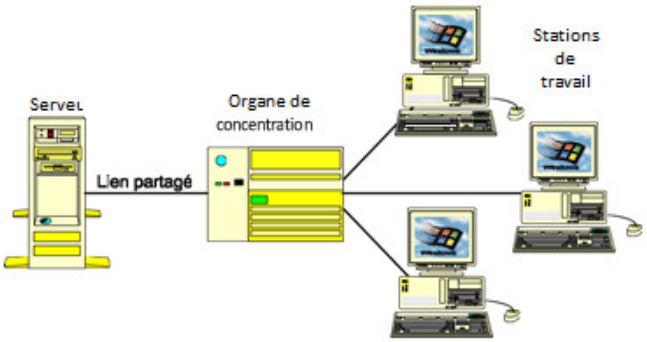


Fig.1.13

1.7.5. Les concentrateurs

Ils autorisent aussi le partage d'une voie composite. Ils analysent le contenu des blocs d'informations, provenant généralement d'un ordinateur gérant les stations de travail, le serveur, et les redirigent vers la seule station de travail concernée. Ils possèdent une logique programmée ce qui les rendent fortement dépendant des protocoles.

Fig.1.14

1.7.6. Les autocommutateurs (PABX)

Souvent désignés sous le nom de PABX (Private Automatic Branch eXchange), ces équipements sont conçus pour transmettre sur le réseau public les données (Communications téléphoniques ou messages informatiques). Ils étaient avant analogiques maintenant ils sont numériques et permettent d'atteindre un débit de 64 kbits/s.

1.7.7. Adaptateur

Un adaptateur (*adapter*) est destiné à être insérés dans un poste de travail ou un serveur an de les connecter à un système de câblage.

1.8. Les topologies de base utilisées dans les réseaux

1.8.1. Topologie en bus

Tous les éléments sont connectés à un même bus et se partagent le support de transmission. Cette topologie a quelques avantage comme l'absence de matériel supplémentaire, la simplicité puisqu'un seul câble permet toutes les communications ou la facilité d'ajouter des postes. Par contre elle présente plusieurs inconvénients comme l'obligation de **[9]** rajouter des terminaisons aux extrémités du bus pour éviter les phénomènes de réflexion dus à l'écho du signal. Un défaut de liaison à un seul endroit rend tout le réseau inopérant. La bande passante est partagée entre tous les éléments d'où la diminution de début de transmission dès que des postes sont rajoutés

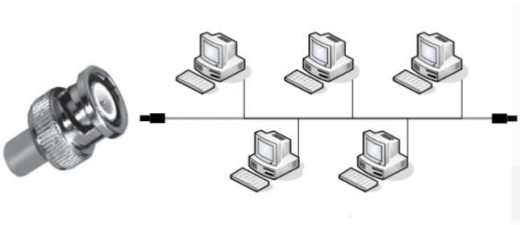


Fig.1.15

1.8.2. Topologie en étoile

Elle est basée sur un équipement central, tel qu'un commutateur, les commutateurs étant des éléments actifs, cette topologie nécessite une alimentation. De plus, le nombre de ports d'un commutateur étant limité, rajouter des éléments est plus difficile. Et enfin, les commutateurs représentent un cout supplémentaire. L'avantage est qu'une liaison en panne n'empêche pas les autres liassions de fonctionner, la bande passante globale dépend du commutateur et non du nombre de postes et qu'on peut augmenter la taille du réseau sans dégrader les performances. La confidentialité est assurée avec des commutateurs, les concentrateurs, eux, relaient les trames sur tous les ports.

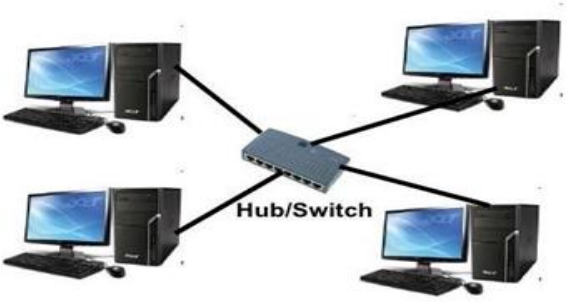


Fig.1.16

1.8.3. Topologies en arbre

Il s'agit en réalité d'une mise en cascade de réseaux en étiole

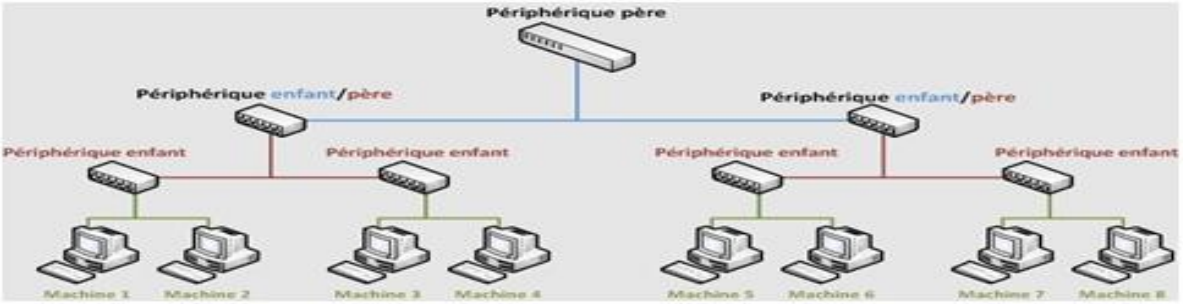


Fig.1.17

1.8.5. Topologie en anneau

Les éléments sont chaînés dans un anneau (boucle) fermé. Il n'y a pas d'extrémités dotées de bouchons de terminaison. Chaque hôte communique avec ses voisins pour véhiculer l'information. Les signaux se déplacent le long de la boucle dans une seule direction et passant par chacun des ordinateurs.

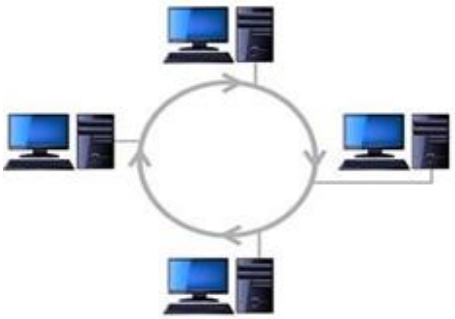


Fig.1.18

1.8.6. Topologies maillée

Cette topologie est utile pour lutter contre les ruptures de communication. Chaque hôte possède ses propres connexions à tous les autres hôtes. Ceci est le cas de la conception de l'Internet, qui possède de nombreux chemins vers un emplacement.

1.9. conclusion

Au cours de ce chapitre, nous avons parcouru des généralités sur les réseaux informatiques en soulignant leur importance, leurs différents composants.

Par la suite, nous avons présenté la manière dont les données sont transmises à travers les couches des deux modèles OSI et TCP/IP, en passant par les Protocoles, les services offerts par ces derniers ainsi que l'adressage et ses classes. En citant les équipements d'interconnexion dans un réseau local afin de bien aborder le chapitre suivant qui sera consacré aux réseaux virtuels (VLAN).

Chapitre 02 :

Les réseaux VLANs

2.1 Introduction

Généralement, un réseau local (LAN) est défini par un domaine de diffusion. Tous les hôtes d'un réseau local reçoivent les messages de diffusion émis par n'importe quel autre hôte de ce réseau. Par définition, un réseau local est délimité par des équipements fonctionnant au niveau 3 du modèle OSI : la couche réseau, les VLAN sont utilisés pour segmenter un réseau. La limitation de l'étendue de chaque domaine de diffusion sur le réseau local grâce à la segmentation VLAN permet d'améliorer les performances et la sécurité sur le réseau. Le protocole VTP permet de partager les informations VLAN entre plusieurs commutateurs dans un environnement LAN pour simplifier la gestion des réseaux locaux virtuels. Le routage entre les réseaux VLAN et son utilisation pour permettre à des périphériques de réseaux VLAN distincts de communiquer.

2.2 Concepts VLAN

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

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

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

Les principales différences entre la commutation traditionnelle et les VLAN sont :

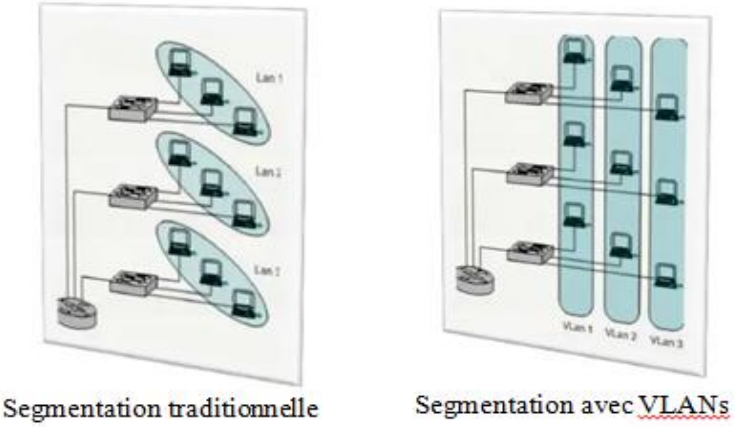


Fig.2.1

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

Segmentation par pont
Segmentation du domaine de collision en 2 grâce au pont, dispositif de couche 2 permettant un filtrage des trames en fonction des a dresses M AC des hôtes.

Segmentation par routeurs
Segmentation du domaine de broadcast en fonction des adresses réseau de couche 3.

Segmentation par commutateur

Segmentation du domaine de collision par la mise en place de chemins commutés entre l'hôte et le destinataire (micro segmentation).

2.3 Intérêt à avoir des VLAN

Il existe plusieurs intérêts à avoir des VLAN dans votre entreprise. Par contre, il n'est pas nécessaire d'avoir des VLAN lorsque vous avez un petit réseau avec très peu de fonctionnalité. Voici quelques exemples de besoins qui nécessitent l'utilisation des réseaux virtuels : **[6]**

- Améliorer la gestion du réseau
- Optimiser la bande passante
- Séparer les flux
- Fragmentation : réduire la taille d'un domaine de broadcast
- Sécurité : permet de créer un ensemble logique isolé pour améliorer la sécurité. Le seul moyen de communiquer entre des machines appartenant à des VLAN différents est alors de passer par un routeur

2.4 Les propriétés offertes par les VLAN sont

- 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 a 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 machinesappartiennent de telle sorte que le trafic intra-domaine ne puisse pas être vu par des tiers n'appartenant pas à ce domaine de broadcast.

2.5 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. La technologie de VLAN comporte ainsi de nombreux avantages. Parmi les avantages liés à la mise en œuvre d'un VLAN, on retiendra notamment:

❖ 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 les matériels, 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 information 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 déja en place le remplacer par des commutateurs dont le cout ne cesse d'augmenter avec l'arrivée de toutes ces fonctionnalités nouvelle.

2.6.La technique des VLANs

Généralités

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 : l' Partitionnement en plusieurs domaines de broadcast l' Affectation d'un ou plusieurs ports à un VLAN depuis une console centrale (Amélioration de la bande passante par la fonction de commutation l'Adaptation de la vitesse du Switch à la capacité du réseau l' 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 **[3]**

2.7.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]**

2.7.1. 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. Les ports des Switch sont associés à des VLANs (Figure 2.4) l' Ports 1,2 et 3 appartiennent au VLAN 1 l' Ports 4,5 et 6 au VLAN 2 i' Ports 7 et 8 au VLAN 3

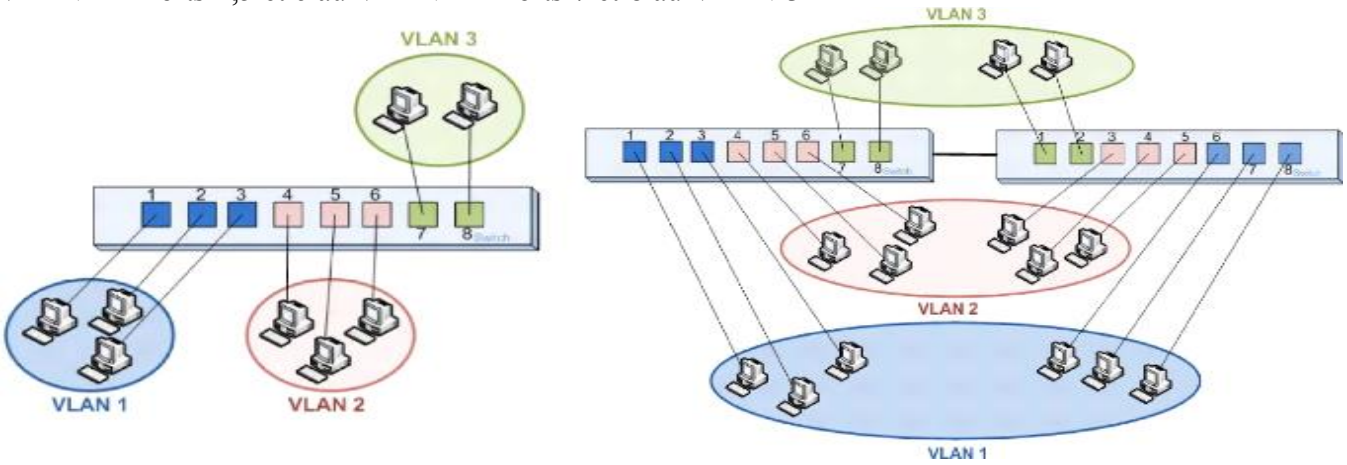


Fig.2.2

2.7.2. 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.

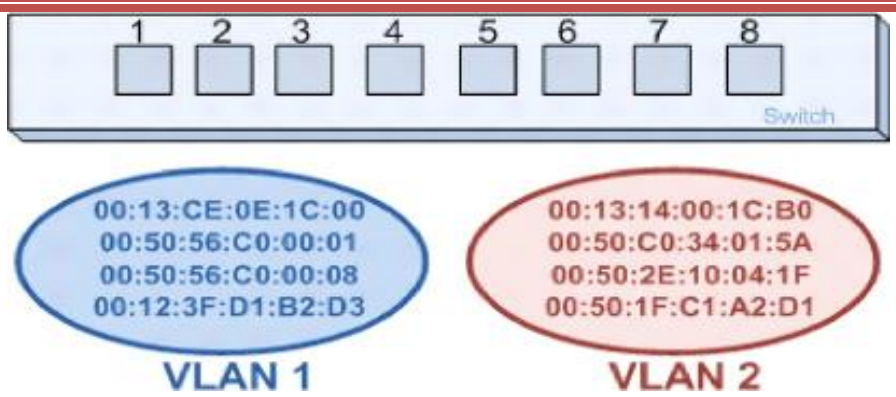


Fig.2.3

2.7.3 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 faite il s'agit à partir de l'association protocole/VLAN d'affecter dynamiquement les ports des commutateurs a chacun des VLAN.

2.8 Principe de fonctionnement de VLANs

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

2.8.1 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

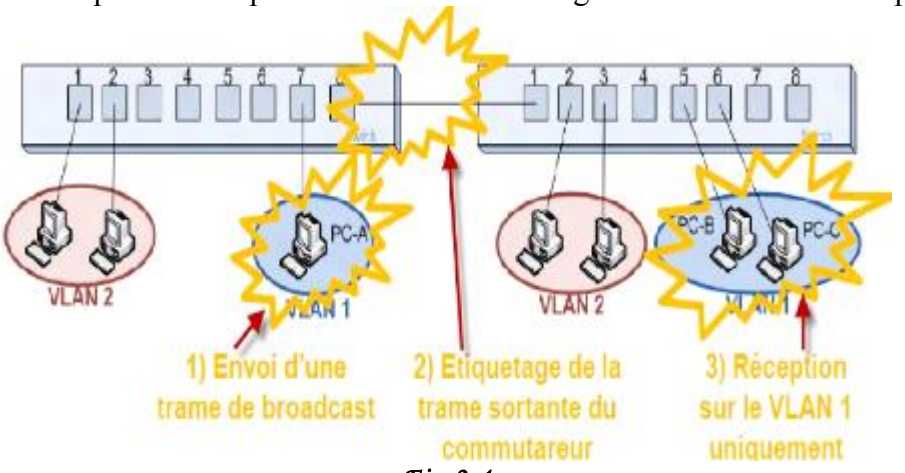


Fig.2.4

2.8.2 La trame Ethernet classique

Cette figure nous montre une trame Ethernet classique sans VLANs

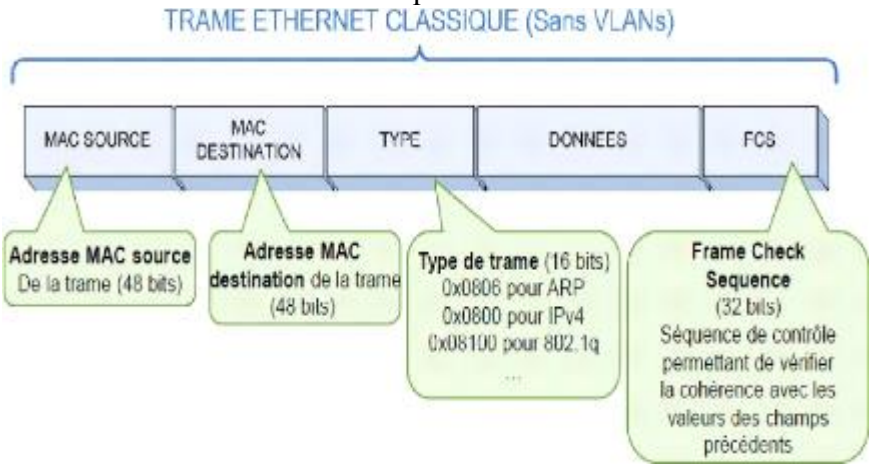


Fig.2.5

2.8.3 La trame Ethernet 802.1q

L'étiquetage se fait grâce à la norme 802.1q (dot1.q) et Les trames ont un champ supplémentaire.

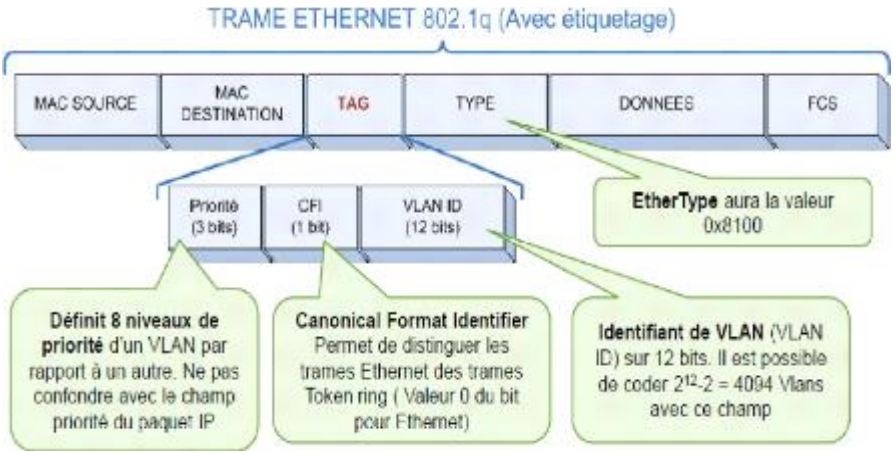


Fig.2.6

2.9 Le Protocol ISL (Inter Switch Link Protocol)

Le protocole Inter-Switch Link (ISL) est un protocole exclusif de Cisco et Inter-Switch Link (ISL) est disponible et pris en charge uniquement sur les produits Cisco. Si vous avez besoin d'un protocole VLAN non propriétaire, envisagez d'utiliser le protocole IEEE 802.1Q.

Le protocole ISL (Inter-Switch Link) est principalement utilisé pour les supports Ethernet (Fast Ethernet ou Gigabit Ethernet). Cisco a également inclus des dispositions pour transporter des trames Token Ring, FDDI et ATM sur Ethernet ISL. Le protocole ISL (Inter-Switch Link) encapsule toute la trame Ethernet (Fast Ethernet ou Gigabit Ethernet) avec un en-tête de 26 octets et une séquence de contrôle de trame (FCS) de 4 octets pour un total de 30 octets de surdébit. Le format de trame Inter-Switch Link (ISL) est illustré ci-dessous.

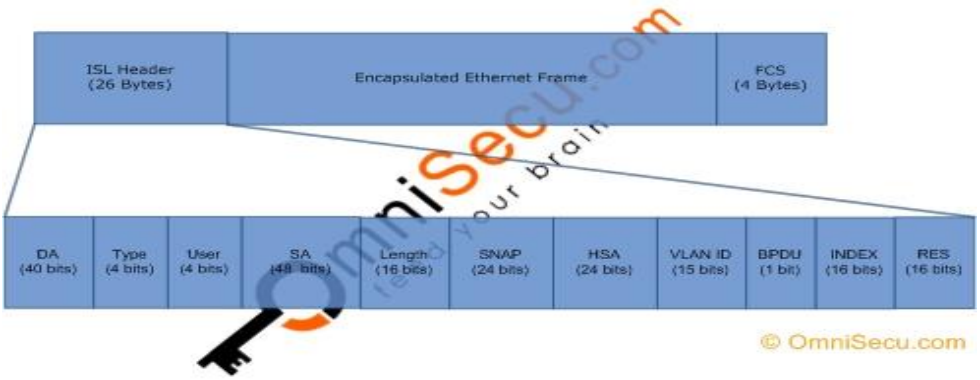


Fig.2.7

Les champs de la trame d'encapsulation du protocole ISL (Inter-Switch Link) sont indiqués ci-dessous.

• DA (adresse de destination): l'adresse de destination utilise l'adresse MAC de multidiffusion 01-00-0C-00-00-00. Les 40 premiers bits du champ DA signalent au récepteur que le paquet est au format ISL (Inter-Switch Link).

• Type: le type de trame encapsulée: Ethernet (0000), Token Ring (0001), FDDI (0010) et ATM (0011).

• Utilisateur: le champ USER se compose d'un code à 4 bits. Les bits USER sont utilisés pour étendre la signification du champ TYPE. La valeur par défaut du champ USER est "0000". Pour les trames Ethernet, les bits de champ USER "0" et "1" indiquent la priorité du paquet lorsqu'il passe à travers le commutateur.

• SA (adresse source): adresse source du commutateur transmettant la trame ISL (Inter-Switch Link).

• Len: la longueur du paquet.

• SNAP: protocole d'accès au sous-réseau (SNAP) et contrôle de liaison logique (LLC). Le champ SNAP AAAA03 est une valeur constante de 24 bits de "AAAA03".

• HSA (High Bits of Source Address): le champ HSA est une valeur de 24 bits qui représente les 3 octets supérieurs (la partie ID du fabricant) du champ SA.

• VLAN (Destination VLAN ID): indique l'ID VLAN du paquet. L'ID de VLAN est une valeur de 15 bits utilisée pour distinguer les trames sur différents VLAN. L'ID de VLAN est également connu sous le nom de «couleur» de la trame.

• BPDU: Indiquez si une trame BPDU, CDP ou VTP

• Index: l'index du port de la source du paquet.

• Res: champ réservé pour des informations supplémentaires, par exemple, champ Token Ring ou FDDI Frame Check Sequence. Pour Ethernet, ce champ doit être égal à zéro.

• Trame Ethernet encapsulée: la trame Ethernet réelle.

• ISL CRC: contrôle de quatre octets sur le paquet ISL pour s'assurer qu'il n'est pas corrompu.

2.10 La notion des trunks

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

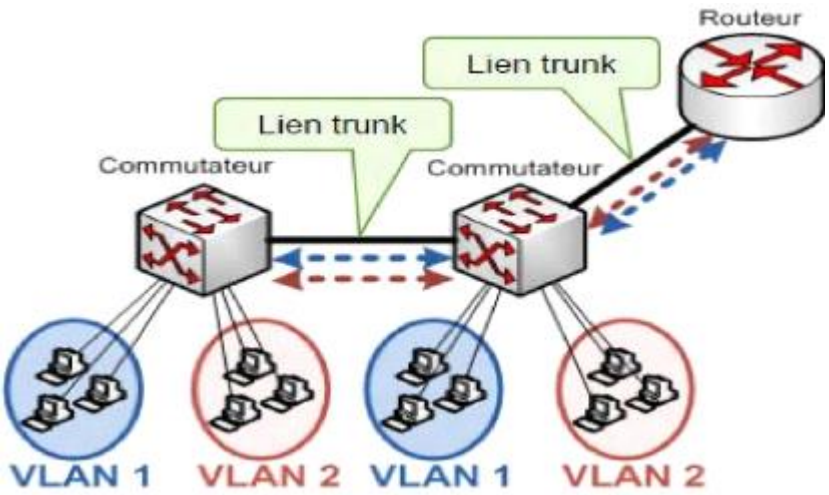


Fig.2.8

2.11. Types de VLAN

Il existe trois types d'appartenance à un VLAN: **[7]**

2.11.1VLAN de données

Un VLAN de données est un réseau local virtuel qui est configuré pour ne transporter que le trafic généré par l'utilisateur. Un VLAN peut transporter le trafic vocal ou le trafic utilisé pour gérer le commutateur.

2.11.2. VLAN par défaut

Tous les ports du commutateur deviennent membres du VLAN par défaut après le démarrage initial du commutateur. Étant donné que tous les ports du commutateur participent au VLAN par défaut.

2.11.3. VLAN natif Un VLAN

Natif est affecté à un port d'agrégation 802.1Q.

2.11.4. VLAN de gestion

Un VLAN de gestion est un VLAN que vous configurez pour accéder aux fonctionnalités de gestion d'un commutateur. VLAN 1 est le VLAN de gestion si vous ne définissez pas un VLAN différent pour remplir cette fonction.

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

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

2.12 Protocoles de transport des VLANs

2.12.1 VTP (Virtual Trunking Protocol)

VTP (Virtual Trunking Protocol), protocole propriétaire Cisco permet, aux commutateurs et routeurs qui l'implémentent, d'échanger des informations de configuration des VLAN. Il permet donc de redistribuer une configuration à d'autres commutateurs, évitant par la même occasion à l'administrateur de faire des erreurs, en se trompant par exemple de nom de VLAN.

VTP diffuse ses mises à jour au sein du domaine VTP toutes les 5 min ou lorsqu'une modification a lieu. Les mises à jour VTP comportent:

• Un numéro de révision (Revision Number) qui est incrémenté à chaque nouvelle diffusion. Cela permet aux commutateurs de savoir s'ils sont à jour.

• Les noms et numéro de VLAN.

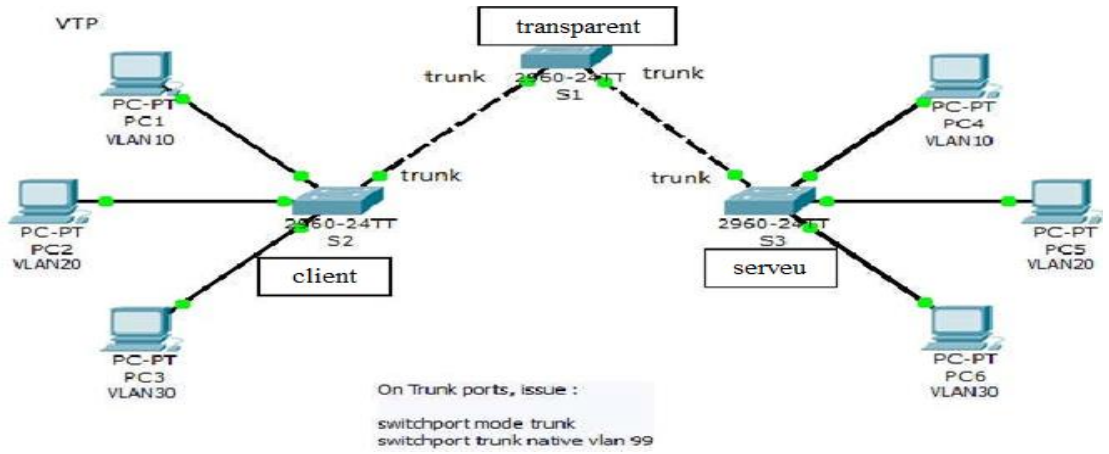


Fig.2.9

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

❖ VTP Server

Le Switch en mode Server (mode par défaut), permet à l'administrateur de faire des modifications sur les VLANs et de les propager automatiquement vers tous les Switch du réseau.

❖ VTP Client

Le switch en mode Client reçoit les mises à jour, les prend en charge, les transmet, mais ne permet pas à l'administrateur de faire des modifications sur les VLANs.

❖ VTP Transparent

Le switch en mode Transparent reçoit les mises à jour et les transmet sans les prendre en compte. Il permet à l'administrateur de faire toutes sortes de modifications sur les VLANs (en local uniquement) donc il ne propage pas ses modifications vers tous les switchs du réseau.

2.12.2 Fonctionnement

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

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

fonction	mode serveur	Mode client	Mode transparent
Envoi de messages VTP	Oui	Non	Non
Réception de messages VTP ; synchronisation VLAN	Oui	Oui	Non
Transmission des messages VTP reçus	Oui	Oui	Oui
Sauvegarde de configuration VLAN (en NVRAM ou Flash)	Oui	Non	Oui
Edition des VLANs (création, modification, suppression)	Oui	Non	Oui

Tab.2.1

2.13 Rappel sur la notion de VLAN (Vertual 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.

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).

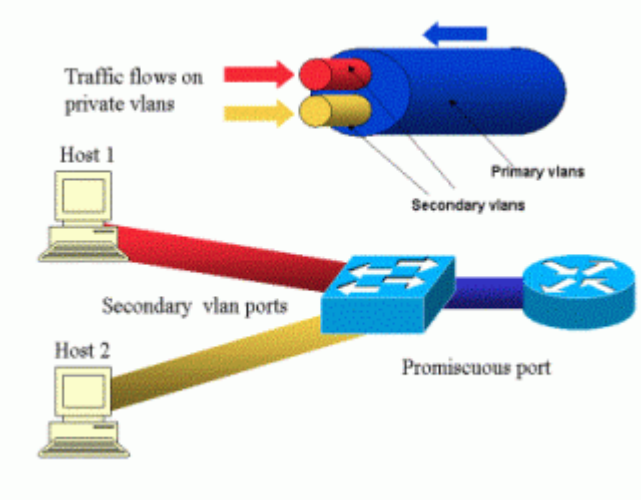


Fig.2.10

2.13.1Type 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 VLAN s 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.

Cas particulier de la connexion d'un téléphone IP suivi d'un PC sur un port.
Dans le cas de l'utilisation d'un ordinateur connecté à un téléphone IP (ce dernier étant connecté à un port du switch), le port aura deux VLANs (un VLAN dédié au réseau donné et un vlan dédié au réseau voix). Le port sera configuré en général en mode access, une commande sera ajoutée pour la configuration du VLAN voix (voice VLAN).

2.13.2 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.

2.13.3 Communication entre les VLAN.
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 VLAN1). 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.

2.13.4 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.

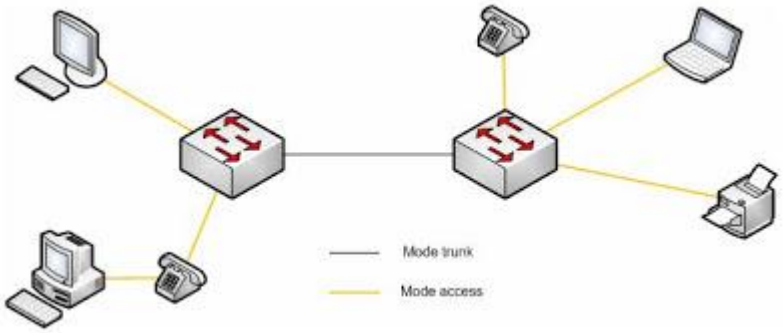


Fig.2.11

2.14 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. **[4]**

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.

Les premières configurations de VLAN reposaient sur des routeurs externes connectés à 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.

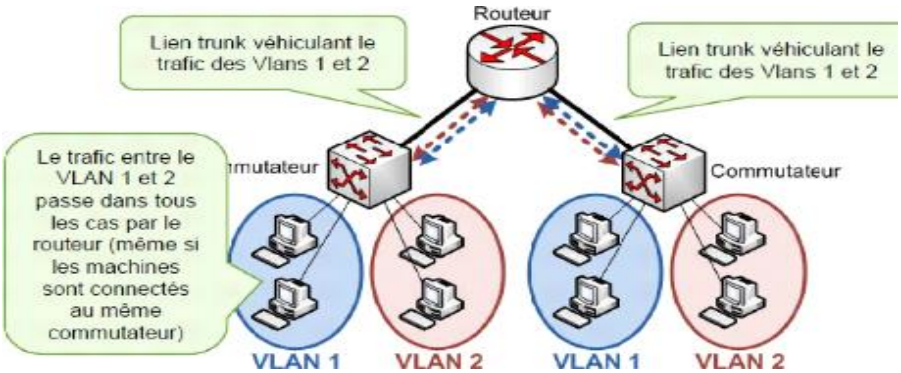


Fig.2.12 routage INTER-VLAN

2.15 Conclusion

Les Vlans sont une réponse bien adaptée à la problématique de la séparation des communautés d'utilisateurs sur un réseau local. La mise en œuvre est relativement simple et facilite les tâches d'administration. Un soin tout particulier doit être apporté à la mise en œuvre selon le type de Vlans (par port, par adresse MAC, etc.). Il faut tout de même faire attention à la technologie des Vlans, car elle n'est pas exempte de problèmes de sécurité. Ce dernier se comporte à des problèmes d'implémentation, gestion et attribution des numéros de Vlans, etc.

Chapitre03 :

La mise en place de VLANs

3.1 Introduction

Dans le but d'illustrer et de compléter ce qui a été traité dans les deux chapitres précédents de notre mémoire, plus exactement dans le premier et le deuxième chapitre, nous faisons une simulation de réseau informatique, en commençant par une étude de l'existant puis en configurant sur ce dernier les équipements utilisés en appliquant le sécurité des VLANs. Dans ce chapitre, nous présentons le logiciel utilisé et l'environnement de travail ainsi que les différentes configurations utilisées, enfin nous donnerons les résultats obtenus de la configuration.

***Partie01* : structure et adressage du réseau**

3.2 Présentation

Dans ce chapitre, nous allons voir comment mettre en place un réseau simple, pour bien expliquer les détails et aborder tous les aspects techniques de la mise en œuvre des VLANs.

Le réseau composé de 2 postes de travail,2 IP phones, un switch et un routeur. Le switch partagera 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.

3.3 Architecture scenario de déploiement

Pour illustrer ce scenario de déploiement, nous utilisons ce schéma fait sous Cisco Packet Tracer :

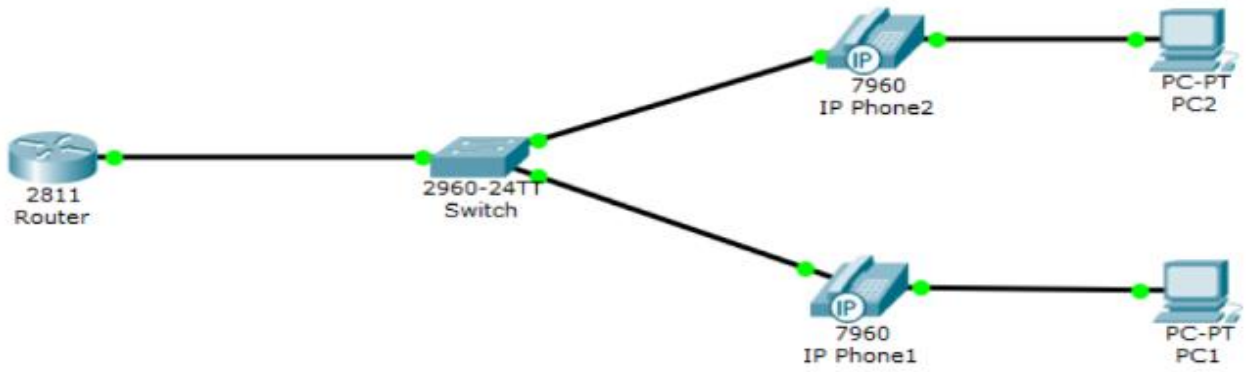


Fig.3.1

3.4 Présentation de simulateur « Cisco Packet Tracer »

3.4.1 Définition

Dans cette présentation, on essaye de configurer notre modèle type en utilisant le simulateur « Cisco Packet Taraser », faire aussi les différentes tests et la validation de la configuration.

Le « Cisco Packet Taraser » est un programme puissant de simulation qui permet aux étudiants d'expérimenter le comportement du réseau. En effet Packet Taraser fournit la simulation, la visualisation, la création, l'évaluation et les capacités de collaboration et facilite l'enseignement et l'apprentissage des technologies complexes. A travers le logiciel de simulation Packet Tracer nous avion reproduit notre environnement de travail. Cet environnement nous permettra d'aboutir à une bonne configuration de notre solution VLAN.

3.4.2 Présentation de l'écran

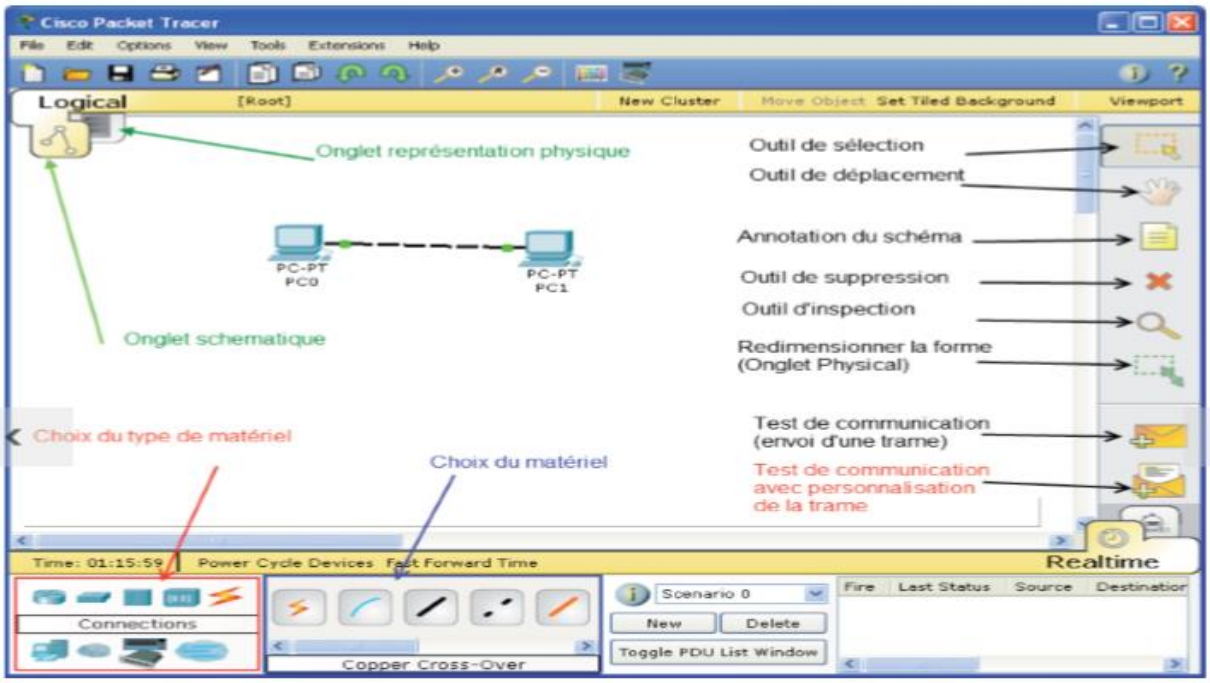


Fig.3.2

Trois éléments de la fenêtre de Packet Tracer seront nécessaires :

1. La zone de travail.

2. Les types d'appareillages.

3. Les différents modèles d'appareils du type sélectionné dans la zone 2.

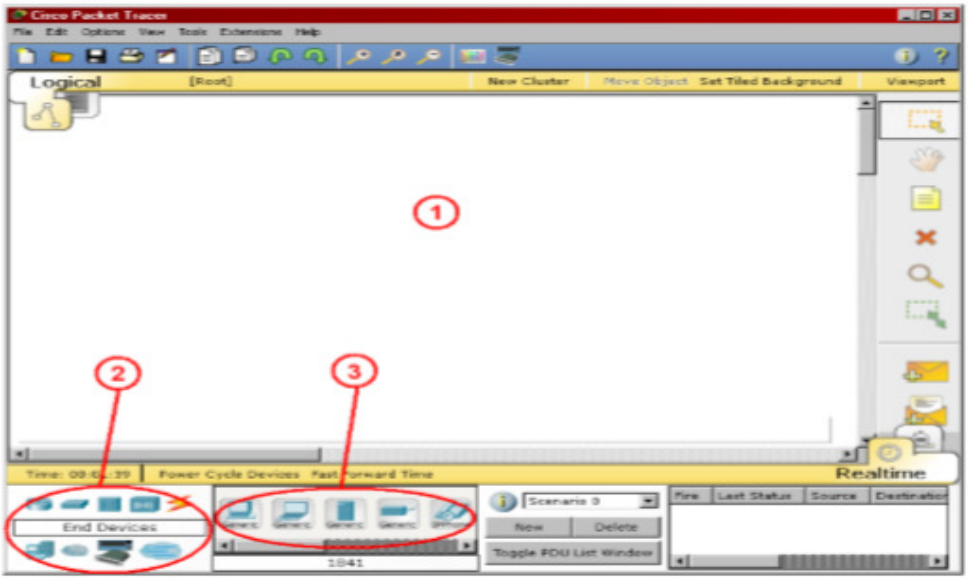
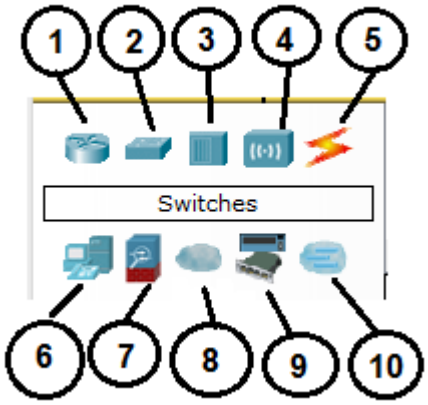


Fig.3.3

Les différents types d'appareils disponibles dans la boîte à outils de la zone 2 sont les suivants:

1. Les routeurs.
2. Les commutateurs (switches).
3. Les concentrateurs (hubs).
4. Les bornes sans fil (wifi).
5. Les connexions.
6. Les ordinateurs.
7. La sécurité.
8. et 9. Des appareils divers.
10. Les connexions multi-usagers.



3.4.3 Spécification des connexions possibles


Choix automatique


Câble Console : les connexions console peuvent être établies entre PCs et routeurs ou commutateurs. Elles servent principalement à configurer les équipements.


Câble droit : standard Ethernet pour connecter les équipements opérant dans les différentes couches du modèle OSI. Packet Tracer supporte le 10, 100 et 1000 Mbps.


Câble croisé : standard Ethernet pour connecter les équipements opérant dans les mêmes couches du modèle OSI. Packet Tracer supporte le 10, 100 et 1000 Mbps.


Fibre optique : les connexions fibres peuvent être établies si les équipements possèdent les ports fibre adéquates. Packet Tracer supporte le 100 et 1000 Mbps.


Ligne téléphonique : Les connexions téléphoniques ne sont disponibles qu'entre les équipements possédant des ports modem. Ces connexions se font généralement à travers un nuage réseau.


Câble Coaxial : Même chose que pour la ligne téléphonique, sauf que les ports utilisés sont des ports coaxiales.



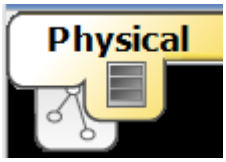
Câbles DCE et DTE : les connexions sérials se font entre 2 ports séries. Elles sont souvent utilisées pour simuler des liens WAN. Le doit être activé sur le câble DCE pour activer la connexion. En fonction du premier câble sélectionné (DTE ou DCE) le deuxième sera forcément de l'autre type afin d'assurer la connexion

Le câble asynchrone à 8 ports fournit le connecteur haute densité à une extrémité et huit fiches RJ-45 à l'autre.

3.4.4 Affichage physique du matériel

Loin d'être un gadget, la visualisation du matériel permet, dans un projet réel de câblage informatique de positionner le matériel dans les locaux.

• Afficher l'onglet Physical



• Par défaut, il présente une carte Intercité (Intercity) sur laquelle se trouve la ville (HomeCity)

• Par glisser-déposer, on peut placer la ville où on le souhaite. On peut également rajouter d'autres villes en cliquant sur le bouton New City.

• En cliquant sur la ville, on réalise un zoom géographique qui permet de voir l'immeuble dans la ville. Cet immeuble peut également être placé où on le souhaite et d'autres immeubles (bouton New Building) peuvent être rajoutés.

• De la même manière, un clic gauche sur l'immeuble permet de voir les bureaux et les équipements réseaux sont représentés dans une fenêtre flottante que l'on peut placer dans le bureau que l'on souhaite.

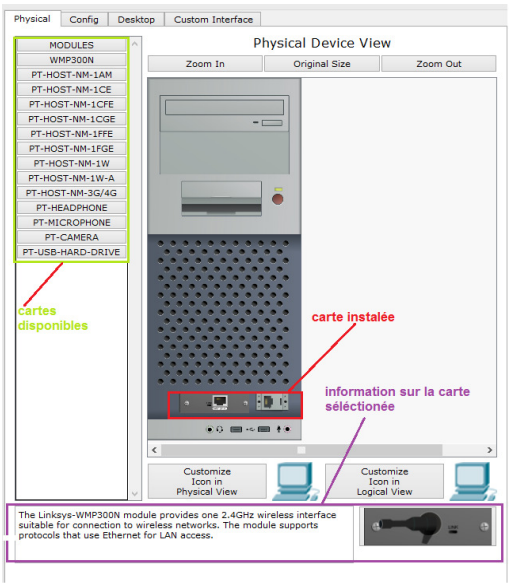
• Pour finir, un clic sur l'équipement réseau montre la table supportant les équipements de bureau et une baie présente les éléments actifs du réseau.

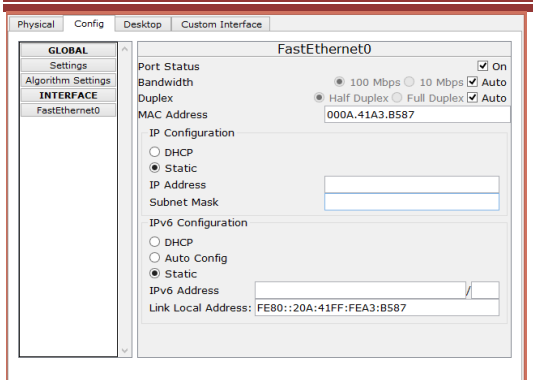
• En cliquant sur la représentation d'un équipement, on ouvre sa fenêtre de paramétrage.

3.4.5 Paramétrage des appareils

Pour accéder au paramétrage d'un appareil, il faut cliquer, dans l'affichage physique (Physical) ou Schématique (Logical), sur la représentation de l'appareil.

Paramétragephysique (Physical) : Le paramétrage physique consiste à placer les bonnes cartes dans l'appareil. Les cartes disponibles. Pour le placer, commencer par éteindre l'appareil avec le bouton Marche/Arrêt (M/A) • Si besoin retirer la carte en place, par glisser et déplacer de l'appareil vers la liste des cartes. • Glisser la nouvelle carte sélectionnée de la liste des modules à l'emplacement vide.





Configuration : L'onglet Config permet de configurer l'équipement sélectionné. Les boutons situés à gauche de la fenêtre déterminent le groupe de paramètres à configurer.

Desktop : L'onglet Desktop met à la disposition de l'utilisateur les outils logiciels habituels des équipements.

• **IP configuration** permet de configurer les paramètres réseau de la machine

• **Dial-Up** permet de configurer un modem s'il est présent dans l'équipement

• **Terminal** permet d'accéder à une fenêtre de programmation (HyperTerminal)

• **Command prompt** est la fenêtre DOS classique permettant de lancer des commandes en ligne de commande (PING, IPCONFIG, ARP, etc...)

• **WEB Browser :** il s'agit d'un navigateur Internet

• **PC Wireless :** permet de configurer une carte WIFI si elle est présente dans l'équipement

• **VPN :** permet de configurer un canal VPN sécurisé au sein du réseau.

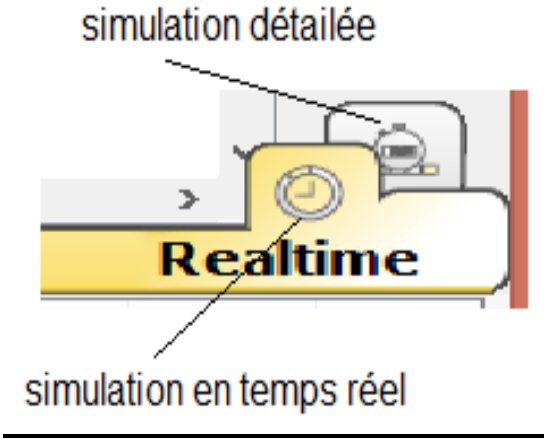
• **Traffic generator :** permet pour la simulation et l'équipement considéré de paramétrer des trames de communications particulières (exemple : requête FTP vers une machine spécifiée)

• **MIB Browser :** permet par l'analyse des fichiers MIB d'analyser les performances du réseau

• **CISCO IP Communicator :** Permet de simuler l'application logicielle de téléphonie développée par CISCO

• E Mail : client de messagerie

• **PPPOE Dialer :** pour une liaison Point à Point (Point to Point Protocol) • Text Editor : Editeur de texte



Simulation : Packet Tracer permet de simuler le fonctionnement d'un réseau par l'échange de trames Ethernet et la visualisation de celles-ci. Il existe deux modes de simulation :

• la simulation en temps réel (REALTIME): elle visionne immédiatement tous les séquences qui se produisent en temps réel.

• la simulation permet de visualiser les séquences au ralenti entre deux ou plusieurs équipements

Simulation en temps réel :

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC1	PC2	ICMP		0.000	N	0	(edit)	(delete)

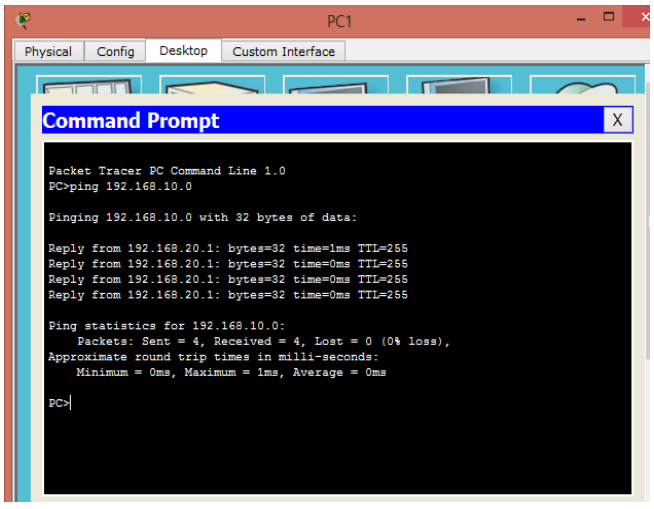
Réalisation d'un PING Un ping fait appel au protocole ICMP avec le message n°8. Packet Tracer permet de faire un ping rapidement avec l'outil Add Simple PDU. • Sélectionner l'outil

• Cliquer sur l'ordinateur émetteur du PING

• Cliquer ensuite sur l'ordinateur Destinataire du PING

• La fenêtre d'état informera de la réussite (Successfull) ou de l'échec (Failed) de la transaction

Simulation en ligne de commande :
Comme sur un vrai ordinateur, il est possible par ligne de commande de saisir des commande réseau (IPCONFIG, PING, ARP...)
• Ouvrir la fenêtre de configuration de l'ordinateur en cliquant sur sa représentation
• Choisir l'onglet Desktop
• Sélectionner l'outil Command Prompt
• Saisir la commande souhaitée
• Valider par la touche ENTREE



3.4.6 Les principales commandes CISCO (CLI)

Fonction Configuration Basiques	Commandes Cisco
Entrer en mode privilégié	Enable
Se déconnecter	Logout
Configurer un mot de passe pour les sessions telnet	Router(config)#**line vty 0 4** Router(config-line)#**login** Router(config-line)#**password cisco**
Configurer un mot de passe pour le mode privilégié	Router(config)#enable password cisco
Activer une interface	Router(config-if)#**no shutdown**
Désactiver une interface	Router(config-if)#**shutdown**
Ajouter une adresse IP à une interface	Router(config-if)#ip addr 10.1.1.1 255.255.255.0
Active le routage dynamique RIP pour le réseau 172.16.x.y	Router(config)#**router rip** Router(config-router)#**network 172.16.0.0**
Désactiver le routage RIP	Router(config)#**no router rip**
Active le routage dynamique OSPF pour le réseau 192.168.2.0 dans l'area 2	Router(config)#router ospf 200 Router(config-router)# network 192.168.2.0 0.0.0.255 area 2
Désactiver le routage OSPF	Router(config)#no router ospf 200
Ajouter une route statique sur un routeur. La route précise que pour le réseau 172.16.1.0 dont le masque est 255.255.255.0, il faut utiliser le "Next Hop" 172.16.2.1 avec une métrique de 5.	Router(config)#ip route 172.16.1.0 255.255.255.0 172.16.2.1 5

Création d'une interface virtuelle	Router(config)#int fa 0/0.1
Désactiver le CDP pour tout le routeur	Router(config)#**no cdp run**
Activer CDP pour tout le routeur	Router(config)#**cdp run**
Désactiver CDP sur une interface	Router(config-if)#**no cdp enable**

Fonction de visualisation	Commandes Cisco
Visualisation du système hardware et software	show version
Visualisation de la configuration courante (DRAM)	show running-config
Visualisation de la configuration de démarrage (NVRAM)	show startup-config
Visualisation des informations de la flash:	show flash
Visualisation des Logs	show log
Visualisation de l'interface Ethernet 0	show interface e0
Visualisation de toutes les interfaces (Affichage bref)	show ip interfaces brief
Affichage des composants connectés utilisant CDP	show cdp neighbor
Affichage des protocoles de routages utilisés	show ip protocols

Tab3.1

3.5 Interface commande de Packet Tracer

Toutes les configurations des équipements du réseau, c'est au niveau de CLI (Command Language Interface) quelques seront réalisées. CLI est une interface de simulateur Packet Tracer qui permet la configuration des équipements du réseau laide 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.

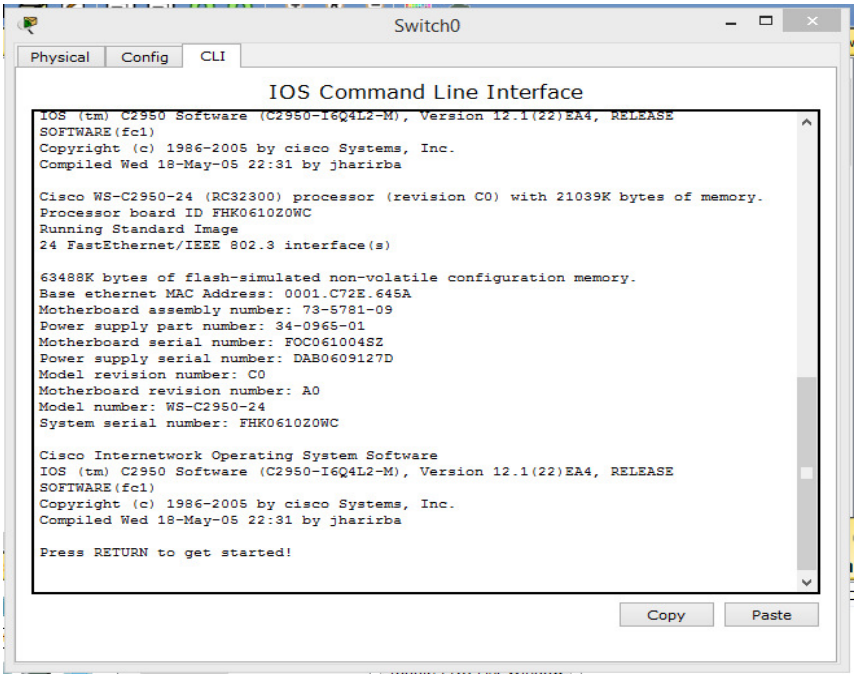


Fig.3.4

3.6 L'adressage de différents VLANs

VLAN	IP adresse	Gateway
Vlan 10	Ip phone1 :192.168.10.10 Ip phone2 :192.168.10.11	Ip phone 1 :192.168.10.1 Ip phone2 :192.168.10.1
Vlan 20	Pc1 :192.168.20.11 Pc2 :192.168.20.10	Pc1 :192.168.20.1 Pc2 :192.168.20.1

Tab.3.2

3.7 Les éléments fonctionnels de VLAN

3.7.1 Les normes

3.7.1.1 La norme 802.1q (etiquetage de trames)

Ici, l'idée serait d'arriver ce que certains ports du switch puissent être assignés plusieurs VLANs, a fera économiser du câble (et aussi des ports sur le SWITCH). Le principe consiste 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 qui est née en 1998 pour répondre un besoin de normalisation sur transport des VLANs

3.7.1.2 ISL (Encapsulation de trames)

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 ces réseaux décharger des trames.

3.7.1.3 Lien des Trunks

Le réseau local est distribué sur différents équipements via des liaisons dédiées appelées Trunks. Un trunk est une connexion physique unique sur laquelle on transmet le trac de plusieurs réseaux virtuels. Les trames qui traversent le trunk sont complétées avec un identificateur de réseau local virtuel (VLAN id). Grâce cette identification, les trames sont conservées dans un même VLAN (ou domaine de diffusion).

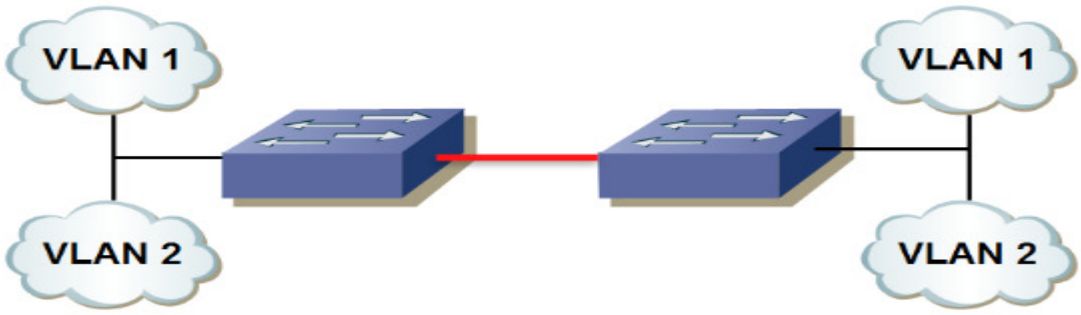


Fig.3.5

-Entre deux commutateurs : C'est le mode de distribution des réseaux locaux le plus courant.
-Entre un commutateur et un hôte : C'est le mode de fonctionnement sur veiller étroitement. Un hôte qui supporte le trunking a la possibilité d'analyser le trac de tous les réseaux locaux virtuels.
-Entre un commutateur et un routeur : C'est le mode de fonctionnement qui permet d'accéder aux fonctions de routage ; donc l'interconnexion des réseaux virtuels par routage inter-VLAN.

```
SW1(config-if)#switchport mode
trunk
```

Fig.3.6 Commande lien trunk

3.7.1.4 Le routage inter-vlan

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

-Un routeur : pour assurer le routage inter-Vlan au niveau du routeur, il faut créer des sous interfaces sur le routeur. A chaque sous interface affecter une adresse IP et le masque de sous réseau correspondant.

-commutateur de niveau 3 : pour assurer le routage inter-Vlan au niveau du commutateur de niveau 3, il faut donner des adresses IP aux différents VLAN et activer le routage à travers la commande « ip routing » en mode de configuration global.

3.7.2 Les protocoles

3.7.2.1 Protocole VTP (VLAN Trunking Protocol)

An de ne pas redéfinir tous les VLANs existant sur chaque commutateur, CISCO a développé un protocole permettant un héritage de VLANs entre commutateurs. C'est le protocole VTP, ce protocole est basé sur la norme 802.1q et exploite une architecture client-serveur avec la possibilité d'instancier plusieurs serveurs.

3.7.2.2 Protocol DHCP

DHCP signifie (Dynamic Host Configuration Protocol). S'agit dun protocole qui permet un ordinateur qui se connecte sur un réseau local d'obtenir dynamiquement (c'est-dire sans intervention particulière) sa configuration (principalement, sa configuration réseau). Vous n'avez qu'à spécifier l'ordinateur de se trouver une adresse IP tout seul par DHCP. Le but principal étant la simplification de l'administration d'un réseau.

Le protocole DHCP sert principalement distribuer des adresses IP sur un réseau, mais il a été conçu au départ comme complément au protocole BOOTP (Boot strap Protocol) qui est utilisé par exemple lorsque l'on installe une machine à travers un réseau (BOOTP est utilisé en étroite collaboration avec un serveur TFTP sur lequel le client va trouver les fichiers charger et copier sur le disque dur). Un serveur DHCP peut renvoyer des paramètres BOOTP (Boot strap Protocol) ou de configuration propres un hôte donné.

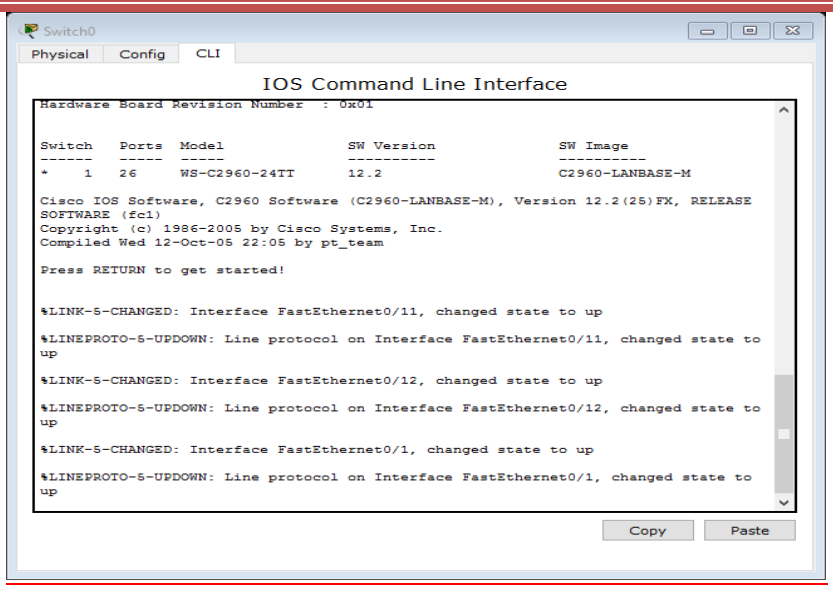
3.7.2.3 Protocole IEEE802.3ad

Est un protocole de niveau 2 du modèle OSI qui permet de grouper plusieurs ports physiques en une seule voie logique. La norme décrit l'utilisation de multiples câbles réseau Ethernet en parallèle pour augmenter la rapidité du lien au-delà des limites d'un câble ou d'un seul port, et d'accroitre la redondance pour une plus grande disponibilité.

Partie02 : configuration des équipements

3.8 Configuration des équipements

Pour configurer le commutateur via l'onglet CLI (interface de ligne de commande), l'accès au CLI se fait via la console. Le port de console nous permet de nous connecter au commutateur CLI même si le commutateur n'est pas déjà sur le réseau. Il contient un port de contrôleur qui est physiquement le port RJ45. Un ordinateur est connecté au commutateur via le câble de console. Lorsqu'un PC est physiquement connecté au port de console du commutateur, l'adaptateur doit être configuré.



Nous allons lancer des séries des configurations sur tous les équipements du réseau. Dans ce qui suit on va présenter la configuration en générale de tous les équipements.

3.8.1 Configuration du commutateur

3.8.1.1 Crée 2 vlans (vlan 10 et vlan 20)

```
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#name VOICE
Switch(config-vlan)#EXIT
Switch(config)#vlan 20
Switch(config-vlan)#name DATA
Switch(config-vlan)#EXIT
```

3.8.1.2 Attribuer des ports au vlan de données

```
Switch(config)#interface fa0/11
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
Switch(config-if)#exit
Switch(config)#interface fa0/12
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
Switch(config-if)#exit
```

3.8.1.3 Attribuer des ports au vlan vocal

```
Switch(config)#interface fa0/11
Switch(config-if)#switchport voice vlan 10
Switch(config-if)#interface fa0/12
Switch(config-if)#switchport voice vlan 10
Switch(config-if)#exit
```

3.8.1.4 Configurer le port connecté au routeur en tant que junction

```
Switch(config)#interface fa0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#
```

3.8.2 Configuration du routeur

3.8.2.1 pool DHCP pour telephones IP

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip dhcp excluded-address 192.168.10.1 192.168.10.9
Router(config)#ip dhcp pool VOICE
Router(dhcp-config)#network 192.168.10.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.10.1
Router(dhcp-config)#option 150 ip 192.168.10.1
Router(dhcp-config)#exit
```

3.8.2.2 pool DHCP pour pc IP

```
Router(config)#ip dhcp excluded-address 192.168.20.1 192.168.20.9
Router(config)#ip dhcp pool DATA
Router(dhcp-config)#network 192.168.20.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.20.1
Router(dhcp-config)#EXIT
```

3.8.3 Routeur sur une configuration de baton

3.8.3.1 créer les sous-interfaces et les associer au vlan

```
Router(config)#interface fa0/0.10
Router(config-subif)#encapsulation dot1Q 10
Router(config-subif)#ip address 192.168.10.1 255.255.255.0
Router(config-subif)#EXIT
Router(config)#interface fa0/0.20
Router(config-subif)#encapsulation dot1Q 20
Router(config-subif)#ip address 192.168.20.1 255.255.255.0
Router(config-subif)#EXIT
Router(config)#interface fa0/0
Router(config-if)#no shutdown
```

3.8.4 Configuration du gestionnaire d'appels

3.8.4.1 Difinition de nombre maximmun de téléphones IP et de numéro d'annuaire

```
Router(config-if)#telephony-service
Router(config-telephony)#max-ephones 2
Router(config-telephony)#max-dn 3
Router(config-telephony)#ip source-address 192.168.10.1 port 2000
Router(config-telephony)#create cnf-files
Router(config-telephony)#exit
```

```
Router(config)#ephone 1
Router(config-ephone)#mac-address 00D0.FF59.17E2
Router(config-ephone)#type 7960
Router(config-ephone)#exit
Router(config)#ephone 2
Router(config-ephone)#mac-address 0003.E49A.0A74
Router(config-ephone)#type 7960
Router(config-ephone)#EXIT
```

3.8.5 Configuration du telephone

3.8.5.1 Définition des numéros du telephone

```
Router(config)#ephone-dn 1
Router(config-ephone-dn)#%LINK-3-UPDOWN: Interface ephone_dsp DN 1.1, changed state to up
Router(config-ephone-dn)#number 2001
Router(config-ephone-dn)#EXIT
Router(config)#ephone-dn 2
Router(config-ephone-dn)#%LINK-3-UPDOWN: Interface ephone_dsp DN 2.1, changed state to up

Router(config-ephone-dn)#number 2002
Router(config-ephone-dn)#EXIT
Router(config)#ephone-dn 3
Router(config-ephone-dn)#%LINK-3-UPDOWN: Interface ephone_dsp DN 3.1, changed state to up

Router(config-ephone-dn)#number 2003
Router(config-ephone-dn)#exit
```

3.8.5.2 Configuration du bouton telephone

```
Router(config)#ephone 1
Router(config-ephone)#button 1:1
Router(config-ephone)#exit
Router(config)#ephone 2
Router(config-ephone)#button 1:2
Router(config-ephone)#
```

3.8.6 Attribution d'adresse IP pour PCs à partir de DHCP

On suit les étapes suivantes, chaque PC aura son adresse IP automatiquement.

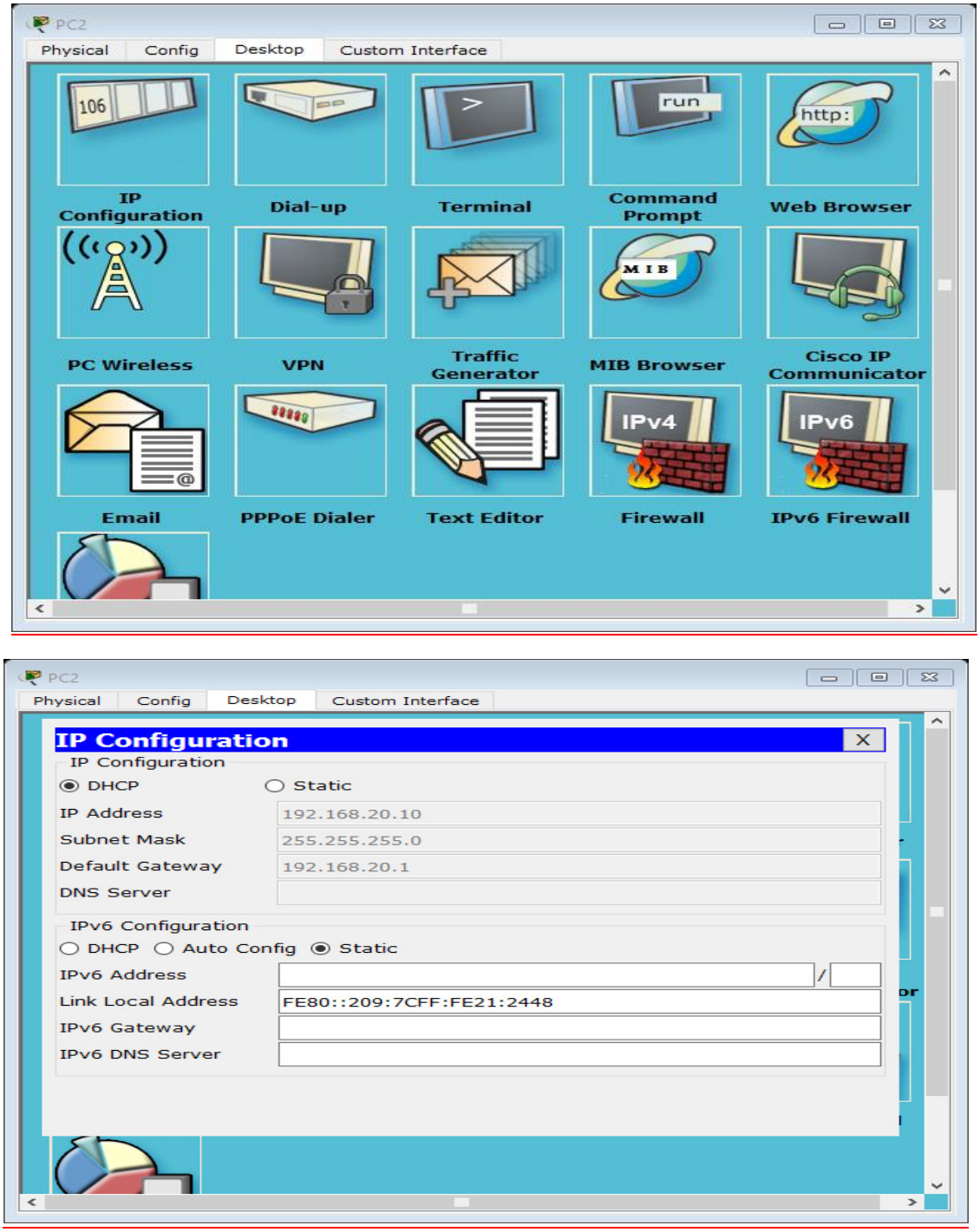


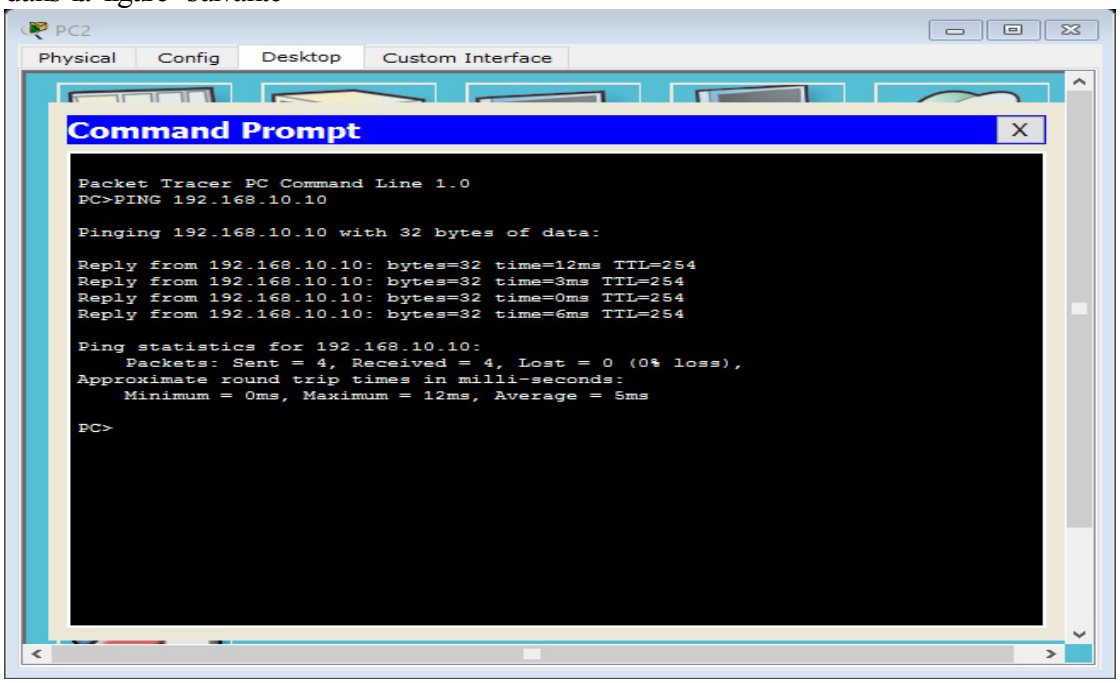
Fig.3.7

3.9 Test et validation de configuration

Pour tester la connexion entre appareils, nous utilisons une commande ping ou effectuons des appels. Ces tests sont effectués entre appareils, entre commutateurs, commutateurs internes, inter-Vlans et entre Vlans. Par conséquent, nous notons que la commande Ping est très utile pour les tests la réponse de l'ordinateur sur le réseau.

3.9.1 Test entre les équipements

1) Nous testons les connexions des commutateurs internes entre PC2 et téléphone IP1 comme indiqué dans la figure suivante



2) Nous testons la communication entre Switch test réussi entre PC1et telephone IP2 comme indiqué dans la figure suivante

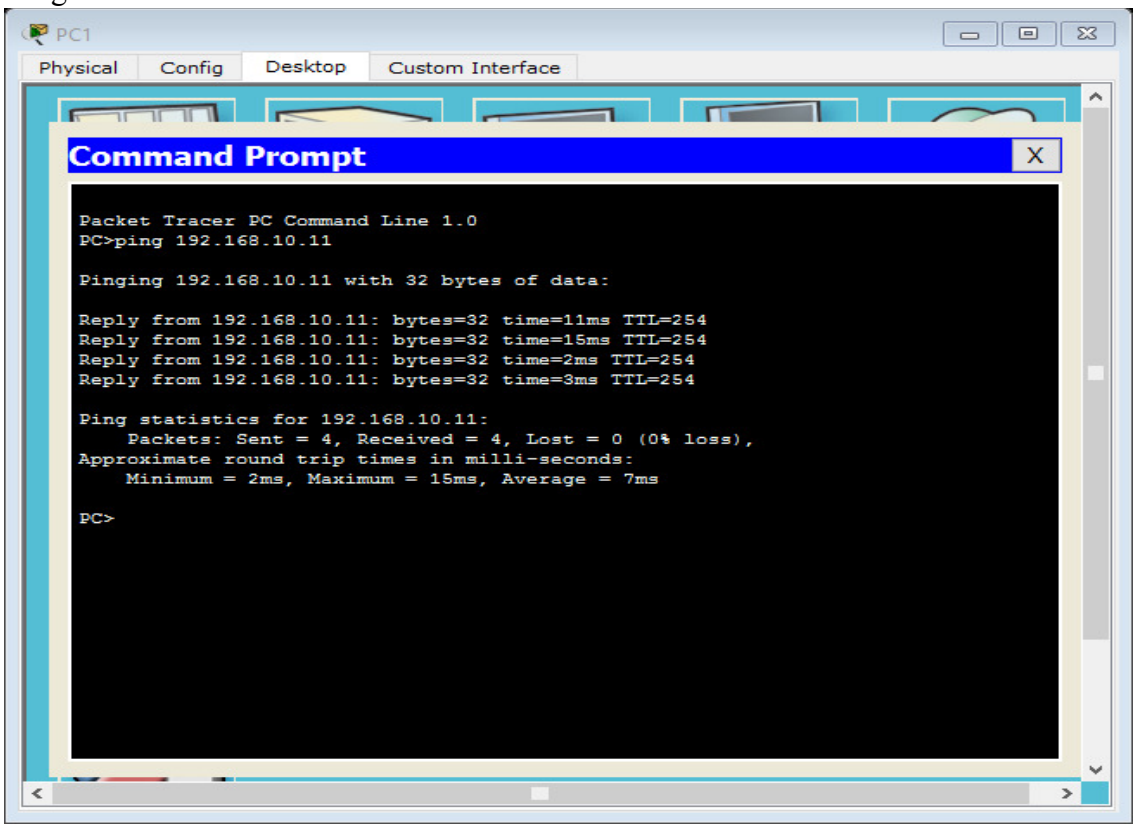


Fig.3.8

3.9.2 Test inter-Vlan

Nous testons la communication entre les téléphones IP : on effectuant un ensemble d'appelles entre eux. On prend par exemple un appelle de telephone 2 ayant le numéro 2002 vers le téléphone 1 qui a le numéro 2001. comme indiqué dans les figures suivantes.

Fig.3.9

3.9.3 Test entre Vlan

La figure suivante illustre le test entre PC1 (Vlan 20) et IP telephone 2 (Vlan 10) :

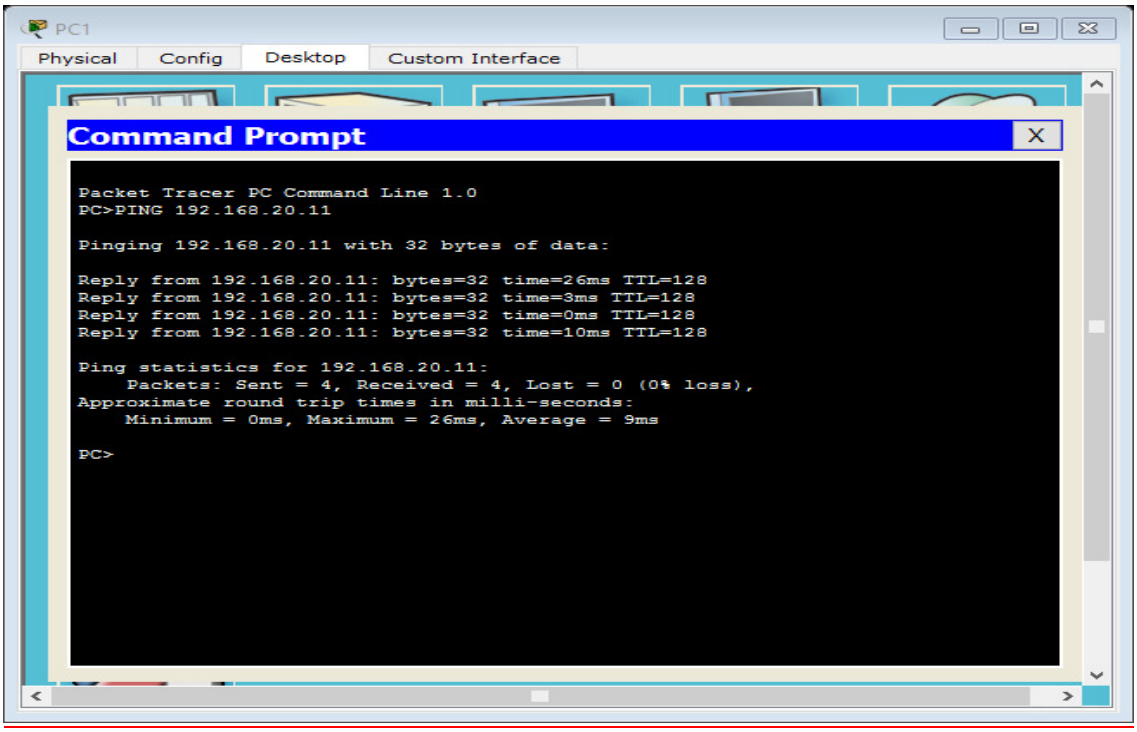


Fig.3.10

3.10 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

3.11 Conclusion

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.

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.

Nous avons créé une plate-forme VoIP dans ce chapitre qui est simulée avec le simulateur Cisco Packet Tracer, basé sur la solution Vlans et protocol DHCP. Nous avons configuré chaque appareil appartenant à ce réseau, avec des tests de validation.

En faisant cette simulation, nous avons conclu qu'aujourd'hui nous utilisons le même équipement et le même «moyen de transport» pour transporter différents contenus tels que des données, de l'audio et de la vidéo ... le tout en même temps.

Chapitre04 :

Résultat de simulation et Discussion

4.1 Introduction

Dans ce dernier chapitre, "Résultats de simulation et discussion", nous nous sommes appuyés sur la conception du modèle standard, la simulation, ainsi que toutes les configurations applicables pour les solutions et les tests de validation. Après avoir étudié les solutions théoriquement proposées dans le troisième chapitre.
Nous proposons 3 réseaux (scénario) en discutant des résultats de Chacun pour justifier les avantages et les inconvénients et clarifier notre solution choisie.

4.2 Simulation résaux01 (Scénarion 01)

4.2.1 Tableau Récapitulatif du réseau (Routeur / Switch / 4 Stations)

stations	Address IP	Masque Réseau	ports	vlans	switches	routers
Station 01	192.168.10.1	255.255.255.0	Fa0/2-5	Vlan 10	2950-24	2811
Station 02	192.168.20.1	255.255.255.0	Fa0/2-5	Vlan 20	2950-24	2811
Station 03	192.168.30.1	255.255.255.0	Fa0/6-7	Vlan 30	2950-24	2811
Station 04	192.168.40.1	255.255.255.0	Fa0/8-9	Vlan 40	2950-24	2811

Tab.4.1

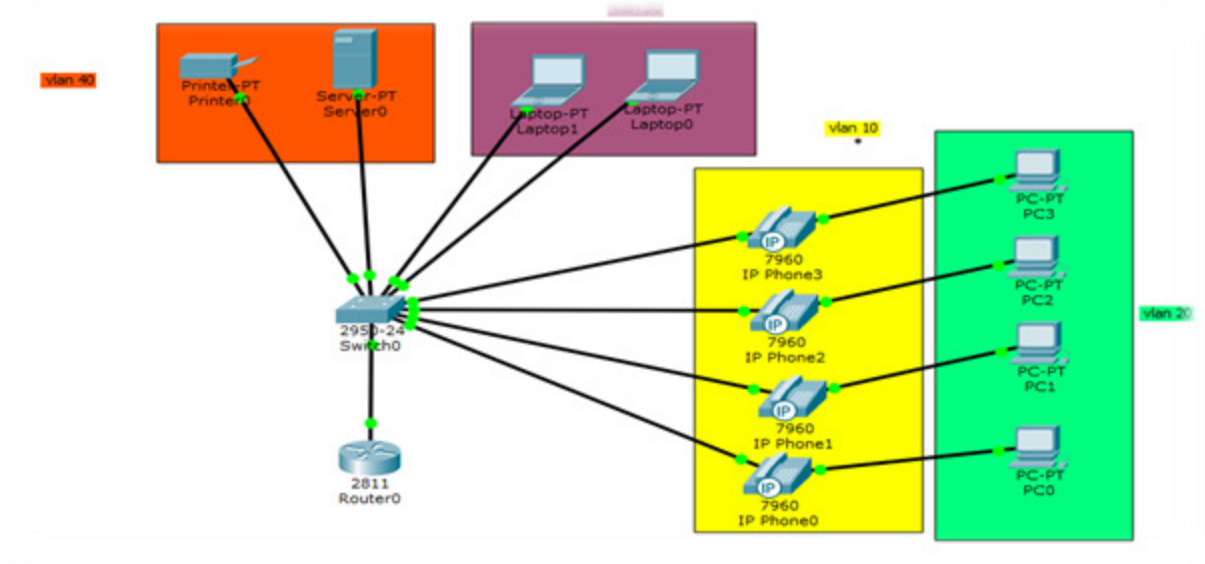


Fig.4.1

4.2.2 Configuration ET discussion des résultats réseau 01

4.2.2.1Configuration du commutateur :

Crée des vlans (vlan 10 et vlan 20,vlan 30 ,vlan 40) :

```
Switch(config)#vlan 10
Switch(config-vlan)#name voice
Switch(config-vlan)#exit
Switch(config)#vlan 20
Switch(config-vlan)#name data
Switch(config-vlan)#exit
Switch(config)#vlan 30
Switch(config-vlan)#name labto
Switch(config-vlan)#exit
Switch(config)#vlan 40
Switch(config-vlan)#name servo
Switch(config-vlan)#exit
```

Attribuer des ports au vlan vocal :

```
Switch(config)#interface range fa0/2-5
Switch(config-if-range)#switchport voice vlan 10
Switch(config-if-range)#exit
```

Attribuer des ports au vlan de données :

```
Switch(config)#interface range fa0/2-5
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 20
Switch(config-if-range)#exit
Switch(config)#interface range fa0/6-7
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 30
Switch(config-if-range)#exit
Switch(config)#interface range fa0/8-9
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 40
Switch(config-if-range)#exit
```

Configurer le port connecté au routeur en tant que junction:

A partir du port FastEthernet0/1 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 :

```
Switch(config)#interface fa0/1
Switch(config-if)#switchport mode trunk
```

4.2.2.2Configuration du routeur :

On va maintenant paramétrer le service dhcp sur le routeur afin que les postes télephoniques et les postes pc reçoivent les configuration nécessaires à leur fonctionnement .

- On va créez un pool dhcp avec la commande : **ip dhcp pool voice**
- Déclarez le réseau attribué à ce pool avec la commande : **network 192.168.10.0.255.255.255.0**

- Déclarez l'addresse ip du routeur de sortie pour ce réseau qui n'est autre que le routeur lui-même avec la commande :**default-router 192.168.10.1**
- Déclarez l'adresse ip du mandataire(le « tftp »)sur les quels les ip phones devront récupérer la configuration de la voip,qui encore une fois,est le routeur lui-même , **L'option 150** :permet au téléphone d'identifier le protocol utilisé, ici le protocole propriétaire de cisco.
- **DHCP :** Dynamic Host Configuration Protocol (Protocole de configuration d'hôte dynamique)
- **ip dhcp excluded-address** 192.168.10.1 192.168.10.9: L'adresse IP configurée sur une interface de périphérique est automatiquement exclue du pool d'adresses DHCP
- **default-router 192.168.10.1 : prenez l'adresse IP de la passerelle suivante 192.168.10.1**

pool DHCP pour telephones IP:

```
Router(config)#ip dhcp excluded-address 192.168.10.1 192.168.10.9
Router(config)#ip dhcp pool voice
Router(dhcp-config)#network 192.168.10.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.10.1
Router(dhcp-config)#option 150 ip 192.168.10.1
Router(dhcp-config)#exit
```

pool DHCP pour pc IP:

```
Router(config)#ip dhcp excluded-address 192.168.20.1 192.168.10.9
Router(config)#ip dhcp pool data
Router(dhcp-config)#network 192.168.20.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.20.1
Router(dhcp-config)#exit
Router(config)#ip dhcp excluded-address 192.168.30.1 192.168.10.9
Router(config)#ip dhcp pool labto
Router(dhcp-config)#network 192.168.30.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.30.1
Router(dhcp-config)#exit
Router(config)#ip dhcp excluded-address 192.168.40.1 192.168.10.9
Router(config)#ip dhcp pool servo
Router(dhcp-config)#network 192.168.40.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.40.1
Router(dhcp-config)#exit
```

créer les sous-interfaces et les associer au vlan:

On diffuse les Sub-adresses IP de chaque station dans le routeur pour le port FastEthernet0/0, 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(config)#interface fa0/0.10
Router(config-subif)#encapsulation dot1Q 10
Router(config-subif)#ip address 192.168.10.1 255.255.255.0
Router(config-subif)#exit
Router(config)#interface fa0/0.20
Router(config-subif)#encapsulation dot1Q 20
Router(config-subif)#ip address 192.168.20.1 255.255.255.0
Router(config-subif)#exit
Router(config)#interface fa0/0.30
Router(config-subif)#encapsulation dot1Q 30
Router(config-subif)#ip address 192.168.30.1 255.255.255.0
```

```
Router(config-subif)#exit

Router(config)#interface fa0/0.40
Router(config-subif)#encapsulation dot1Q 40
Router(config-subif)#ip address 192.168.40.1 255.255.255.0
Router(config-subif)#exit
Router(config)#interface fa0/0
Router(config-if)#no shutdown
```

On va passer à la configuration des services de téléphonie sur notre routeur.

- Déclarez le nombre maximum de téléphones IP que peut prendre en charge ce routeur.
- Déclarez le nombre maximum de numéros de téléphone que peut prendre en charge ce routeur.
- Déclarez l'adress IP source et le numéro de port (par défaut TCP 2000) que le routeur doit utiliser pour l'enregistrement des IP phones.

Difinition de nombre maximmun de téléphones IP et de numéro d'annuaire:

```
Router(config-if)#telephony-service
Router(config-telephony)#max-ephone 4
Router(config-telephony)#max-dn 5
Router(config-telephony)#ip source-address 192.168.10.1 port 2000
Router(config-telephony)#create cnf-files
Router(config-telephony)#exit
Router(config)#ephone 1
Router(config-ephone)#mac-address 000A.F34B.7740
Router(config-ephone)#type 7960
Router(config-ephone)#exit
Router(config)#ephone 2
Router(config-ephone)#mac-address 0060.5C43.14C0
Router(config-ephone)#type 7960
Router(config-ephone)#EXIT
Router(config)#ephone 3
Router(config-ephone)#mac-address 00E0.F7B7.633D
Router(config-ephone)#type 7960
Router(config-ephone)#EXIT
Router(config)#ephone 4
Router(config-ephone)#mac-address 00E0.A37C.4729
Router(config-ephone)#type 7960
Router(config-ephone)#EXI
```

On va maintenant attribuer des numéros à nos IP phones qui seront assignés automatiquement.

- Entrez dans la configuration du 1er numéro de téléphone.
- Définissez un numéro de téléphone (interne) de votre choix.

Définition des numéros du telephone:

```
Router(config)#ephone-dn 1
Router(config-ephone-dn)#number 200
Router(config-ephone-dn)#EXIT
Router(config)#ephone-dn 2
Router(config-ephone-dn)#number 300
Router(config-ephone-dn)#EXIT
```

```
Router(config)#ephone-dn 3

Router(config-ephone-dn)#number 400
Router(config-ephone-dn)#EXIT
Router(config)#ephone-dn 4
Router(config-ephone-dn)#number 500
Router(config-ephone-dn)#EXIT
```

Configuration du bouton telephone:

```
Router(config)#ephone 1
Router(config-ephone)#button 1:1
Router(config-ephone)#exit
Router(config)#ephone 2
Router(config-ephone)#button 1:2
Router(config-ephone)#
Router(config)#ephone 3
Router(config-ephone)#button 1:3
Router(config-ephone)#exit
Router(config)#ephone 4
Router(config-ephone)#button 1:4
```

Avantages de **DHCP** dans l'administration d'un réseau : Le protocole **DHCP** offre une configuration de réseau TCP/IP fiable et simple, empêche les conflits d'adresses et permet de contrôler l'utilisation des adresses IP de façon centralisée.

On parle alors de téléphonie VoIP (voix par IP) ou de téléphonie IP (Internet Protocol), un nouveau mode de communication téléphonique où la voix est numérisée, puis acheminée grâce à une connexion internet à large bande. Apparu il y a seulement quelques années, le marché de la téléphonie IP-PBX a déjà dépassé celui du PBX (téléphones traditionnels). Ce succès s'explique notamment par les économies reliées et qui font de la téléphonie IP un choix stratégique d'avenir.

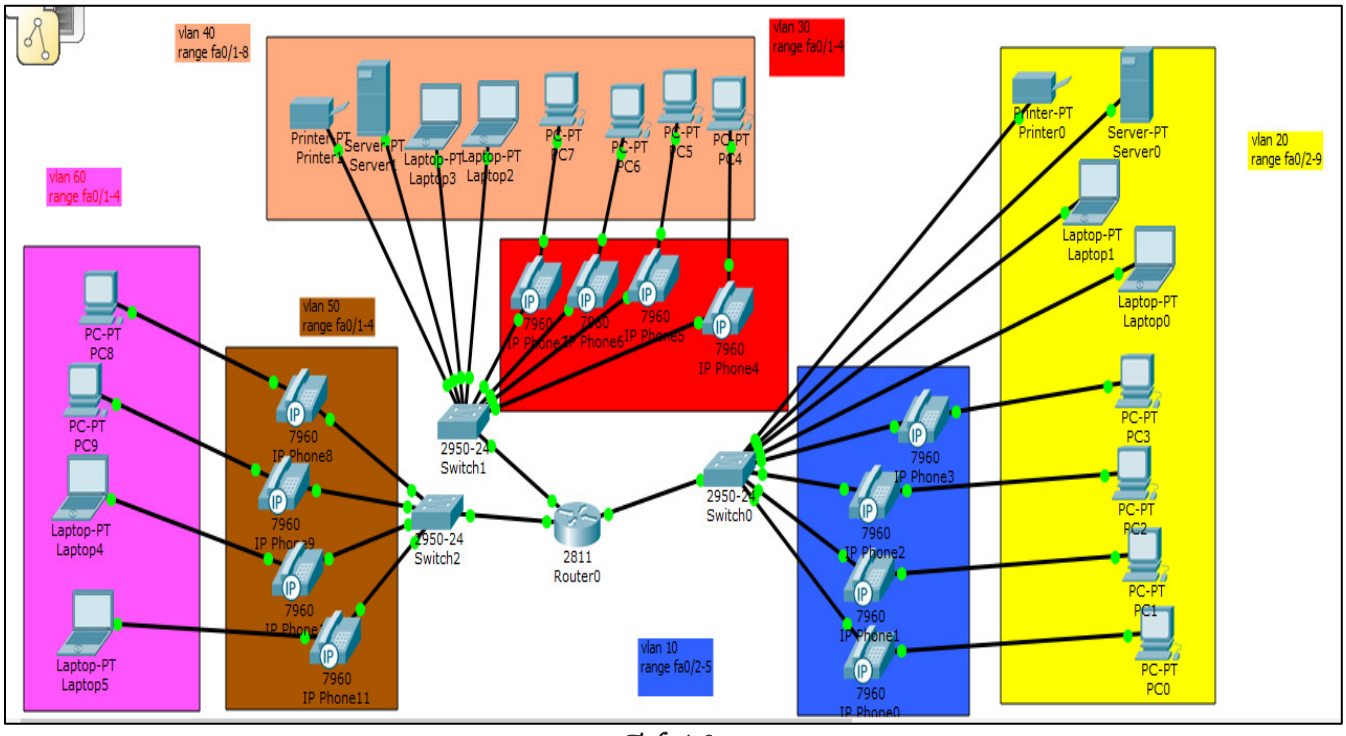
4.3 SIMULATION (résau02)(Scénario 02)

4.3.1 Tableau Récapitulatif du réseau (01 Routeur /03 Switch / 6 Stations)

stations	Address IP	Masque Réseau	Ports	vlans	switches	routers
Station 01	192.168.10.1	255.255.255.0	Fa0/2-5	Vlan 10	2950-24	2811
Station 02	192.168.20.1	255.255.255.0	Fa0/2-9	Vlan 20	2950-24	2811
Station 03	192.168.30.1	255.255.255.0	Fa0/1-4	Vlan 30	2950-24	2811
Station 04	192.168.40.1	255.255.255.0	Fa0/1-8	Vlan 40	2950-24	2811
Station 05	192.168.50.1	255.255.255.0	Fa0/1-4	Vlan 50	2950-24	2811
Station 06	192.168.60.1	255.255.255.0	Fa0/1-4	Vlan 60	2950-24	2811

Tab.4.2

4.3.2 Configuration ET discussion des résultats réseau 02



Tab.4.2

4.3.2.1Configuration du commutateur :

Crée des vlans dans le Switch0

```
Switch(config)#vlan 10
Switch(config-vlan)#name voice
Switch(config-vlan)#exit
Switch(config)#vlan 20
Switch(config-vlan)#name data
Switch(config-vlan)#exit
```

Attribuer des ports au vlan vocal dans le Switch0

```
Switch(config)#interface range fa0/2-5
Switch(config-if-range)#switchport voice vlan 10
Switch(config-if-range)#exit
```

Attribuer des ports au vlan de données dans le Switch0

```
Switch(config)#interface range fa0/2-9
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 20
Switch(config-if-range)#exit
```

Configurer le port connecté au routeur en tant que junction

A partir du port FastEthernet0/1 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 :

```
Switch(config)#interface fa0/1
Switch(config-if)#switchport mode trunk
```

Crée des vlans dans le Switch1

```
Switch(config)#vlan 30
Switch(config-vlan)#name voice1
Switch(config-vlan)#exit
Switch(config)#vlan 40
Switch(config-vlan)#name servo
Switch(config-vlan)#exit
```

Attribuer des ports au vlan vocal dans le Switch1

```
Switch(config)#interface range fa0/1-4
Switch(config-if-range)#switchport voice vlan 30
Switch(config-if-range)#exit
```

Attribuer des ports au vlan de données dans le Switch1

```
Switch(config)#interface range fa0/1-8
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 40
Switch(config-if-range)#exit
```

Configurer le port connecté au routeur en tant que junction

A partir du port FastEthernet0/11 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 :

```
Switch(config)#interface fa0/11
Switch(config-if)#switchport mode trunk
```

Crée des vlans dans le Switch2

```
Switch(config)#vlan 50
Switch(config-vlan)#name voice2
Switch(config-vlan)#exit
Switch(config)#vlan 60
Switch(config-vlan)#name labto
Switch(config-vlan)#exit
```

Attribuer des ports au vlan vocal dans le Switch2

```
Switch(config)#interface range fa0/1-4
Switch(config-if-range)#switchport voice vlan 50
Switch(config-if-range)#exit
```

Attribuer des ports au vlan de données dans le Switch2

```
Switch(config)#interface range fa0/1-4
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 60
Switch(config-if-range)#exit
```

Configurer le port connecté au routeur en tant que junction

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 :

```
Switch(config)#interface fa0/5
Switch(config-if)#switchport mode trunk
```

4.3.2.2Configuration du routeur :

pool DHCP pour telephones IP:

```
Router(config)#ip dhcp excluded-address 192.168.10.1 192.168.10.9
Router(config)#ip dhcp pool voice
Router(dhcp-config)#network 192.168.10.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.10.1
Router(dhcp-config)#option 150 ip 192.168.10.1
Router(dhcp-config)#exit
Router(config)#ip dhcp excluded-address 192.168.30.1 192.168.30.9
Router(config)#ip dhcp pool voice1
Router(dhcp-config)#network 192.168.30.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.30.1
Router(dhcp-config)#option 150 ip 192.168.30.1
Router(dhcp-config)#exit
Router(config)#ip dhcp excluded-address 192.168.50.1 192.168.50.9
Router(config)#ip dhcp pool voice2
Router(dhcp-config)#network 192.168.50.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.50.1
Router(dhcp-config)#option 150 ip 192.168.50.1
Router(dhcp-config)#exit
```

pool DHCP pour pc IP:

```
Router(config)#ip dhcp excluded-address 192.168.20.1 192.168.20.9
Router(config)#ip dhcp pool data
Router(dhcp-config)#network 192.168.20.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.20.1
Router(dhcp-config)#exit
Router(config)#ip dhcp excluded-address 192.168.40.1 192.168.40.9
Router(config)#ip dhcp pool servo
Router(dhcp-config)#network 192.168.40.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.40.1
Router(dhcp-config)#exit
Router(config)#ip dhcp excluded-address 192.168.60.1 192.168.60.9
Router(config)#ip dhcp pool labto
Router(dhcp-config)#network 192.168.60.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.60.1
Router(dhcp-config)#exit
```

créer les sous-interfaces et les associer au vlan:

On diffuse les Sub-adresses IP de chaque station dans le routeur pour le port FastEthernet1/, 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(config)#interface fa1/0.50
Router(config-subif)#encapsulation dot1Q 50
Router(config-subif)#ip address 192.168.50.1 255.255.255.0
Router(config-subif)#exit
Router(config)#interface fa1/0.60
Router(config-subif)#encapsulation dot1Q 60
Router(config-subif)#ip address 192.168.60.1 255.255.255.0
Router(config-subif)#exit
Router(config)#interface fa1/0
Router(config-if)#no shutdown
Router(config-if)#interface fa0/0.10
Router(config-subif)#encapsulation dot1Q 10
Router(config-subif)#ip address 192.168.10.1 255.255.255.0
Router(config-subif)#exit
Router(config)#interface fa0/0.20
Router(config-subif)#encapsulation dot1Q 20
Router(config-subif)#ip address 192.168.20.1 255.255.255.0
Router(config-subif)#EXIT
Router(config)#interface fa0/0
Router(config-if)#no shutdown
Router(config-if)#interface fa0/1.30
Router(config-subif)#encapsulation dot1Q 30
Router(config-subif)#ip address 192.168.30.1 255.255.255.0
Router(config-subif)#EXIT
Router(config)#interface fa0/1.40
Router(config-subif)#encapsulation dot1Q 40
Router(config-subif)#ip address 192.168.40.1 255.255.255.0
Router(config-subif)#exit
Router(config)#interface fa0/1
```

Router(config-if)#no shutdown
Router(config-if)#exit

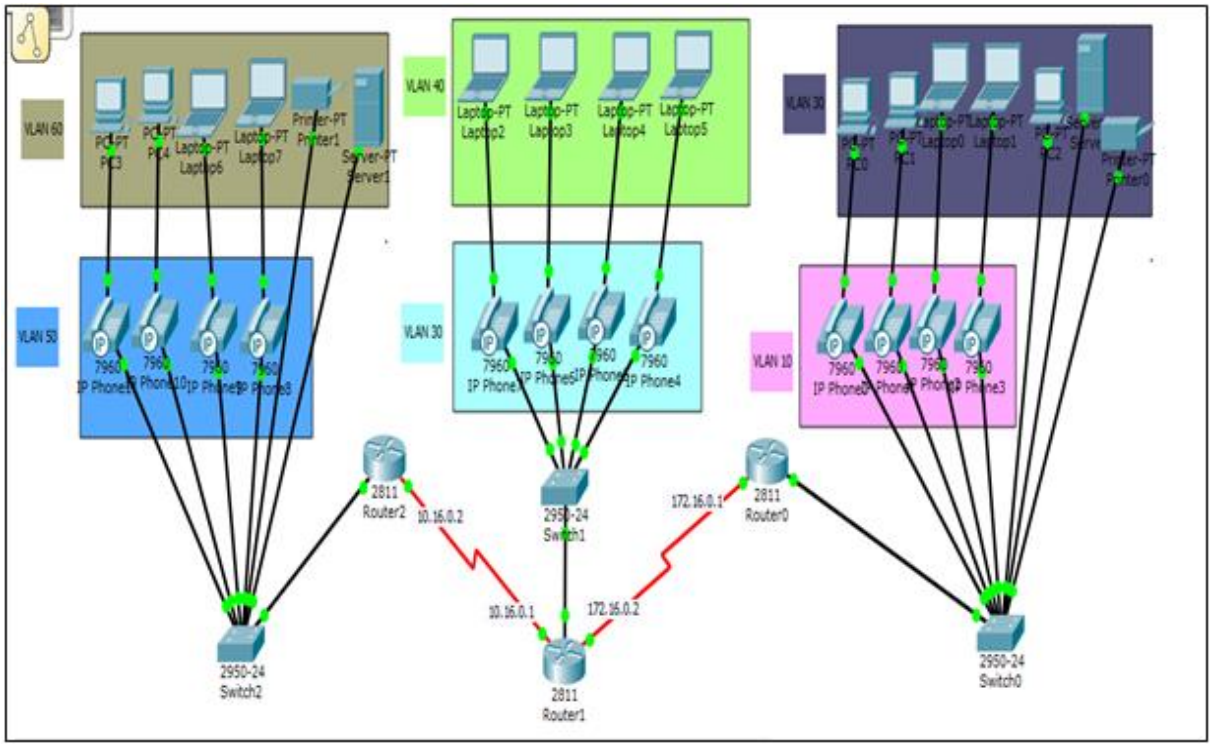
Dynamic Host Configuration Protocol (DHCP) Protocole de configuration d'hôte dynamique est un protocole de configuration automatique pour les réseaux IP . DHCP est conçu pour configurer automatiquement un ordinateur avec une adresse IP , ce qui élimine le besoin d'intervention humaine . Ce protocole assure également le suivi des ordinateurs connectés au réseau et empêche plus d'un ordinateur d'avoir la même adresse IP . Pour toutes les fonctions utiles DHCP offres , il ya quelques inconvénients à l'utilisation de ce système. Problèmes de sécurité

4.4 SIMULATION (résau03)

4.4.1 Tableau Récapitulatif du réseau (03 Routeur /03 Switch / 6 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

Tab.4.3



Tab.4.3

4.4.2 Configuration ET discussion des résultats réseau 03

1) Configuration Switch 0(Switch Droite)

Crée des vlans dans le Switch0

```
Switch(config)#vlan 10
Switch(config-vlan)#name voice
Switch(config-vlan)#exit
Switch(config)#vlan 20
Switch(config-vlan)#name data
Switch(config-vlan)#exit
```

Attribuer des ports au vlan vocal dans le Switch0

```
Switch(config)#interface range fa0/2-5
Switch(config-if-range)#switchport voice vlan 10
Switch(config-if-range)#exit
```

Attribuer des ports au vlan de données dans le Switch0

```
Switch(config)#interface range fa0/2-8
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 20
Switch(config-if-range)#exit
```

Configurer le port connecté au routeur en tant que junction

```
Switch(config)#interface fa0/1
Switch(config-if)#switchport mode trunk
```

2) Configuration Switch 1(Switch Milieu)

Crée des vlans dans le Switch1

```
Switch(config)#vlan 30
Switch(config-vlan)#name voice
Switch(config-vlan)#exit
Switch(config)#vlan 40
Switch(config-vlan)#name data
Switch(config-vlan)#exit
```

Attribuer des ports au vlan vocal dans le Switch1

```
Switch(config)#interface range fa0/2-5
Switch(config-if-range)#switchport voice vlan 30
Switch(config-if-range)#exit
```

Attribuer des ports au vlan de données dans le Switch1

```
Switch(config)#interface range fa0/2-5
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 40
Switch(config-if-range)#exit
```

Configurer le port connecté au routeur en tant que junction

```
Switch(config)#interface fa0/1
Switch(config-if)#switchport mode trunk
```

3) Configuration Switch 2(Switch Gauche)

Crée des vlans dans le Switch2

```
Switch(config)#vlan 50
Switch(config-vlan)#name voice
Switch(config-vlan)#exit
Switch(config)#vlan 60
Switch(config-vlan)#name data
Switch(config-vlan)#exit
```

Attribuer des ports au vlan vocal dans le Switch2

```
Switch(config)#interface range fa0/2-5
Switch(config-if-range)#switchport voice vlan 50
Switch(config-if-range)#exit
```

Attribuer des ports au vlan de données dans le Switch2

```
Switch(config)#interface range fa0/2-7
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 60
Switch(config-if-range)#exit
```

Configurer le port connecté au routeur en tant que junction

```
Switch(config)#interface fa0/1
Switch(config-if)#switchport mode trunk
```

4) Configuration Router 0(Router Droite)

pool DHCP pour telephones IP:

```
Router(config)#ip dhcp excluded-address 192.168.10.1 192.168.10.9
Router(config)#ip dhcp pool voice
Router(dhcp-config)#network 192.168.10.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.10.1
Router(dhcp-config)#option 150 ip 192.168.10.1
Router(dhcp-config)#exit
```

pool DHCP pour pc IP:

```
Router(config)#ip dhcp excluded-address 192.168.20.1 192.168.20.9
Router(config)#ip dhcp pool data
Router(dhcp-config)#network 192.168.20.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.20.1
Router(dhcp-config)#exit
```

créer les sous-interfaces et les associer au vlan:

```
Router(config)#interface fa0/0.10
Router(config-subif)#encapsulation dot1Q 10
Router(config-subif)#ip address 192.168.10.1 255.255.255.0
Router(config-subif)#exit
Router(config)#interface fa0/0.20
Router(config-subif)#encapsulation dot1Q 20
Router(config-subif)#ip address 192.168.20.1 255.255.255.0
Router(config-subif)#exit
Router(config)#interface fa0/0
Router(config-if)#no shutdown
```

Difinition de nombre maximmun de téléphones IP et de numéro d'annuaire:

```
Router(config)#telephony-service
Router(config-telephony)#max-ephones 4
Router(config-telephony)#max-dn 5
Router(config-telephony)#ip source-address 192.168.10.1 port 2000
Router(config-telephony)#create cnf-files
Router(config-telephony)#exit
Router(config)#ephone-dn 1
Router(config-ephone-dn)#number 2000
Router(config-ephone-dn)#exit
Router(config)#ephone-dn 2
Router(config-ephone-dn)#number 2001
Router(config-ephone-dn)#exit
Router(config)#ephone-dn 3
Router(config-ephone-dn)#number 2002
Router(config-ephone-dn)#exit
Router(config)#ephone-dn 4
Router(config-ephone-dn)#number 2003
Router(config-ephone-dn)#exit
```

Configuration du bouton telephone:

```
Router(config)#ephone 1
Router(config-ephone)#button 1:1
Router(config-ephone)#exit
Router(config)#ephone 2
Router(config-ephone)#button 1:2
Router(config)#ex
Router(config)#ephone 3
Router(config-ephone)#button 1:3
Router(config)#ephone 4
Router(config-ephone)#button 1:4
Router(config-ephone)#EXIT
```

5) Configuration Router 1(Router Milieu)

pool DHCP pour telephones IP:

```
Router(config)#ip dhcp excluded-address 192.168.30.1 192.168.30.9
Router(config)#ip dhcp pool voice
Router(dhcp-config)#network 192.168.30.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.30.1
Router(dhcp-config)#option 150 ip 192.168.30.1
Router(dhcp-config)#exit
```

pool DHCP pour pc IP:

```
Router(config)#ip dhcp excluded-address 192.168.40.1 192.168.40.9
Router(config)#ip dhcp pool data
Router(dhcp-config)#network 192.168.40.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.40.1
Router(dhcp-config)#exit
```

créer les sous-interfaces et les associer au vlan:

```
Router(config)#interface fa0/0.30
Router(config-subif)#encapsulation dot1Q 30
Router(config-subif)#ip address 192.168.30.1 255.255.255.0
Router(config-subif)#exit
Router(config)#interface fa0/0.40
Router(config-subif)#encapsulation dot1Q 40
Router(config-subif)#ip address 192.168.40.1 255.255.255.0
Router(config-subif)#exit
Router(config)#interface fa0/0
Router(config-if)#no shutdown
```

Difinition de nombre maximmun de téléphones IP et de numéro d'annuaire:

```
Router(config)#telephony-service
Router(config-telephony)#max-ephones 4
Router(config-telephony)#max-dn 5
Router(config-telephony)#ip source-address 192.168.30.1 port 2000
Router(config-telephony)#create cnf-files
Router(config-telephony)#exit
Router(config)#ephone-dn 1
Router(config-ephone-dn)#number 3000
Router(config-ephone-dn)#exit
Router(config)#ephone-dn 2
Router(config-ephone-dn)#number 3001
Router(config-ephone-dn)#exit
Router(config)#ephone-dn 3
Router(config-ephone-dn)#number 3002
Router(config-ephone-dn)#exit
Router(config)#ephone-dn 4
Router(config-ephone-dn)#number 3003
Router(config-ephone-dn)#exit
```

Configuration du bouton telephone:

```
Router(config)#ephone 1
Router(config-ephone)#button 1:1
Router(config-ephone)#exit
Router(config)#ephone 2
Router(config-ephone)#button 1:2
Router(config-ephone)#exit
Router(config)#exit
Router(config)#ephone 3
Router(config-ephone)#button 1:3
Router(config-ephone)#exit
Router(config)#ephone 4
Router(config-ephone)#button 1:4
Router(config-ephone)#exit
```

6) Configuration Router 2(Router Gauche)

pool DHCP pour telephones IP:

```
Router(config)#ip dhcp excluded-address 192.168.50.1 192.168.50.9
Router(config)#ip dhcp pool voice
Router(dhcp-config)#network 192.168.50.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.50.1
Router(dhcp-config)#option 150 ip 192.168.50.1
Router(dhcp-config)#exit
```

pool DHCP pour pc IP:

```
Router(config)#ip dhcp excluded-address 192.168.60.1 192.168.60.9
Router(config)#ip dhcp pool data
Router(dhcp-config)#network 192.168.60.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.60.1
Router(dhcp-config)#exit
```

créer les sous-interfaces et les associer au vlan:

Affectation des Sub-adresses IP pour chaque station dans le routeur 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(config)#interface fa0/0.50
Router(config-subif)#encapsulation dot1Q 50
Router(config-subif)#ip address 192.168.50.1 255.255.255.0
Router(config-subif)#exit
Router(config)#interface fa0/0.60
Router(config-subif)#encapsulation dot1Q 60
Router(config-subif)#ip address 192.168.60.1 255.255.255.0
Router(config-subif)#exit
Router(config)#interface fa0/0
Router(config-if)#no shutdown
```

Difinition de nombre maximmun de téléphones IP et de numéro d'annuaire:

```
Router(config)#telephony-service
Router(config-telephony)#max-ephones 4
Router(config-telephony)#max-dn 5
Router(config-telephony)#ip source-address 192.168.50.1 port 2000
Router(config-telephony)#create cnf-files
Router(config-telephony)#exit
Router(config)#ephone-dn 1
Router(config-ephone-dn)#number 4000
Router(config-ephone-dn)#exit
Router(config)#ephone-dn 2
Router(config-ephone-dn)#number 4001
Router(config-ephone-dn)#exit
Router(config)#ephone-dn 3
Router(config-ephone-dn)#number 4002
Router(config-ephone-dn)#exit
Router(config)#ephone-dn 4
Router(config-ephone-dn)#number 4003
```

```
Router(config-ephone-dn)#exit
```
Configuration du bouton telephone:
```
Router(config)#ephone 1
Router(config-ephone)#button 1:1
Router(config-ephone)#exit
Router(config)#ephone 2
Router(config-ephone)#button 1:2
Router(config-ephone)#exit
Router(config)#exit
Router(config)#ephone 3
Router(config-ephone)#button 1:3
Router(config-ephone)#exit
Router(config)#ephone 4
Router(config-ephone)#button 1:4
Router(config-ephone)#exit
```

4.4.3 Configuration des interfaces du routeurs (routeur0-routeur1- routeur2) :

1) Configuration d'interface du Routeur 0 (Router Droite)

Il faut configurer l'interface série via la commande interface serie 0/0/0. Et donner l'adresse IP à cettes interface via la commande ip address172.16.0.1 255.255.255.252.

```
Router(config)#interface serial 0/0/0
Router(config-if)#ip address 172.16.0.1 255.255.255.252
Router(config-if)#no shutdown
Router(config-if)#exit
```

On va appliquer la commande « router eigrp 1 » permet d'activer le process EIGRP (The Enhanced Interior Gateway ***Routing*** Protocol) est un protocole de routage propriétaire développé par Cisco à partir de leur protocole original IGRP. et de définir l'AS(1) **(Autonomous-System)** dans lequel il va fonctionner entre l'ensemble des routeurs qui doit être identique si nous souhaitons qu'ils puissent communiquer.

La commande network permet d'activer et d'associer les interfaces à un process EIGRP.

```
Router(config)#router eigrp 1
Router(config-router)#network 172.16.0.0 0.0.0.3
Router(config-router)#network 192.168.10.0 0.0.0.255
Router(config-router)#network 192.168.20.0 0.0.0.255
Router(config-router)#exit
```

Pour communiquer entre les téléphones IP Phone du **routeur 0** et du **routeur 1**,vous devez appliquer la commande : « dial-peer voice 200 voip ».

```
Router(config)#dial-peer voice 200 voip
```

```
Router(config-dial-peer)#destination-pattern 300.

Router(config-dial-peer)#session target ipv4:172.16.0.2
Router(config-dial-peer)#exit
```

Pour communiquer entre les téléphones IP Phone du **routeur 0** et du **routeur 2**,vous devez appliquer la commande : « dial-peer voice 300 voip ».

```
Router(config)#
Router(config)#dial-peer voice 300 voip
Router(config-dial-peer)#destination-pattern 400.
Router(config-dial-peer)#session target ipv4:10.16.0.2
Router(config-dial-peer)#exit
Router(config)#router eigrp 1
Router(config-router)#network 10.16.0.0 0.0.0.3
Router(config-router)#exit
```

2) Configuration d'interface du Routeur 1 (Router Milieu)

Il faut configurer l'interface série via la commande interface serie 0/0/0. Et donner l'adresse IP à cette interface via la commande ip address10.16.0.1 255.255.255.252.

```
Router(config)#interface serial 0/0/0
Router(config-if)#ip address 10.16.0.1 255.255.255.252
Router(config-if)#no shutdown
```

On va appliquer la commande « router eigrp 1 » permet d'activer le process EIGRP (The Enhanced Interior Gateway ***Routing*** Protocol) est un protocole de routage propriétaire développé par Cisco à partir de leur protocole original IGRP. et de définir l'AS(1) **(Autonomous-System)** dans lequel il va fonctionner entre l'ensemble des routeurs qui doit être identique si nous souhaitons qu'ils puissent communiquer.

La commande network permet d'activer et d'associer les interfaces à un process EIGRP.

```
Router(config-if)#router eigrp 1
Router(config-router)#network 10.16.0.0 0.0.0.3
Router(config-router)#network 192.168.30.0 0.0.0.255
Router(config-router)#network 192.168.40.0 0.0.0.255
Router(config-router)#exit
```

Pour communiquer entre les téléphones IP Phone du **routeur 1** et du **routeur 2**,vous devez appliquer la commande : « dial-peer voice 200 voip ».

```
Router(config)#dial-peer voice 200 voip
Router(config-dial-peer)#destination-pattern 400.
Router(config-dial-peer)#session target ipv4:10.16.0.2
Router(config-dial-peer)#exit
```

Il faut configurer l'interface série via la commande interface serie 0/0/1. Et donner l'adresse IP à cette interface via la commande ip address172.16.0.2 255.255.255.252.

```
Router(config)#interface serial 0/0/1
Router(config-if)#ip address 172.16.0.2 255.255.255.252
Router(config-if)#no shutdown
Router(config-if)#exit

Router(config)#router eigrp 1
Router(config-router)#network 172.16.0.0 0.0.0.3
Router(config-router)#network 192.168.30.0 0.0.0.255
Router(config-router)#network 192.168.40.0 0.0.0.255
Router(config-router)#exit
```

Pour communiquer entre les téléphones IP Phone du **routeur 1** et du **routeur 0**,vous devez appliquer la commande : « dial-peer voice 200 voip » .

```
Router(config)#dial-peer voice 200 voip
Router(config-dial-peer)#destination-pattern 200.
Router(config-dial-peer)#session target ipv4:172.16.0.1
Router(config-dial-peer)#exit
Router(config)#router eigrp 1
Router(config-router)#network 172.16.0.0 0.0.0.3
Router(config-router)#exit
Router(config)#router eigrp 1
Router(config-router)#network 10.16.0.0 0.0.0.3
Router(config-router)#exit
```

3) Configuration d'interface du Routeur 2 (Router Gauche)

Il faut configurer l'interface série via la commande interface serie 0/0/0. Et donner l'adresse IP à cette interface via la commande ip address10.16.0.2 255.255.255.252.

```
Router(config)#interface serial 0/0/0
Router(config-if)#ip address 10.16.0.2 255.255.255.252
Router(config-if)#no shutdown
Router(config-if)#exit
```

On va appliquer la commande « router eigrp 1 » permet d'activer le process EIGRP (The Enhanced Interior Gateway ***Routing*** Protocol) Protocole de routage de passerelle intérieure amélioré est un protocole de routage propriétaire développé par Cisco à partir de leur protocole original IGRP. et de définir l'AS(1) **(Autonomous-System)** dans lequel il va fonctionner entre l'ensemble des routeurs qui doit être identique si nous souhaitons qu'ils puissent communiquer.
La commande network permet d'activer et d'associer les interfaces à un process EIGRP.

```
Router(config)#router eigrp 1
Router(config-router)#network 10.16.0.0 0.0.0.3
Router(config-router)#network 192.168.50.0 0.0.0.255
Router(config-router)#network 192.168.60.0 0.0.0.255
```

Pour communiquer entre les téléphones IP Phone du **routeur 2** et du **routeur 1**,vous devez appliquer la commande : « dial-peer voice 100 voip » .

```
Router(config)#dial-peer voice 100 voip
Router(config-dial-peer)#destination-pattern 300.
Router(config-dial-peer)#session target ipv4:10.16.0.1
Router(config-dial-peer)#exit
```

Pour communiquer entre les téléphones IP du **routeur 2** et du **routeur 0**,vous devez appliquer la commande : « dial-peer voice 300 voip ».

```
Router(config)#dial-peer voice 300 voip
Router(config-dial-peer)#destination-pattern 200.
Router(config-dial-peer)#session target ipv4:172.16.0?
 Router(config-dial-peer)#session target ipv4:172.16.0.1
Router(config-dial-peer)#exit
Router(config)#router eigrp 1
Router(config-router)#network 172.16.0.0 0.0.0.3
Router(config-router)#exit
```

4.5 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 VOIP-DHCP 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 switch et dans la facilité du control de ce réseau avec des adresses IP différentes et c'est robuste à contrôlés ainsi rapide.
- Chaque périphérique sur un réseau informatique doit avoir sa propre adresse de protocole Internet unique, permettant aux routeurs et commutateurs réseau pour envoyer des données à l'ordinateur spécifique la demande. Un nouvel utilisateur au réseau peut entrer son adresse IP manuellement , ou le protocole de configuration d'hôte dynamique ou DHCP , un serveur peut attribuer une adresse IP à l'ordinateur automatiquement .
- **L'inconvénient** de l'utilisation et l'application des Vlans VOIP -DHCP 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

4.6.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) Switch via des Vlans VOIP -DHCP 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.
- DHCP permet à des ordinateurs ou d'autres appareils tels que les lecteurs multimédia pour recevoir les informations de configuration pertinente automatiquement lorsqu'ils se connectent à un 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 VOIP -DHCP 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 VOIP -DHCP est basé sur le bon fonctionnement de la connexion entre les différents PC avec des adresses IP différentes et leurs Vlans VIOP-DHCP créent dans chaque Switch et routers, 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.
- Lorsqu'un périphérique souhaite se connecter au réseau, il envoie une requête de diffusion sur le serveur DHCP. Le serveur DHCP renvoie un paquet d'offre , contenant une adresse IP , les détails de sous-réseau et les adresses de serveur DNS . Le client répond alors avec un paquet de requête , confirmant qu'il utilisera l'adresse IP attribuée.

- Afin de préserver les données et renforcer la sécurité de notre réseau, les points d'accès doivent être protégés par un mot de passe ou bien une clé wifi (WPA- MSK) du réseau public. Ainsi, mettre en place un bon système de filtrage s'impose.
- Ainsi l'utilisation du protocole RIP est nécessaire pour nous permettre de contrôler l'échange d'information et assurer la communication entre les différents stations, interdire les stations qui nous ramènent de risque pour notre réseau, et on laisse les autres en contact entre eux, grâce au protocole RIP pour assurer la protection de notre réseau des risques qui viennent de l'extérieure.
- **L'inconvénient** de l'utilisation et l'application des Vlans dans un réseau constitué de trois Router et trois (03) Switch via des Vlans VOIP -DHCP est basé seulement sur la sécurité du réseau qui n'est pas vérifier par contre la configuration du protocole (RIP) couramment utilisé pour 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 par le protocole VOIP -DHCP.

4.9.Les avantages et inconvénients du voip :

La VoIP offre de nombreux avantage, voici ceux qui nous paraissent être susceptible de jouer un rôle important dans les réseaux informatiques. **[8]**

4.9.1 AVANTAGES

L'utilisation d'un système téléphonique VOIP, suivi de ses inconvénients.

- **DES COÛTS RÉDUITS**

Il est possible de téléphoner d'un ordinateur à un autre, sans frais additionnel, dans le monde entier. Les frais d'appel vers un téléphone seront aussi beaucoup plus bas en utilisant la téléphonie « cloud ».

- **AJOUT DE SERVICES CONNEXES**

Un système téléphonique VOIP se présente généralement avec une large gamme de services supplémentaires. Notons entre autres le renvoi d'appel, l'identification du numéro de téléphone entrant et la possibilité d'échanger des documents et images.

- **UTILISATION HORS BUREAU**

En utilisant le système VOIP, on peuvent s'y connecter de la maison, de leur voiture, ou tout autre endroit où il y a un accès au réseau (bande passante).

- **FRAIS DE MATÉRIEL RESTREINT**

Contrairement aux systèmes traditionnels, la téléphonie par « Cloud » n'exige pas une pose de matériel importante, dans les bureaux physiques de l'entreprise.

4.9.2 INCONVÉNIENTS

- **FIABILITÉ ET QUALITÉ DE LA VOIX**

Le niveau du service Internet peut affecter la qualité des communications.

- **SÉCURITÉ**

Comme tout autre objet relié à l'Internet, il peut exister des dangers au niveau de la sécurité, desquels il faut simplement se protéger.

Il est évident que la technologie VOIP poursuivra son développement et offrira encore plus de services à ceux qui l'utilisent, dans les années à venir. De nouvelles applications naîtront qui viendront enrichir l'offre des fournisseurs. Mais la téléphonie « cloud » a déjà un grand pas d'avance sur les systèmes traditionnels.

4.10.conclusion :

Dans ce chapitre nous avons réalisé une plate-forme VoIP simulée avec le simulateur «(Cisco) Packet Tracer», basée sur la solution Vlans et le protocole DHCP. Nous avons configuré chaque équipement appartenant à ce réseau, avec des tests de validation et vérification pour chaque scénario afin de prouver l'efficacité de notre solution retenue.

Conclusion générale

La technologie de VLAN comporte ainsi de nombreux avantages et permet de nombreuses applications intéressantes. Parmi les avantages liés à la mise en œuvre d'un VLAN, on retiendra notamment :

- La flexibilité de segmentation du réseau : Les utilisateurs et les ressources entre lesquels les communications sont fréquentes peuvent être regroupés sans devoir prendre en considération leur localisation physique.
- La simplification de la gestion : L'ajout de nouveaux éléments ou le déplacement d'éléments existants peut être réalisé rapidement.
- L'augmentation considérable des performances du réseau (réduction du domaine de collision) Comme le trafic réseau d'un groupe d'utilisateurs est confiné au sein du VLAN qui lui est associé, de la bande passante est libérée, ce qui augmente les performances du réseau.
- Une meilleure utilisation des serveurs réseaux.
- Le renforcement de la sécurité du réseau : Les frontières virtuelles créées par les VLANs ne pouvant être franchies que par le biais de fonctionnalités de routage, la sécurité des communications est renforcée.
- Un système téléphonique VOIP se présente généralement avec une large gamme de services supplémentaires. Notons entre autres le renvoi d'appel, l'identification du numéro de téléphone entrant et la possibilité d'échanger des documents et images.

- En effet, nous avons constaté l'intérêt majeur que joue les VLANs et la solution VOIP-DHCP, 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.

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.

Cependant, Grâce à l'évolution des réseaux locaux virtuels a vu l'introduction d'un concept appelé (VLANs) et la solution VOIP(voix par IP) et le protocole DHCP (Protocole de configuration de l'hôte dynamique) 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.
However, Through to the evolution of VLANs has seen the introduction of a concept called (VLANs) and VOIP (Voice over IP) and DHCP (Dynamic Host Configuration Protocol) 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 using 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-VOIP-DHCP), 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- تخطيطا أفضل للانتشار المستقبلي.

Bibliographie

[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] Etude de la solution VLANs
https://www.memoireonline.com/04/10/3431/m_Etude-et-optimisation-du-reseau-local-de-inova-si6.html

[3] La technique des VLANs

https://fr.scribd.com/doc/119853295/Rapport-VLAN-pdf

[4] Concepts de base de la VOIP

https://www.networklab.fr/category/ccnp_switch/voip/

[5] Création d'un câble RJ45 croisé
https://www.commentcamarche.net/contents/304-creation-d-un-cable-rj45-croise

[6] Mise en place d'un réseau inter-Vlan

https://sites.google.com/site/portefeuillemalikchetouane/mise-en-place-d-un-reseau-inter-vlan?overridemobile=true

[7] Différents types de VLAN

https://www.ionos.fr/digitalguide/serveur/know-how/fondamentaux-vlan/

[8] Avantages et inconvénients de la VOIP

https://www.geekeries.com/avantages-et-inconvenients-de-la-voip/

[9] Les topologies de base utilisées dans les réseaux
https://fr.slideshare.net/mobile/amichia1992/mise-en-place-de-vlan-au-sein-dun-rseau