N° d'ordre : 10 / M2P/STI/TCO Année Universitaire : 2014 / 2015

UNIVERSITE D'ANTANANARIVO

ECOLE SUPERIEURE POLYTECHNIQUE

DEPARTEMENT TELECOMMUNICATION

MEMOIRE DE FIN D'ETUDES

en vue de l'obtention

du DIPLOME de MASTER A VISEE PROFESSIONNELLE

Domaine : Science de l'ingénieur

Mention : Télécommunications

Parcours : Système de Traitement de l'Information (STI)

par : **RAJAONASON Johary Andrianina**

MISE EN EVIDENCE DES PROTOCOLES DE HAUTE DISPONIBILITE ET DE SECURITE DANS UN RESEAU CAMPUS

Soutenu le 28 avril 2016 devant la Commission d'Examen composée de :

Président :
M. RATSIHOARANA Constant

Examinateurs :
Mme RAMAFIARISONA Malalatiana Hajasoa
M. RANDRIANANDRASANA Marie Emile

Encadreur pédagogique : M. RABEMANANTSOA Josh

Encadreur professionnel : M. RAFANAMBINANTSOA Valohery

REMERCIEMENTS

Avant tout, il m’est particulièrement agréable d’exprimer mes remerciements au Seigneur de m’avoir donné la force pour mener à bien l’élaboration de ce mémoire de fin d’études.

Je tiens à remercier sincèrement Monsieur RANDRIANAHARISON Yvon, Responsable du domaine de l’ingénieur de l’Ecole Supérieure Polytechnique d’Antananarivo.

Mes remerciements s’adressent également à Monsieur RATSIHOARANA Constant, Maître de Conférences, Enseignant Chercheur en Télécommunication à l’Ecole Supérieure Polytechnique d’Antananarivo.

Je tiens à témoigner ma reconnaissance et ma gratitude les plus sincères à Monsieur RABEMANANTSOA Josh, Docteur en Télécommunication qui, en tant que Directeur de ce mémoire, s'est toujours montré à l'écoute et très disponible tout au long de sa réalisation.

J’exprime également ma gratitude aux membres de jury qui ont accepté d’examiner ce mémoire malgré leurs innombrables occupations:

- Monsieur RAFANAMBINANTSOA Valohery, Cadre de Maintenance Réseaux et Systèmes Informatiques à l’ASECNA.
- Madame RAMAFIARISONA Malalatiana Hajasoa, Maître de Conférences, Enseignante Chercheur à l’Ecole Supérieure Polytechnique d’Antananarivo
- Monsieur RANDRIANANDRASANA Marie Emile, Assistant d’Enseignement et de Recherche en Télécommunication à l’ESPA.

Ce travail de mémoire n’aurait pu être mené de façon efficace et rigoureuse en parallèle à ma formation académique sans l’aide des différents enseignants et personnel administratif de l’Ecole, à qui j’adresse toute ma gratitude.

Enfin, je n'oublie pas mes parents pour leur contribution, leur soutien et leur patience. J'adresse mes plus sincères remerciements à tous mes proches et amis, qui m'ont toujours soutenu et encouragé au cours de la réalisation de ce mémoire.

TABLE DES MATIERES

ABREVIATIONS

ACL	Access Control List
AH	Authentication Header
AIM	Adaptive Identification and Mitigation
APDU	Application Protocol Data Unit
ARP	Address Resolution Protocol
ATM	Asynchronous Transfer Mode
AVF	Active Virtual Forwarder
AVG	Active Virtual Gateway
BID	Bridge Identification
BPDU	Bridge Protocol Data Unit
CRC	Contrôle de Redondance Cyclique
DECNET	Digital Equipment Corporation Network
DMVPN	Dynamic Multipoint Virtual Private Network
DMZ	Demilitarized Zone
ESP	Encapsulating Security Payload
FHRP	First Hop Redundancy Protocol
FTP	File Transfer Protocol
GETVPN	Group Encrypted Transport VPN
GLBP	Gateway Load Balancing Protocol
GRE	Generic Routing Encapsulation
HSRP	Hot Standby Router Protocol
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPSec	Internet Protocol Security
ISO	International Organization for Standardization
L2TP	Layer 2 Tunneling Protocol
LACP	Link Aggregation Control Protocol
LAN	Local Area Network

MAC	Message Authentication Code
MAN	Metropolitan Area Network
MEC	Multichassis EtherChannel
NAT	Network Address Translation
NPDU	Network Protocol Data Unit
OSI	Open Systems Interconnexion
PAGP	Port Aggregation Protocol
PAT	Port Address Translation
PCI	Protocol Control Information
PDU	Protocol Data Unit
Po	Port Channel
PPDU	Presentation Protocol Data Unit
QoS	Quality of Service
RSTP	Rapid Spanning Tree Protocol
RTCP	Real Time Transport Control Protocol
RTP	Real Time Protocol
SA	Security Association
SIP	Session Initial Protocol
SNMP	Simple Network Management Protocol
SPI	Security Parameters Index
SRE	Services Ready Engine
STP	Spanning Tree Protocol
TCP	Transmission Control Protocol
TTL	Time To Live
UDP	User Datagram Protocol
UIT-T	Union International des Télécommunications-Télécommunication
VLAN	Virtual Local Area Network
VLC	Video Lan Community
VPN	Virtual Private Network
VRID	Virtual Router Identifier
VRRP	Virtual Router Redundancy Protocol
VTP	Virtual Local Area Network Trunking Protocol
WAN	Wide Area Network

INTRODUCTION GENERALE

De nos jours, la modélisation des réseaux est tendance. Il existe des normes qui régissent les architectures pour aider les utilisateurs à mieux contrôlés les leurs. Vu la croissance excessive des interconnexions, la sécurité des données qui y transitent sont primordiales. De plus, la numérisation des informations facilite la vie quotidienne de l'homme grâce à la technologie. Ces dernières sont stockées dans des bases de données pour ensuite être exploité par les utilisateurs. Cependant une perte ou une interception de ces données s'avère fatale.

Au niveau réseau, ceci se traduit par une panne au niveau des équipements de transmission ou une sécurité défaillante. C'est pour cela que les organisations comme l'UIT-T, l'IETF, Cisco, ont conçus des protocoles de sécurisation et de disponibilité pour les réseaux informatiques. Grâce à cela, les risques sont minimisés. Ce présent mémoire de fin d'études intitulé : « Mise en évidence des protocoles de haute disponibilité et de sécurité dans un réseau campus » traite ces protocoles afin d'en dégager des solutions sur la conception modèle pour la majorité des architectures réseaux.

En effet, le problème est de trouver le modèle qui s'adapte aux situations de l'individu ou de l'entreprise, d'où le choix du réseau campus qui est une architecture utilisée par la majorité. Comment les utilisateurs vont faire face aux pannes des équipements et à la prévention d'intrusion d'utilisateurs indésirables ? Comment éviter les pertes de données ?

La création d'un réseau redondant et une politique de sécurité convenable offrent un moyen efficace pour assurer la connectivité inter-réseau et la sureté des données en permanence. Par l'utilisation de protocoles appropriés, on arrive à soulever les problèmes posés tout en configurant les équipements. Et enfin, tout est facilité par l'implémentation des outils de sécurités dans les équipements Cisco.

Pour décortiquer les problèmes, on va voir en premier lieu une généralité sur les réseaux en explicitant l'intérêt des VLAN et d'une architecture campus ordonnée, puis les protocoles permettant de gérer les redondances dans la haute disponibilité, et en dernier lieu les systèmes de sécurités en se basant sur les routeurs Cisco.

CHAPITRE 1

Réseaux informatiques

1.1 Introduction

Les réseaux informatiques sont nés du besoin de relier des terminaux distants à un site central puis des ordinateurs entre eux et enfin des machines terminales, telles que stations de travail ou serveurs. Dans un premier temps, ces communications étaient destinées au transport des données informatiques. Aujourd'hui, l'intégration de la parole téléphonique et de la vidéo est généralisée dans ces réseaux, même si cela ne va pas sans difficulté. D'où la nécessité de la conception de protocoles et de normes pour l'architecture et les échanges.

1.2 Modèle OSI

L'expansion des réseaux a créé des problèmes d'incompatibilité et leur incapacité à communiquer entre eux, l'Organisation Internationale de Normalisation (ISO) a examiné des structures de réseau telles que DECNET, SNA et TCP/IP afin d'en dégager un ensemble de règles. À la suite de ces recherches, l'ISO a mis au point un modèle de réseau pour aider les fournisseurs à créer des réseaux compatibles avec d'autres. [1]

Dans le modèle de référence OSI, le problème consistant à déplacer des informations entre des ordinateurs est divisé en sept problèmes plus petits et plus faciles à gérer. Chacun des sept petits problèmes est représenté par une couche particulière du modèle. Voici les sept couches du modèle:

- Couche 7 : la couche application
- Couche 6 : la couche présentation
- Couche 5 : la couche session
- Couche 4 : la couche transport
- Couche 3 : la couche réseau
- Couche 2 : la couche liaison de données
- Couche 1 : la couche physique

1.2.1 Présentation des couches

1.2.1.1 Couche 7 : La couche application

La couche application est la couche OSI la plus proche de l'utilisateur. Elle fournit des services réseau aux applications de l'utilisateur. Elle se distingue des autres couches en ce sens qu'elle ne fournit pas de services aux autres couches OSI, mais seulement aux applications à l'extérieur du modèle OSI. Voici quelques exemples de ce type d'application : tableurs, traitements de texte et logiciels de terminaux bancaires. La couche application détermine la disponibilité des partenaires de communication voulus, assure la synchronisation et établit une entente sur les procédures de correction d'erreur et de contrôle d'intégrité des données.

1.2.1.2 Couche 6 : La couche présentation

La couche présentation s'assure que les informations envoyées par la couche application d'un système sont lisibles par la couche application d'un autre système. Au besoin, la couche présentation traduit différents formats de représentation des données en utilisant un format commun

1.2.1.3 Couche 5 : La couche session

Comme son nom l'indique, la couche session ouvre, gère et ferme les sessions entre deux systèmes hôtes en communication. Cette couche fournit des services à la couche présentation. Elle synchronise également le dialogue entre les couches de présentation des deux hôtes et gère l'échange des données. Outre la régulation de la session, la couche session assure un transfert efficace des données, classe de service, ainsi que la signalisation des écarts de la couche session, de la couche présentation et de la couche application.

1.2.1.4 Couche 4 : La couche transport

La couche transport segmente les données envoyées par le système de l'hôte émetteur et les rassemble en flux de données sur le système de l'hôte récepteur. La frontière entre la couche transport et la couche session peut être vue comme la frontière entre les protocoles d'application et

les protocoles de flux de données. Alors que les couches application, de présentation et transport se rapportent aux applications, les quatre couches dites inférieures se rapportent au transport des données.

1.2.1.5 Couche 3 : La couche réseau

La couche réseau est une couche complexe qui assure la connectivité et la sélection du chemin entre deux systèmes hôtes pouvant être situés sur des réseaux géographiquement éloignés.

1.2.1.6 Couche 2 : La couche liaison de données

La couche liaison de données assure un transit fiable des données sur une liaison physique. Ainsi, la couche liaison de données s'occupe de l'adressage physique (plutôt que logique), de la topologie du réseau, de l'accès au réseau, de la notification des erreurs, de la livraison ordonnée des trames et du contrôle de flux.

1.2.1.7 Couche 1 : La couche physique

La couche physique définit les spécifications électriques, mécaniques, procédurales et fonctionnelles permettant d'activer, de maintenir et de désactiver la liaison physique entre les systèmes d'extrémité. Les caractéristiques telles que les niveaux de tension, la synchronisation des changements de tension, les débits physiques, les distances maximales de transmission, les connecteurs physiques et d'autres attributs semblables sont définies par la couche physique.

1.2.2 Encapsulation lors de l'échange transversal de données

La figure 1.01 ci-après montre un exemple d'échange de données dans un réseau et l'encapsulation intervenant à l'intérieur. Le processus d'envoi à partir de l'ordinateur A transmet des données vers le processus de réception de l'ordinateur B.

Les données transitent de haut en bas au niveau de l'extrémité locale, les informations de contrôle de protocole (en-tête/ en-queue) utilisées comme enveloppe sur chaque couche, les données transitent de bas en haut au niveau de l'extrémité distante, et les informations de contrôle de protocole (en-tête/en queue) supprimées à mesure que les données remontent les couches.

La couche application de chaque terminale crée le message et ajoute des bits en en-tête du message. Ces bits sont appelés PCI (Protocol Control Information) et représentent des informations sur le processus. Elles peuvent contenir des informations identifiant les entités application (adresses des couches sources et destination de l'application). Le PCI et le message original sont appelés APDU (Application Protocol Data Unit).

L'APDU est envoyé à la couche immédiatement inférieure. Cette couche ajoute son PCI aux données reçues de la couche application, et le message résultant devient le PPDU (Presentation Protocol Data Unit). Le message original est encapsulé dans l'APDU et l'APDU est encapsulé à son tour dans le PPDU. Chaque couche ajoute ainsi son information d'en-tête au message reçu de la couche supérieure. C'est comme si chaque message était placé dans une enveloppe. L'enveloppe avec son contenu forme le PDU (Protocol Data Unit) de la couche.

Le processus continue ainsi jusqu'à la couche physique. Au niveau de la couche liaison des données, un champ de vérification CRC (Contrôle de Redondance Cyclique) est ajouté aux données. Cette vérification est générée par un mécanisme matériel de la couche liaison des données (cartes réseaux).

Au niveau de la couche physique, l'information d'en-tête prend la forme d'une indication informant le destinataire de l'arrivée d'un paquet. Sur les réseaux Ethernet, cette information est représentée par un préambule de 56 bits, utilisé par le destinataire pour se synchroniser.

A l'autre extrémité (ordinateur B), la couche physique reçoit les bits, supprime celles de la synchronisation et envoie le reste à la couche liaison des données. Cette couche regroupe les bits dans une trame et vérifie si le CRC est valide. Ensuite, elle supprime le PCI et envoie le reste NPDU (Network PDU) à la couche réseau. [2] [3] [4]

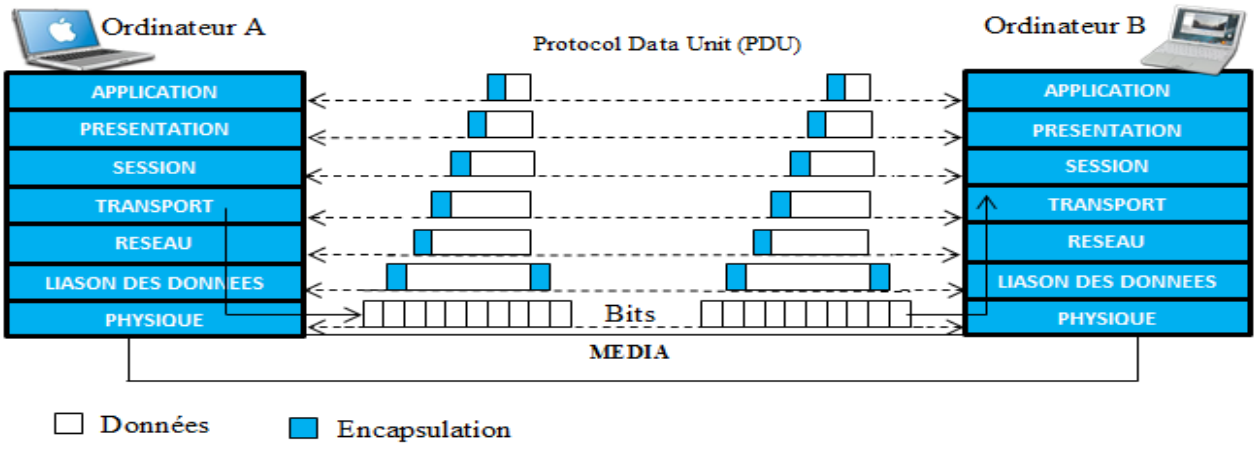


Figure 1.01 : *Echange transversal des données*

A chaque extrémité d'une couche, le paquet est traité d'après les informations PCI de la couche. Le PCI est supprimé, puis les données sont envoyées à la couche supérieure. Ce processus continue jusqu'à la couche application qui récupère les données originales.
Si l'on examine les couches au niveau local et au niveau distant, on s'aperçoit que chaque couche communique avec la couche homologue à l'autre extrémité.
Les éléments actifs dans chaque couche OSI sont appelés des entités protocoles. Ces entités protocoles implémentent les services dans chaque couche OSI et communiquent avec les entités protocoles de la couche correspondante de l'autre système.

1.3 Topologie des réseaux

Il existe différents types de classification selon le point de vue. Pour notre cas, on va considérer le mode d'interconnexion entre les machines comme repère.

1.3.1 Réseaux point-à-point

Un réseau point-à-point est un réseau dans lequel les interconnexions entre les deux nœuds sont réalisés deux par deux. On distingue quatre structures différentes : en étoile, en arbre, en boucle, ou maillé.

1.3.1.1 Réseau point-à-point en étoile

Dans ce type de réseau, tous les nœuds sont reliés à un nœud central (exemple : serveur). Mais il est limité par les possibilités du nœud central (bloqué en cas de défaillance, taille limitée aux possibilités de connectivité).

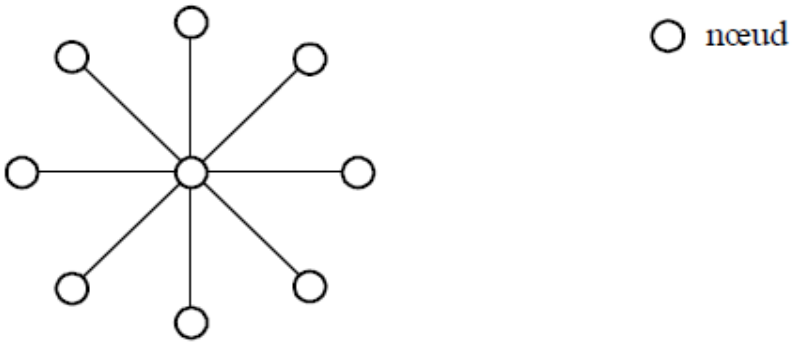


Figure 1.02 : *Topologie d'un réseau point-à-point en étoile*

1.3.1.2 Réseau point-à-point en arbre

C’est un assemblage de réseaux point-à-point en étoile.

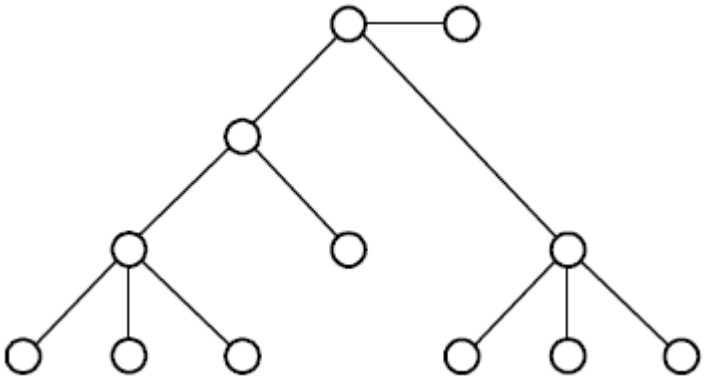


Figure 1.03 : *Topologie d’un réseau point-à-point en arbre*

1.3.1.3 Réseau point-à-point en boucle

Chaque nœud est relié à deux autres nœuds, le nombre de liaisons est faible (N liaisons pour N nœuds).

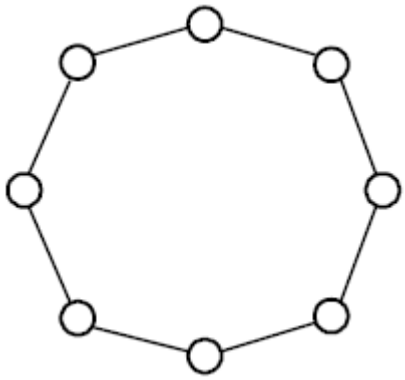


Figure 1.04 : *Topologie d’un réseau point-à-point en boucle*

1.3.1.4 Réseau point-à-point maillé

Chaque nœud est relié à un ou plusieurs autres nœuds sans logique particulière, ainsi, plusieurs chemins différents entre deux nœuds quelconques.

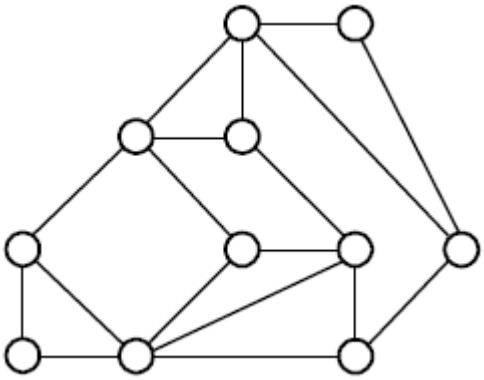


Figure 1.05 : *Topologie d'un réseau point-à-point maillé*

1.3.2 Réseaux multipoints

Un réseau multipoint est un réseau dans lequel tous les nœuds sont reliés entre eux via une liaison unique ; chaque nœud y étant connecté, il s'agit donc d'un réseau à diffusion.
On a trois structures : en bus, en anneau, ou en boucle.

1.3.2.1 Réseau multipoints en bus

Tous les nœuds sont reliés directement à la liaison centrale, laquelle est tirée entre les nœuds les plus éloignés.

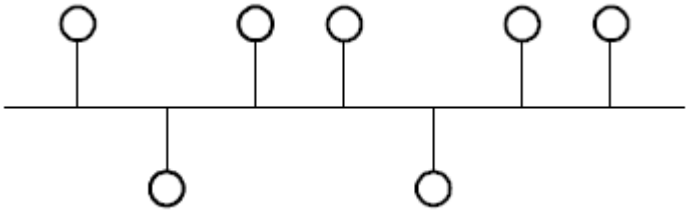


Figure 1.06 : *Topologie d'un réseau multipoint en bus*

1.3.2.2 Réseau multipoint en anneau

Tous les nœuds sont reliés à la liaison centrale, laquelle reboucle sur elle-même, les communications sont monodirectionnelles.

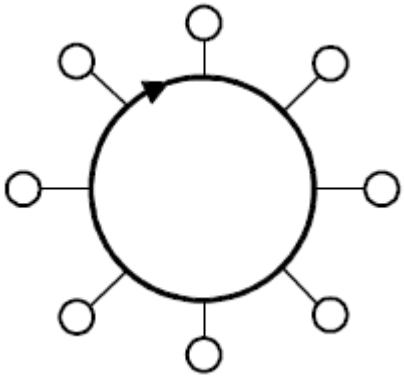


Figure 1.07 : *Topologie d'un réseau multipoint en anneau*

1.3.2.3 Réseau multipoint en boucle

Il est identique à celui du réseau en anneau, juste que les communications sont bidirectionnelles.

1.4 Protocoles

1.4.1 Définitions et rôles

C'est un ensemble de conventions préétablies pour réaliser un échange (fiable) de données entre deux entités. Il définit le format des données et les règles d'échange. Le protocole est un terme utilisé à la place de procédure dans certains types d'échange. Pour pouvoir envoyer de l'information entre deux équipements, les deux appareils doivent parler le même langage. [5]
Ce langage est appelé protocole.

Protocole et procédure doit :

- **Définir la structure des trames** : en précisant les bits qui constituent les caractères, et les caractères qui forment le message.
- **Détecter et corriger les erreurs.**
- **Gérer les séquences de commandes** pour identifier les messages et éviter les duplications et les pertes.
- **Garantir la transparence** afin d'éviter la confusion entre message et caractère de commande.

- **Indiquer comment se fait l'attribut des lignes dans le cas des liaisons multipoints** en half duplex ou full duplex.
- **Permettre de résoudre le problème de conflit d'accès ou demande simultanée, problème de la perte de liaison, problème d'émission sans données disponibles.**

1.4.2 Classification

Il existe 3 catégories :

- Protocole orienté bit
- Protocole orienté octet
- Protocole orienté caractère

1.4.2.1 Protocole orienté bit

Délimite les bits constituant les messages à l'aide d'indicateurs spéciaux. [5]
Exemple: l'HDLC (High Level Data Link Protocol)

1.4.2.2 Protocoleorienté octet

Le message est précédé d'un en-tête qui contient le nombre d'octets contenu dans le champ de données. [5]
Exemple : IP (Internet Protocol)

1.4.2.3 Protocole orienté caractère

Caractères spéciaux pour indiquer le début du message, la fin d'un bloc. [5]
Exemple : pour signaler l'arrivée du caractère ou bloc de test d'erreur, on utilise :
ϕϕ : NULL (notés en code ASCII)
EOT (End Of Text)
ETX (End of Text)
STX (Start of Text)
SOH (Start Of Heading)
ETB (End of Text Block)

DC1 (Device Control)

DC2

BEL (ϕ7)

1.5 VLAN

Vu la prolifération des ordinateurs, leur mise en réseau est non seulement indispensable mais doit être planifiée et organisée.

VLAN ou Virtual Local Area Network est né de la nécessité d'isoler le trafic entre les segments du réseau et d'augmenter la bande passante disponible. Les zones qu'on segmente sont les domaines de collision et de broadcast et utilisant des **commutateurs** et/ou **routeurs**. [6]

- Domaine de collision : zone du réseau dans laquelle transitent des trames qui peuvent entrer en collision avec d'autres.
- Domaine de broadcast : ensemble de tous les dispositifs qui recevront des trames de diffusion provenant de n'importe quel dispositifs faisant partie de cet ensemble.

1.5.1 Définitions

Un réseau local virtuel (VLAN) est un sous-réseau logique et indépendant (virtuel) construit dans le réseau physique précédent et permettant de segmenter ce réseau. [6] [7]

Un VLAN permet donc de créer des domaines de diffusion (broadcast domains) gérés par les commutateurs indépendamment de l'emplacement où se situent les nœuds, ce sont des domaines de diffusion gérés logiquement. [7]

Dans l'exemple ci-contre, il y a trois domaines de diffusion au lieu d'un :

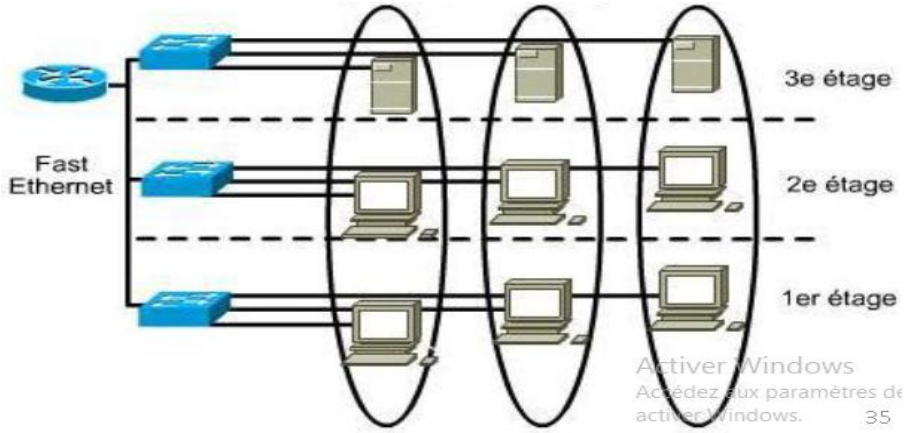


Figure 1.08 : *Exemple de trois VLAN*

1.5.2 Caractéristiques

1.5.2.1 ID ou indentification de VLAN

- Compris entre 1 et 1005.
- 1002-1005 réservés aux VLAN Token Ring et FDDI.
- 1 et 1002-1005 sont automatiquement créés et ne peuvent pas être supprimés.
- Stockés dans le fichier .dat dans la mémoire flash.

1.5.2.2 ID de plage étendue

- Compris entre 1006 et 4094.
- Conçus pour les fournisseurs de services.
- Moins d'options que les réseaux locaux virtuels à plage normale.
- Stockés dans le fichier de configuration en cours.

1.5.3 Types

Ceci dépend des critères et point de vue de l'utilisateur. La méthode d'implémentation est basée sur le port. Ce type de VLAN est associé à un port appelé « access VLAN ». Par défaut tous les ports du commutateur sont membres du VLAN par défaut. [6]

- Un **VLAN de données** est configuré pour ne transporter que le trafic généré par l'utilisateur.
- Un **VLAN natif** est affecté à un port d'agrégation 802.1Q. Un port d'agrégation 802.1Q prend en charge le trafic provenant de nombreux VLAN (trafic étiqueté ou «taggedtraffic»), ainsi que le trafic qui ne provient pas d'un VLAN (trafic non étiqueté ou «untaggedtraffic»). Le port d'agrégation 802.1Q place le trafic non étiqueté sur le VLAN natif. En ce qui nous concerne, un VLAN natif sert d'identificateur commun aux extrémités d'une liaison agrégée
- Un **VLAN de gestion** est un réseau local virtuel qu'on configure pour accéder aux fonctionnalités de gestion d'un commutateur. C'est le VLAN 1 qui fait office de VLAN de gestion si on ne définit pas explicitement un VLAN distinct pour remplir cette fonction.

D'un point de vue configuration, on a deux types :

- **VLAN statique** : axés sur le port

Il est facile à mettre en œuvre et sécurisé. Chaque port est affecté à un VLAN manuellement. [6]

- **VLAN dynamique** : axés sur l'adresse MAC (Medium Access Control)

Sa mise en œuvre est plus complexe et prend en compte la mobilité des utilisateurs. L'affectation à un VLAN se fait « à la volée ». [6]

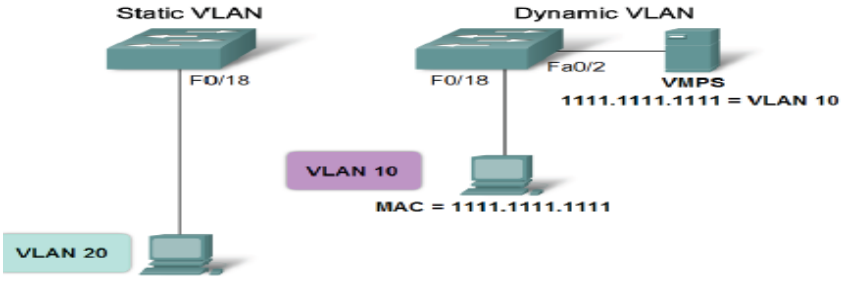


Figure 1.09 : *Exemples de VLAN statique et dynamique*

1.5.4 Fonctionnement

A un VLAN correspond un domaine de broadcast. Une trame émise par un équipement A ne peut atteindre que les équipements affectés à son VLAN. [6]

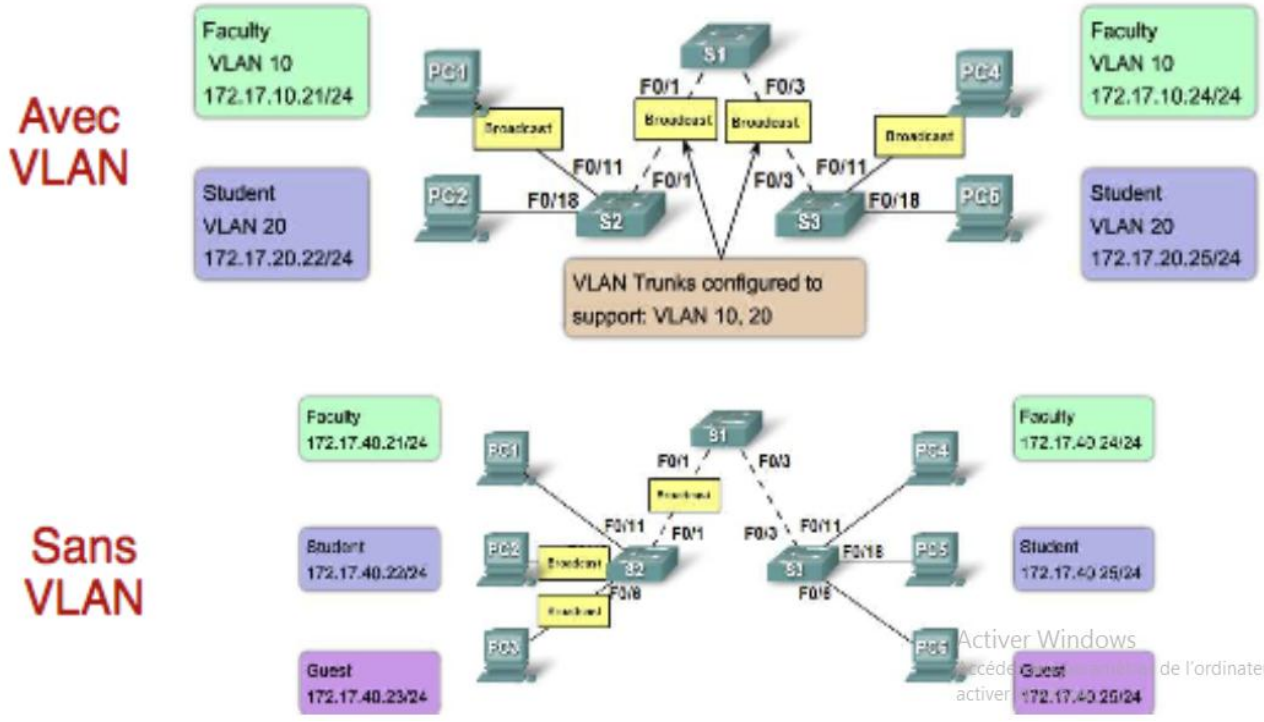


Figure 1.10 : *Cas de transmissions avec et sans VLAN*

Les émissions des broadcast sans VLAN est aléatoire, donc les données mettent plus de temps à retrouver leurs chemins.

1.5.5 Agrégation ou « Trunk »

C'est une subdivision d'un lien physique en plusieurs liens logiques dont chacun est affecté à un VLAN bien défini. Elle suit le standard 802.1Q du standard IEEE et utilise le protocole ISL (Inter Switch Link) pour les échanges (protocole propriétaire Cisco). [6]

Avec un trunk, une seule liaison est nécessaire quel que soit le nombre de VLAN actifs. [7]

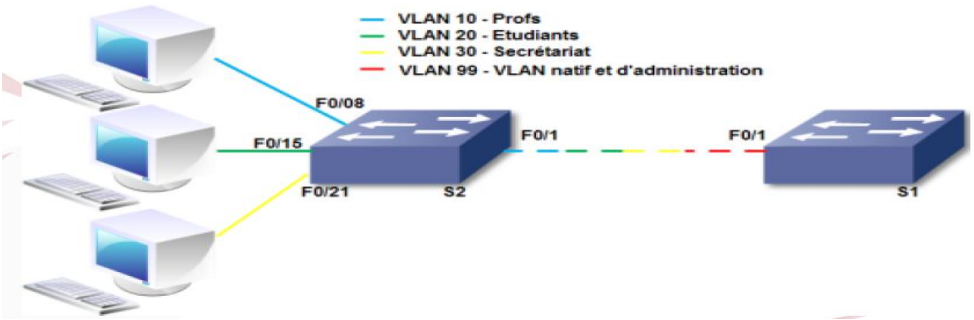


Figure 1.11 : *Exemple d'agrégation*

Ici, un seul lien supporte la liaison de quatre (4) VLAN différents.

1.5.6 Routage entre VLAN

Un routeur est nécessaire pour acheminer le trafic inter VLAN. [6]

Le principe est de configurer les sous interfaces du routeur pour acheminer des VLAN différents.

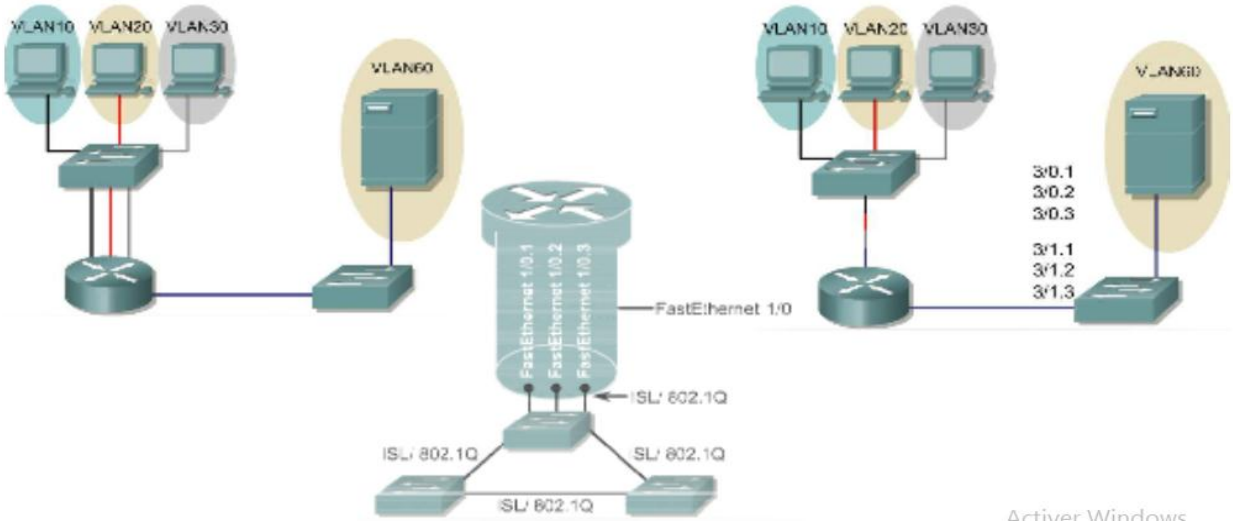


Figure 1.12 : *Exemple de routage inter VLAN*

L'objectif est de faire communiquer les VLAN entre eux avec économie de liens en attribuant à chaque lien logique une adresse IP. Il doit être combiné à des agrégations entre les commutateurs.

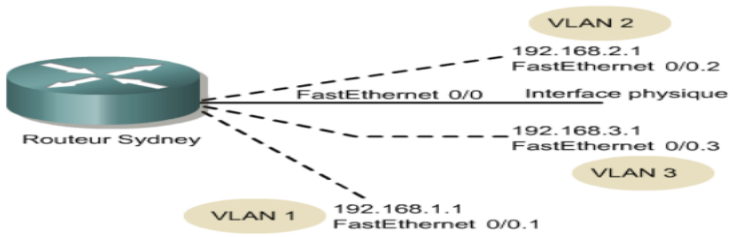


Figure 1.13 : *Séparation des interfaces physiques en sous interfaces*

Il existe deux types de configuration pour le routage : soit on utilise les deux interfaces physiques du routeur soit un seul mais en subdivisant en sous interfaces. [8]

Voici des exemples pour les deux cas :

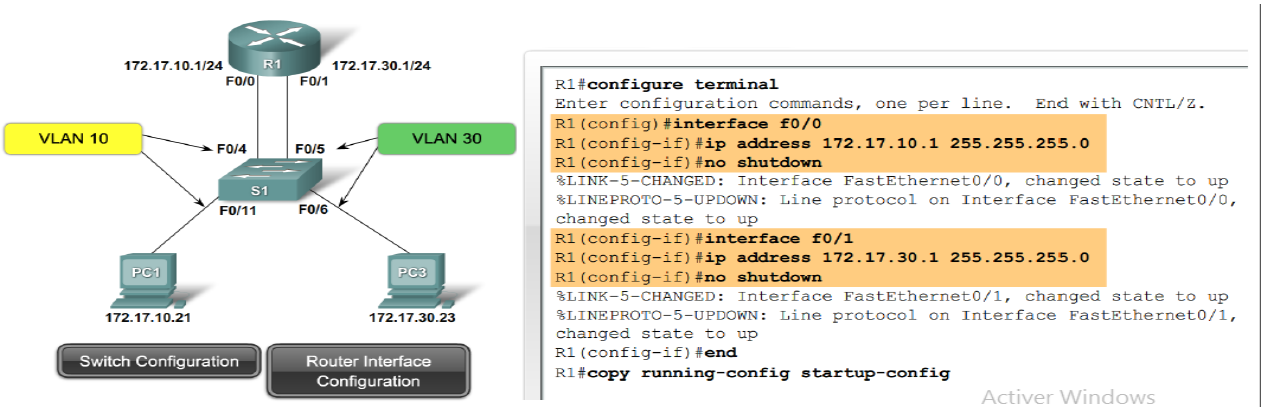


Figure 1.14 : *Cas pour deux interfaces physiques*

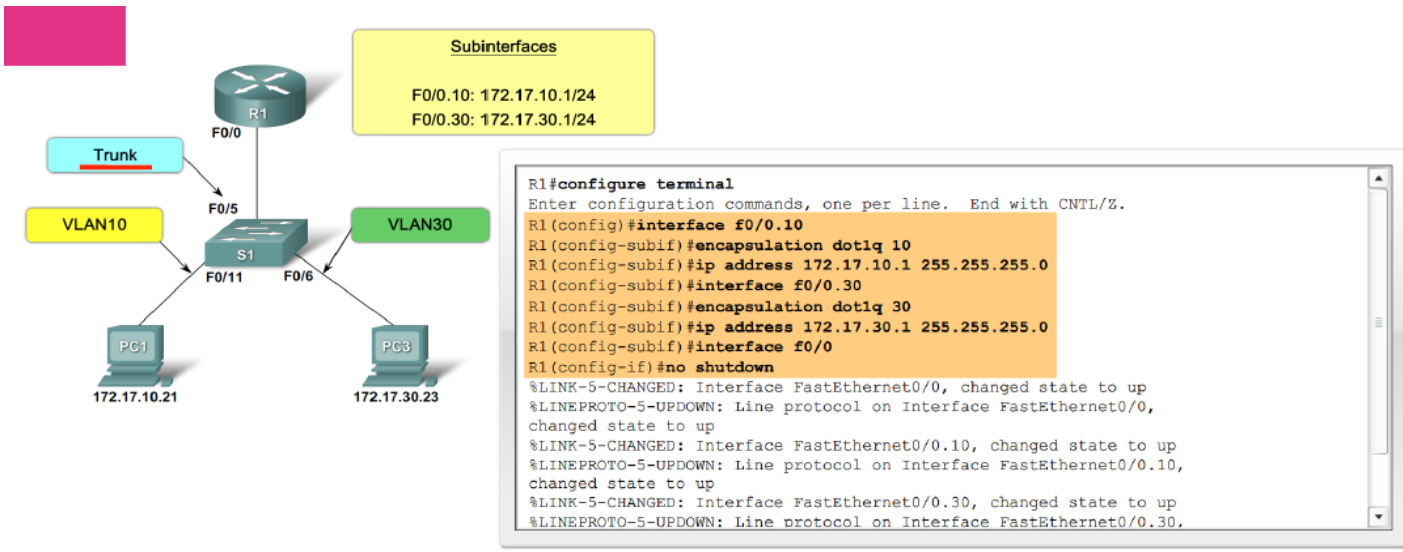


Figure 1.15 : *Configuration de sous interfaces*

1.5.7 VTP

VTP ou VLAN Trunking Protocol est un protocole propriétaire de Cisco. Il sert à la propagation de création/suppression/modification de VLAN sur tous les switchs du réseau à partir d'un seul switch. [6] [7]

On distingue trois types :

- VTP Server: switch qui crée les annonces VTP

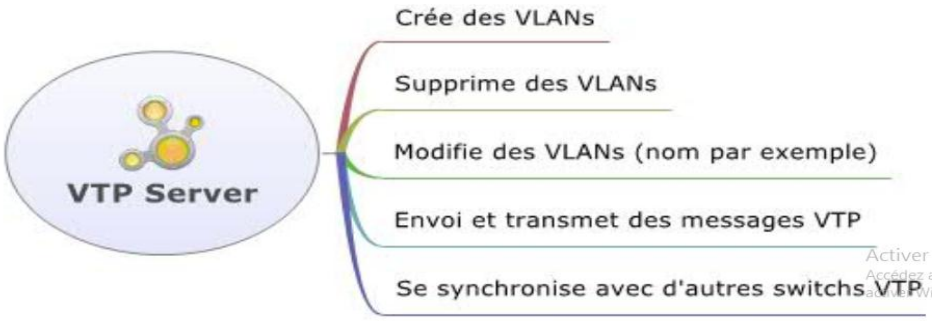


Figure 1.16 : *Fonctions de VTP Server*

- VTP Client: switch qui reçoit, se synchronise et propage les annonces VTP

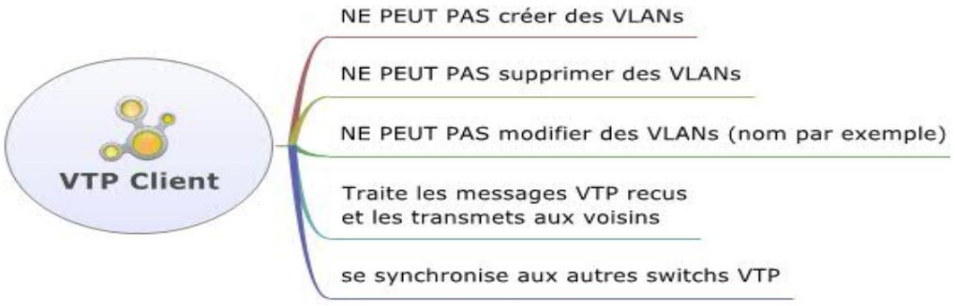


Figure 1.17 : *Fonctions de VTP Client*

- VTP Transparent: switch qui ne traite pas les annonces VTP

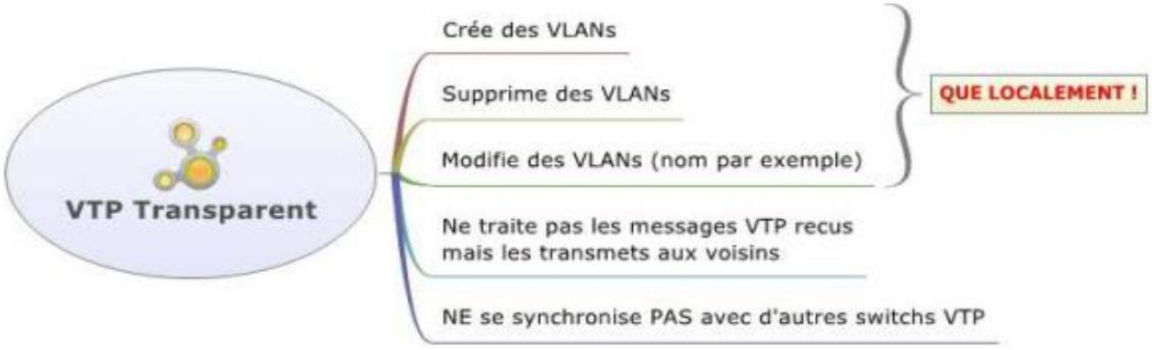


Figure 1.18 : *Fonctions de VTP Transparent*

1.5.8 Exemple de configuration de VLAN

Considérons un commutateur nommé Switch1

Switch1>enable

Switch1#configure terminal

Switch1(config)#vlan 2

Switch1(config-vlan)#namevlanIngenierie

Switch1(config)#interface FastEthernet0/1

Switch1(config-if)#switchport mode access vlan 2

La première ligne permet d'entrer en mode privilège dans le matériel. La ligne suivante permet deconfigurer le switch, en suite on à la base de données du matériel (switch) et d'entrer le numéro etle nom du VLAN (vlan 2, vlanIngenierie).Puis on accède le port concerné par le commande « interface *TypePort »*. Enfin on définit le mode d'accès au port concerné, dans notre cas«*access*» qui veut dire accès directe au port. [9]

On définit deux types de mode d'accès au port. Un port access-link n'est associé qu'à un seul VLAN, un port trunk-link est associé à tous les VLAN. [9]

1.6 Réseau campus

Un réseau de campus est une des dénominations du réseau MAN (Métropolitan Area Network), c'est-à-dire il s'étend à l'échelle d'une ville mais à haut débit. [10]

Le Gigabit Ethernet convient parfaitement à ce type de besoin, d'où l'utilisation de la fibre optique dans la plupart des liaisons.

Côté performances, le Gigabit Ethernet est à la hauteur des débits voulus :

- Débit réel de 761 Mbits/s pour des trames de 64 octets (soit 1 488 095 paquets par seconde) ;
- Débit réel de 986 Mbit/s pour des trames de 1 518 octets (soit 81 274 paquets par seconde).

On peut dire que le réseau de campus est une extension du réseau fédérateur ou LAN avec l'intégration des redondances et partage de charges.

Dans notre cas, nous allons mettre en évidence le bon design ainsi que les protocoles utilisés dans la conception du réseau.

1.6.1 Design multicouche

Les architectures hiérarchiques et multicouches sont des normes très réputés et demandés dans la conception du réseau campus, ce qui nous a conduits à ce choix.

Ils offrent plusieurs avantages très pertinents, qui sont : [11]

- D'un point de vue hiérarchie : chaque couche joue un rôle spécifique.
- Modularité : la topologie est basée sur une conception modulaire
- Avec des modules, il est plus facile de croître de comprendre et de dépanner
- Le design multicouche promouvoit l'efficacité et la redondance
- Un bon design assure des configurations de trafic uniformes et déterminantes

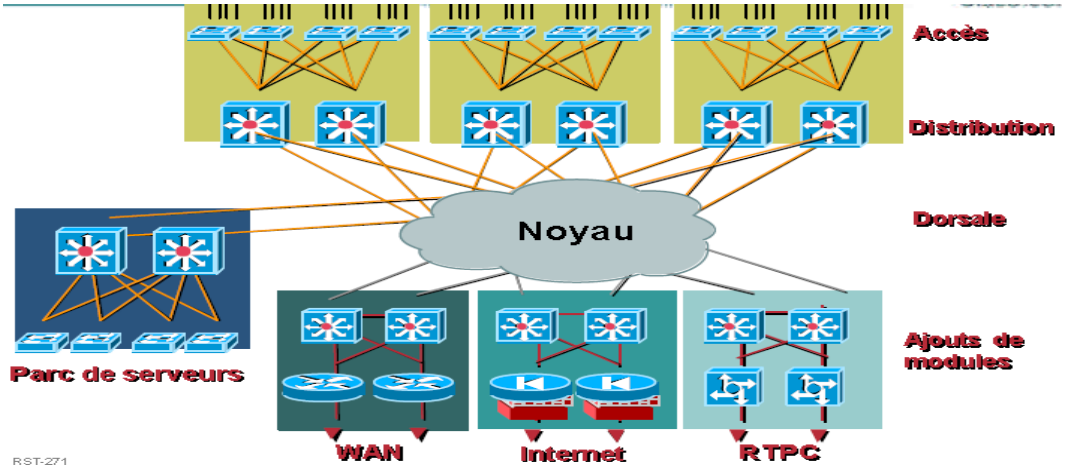


Figure 1.19 : *Exemple de design de réseau multicouche*

Voici les directives générales de ce design :

- Accès

Commutation de couche 2 au niveau de l'armoire de câblage (peut être sensible à la couche 3) ; frontière de confiance (trust boundary) et de politique (policyboundary)

- Distribution

Commutation de niveau 3 ; utilisation de protocoles de routage pour assurer des avantages comme l'équilibre de charge, la convergence rapide et l'évolutivité ; procure une redondance/résilience de premier bond

Regroupe les éléments de la couche d'accès

- Noyau

Commutation de couche 3 au niveau de la dorsale pour assurer équilibre de charge, convergence rapide et évolutivité ; nécessité d'un service haute vitesse sans exécution des politiques.

1.6.2 Réseaux hiérarchiques

1.6.2.1 Conception de réseau hiérarchique

En matière de réseau, une conception hiérarchique permet de regrouper des périphériques en un certain nombre de réseaux distincts qui sont alors organisés en couches. Le modèle de conception hiérarchique possède trois couches de base [12] :

- Couche cœur de réseau : relie les périphériques de la couche de distribution.
- Couche de distribution : assure l'interconnexion entre les petits réseaux locaux.
- Couche d'accès : fournit la connectivité pour les hôtes et les périphériques du réseau.

1.6.2.2 Avantages par rapport aux réseaux non hiérarchiques

- Les réseaux hiérarchiques sont plus avantageux que les réseaux linéaires. De par la division des réseaux linéaires non hiérarchiques en sections plus petites et plus faciles à gérer, le trafic local reste véritablement local. Seul le trafic destiné aux autres réseaux est acheminé vers une couche supérieure. [12]
- Sur un réseau non hiérarchique, les périphériques de couche 2 offrent peu d'opportunités de contrôle de diffusion et de filtrage du trafic indésirable. À mesure que de nouveaux périphériques et applications sont ajoutés à ce type de réseau, les temps de réponse se dégradent jusqu'à ce que le réseau devienne complètement inutilisable. [12]

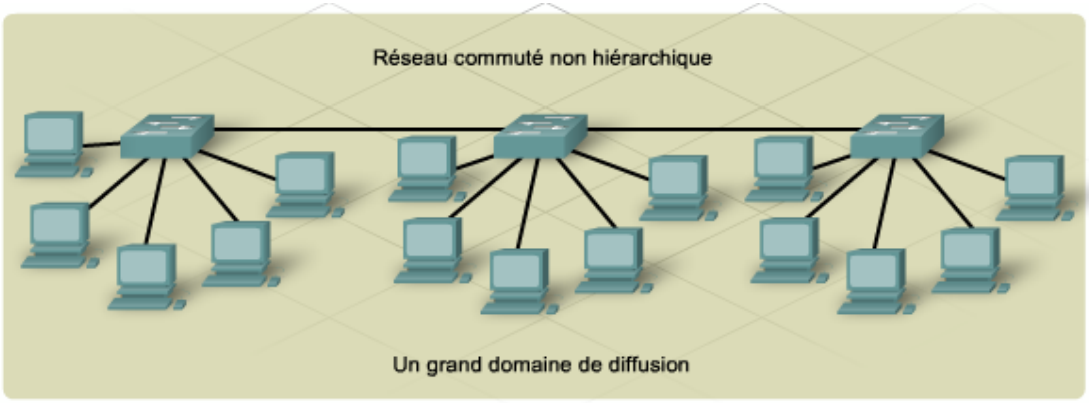


Figure 1.20 : *Réseau non hiérarchique*

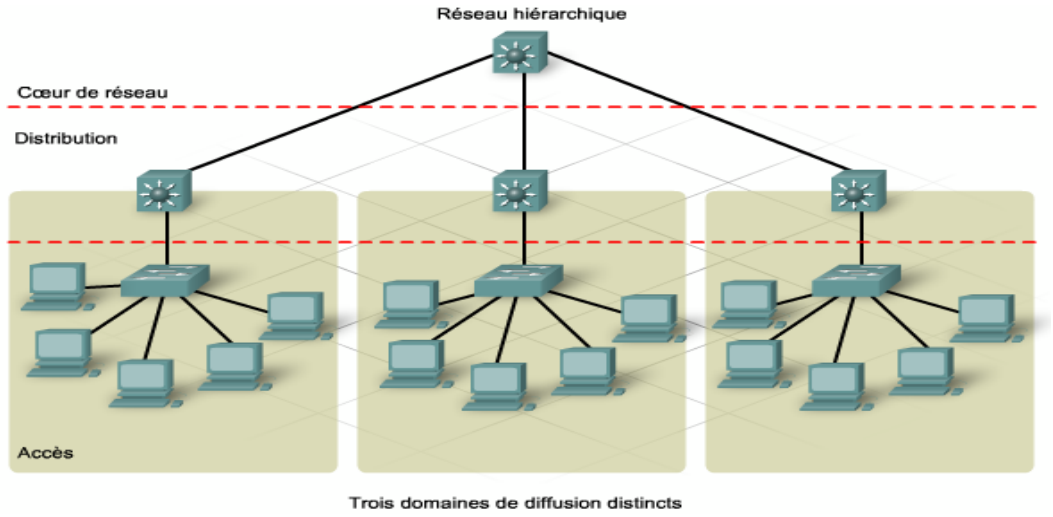


Figure 1.21 : *Réseau hiérarchique*

1.6.3 Caractéristiques et normes dans chaque couche

1.6.3.1 Couche cœur du réseau

La couche cœur de réseau est parfois appelée réseau fédérateur. Les routeurs et les commutateurs de cette couche offrent une connectivité haute vitesse. Dans un réseau local d'entreprise, la couche cœur de réseau peut assurer la connexion de plusieurs bâtiments ou sites et fournir une connectivité pour la batterie de serveurs. Cette couche contient une ou plusieurs liaisons vers les périphériques de la périphérie du réseau, pour la prise en charge de l'accès à Internet, aux réseaux privés virtuels (VPN), à l'extranet et au réseau étendu (WAN).
La mise en œuvre d'une couche cœur de réseau réduit la complexité du réseau, facilitant ainsi sa gestion et son dépannage.

- Objectifs de la couche cœur de réseau

La conception de la couche cœur de réseau permet des transferts de données efficaces et très rapides entre une section du réseau et une autre. Les principaux objectifs de conception de la couche cœur de réseau sont les suivants :

- fournir un temps utile de 100 % ;
- optimiser le débit ;
- faciliter la croissance du réseau.

- Technologies de la couche cœur de réseau

Les technologies utilisées au niveau de la couche cœur de réseau incluent :

- routeurs ou commutateurs multicouche combinant routage et commutation dans un même périphérique ;
- redondance et équilibrage de la charge ;
- liaisons haute vitesse et agrégées.

➢ Liaisons redondantes

La mise en œuvre de liaisons redondantes au niveau de la couche cœur de réseau permet aux périphériques du réseau de trouver un chemin d'accès alternatif pour l'envoi des données, en cas de panne. Lorsque les périphériques de couche 3 sont placés dans la couche cœur de réseau, ces liaisons redondantes peuvent être utilisées pour l'équilibrage de charge ainsi que pour la sauvegarde. Dans une conception de réseau linéaire de couche 2, le protocole STP (SpanningTree Protocol) désactive les liaisons redondantes, sauf en cas d'échec de la liaison principale. Ce comportement empêche l'équilibrage de charge sur les liaisons redondantes.

➢ Topologie maillée

La plupart des couches cœur de réseau sont câblées selon une topologie à maillage global ou à maillage partiel. Dans une topologie à maillage global, chaque périphérique dispose d'une connexion avec tous les autres périphériques. Ce type de topologie offre l'avantage d'un réseau entièrement redondant, mais sa gestion et son câblage peuvent s'avérer difficiles et onéreux. Pour les installations de grande taille, on utilise plus couramment une topologie à maillage partiel modifié. Dans ce type de topologie, chaque périphérique est connecté à au moins deux autres, créant une redondance suffisante sans la complexité d'un maillage global.

1.6.3.2 Couche distribution

La couche d'accès est généralement créée à l'aide de la technologie de commutation de couche 2. La couche de distribution, quant à elle, est créée à partir des périphériques de couche 3. Les routeurs ou les commutateurs multicouches, situés dans la couche de distribution, fournissent diverses fonctionnalités essentielles à la réalisation des objectifs de conception du réseau. Ces objectifs incluent :

- le filtrage et la gestion des flux de trafic ;
- la mise en application des stratégies de contrôle d'accès ;
- le résumé des routes avant notification à la couche cœur de réseau ;

- l’isolation de la couche cœur de réseau par rapport aux pannes ou interruptions de service de la couche d’accès ;
- le routage entre les réseaux locaux virtuels de la couche d’accès.

Les périphériques de la couche de distribution servent également à gérer les files d’attente et la hiérarchisation du trafic, avant la transmission via le cœur du campus.

- Agrégations

Des liaisons agrégées sont souvent configurées entre les périphériques de mise en réseau des couches d’accès et de distribution. Elles servent à acheminer le trafic appartenant à plusieurs réseaux locaux virtuels entre différents périphériques, sur la même liaison. Lors de la conception des liaisons agrégées, le concepteur du réseau prend en compte la stratégie de réseau local virtuel globale et les modèles de trafic réseau.

- Liaisons redondantes

Les périphériques de la couche de distribution entre lesquels il existe des liaisons redondantes peuvent être configurés de manière à équilibrer la charge du trafic entre les différentes liaisons. L’équilibrage de charge augmente la bande passante disponible pour les applications.

- Topologie de la couche de distribution

Les réseaux dotés d’une couche de distribution sont généralement câblés selon une topologie à maillage partiel. Cette topologie offre un nombre suffisant de chemins d’accès redondants pour garantir le fonctionnement du réseau en cas de panne de périphérique ou de liaison. Les périphériques de la couche de distribution situés dans le même local technique ou centre de calcul, sont interconnectés à l’aide de liaisons Gigabit. S’ils sont séparés par de longues distances, un câble en fibre optique est utilisé. Les commutateurs capables de prendre en charge plusieurs connexions en fibre haute vitesse sont assez onéreuses ; une planification minutieuse est donc nécessaire pour garantir qu’un nombre suffisant de ports à fibre optique est disponible pour la bande passante et la redondance souhaitées.

1.6.3.3 Couche accès

La couche d’accès correspond à la périphérie du réseau, l’endroit où les périphériques finaux se connectent. Les services et les périphériques de la couche d’accès sont situés dans chaque bâtiment du campus, chaque site distant et batterie de serveurs, et à la périphérie du réseau d’entreprise.

- Considérations physiques sur la couche d'accès

La couche d'accès de l'infrastructure de campus utilise la technologie de commutation de couche 2 pour fournir l'accès au réseau. L'accès peut se faire par l'intermédiaire d'une infrastructure câblée permanente ou de points d'accès sans fil. La technologie Ethernet utilisée sur un câblage en cuivre impose des contraintes en termes de distance. Par conséquent, l'emplacement physique des équipements constitue l'une des principales préoccupations lors de la conception d'une couche d'accès pour une infrastructure de campus.

- Exigences en matière de disponibilité

Dans les premiers réseaux, les seuls endroits à haute disponibilité étaient le cœur du réseau, la périphérie et les réseaux de centre de calcul. Avec la téléphonie IP, chaque téléphone doit être disponible en permanence.

Des composants redondants et des stratégies de basculement peuvent être mis en œuvre au niveau de la couche d'accès, afin d'améliorer la fiabilité et la disponibilité pour les périphériques finaux.

- Conception et facilité de gestion

Outre la connectivité de base à la couche d'accès, le concepteur doit prévoir les éléments suivants :

- Structures de création de noms
- Architecture de réseau local virtuel
- Modèles de trafic
- Stratégies de hiérarchisation

La configuration et l'utilisation sont des opérations cruciales pour les systèmes de gestion des réseaux convergents de grande taille. Il est également important de normaliser les configurations et les équipements, lorsque cela est possible.

Le respect de principes de conception éprouvés permet d'améliorer la gestion et la prise en charge continue du réseau :

- en garantissant que le réseau ne devienne pas trop complexe ;
- en permettant un dépannage facile en cas de problème ;
- en facilitant l'ajout futur de nouveaux services et fonctions.

En résumé, voici une architecture normalisée qu'on a prise en compte dans le cadre de ce mémoire :

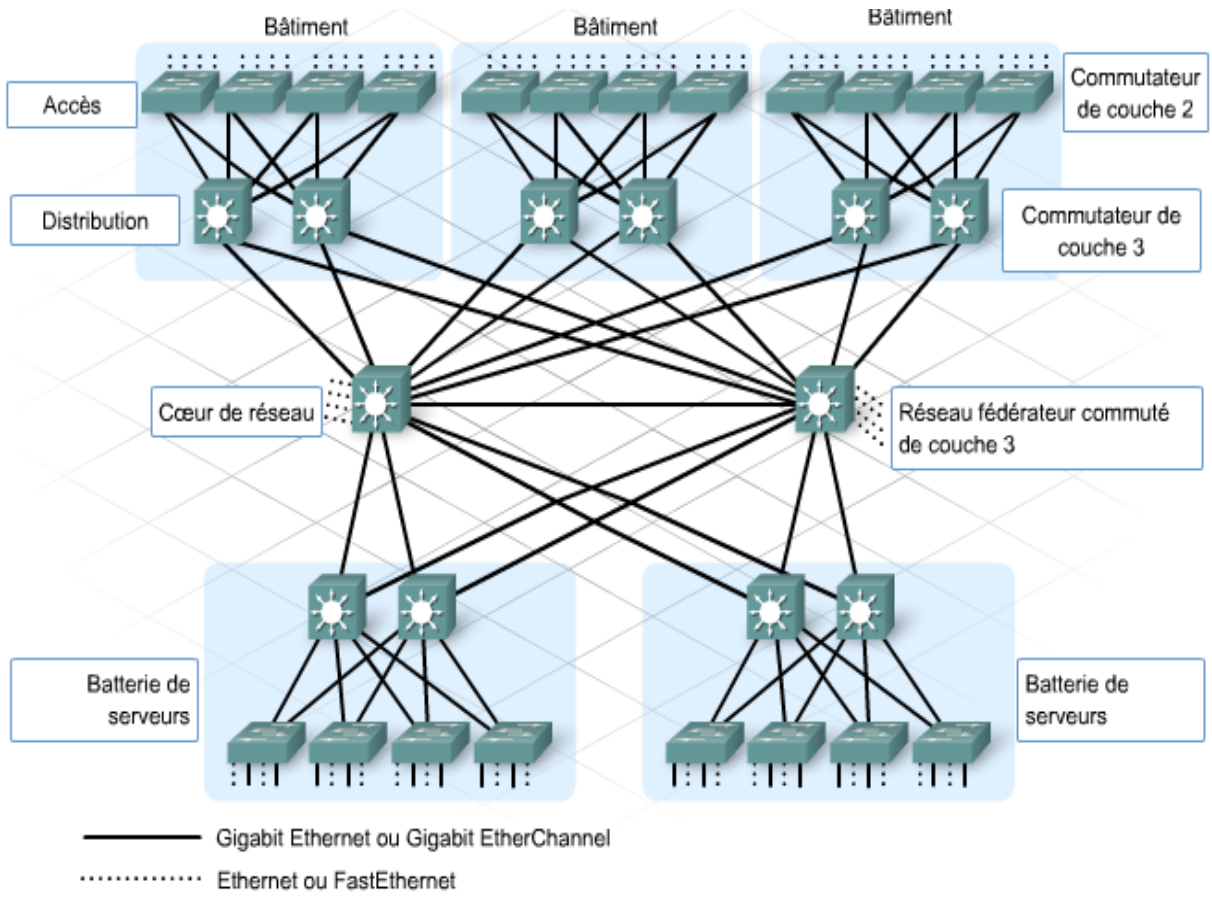


Figure 1.22 : *Architecture générale du réseau campus*

1.7 Conclusion

L'évolution de la taille ainsi que des technologies dans les réseaux augmentait les diverses problèmes de compatibilités et de gestion. Les demandes des clients et utilisateurs conduisent aussi à la recherche de nouvelles normes. C'est ainsi qu'a été créé le réseau campus qui est une évolution des réseaux LAN suivant des critères bien précis. L'approche sur les VLAN a solutionné le monde du partage du réseau tout en gardant les communications. Elle a permis aussi une facilité de gestion surtout au niveau de la couche accès.

CHAPITRE 2

Haute disponibilité dans le réseau

2.1 Introduction

Les pannes d'origines techniques sont fréquentes et une coupure de quelques minutes peut faire perdre à une entreprise une importante somme. Le réseau doit avoir un plan de secours en cas de défaillance à l'intérieur en continuant de transmettre jusqu'à la détection de la panne.

2.2 Généralités

La « haute disponibilité » est un domaine très large qui se retrouve dans les différentes briques composant les systèmes informatiques modernes (matériels réseau, serveurs, *SAN*, procédures, logiciels, …). Elle est souvent appliquée depuis les couches les plus basses (composants électroniques, redondances physiques, code de correction d'erreur, …) jusqu'aux couches les plus hautes (protocoles et procédures fiabilisées, *clusters*, …). [13]
Dans un réseau, c'est sa capacité à s'adapter à une coupure de lien ou à une défaillance d'un équipement (commutateur, routeur…). Ici, dans notre cas, on s'intéresse notamment aux couches 2 et 3 du modèle OSI.
L'objectif est que si il y a panne, un autre lien ou équipement prend le relai jusqu'à la détection et réparation de l'anomalie.

2.3 STP : gestion de niveau 2

2.3.1 Présentation

Le protocole STP(Spanning Tree Protocol), défini par la norme 802.1d, est un protocole de niveau 2(liaison de données) de la couche OSI conçu pour les commutateurs et dont le but est de s'assurer qu'il n'y a pas de boucle« logique » dans un réseau qui offrirait (volontairement ou non) des liaisons redondantes entre commutateurs. STP a pour rôle de détecter et de désactiver cette « boucle ». Il fait donc en sorte que les matériels ne fournissent qu'un seul chemin « logique » entre deux stations d'extrémité. Ce chemin logique sans boucle est appelé « arbre déployé ». [14]

2.3.2 Problématique

Dans un contexte de liaisons redondantes (boucles) sans utilisation de STP, divers problèmes peuvent survenir et notamment les « tempêtes de broadcast ».

Lorsque des trames de diffusion (*broadcast*) sont envoyées (soit FF-FF-FF-FF-FF-FF comme adresse MAC de destination), les switchs envoient ces trames sur tous leurs ports. Or les trames Ethernet (niveau 2) n'ayant pas de durée de vie TTL (*Time To Live* - comme il en existe dans les datagrammes IP – niveau 3), elles peuvent tourner « indéfiniment ». Elles circulent donc en boucle et sont répercutées de switch en switch, c'est la « tempête de broadcast » (*broadcast storming*). [14]

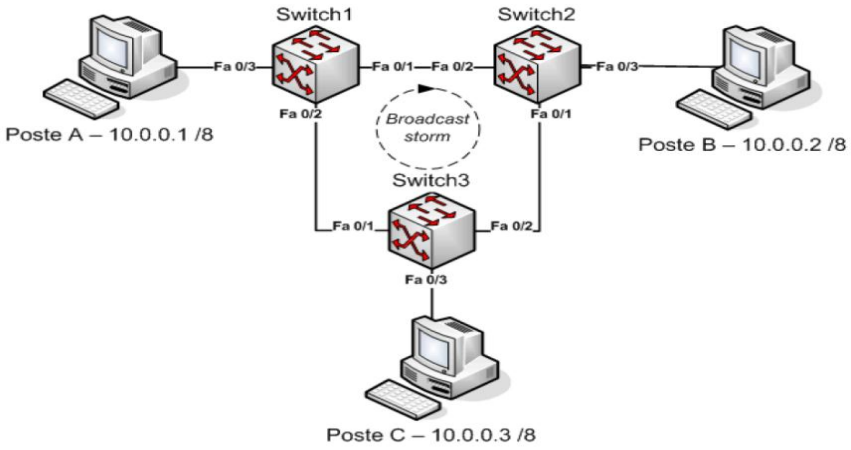


Figure 2.01 : *Envoi de broadcast en boucle entre les trois switch*

2.3.3 Norme 802.1D

La norme 802.1D est une norme définie par IEEE pour gérer les redondances des liens. Le spanning tree protocole est basé sur cette norme. Cette version de spanning tree protocole fonctionne sur tous les matériels gérant la redondance des liens (exemple tous les commutateurs CISCO). [9]

2.3.4 Fonctionnement

Le protocole de spanning tree vérifie la topologie du réseau et élimine les boucles dans la liaison en échangeant une information appelée BPDU (Bridge protocole Data Unit). Pour assurer ces opérations le protocole réalise une élection d'un pont racine (root bridge) dans le réseau tout entier (c'est le seul pont racine dans une topologie donnée). Les ports d'un pont racine sont appelés ports désignés. L'élimination d'une boucle se fait par le blocage d'un port appelé port non-désigné qui est celui d'un pont autre que le pont racine et la sélection des ports fait intervenir une notion de coût sur la liaison.

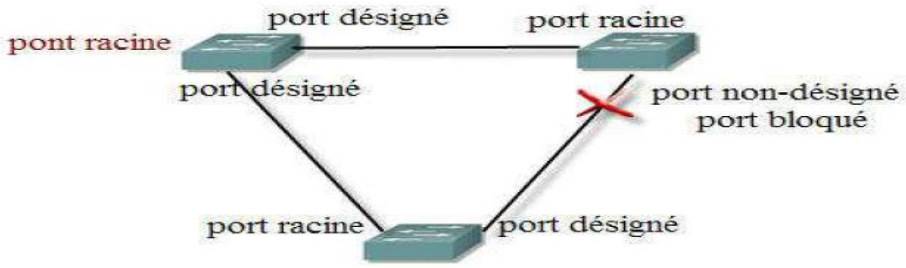


Figure 2.02 : *Elimination d'un port*

Ces opérations se font automatiquement sans configurer les commutateurs.

2.3.4.1 Protocole BPDU

Le BPDU est utilisé soit pour configurer la topologie du réseau (blocage des ports, élections des ponts…), soit pour signaler le changement de la topologie.

Types BPDU	Valeur (entête STP)
BPDU de configuration	0x00
BPDU de changement de topologie	0x80

Tableau 2.01: *Type de BPDU*

Les BPDU sont envoyés tous les 2 secondes dans le réseau par les ponts pour connaitre l'état du réseau. Le BPDU est une information échangée entre les ponts du réseau.

L'ID (identité) du pont ou BID (Bridge Indentification) est utilisée pour déterminer le pont racine et le port racine. Les 8 octets de l'identifiant du pont inclus la priorité et l'adresse physique du pont. La valeur de la priorité pour un matériel fonctionnant avec le STP standard de l'IEEE est de 32768. Le champ coût est la somme des coûts de traversée d'un lien sur le chemin (le coût est une valeur de 2octets). L'âge du message (BPDU) est le délai écoulé depuis la génération de la configuration par le commutateur émetteur (incrémenté à chaque retransmission). L'âge maximum du message est le délai maximum de prise en compte de la configuration. La période est le délai entre l'envoi successif de la configuration. Le délai de déblocage est le délai minimum entre la décision de déblocage et le déblocage effectif.

Voici un exemple d'une trame Ethernet complet avec un BPDU de configuration dans un pont racine d'adresse physique (00:b0:64:75:6b:c0).

Voici le format de la trame BPDU :

ID pont racine ou BID (8octet)	Coût (4octets)	ID pont émetteur (8octets)	ID port du pont émmetteur (2octets)	Age du message (2octets)	Age maximum du message (2octets)	Periode (2octets)	Délai de deblocage (2octets)

Figure 2.03 : *Trame BPDU*

- Le bridge ID

Avant l'apparition des VLAN, la priorité était codé sur 16 bits. Puis avec l'existence des VLAN, la priorité est codé sur 4 bits auquel : on ajoute 12 bits pour l'identifiant du VLAN sur lequel se construit le Spanning Tree.

La priorité ne peut donc prendre que des valeurs multiples de 4096 (212).

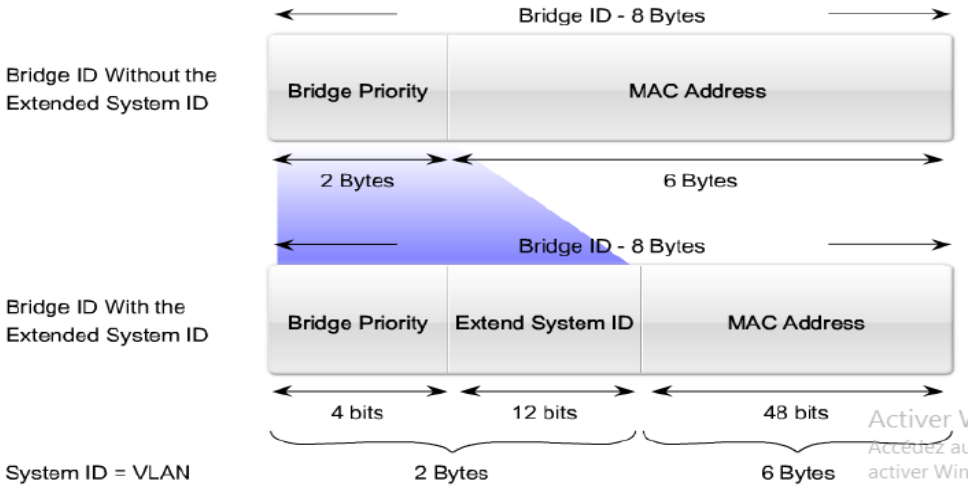


Figure 2.04 : *Configurations du BID*

2.3.4.2 Calculs du STP

Les ponts et les commutateurs s'échangent d'information de l'état du réseau via le paquet BPDU. Si dans le cas où il y changement, coupure, panne d'un matériel dans le réseau. Chaque pont et commutateur effectue les opérations suivantes pour assurer l'état de fonctionnement du réseau.

- Election du commutateur racine (pont racine)

Une topologie sans boucle ressemble à un arbre et à la base de chaque arbre, on trouve ses racines (roots). Dans un réseau commuté, un root bridge (pont/commutateur maître) est automatiquement choisi par l'algorithme du spanning tree. Pour déterminer le pont racine les priorités des ponts et les adresses MAC sont combinés. Si deux ponts ou commutateurs ont les mêmes valeurs de priorité. Alors l'adresse MAC est utilisée, et ce qui a la plus faible valeur d'adresse est élue racine.

A noter que le numéro de priorité est normalement laissé par défaut, mais l'administrateur du réseau peut s'il le souhaite modifier ce numéro pour faire élire un commutateur particulier ; dans le cas contraire, tout le processus est automatique.

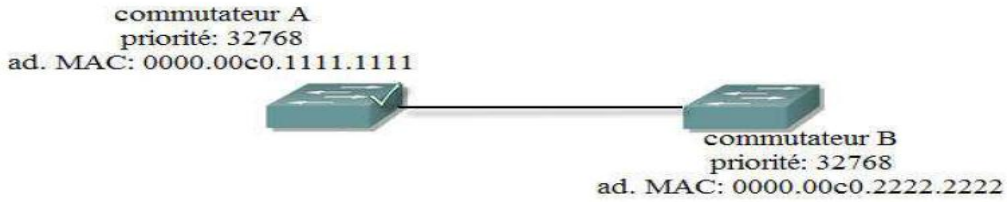


Figure 2.05 : *Election du pont racine ou root bridge*

La figure 2.06 ci-dessous montre que le commutateur A et B possède les mêmes priorités, donc on choisit comme commutateur root le commutateur A, car il a la faible (à partir du poids le plus faible des bits d'adresse) d'adresse physique par rapport à celui de B.

- Election des ports racine (root port)

Un root port est un port qui sera utilisé pour transmettre les données (par opposition à un port bloqué). Chaque commutateur doit avoir un seul root port. L'élection d'un root port est effectuée d'après les champs **path cost** (coût du chemin jusqu'au root bridge) et **port ID** d'un paquet BPDU. En cas d'égalité, c'est le port ayant le port ID le plus faible qui sera élu. Un port bloqué peut émettre et recevoir des paquets BPDU. Les autres ports d'un commutateur sont des ports désignés (designated ports), ce sont eux qui transmettent les paquets BPDU.

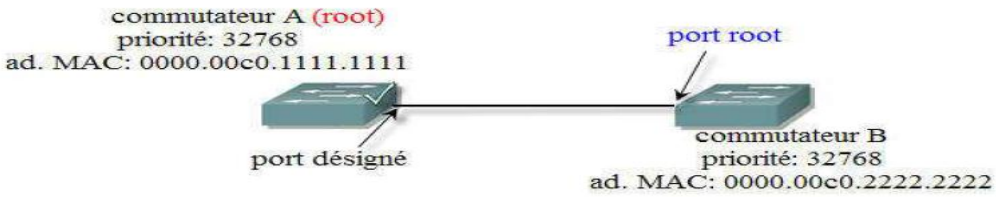


Figure 2.06 : *Election du port racine ou root port*

- Notion de coûts

Un critère utile dans l'élection d'un pont racine est la notion de coût de la liaison. Le coût est une valeur numérique attribuée à chaque traversée d'un pont à un autre. Un pont est élu racine lorsque le coût allant vers ce pont est minimale.

Pour garder une meilleure performance du réseau nous ne voulons pas expédier le trafic sur des liens à bas débit, donc la notion de coût trouve bien sa place pour assurer la qualité de liaison.

Nous trouvons dans le tableau ci-dessous les coûts recommandés par IEEE pour différentes types de liaisons caractérisées par ses débits de transmission.

Débits de liaison	Valeur recommandée pour le coût de la liaison
4 Mb/s	250
10 Mb/s	100
16 Mb/s	62
100 Mb/s	19
1 Gb/s	4
10 Gb/s	2

Tableau 2.02: *Coûts des liaisons*

La priorité sera celle qui a le coût minimal.

- Calcul du plus court chemin

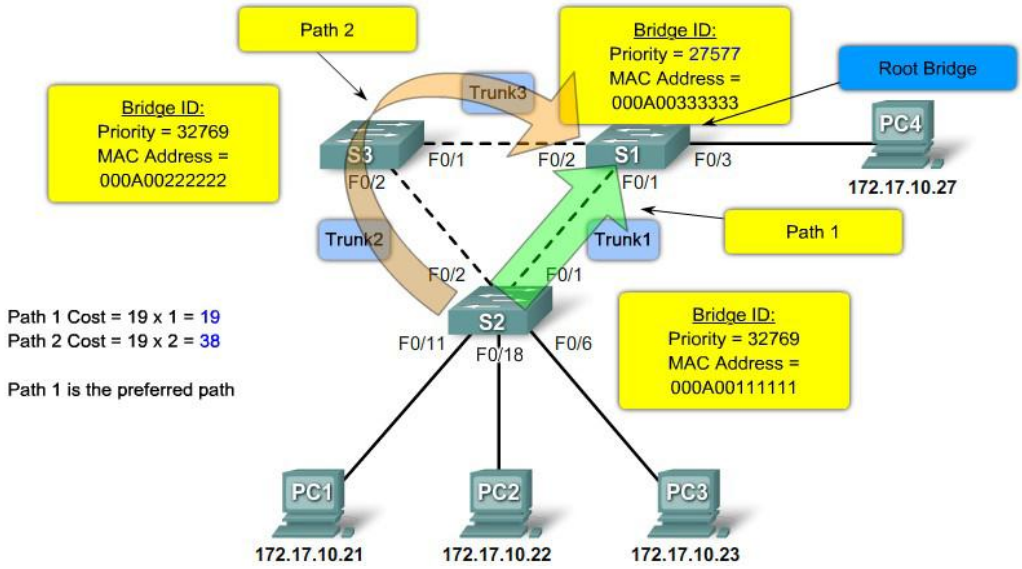


Figure 2.07 : *Exemple de calcul de coûts*

L'objectif de l'algorithme de STP est de trouver le plus court chemin. Ici, il calcul la somme des coûts des liens et le lien le plus petit sera le chemin emprunté qui es ici path 1.

2.3.5 Etats de STP

Cinq états de ports peuvent rencontrés consécutivement sur un port avant que STP ait convergé. Chaque état comporte un délai qui varie en fonction de la version de STP utilisée sur le commutateur. Voici les propriétés :

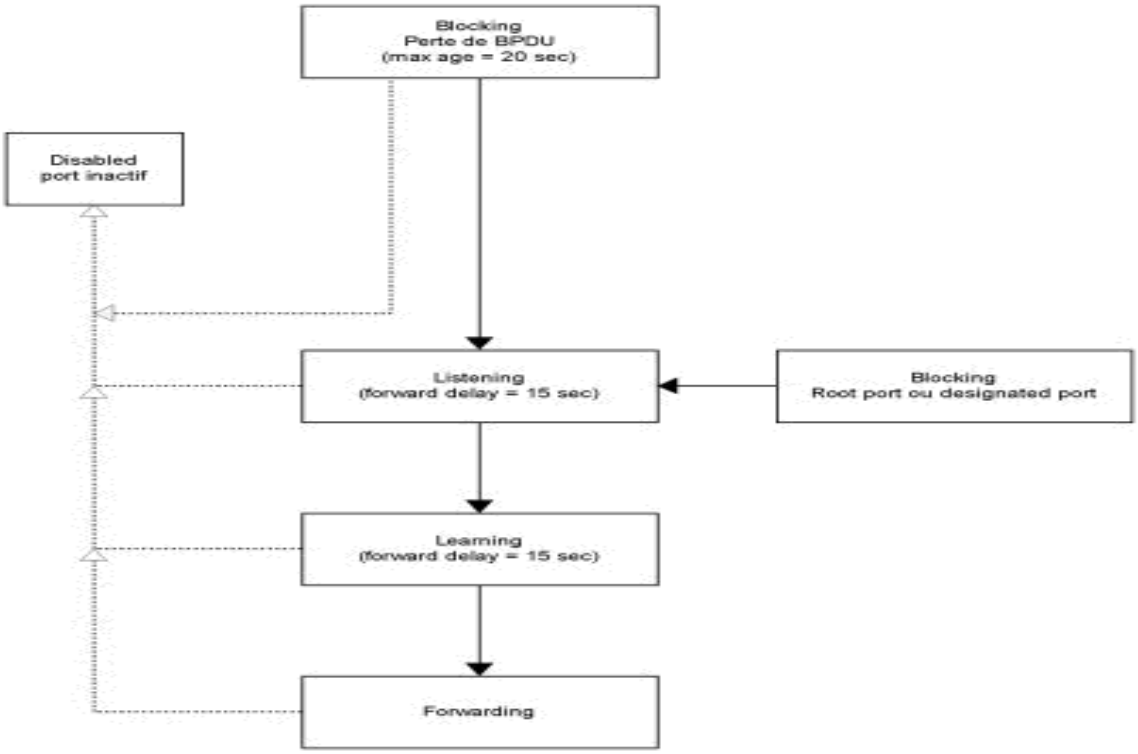


Figure 2.08 : *Etats des ports et délais d'attente*

Le compteur "age maximum" (Max Age) de 20 secondes par défaut est le temps maximal que STP effectue de nouveaux calculs quand une interface ne reçoit plus de BPDUs. Le temps de "forwarding" de 15 secondes par défaut est le temps de passage d'un état "listening" à "learning" et de "learning" à "forwarding". Bref, une topologie peut prendre jusqu'à 50 secondes avant de converger et de transférer du trafic. Aussi, la fréquence d'envoi de BPDUs Hello est de 2 secondes par défaut. [15]

2.3.5.1 Etat « Blocking »

Le port ne peut pas acheminer les paquets entrant et sortant. Pourtant il peut écouter s'il y a des paquets de configuration (BPDU). A noter que tous les ports sont dans l'état bloqué par défaut au commencement du processus (ou que si le commutateur vient de se démarrer).

2.3.5.2 Etat « Listening »

Dans le mode écoute, les ports écoutent tout d'abord les paquets BPDU pour assurer qu'il n'y a pas de boucle dans le réseau avant de faire passer les trames de données.

2.3.5.3 Etat « Learning »

Dans le mode Apprentissage, le port n'achemine pas les trames mais il recueille les adresses MAC et constitue un filtre pour la table nécessaire à la commutation.

2.3.5.4 Etat « Forwarding »

En mode acheminement, le port peut envoyer et recevoir les trames de données.

2.3.5.5 Etat « Disabled »

Cet état est similaire à l'état « blocking » sauf que le port est considéré physiquement non opérationnel (*shut down ou problème physique*).

2.3.6 Configurations manuelles

Dès fois, il est important de définir soit même, les règles des échanges dans STP. Comme par exemple, un commutateur qui donne accès à des routeurs et serveurs doivent être protégé et élu racine.
Voici les configurations utilisés :

2.3.6.1 Election du commutateur racine

Pour désigner un commutateur comme commutateur racine:

- Méthode 1: *S1(config) # spanning-tree vlan 1 root primary*

Remarque : vlan 1 est le réseau virtuel par défaut dans lequel se trouvent tous les ports d'un commutateur. Si on utilise les VLAN, il faudra donc désigner un commutateur racine par VLAN (et remplacer le 1 par l'id du VLAN) Pour configurer un commutateur racine secondaire prenant la place du premier en cas de défaillance:
S3(config) # spanning-tree vlan 1 root secondary.

- Méthode 2: *S1(config) # spanning-tree vlan 1 root priority valeur*

où valeur est un nombre compris entre 0 et 65536 par pas de 4096 Par défaut, tous les commutateurs reçoivent la priorité 32768 Par défaut, l'utilisation de primary (méthode 1)impose 24576 comme priorité et l'utilisation de secondary impose 28672.

2.3.6.2 Imposer le coût des liens

- Pour modifier ce coût par défaut (au niveau d'une interface): *S2(config-if) # spanning-tree cost 25*
- Pour rétablir le coût par défaut: *S2(config-if) # no spanning-tree cost*

2.3.6.3 Fixer les priorités des ports

Le système fixe une priorité de port par défaut égale à 128 à laquelle est associée l'id de port.
Ainsi le premier port aura une priorité par défaut de 128.1.
On peut modifier cette priorité par défaut: *S2(config-if) # spanning-tree vlan 1 port-priority 112*
La plage va de 0 à 240 par pas de 16
Comme pour la désignation du commutateur racine, c'est la valeur la plus faible qui sera retenue. Cela permettra, par exemple, de forcer la sélection d'un port racine.

2.3.6.4 Diagnostic

switch# show spanning-tree (*sh sp*)

Cette commande permet de voir le commutateur racine, le statut des ports connectés, leur coût, le coût des chemins, … et n'est valable que sous l'environnement Cisco.

2.3.7 Convergence

Il y a notion de convergence lorsque les ponts ou les commutateurs sont en mode de transition à l'état d'acheminement (forwarding) ou à l'état bloqué (blocking). Il n'y aura pas donc de données transmis pendant ce moment puisque les ports sont occupés pendant quelques secondes. La convergence est importante pour être sûre que tous les dispositifs ont la même base de données pour faire fonctionner le processus (transmission de données, changement de topologie…). Avant que les données soient acheminées, tous les dispositifs doivent être mis à jour. Le problème avec la convergence c'est que les dispositifs prennent du temps pour faire les mis à jour.
Habituellement sa prend 50 secondes environ pour passer de l'état bloqué à l'état acheminement

(Forwarding). Il n'est pas recommandé de changer le temps par défaut définie par STP, pourtant il est possible de changer le délai si nécessaire. Le délai d'acheminement est le temps pour qu'un port passe de l'état d'écoute à l'état d'apprentissage ou de l'état d'apprentissage à l'état d'acheminement.

2.3.8 PortFast de Cisco

Lorsqu'un port de commutateur configuré avec la technologie PortFast est défini comme port d'accès, ce port passe immédiatement de l'état de blocage à l'état activé, sans passer par les états traditionnels d'écoute et d'apprentissage STP.
On peut utiliser PortFast uniquement sur les ports d'accès (qui sont connectés à une station de travail ou à un serveur unique) pour permettre à ces périphériques de se connecter immédiatement au réseau au lieu d'attendre la convergence STP.

2.3.9 RSTP

RSTP (Rapid Spanning Tree Protocol) fait passer le temps de convergence à 6 secondes maximum ce qui le rend beaucoup plus opérationnel que STP.
RSTP fonctionne de la même manière que STP. Il y a toutefois quelques différences :

- Il n'y a plus que trois états pour les ports RSTP : Discarding (au lieu de Disabled, Blocking et Listening), Learning et Forwarding (ayant la même fonction)
- Les rôles port Root et port Designated subsitent. Les meilleurs ports alternatifs prennent le nom de lien de sauvegarde de ces derniers : port Alternate et port Backup. Ils prennent le rôle port Root et port Designated en cas de défaillance.
- Les ports connectant des périphériques terminaux s'appellent des ports Edge qui remplissent la même fonction que la fonction Portfast en PVST+.

Pour l'activer, en mode de configuration globale :

(config)#spanning-tree mode rapid-pvst

2.4 FHRP : gestion de niveau 3

FHRP (First Hop Redondancy Protocol) permet de gérer les redondances et les partages de charges au niveau réseau du modèle OSI. Comme pour STP, en cas de défaillance d'un routeur ou d'un lien, un autre prend le relai dans la transmission. L'existence d'adresse IP virtuel facilite

l'automatisation des tâches. Les protocoles de redondance au premier saut fournissent des passerelles par défaut redondantes pour les périphériques finaux sans configuration nécessaire au niveau de l'utilisateur final. Bref, quand un routeur du groupe tombe en panne, un autre transmet à la place utilisant l'adresse IP virtuel. Voici les trois principaux protocoles :

2.4.1 HSRP

2.4.1.1 Présentation

HSRP (Hot Standby Router Protocol) est un protocole de redondance, propriétaire Cisco, permettant de mettre en place une tolérance de panne pour les passerelles par défaut (RFC2281) et est basé sur le fonctionnement d'ARP (Adress Resolution Protocol). Ses particularités :

- Version 1 (IPv4):
- Adresse multicast : 224.0.0.2
- Port : UDP 1985
- MAC Virtuelle: 0000.0c07.acXX
- Version 2 (IPv4):
- Adresse multicast : 224.0.0.102
- Port : UDP 1985
- MAC Virtuelle : 0000.0c9f.fXXX
- Version 2 (IPv6):
- Adresse multicast : FF02::66
- Port : UDP 2029
- MAC Virutelle : 0005.73A0.0XXX

(XX est le numéro du groupe exprimé en hexadécimal)

2.4.1.2 Entête HSRP

Après configuration, les routeurs d'un même groupe s'échangent des paquets contenant les informations sur eux-mêmes et les règles à suivre dans HSRP.

- **OpCode** : 0 = Hello (le routeur est actif), 1 = Coup (le routeur veut devenir la passerelle active), 2 = Resign (le routeur cède sa place de passerelle active).
- **Etat** : Défini l'état du routeur qui envoi le message (0 = initial, 1=learn, 2=listen, 4=Speak, 8=Standby, 16=active)
- **HelloTime**: Intervalle en secondes entre deux messages de type «hello»

- **HoldTime**: Délai en secondes au-delà duquel un routeur est considéré comme hors service si aucun message «hello» n'est reçu de sa part.
- **Priorité**: Influence le choix de la passerelle active. La préférence va à la plus grande priorité. (Défaut = 100)
- **Groupe**: identifiant du groupe HSRP.
- **Authentification**: 8 caractères (8x8bits) définissant un mot de passe en clair
- **Adresse IP Virtuelle**: Adresse IP virtuelle pour le groupe HSRP en question.

Version (8)	OpCode (8)	Etat (8)	HelloTime (8)
HoldTime (8)	Priorité (8)	Groupe (8)	Réserve (8)
Authentification			
Authentification			
Adresse IP Virtuelle			

Figure 2.09 : *Informations dans l'entête*

2.4.1.3 Etats du routeur HSRP

- **Initial :** Etat initial lorsque HSRP se met route ou qu'un changement de configuration a lieu.
- **Learn :** Le routeur n'a pas encore appris son adresse IP virtuelle, ni reçu de messages «hello». Le routeur est en attente d'un message du routeur actif.
- **Listen :** Le routeur connait son adresse IP virtuelle mais n'est ni le routeur actif, ni standby et attend un message de ceux-ci.
- **Initial :** Etat initial lorsque HSRP se met route ou qu'un changement de configuration a lieu.
- **Speak :** Le routeur participe à l'élection du routeur actif et émet les messages «hello» périodiques.
- **Standby :** Le routeur est candidat pour devenir le prochain routeur actif et envoi des messages «hello» périodiques.
- **Active :** Le routeur est la passerelle active et route le trafic destiné à l'adresse MAC virtuelle du groupe.

Timers :

- Hello: 3s

- Hold timer: 10s
- Modifiables via la commande standby [#] timers *hello hold*

2.4.1.4 Fonctionnement

Un groupe de routeurs fonctionne comme un routeur virtuel en partageant une adresse IP virtuelle et une adresse MAC virtuelle. Un routeur actif exécute l'acheminement des paquets pour les hôtes locaux. Les autres routeurs fournissent un « secours automatique » en cas de panne du routeur actif.Les routeurs en attente demeurent au repos en ce qui a trait à l'acheminement des paquets du côté client. [11]
Cet état de repos est appelé aussi standby.

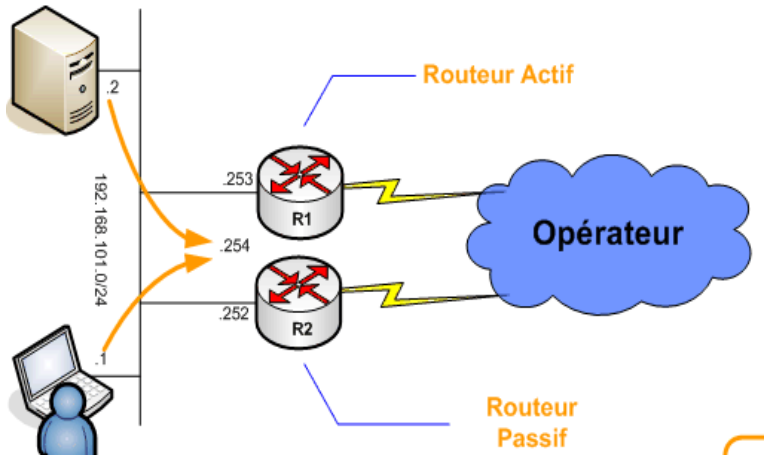


Figure 2.10 : *Etat initial des routeurs*

En partageant une seule même adresse IP et MAC, plusieurs routeurs peuvent être considérés comme un seul routeur "Virtuel". Les membres du groupe de ce routeur virtuel sont capables de s'échanger des messages d'état et des informations.
Un routeur physique peut donc être "responsable" du routage et un autre en redondance.
Si le routeur, que nous appellerons primaire, a un problème, le routeur secondaire prendra sa place automatiquement. Les paquets continueront de transiter de façon transparente car les 2 routeurs partagent les mêmes adresses IP et MAC.

Un groupe de routeur va négocier au sein d'un même groupe HSRP (ou *standby group*), un routeur primaire (*Active router*), élu au moyen d'une priorité, pour transmettre les paquets envoyés au routeur virtuel.

Un autre routeur, le routeur secondaire (*Standby router*), sera élu lui aussi afin de remplacer le routeur primaire en cas de problème. Le secondaire assumera donc la tâche de transmettre les paquets à la place du primaire en cas de défaillance.

Le processus d'élection se déroule pendant la mise en place des liens, une fois ce processus terminé, seul le routeur primaire (*Active*) va envoyer des messages multicast en UDP périodiques HSRP aux autres afin de minimiser le trafic réseau.

Si ces messages ne sont plus reçus par le routeur secondaire (*Standby*), c'est que le routeur primaire à un problème et le secondaire devient donc Actif.

L'élection se fait un peu à la manière de spanning-tree, en prenant en compte une priorité. Cette priorité est composée d'un paramètre "priority" compris entre 1 et 255 (255 étant le plus prioritaire) et de l'adresse IP de l'interface.

A priorités statiques égales, la plus haute adresse IP sera élue.

Plusieurs groupes HSRP peuvent exister au sein d'un même routeur sans que cela ne pose problème (depuis l'IOS 10.3). Seuls les routeurs du même numéro de groupe s'échangeront les messages HSRP.

Il existe aussi une caractéristique d'authentification HSRP qui se compose d'une clé partagée en texte clair contenue dans les paquets HSRP. Cette caractéristique empêche le routeur de basse priorité d'apprendre l'adresse IP de veille et les valeurs de temporisateurs de veille d'un routeur à la priorité plus élevée.

2.4.1.5 Configurations

Voici un exemple de code :

R1(config)#interface Fastethernet 0/0
R1(config-if)# ip address 192.168.0.2 255.255.255.0
R1(config-if)#standby 1 ip 192.168.0.1
R1(config-if)#standby 1 priority 105
R1(config-if)#standby 1 preempt
R1(config-if)#standby 1 track fa0/0
R1(config-if)#standby authentication string x

- La commande *« standby x »* permet de définir le groupe HSRP où le routeur est placé

- "*standby priority xxx*" définit une priorité au routeur. Celui qui possédera la plus grande valeur sera élus actif. Si la configuration du routeur ne stipule pas la priorité, alors la valeur par défaut de 100 sera appliquée.
- "*standby preempt*" permet d'accélérer le processus d'élection.
- "*standby ip xxx.xxx.xxx.xxx*" indique l'adresse IP virtuelle partagée entre les deux routeurs.
- "*standby track xxxxxx*" permet de superviser une interface et de baisser de 10 la valeur de la priorité HSRP si elle devenait Down.
- *standby authentication string x* configuration de la clé partagée

2.4.1.6 Bilans

Le protocole HSRP est très répandu avec du matériel Cisco sur les LAN. Cela permet une souplesse de configuration sur tous les matériels Cisco, y compris Wireless.
D'autres options sont utilisables, notamment les groupes multiples HSRP ou le support dans une architecture MPLS-VPN.
Cependant, HSRP présente quelques failles non négligeables. En effet, le protocole HSRP utilise pour authentifier les requêtes un mot de passe qui transite en clair sur le réseau (même principe que les noms de communauté SNMP - *Simple Network Management Protocol*).
Au-delà de cette faiblesse, il existe aussi un problème dans la gestion des adresses IP par HSRP. En effet, bien que les messages HSPR soient de type Multicast, les paquets de type Unicast sont acceptés et traités par HSRP. Cela signifie que les paquets HSRP, ayant pour adresse de destination celle du routeur, seront traités par ce dernier sans contrainte. Ce comportement peut permettre des attaques à distance en s'affranchissant des contraintes de sécurité liées au trafic Multicast (le trafic Multicast peut être interdit au niveau de la politique de sécurité des routeurs).
La solution serait de filtrer le port 1985, relatif au protocole HSRP. [16]

2.4.2 VRRP

Virtual Router Redundancy Protocol (VRRP) est un protocole standard normalisé par IETF Standard RFC 2338 (avril 1998). [11]
VRRP fonctionne de la même manière que HSRP, quelques nuances toute fois, les rôles active/standby sont définis respectivement comme master/backup, et le standby group devient le vrrp group.
La configuration se fait à l'identique que HSRP, en remplaçant la commande standby par VRRP.

2.4.2.1 Timers

Une des nuances avec HSRP se trouve dans le temps de fonctionnement :

- Hello: 1s
- Hold timer: 3xHello (3s) + Skew timer
- Skew timer = 256-priority/256 s (priority = 100 par défaut). Cela permets d'ajouter un délai au cas où le 3e ping arriverai avec du retard (< 1s)
- Les timers VRRP HOLD ne sont pas configurable (toujours égaux à 3x le hello timer).
- Les timers sont configurés sur le master (vrrp # timers advertise {hello}), et sont appris par le backup (vrrp # timers learn, par défaut)

2.4.2.2 Fonctionnement

Identique à HSRP, mais il y a quelques exceptions :

- Il n'y a pas d'authentification entre les extrémités
- La commande « preempt » est activé par défaut
- Il n'y a que trois (3) états du routeur VRRP :
  - Initialize : attente de l'envoi des paquets
  - Backup : enregistre l'état du routeur maître. Contrairement à HSRP, plusieurs routeurs peuvent avoir le rôle Backup.
  - Master (Actif en HSRP) : Concernant la priorité, elle est de 100 par défaut. Quand un routeur devient Master, il annonce une priorité de 255. La priorité 0 est réservée au Master pour annoncer qu'il ne participe plus au groupe VRRP. Cela permet aux routeurs Backup de prendre le relai plus rapidement. En cas d'égalité sur la priorité, c'est le routeur avec la plus haute IP qui devient Master.
- Les messages VRRP sont envoyés sur l'IP de multicast 224.0.0.18. L'adresse Mac virtuelle de la passerelle est 00-00-5E-00-01-XX, où XX correspond au numéro du VRRP Group (VRID – Virtual Routeur Identifier). Concernant les Timers, nous en retrouvons 3 :
- Le Skew Timer a le même rôle que le second bonus du Timer par défaut en HSRP. Il est exprimé en millisecondes. Seul le Hello Timer peut être changé. Le Dead Timer changera en conséquence. Il est possible de configurer les routeurs Backup pour qu'ils apprennent le Timer du Master. Par contre, cela ne fonctionne que si le Timer est supérieur ou égal 1s.

Autre changement, en VRRP l'IP virtuelle peut être configuré directement sur l'interface du routeur Master. En HSRP il faut trois adresses IP : une pour R1, une pour R2, et une pour l'IP virtuelle. EN VRRP il n'en faut que deux : une pour le master (qui sera l'IP virtuelle) et une pour R2. Néanmoins, nous pouvons aussi utiliser trois IP, à la manière d'HSRP.

- La Configuration Le protocole VRRP n'est pas disponible sur mes switchs de niveau 3.

1.4.2.3 Configurations

*R1(config) #interface FastEthernet0/1 !*interface vers LAN (segment à redonder)

*R1(config-if)# vrrp 1 ip 10.0.0.1 !*IP Virtuelle, correspond au master !

*R1(config-if)#vrrp 1 preempt !*active la preemtion

*R1(config-if)#vrrp 1 desc VRRP1 !*Définition d'une description, optionnel

R1(config-if)# vrrp 1 priority 110 ! change la priorité par défaut (100)

2.4.3 GLBP

2.4.3.1 Présentation

Gateway Load Balancing Protocol (GLBP) est de conception Cisco, avec partage de charge, brevet encore en instance. [11]

Il permet de faire de la redondance ainsi que de la répartition de charge sur plusieurs routeurs utilisant une seule adresse IP virtuelle, mais plusieurs adresses MAC virtuelles.

Le protocole GLBP élit un Active Virtual Gateway (AVG) qui va répondre aux requêtes ARP pour l'adresse IP virtuelle. GLBP permet de donner un poids variable à chacun des routeurs participants pour la répartition de la charge entre ces routeurs. La charge est donc répartie par hôte dans le sous-réseau. L'adresse de Multicast utilisée est la suivante : 224.0.0.102.

1.4.3.2 Timers

Les timers de GLBP sont :

- **Hello** : 3s
- **Dead** : 10s est le temps à partir duquel un AVF sera Dead, son adresse mac sera associée à un autre AVF
- **Redirect** (Temps à partir duquel on arrêtera de rediriger l'adresse mac d'une AVF Dead vers une autre AVF) : 600s

- **Timeout** (Temps à partir duquel un routeur est considéré comme inactif, son adresse MAC ne sera plus utilisée) : 14,400s (4 heures), doit être supérieur au temps de conservation des entrées ARP des clients.

2.4.3.2 Fonctionnement

GLBP reprend les concepts de base de HSRP et VRRP.
Contrairement à ces deux protocoles, tous les routeurs du groupe GLBP participent activement au routage alors que dans VRRP ou HSRP, il n'y en a qu'un qui est en mode actif, tandis que les autres patientent. Plus concrètement, à l'intérieur du groupe GLBP, le routeur ayant la plus haute priorité ou la plus haute adresse IP du groupe prendra le statut de « AVG ». Ce routeur va intercepter toutes les requêtes ARP effectuées par les clients pour avoir l'adresse MAC de la passerelle par défaut, et grâce à l'algorithme d'équilibrage de charge préalablement configuré, il va renvoyer l'adresse MAC virtuelle d'un des routeurs du groupe GLBP. C'est d'ailleurs le Routeur AVG (Active Virtual Gateway) qui va assigner les adresses MAC virtuelles aux routeurs du groupe, Ainsi ils ont le statut « AVF » (Active Virtual Forwarder). Un maximum de 4 adresses MAC virtuelle est défini par groupe, les autres routeurs ayant des rôles de backup en cas de défaillance des AVF.

2.4.3.3 Etats

- AVG :
  - Disabled : pas d'adresse IP virtuelle configuré.
  - Initial : adresse IP virtuel configuré, mais la passerelle virtuel n'est pas complète
  - Listen : La passerelle virtuelle reçoit les messages hello et est prêt à entrer en état "speak" si AVG n'est pas disponible
  - Speak la passerelle virtuelle est attendu pour devenir Active Virtual Gateway (AVG).
  - Standby : la passerelle virtuelle est prête à devenir le prochain AVG.
  - Active : la passerelle virtuelle est AVG, répond au client ARP des requêtes pour l'adresse IP virtuelle, fourni une des AVF MACs basé en schéma de partage de charge.
- AVF :
  - Disabled : Pas d'adresse MAC assigné

- Initial : L’adresse MAC virtuelle est configurée, mais la configuration de AVF est incomplète.
- Listen : AVF écoute les messages ‘hello’ et est prêt pour être en état “active”, si un autre n’est pas disponible
- Active : être un AVF, et responsable pour transmettre les paquets envoyés à l’adresse MAC d’un AVF.

2.5 Les agrégations de liens : Etherchannel

2.5.1 Principes

L'agrégation de liens est le regroupement de plusieurs ports physiques d'un switch pour augmenter sa bande passante. Par exemple l'agrégation de 2 ports 100Mb/s permet d'avoir un agrégat (une interface virtuel) de 200Mb/s, mais entre deux machines on n’aura pas 200Mb/s (c'est du à la méthode de partage de charge), il faut plusieurs machines pour qu'au global on s'approche des 200Mb/s. Dans la configuration cet agrégat ou Etherchannel est vu/configuré comme un port channel raccourci à **Po**.
La tolérance aux pannes est un autre aspect essentiel d’EtherChannel. Si un lien tombe, la charge est automatiquement redistribuée sur les liens restants. Ce processus de remise sur pied prend moins d'une seconde et est transparent aux applications réseau.
Un EtherChannel permet d'agréger de 1 à 8 ports physiques, il y a la possibilité de modifier la méthode de load-balancing (partage de charge) sur ces ports. Un EtherChannel peut être de niveau 2 ou niveau 3, de protocole standard LACP (Link Aggregation Control Protocol) IEEE 802.3ad, propriétaire Cisco, PAgP (Port Aggregation Protocol) ou forcé. Les ports doivent être avoir le même duplex, speed et VLAN information. En fonction des modèles de switchs/IOS/protocole, un etherchannel sur des ports des switchs différent (cas par exemple dans un stack aussi appelé un etherchannel MEC "Multichassis EtherChannel") n'est pas possible. [17]

2.5.2 Protocoles

2.5.2.1 PAGP

PAGP (Port Aggregation Protocol) est le protocole de négociation propriétaire Cisco.
En choisissant ce protocole, il est possible de configurer les ports dans 2 modes différents :

- Auto
- Desirable

A noter que si nous ne voulons pas utiliser de protocole de négociation, le port devra être mis en mode **ON**, pour forcer l'agrégation de lien.

Avec PAGP, si le port est en mode Auto, une agrégation de lien sera créée si le port d'en face est en mode **Desirable.** Si le port d'en face est en mode Auto, aucune agrégation n'est créée.

Si le port est configuré en mode **Desirable**, une agrégation sera créée à condition que le port d'en face soit en mode **Auto** ou **Desirable**.

Il n'est pas possible d'avoir un port en mode ON d'un côté, et d'utiliser un protocole de négociation (PAGP ou LACP) de l'autre côté d'une agrégation.

A partir du moment où nous utilisons le mode ON pour créer une agrégation de lien, aucun protocole de négociation ne sera utilisé. Les ports en face devrons donc être en mode ON eux aussi.

2.5.2.2 LACP

LACP (Link Agregation Control Protocol) est un protocole standard (802.3AD) très similaire à PAGP.

La seule différence est le nom des modes de port.

Nous retrouvons donc deux modes de ports :

- Passive
- Active

Passive correspond au mode Auto de PAGP : création d'une agrégation si le port en face est en Active.

Active correspond au mode Desirable de PAGP : création d'une agrégation si le port d'en face est en Passive ou Active.

Il conviendra donc de choisir un protocole de négociation (de préférence LACP car il est standard) puis de choisir le mode des ports.

Par sécurité, le mieux est d'utiliser le mode Desirable (ou Active) des deux côtés.

Il est aussi tout à fait possible de se passer de protocole de négociation, en utilisant le mode ON. En cas de mauvaise configuration, cela peut parfois mener à des boucles réseau, que même Spanning Tree ne pourra empêcher. Le mode ON est donc à utiliser avec précaution.

Protocole	Mode	Description
PAgP	Auto	Ce mode PAgP met l'interface en négociation passive, c'est-à-dire qu'elle répond aux packets PAgP reçus mais n'initialise pas la négociation (défaut)
	Desirable	Ce mode de PAgP place l'interface en mode active, elle initialisera les négociations en envoyant des packets PAgP
LACP	Passive	Ce mode LACP place l'interface en négociation passive (défaut).
	Active	Ce mode LACP place l'interface en négociation active.
	On	Ce mode force l'interface en EtherChannel sans négociation, sans PAgP et sans LACP
	Off	Désactive l'EtherChannel

Tableau 2.03: *Fonctionnement des protocoles d'Etherchannel*

1.5.3 Configurations

Voici les commandes utilisées an etherchannel :

Commandes	Descriptions
Switch(config)# interface range fastEthernet 0/10 - 11	On spécifie les interfaces qui vont former l'EtherChannel
Switch(config-if-range)# channel-protocol {pagp|lacp}	Protocole de channel : PAgP ou LACP
Switch(config-if-range)# channel-group 2 mode {on|active|passive|auto|desirable}	Mode de négociation et création du Po ou port channel
Switch(config)# interface port-channel 2	configuration du Po précédement créé

Tableau 2.04: *Commandes de configurations*

2.6 Choix des protocoles de gestions des redondances et explications

2.6.1 Pour la redondance de niveau 2

On a choisi d'utiliser STP. Ce protocole permet de :

- Gérer le trafic en boucle des broadcast dans les switch

- En cas de coupure de lien un autre remplace tout de suite
- En cas de panne d'un commutateur, même le commutateur racine, celui-ci peut être remplacé par le commutateur secondaire.

2.6.2 Pour la redondance de niveau 3

HSRP est le choix le plus cohérent car :

- C'est le plus utilisé dans les réseaux campus, d'ailleurs conseillé, même s'il ne fonctionne que dans les environnements Cisco.
- Facile à configurer par rapport aux autres FHRP. C'est la base de tous, donc intéressant pour une étude.
- Par rapport à GLBP, il consomme moins de mémoire dans les routeurs car avant la défaillance du routeur actif, les autres sont en veille (standby).
- La simplicité des commandes aussi réduit le fonctionnement de la mémoire de l'équipement où il est implémenté.
- Il peut être implémenté dans les commutateurs de niveau 3.

2.6.3 Gestion des agrégations

LACP est un protocole standard qui est compatible avec tout protocole des constructeurs réseaux. La combinaison de ces protocoles permet de garantir la stabilité du réseau même en cas de panne des équipements. Ils permettent aussi d'avoir des débits suffisant pour les transmissions dans le réseau campus.

2.7 Conclusion

La haute disponibilité et le partage des charges sont des éléments essentiels de la conception du réseau. On peut éviter les pertes de données en cas de panne donc elle offre la fiabilité. Mais il faut savoir gérer les redondances, trop de redondance nuit aussi à la vitesse de transmission et la convergence. Le protocole STP assure la disponibilité au niveau accès, HSRP au niveau distribution, LACP assure au niveau cœur tout en favorisant un débit élevé.

CHAPITRE 3

Sécurités des routeurs Cisco

3.1 Introduction

Les attaques d'origine informatique sont de plus en plus nombreuses et prend plusieurs formes de nos jours. Aucun système connecté à internet ou simplement à un réseau externe n'est à l'abri du danger. Des données volées ou supprimés peuvent être fatales à son détenteur. Cisco a implémenté des systèmes permettant de sécuriser les réseaux dans la plupart de ses équipements. Dans notre cas, nous allons nous basés sur les routeurs.

3.2 Notions de sécurité informatique

Le système d'information est généralement défini par l'ensemble des données et des ressources matérielles et logicielles de l'entreprise permettant de les stocker ou de les faire circuler. Le système d'information représente un patrimoine essentiel de l'entreprise, qu'il convient de protéger. La sécurité informatique, d'une manière générale, consiste à assurer que les ressources matérielles ou logicielles d'une organisation sont uniquement utilisées dans le cadre prévu. [18]
Les exigences fondamentales de la sécurité Informatiques se résument à assurer:

- La disponibilité : L'information sur le système doit être toujours disponible aux personnes autorisées.
- La confidentialité : L'information sur le système ne doit être diffusée qu'aux personnes autorisées.
- L'intégrité : L'information sur le système ne doit pouvoir être modifiée que par les personnes autorisées.
- L'authentification : consiste à assurer l'identité d'un utilisateur, c'est-à-dire de garantir à chacun des correspondants que son partenaire est bien celui qu'il croit être. Un contrôle d'accès peut permettre (par exemple par le moyen d'un mot de passe qui devra être crypté) l'accès à des ressources uniquement aux personnes autorisées.
- La non-répudiation et l'imputabilité : seules les entités identifiées et authentifiées ont pu réaliser une certaine action (preuve de l'origine d'un message ou d'une transaction, preuve de la destination d'un message…).

La méthodologie de la sécurité se divise en deux :

- Analyse de risques
- Etablissement d'une politique de sécurité

3.2.1 Analyse de risques

Il n'est possible de se protéger que contre les risques que l'on ne connait. Ceci dit, il convient pour chaque entreprise d'évaluer les risques, c'est-à-dire les mesurer en fonction de la probabilité de leurs apparitions et de leurs effets possibles. Les entreprises ont tout intérêt à évaluer, quoique grossièrement ces risques et les moyens à mettre en œuvre, en fonction de leurs coûts. La notion de risque peut être appréhendée comme étant le produit d'un préjudice par la probabilité d'occurrence de celui-ci. La notion de risques est définie par les spécialistes selon l'équation suivante :

Risque = Préjudice x Probabilité d'occurrence

Cette formule sous-entend qu'un événement dont la probabilité est assez élevée mais dont il est possible de prévenir le préjudice qu'il peut causer, représente un risque acceptable. Il en va de même pour un événement à la gravité imparable (ex : effondrement d'un immeuble), mais à probabilité d'occurrence faible. Il va de soi que dans le premier cas, le risque ne devient acceptable que si les mesures de prévention contre le préjudice sont effectives et efficaces.

3.2.2 Conception d'une politique de sécurité

Une politique de sécurité informatique est un plan d'actions définies pour maintenir un certain niveau de sécurité. Elle reflète la vision stratégique de la direction de l'organisme (PME, PMI, industrie, administration, état, unions d'états …) en matière de sécurité des systèmes d'information.

La sécurité des systèmes informatiques se cantonne généralement à garantir les droits d'accès aux données et ressources d'un système en mettant en place des mécanismes d'authentification et de contrôle permettant d'assurer que les utilisateurs des dites ressources possèdent uniquement les droits qui leur ont été octroyés. [19]

Les mécanismes de sécurité mis en place peuvent néanmoins provoquer une gêne au niveau des utilisateurs et les consignes et règles deviennent de plus en plus compliquées au fur et à mesure que le réseau s'étend. Ainsi, la sécurité informatique doit être étudiée de telle manière à ne pas empêcher les utilisateurs de développer les usages qui leur sont nécessaires, et de faire en sorte qu'ils puissent utiliser le système d'information en toute confiance.

C'est la raison pour laquelle il est nécessaire de définir dans un premier temps une politique de sécurité, dont la mise en œuvre se fait selon les quatre étapes suivantes :

- Identifier les besoins en terme de sécurité, les risques informatiques pesant sur l'entreprise et leurs éventuelles conséquences ;
- Elaborer des règles et des procédures à mettre en œuvre dans les différents services de l'organisation pour les risques identifiés ;
- Surveiller et détecter les vulnérabilités du système d'information et se tenir informé des failles sur les applications et matériels utilisés ;
- Définir les actions à entreprendre et les personnes à contacter en cas de détection d'une menace ;

Le rôle de l'administrateur informatique est donc de s'assurer que les ressources informatiques et les droits d'accès à celles-ci sont en cohérence avec la politique de sécurité définie par l'organisation.

On distingue notamment :

- la sécurité de l'information ;
- la sécurité des données, liée aux questions d'interopérabilité, et aux besoins de cohérence des données en univers réparti ;
- la sécurité des réseaux ;
- la sécurité des systèmes d'exploitation ;
- la sécurité des télécommunications ;
- la sécurité des applications (dépassement de tampon), cela passe par exemple par la programmation sécurisée ;
- la sécurité physique, soit la sécurité au niveau des infrastructures matérielles.

Ce qui nous intéresse ici c’est la sécurité des réseaux.

3.3 Les translations d’adresse : NAT et PAT

Le NAT (Network Address Translation) a été proposé en 1994 sous la RFC 1631 comme solution à court terme face au manque d'adresses IP. Son objectif principal était de permettre aux adresses IP d'être partagées par un grand nombre de périphériques réseau. Il est à l’origine de la création d’IPv6.

Le NAT permet d'utiliser des adresses n'ayant pas de signification globale (par exemple des adresses privées définies dans la RFC 1918, non routables) pour se connecter à travers l'Internet en

traduisant celles-ci en adresses globales routables. Le NAT permet aussi de fournir une solution élégante de renumérotation pour les organisations qui changent de fournisseur de service. [20]
Pour cela on distingue :

3.3.1 NAT Statique

Il permet de translater/transformer une adresse IP par une autre adresse IP.
Par exemple : Sur notre réseau local, on possède un serveur web qu'on souhaite rendre accessible depuis internet, notre serveur est configuré avec l'adresse IP 192.168.1.1.
Sur notre connexion internet, on possède plusieurs adresses IP public 80.22.33.45, 80.22.33.46, 80.22.33.47.
Le nom de notre site web hébergé sur notre serveur correspondra à l'adresse publique 80.22.33.47.
On va donc configurer une règle NAT Statique sur notre routeur pour translater toutes les requêtes arrivant sur 80.22.33.47 vers 192.168.1.1 de notre réseau local.
Plus techniquement, lorsque notre routeur va recevoir une requête arrivant d'internet ayant pour adresse de destination 80.22.33.47, celui-ci va substituer l'adresse de destination par l'adresse IP 192.168.1.1.

3.3.2 NAT dynamique

Le NAT Dynamique permet de translater plusieurs adresses IP par un pool d'adresses.
Par exemple, on a :
Sur notre réseau local, on possède dix PC devant naviguer sur internet.
Sur notre connexion internet, je possède un pool d'adresses IP public 80.22.33.45 à 80.22.33.55 (soit 10 adresses public).
On va donc configurer une règle NAT dynamique sur notre routeur, pour translater automatiquement les requêtes qui partent de nos PC vers Internet.
Plus techniquement, lorsque notre routeur va recevoir une requête d'un PC pour naviguer sur internet, il va regarder la table de NAT et prendre la première adresse publique du pool disponible. Il va associer les deux adresses durant l'échange HTTP. Une fois l'échange http terminé, l'adresse sera libérée.
On pourrait configurer un réseau ayant par exemple 20 PC pour 10 adresses IP publiques. Mais si les 20 PC veulent naviguer sur internet en même temps, uniquement les 10 premiers pc pourront naviguer.

3.3.3 NAT Overload ou PAT

PAT (Port Address Translation) permet de translater plusieurs adresses IP par une adresse IP.
Sur notre réseau, on possède X PC devant naviguer sur Internet.
Sur notre connexion internet, on possède seulement une adresse IP Public 80.22.33.45.
Si on utilise le NAT Statique, un seul de nos PC pourra naviguer sur Internet.
Si on utilise le NAT Dynamique, nos X PC pourront naviguer sur Internet, mais seulement un seul à la fois.
Avec le NAT Overload, tous mes PC peuvent naviguer sur Internet en même temps.
Plus techniquement, lorsque notre routeur reçoit une requête, il crée une sorte de session en ajoutant un port sur la requête (port compris entre 0 et 65535).

- PC1 - 192.168.1.1 envoie la requête au routeur.
- Le routeur crée la session 192.168.1.1:1025 - 80.22.33.45:1025
- La requête est envoyée sur internet.
- Le serveur répond à l'adresse 80.22.33.45:1025
- Le routeur regarde dans sa table NAT et cherche la correspondance avec 80.22.33.45:1025
- Il trouve 192.168.1.1:1025
- Il envoie la réponse au PC1.

3.3.4 Avantages

On peut utiliser le NAT dans différents cas :

- On dispose d'une multitude d'hôtes adressés de manière privée et on a une seule ou quelques adresses IP globales (publiques). Le NAT est configuré sur un routeur en bordure d'un réseau d'extrémité, étant identifié comme étant le côté interne (*inside*), qui connecte un réseau publique comme l'Internet, identifié comme étant le côté externe (*outside*). Le NAT traduit les adresses locales internes en une adresse globale unique avant d'envoyer les paquets vers le réseau externe.
- On doit changer des adresses internes. Au lieu de les changer, on les traduit par du NAT.
- On veut rendre accessible des hôtes qui sont localement et globalement dans le même adressage, autrement dit on permet une connectivité d'adresses qui se chevauchent (overlapping) de part et d'autre du routeur NAT.
- On peut utiliser également le NAT pour distribuer la charge TCP vers un hôte virtuel qui répond à la place de plusieurs serveurs réels selon un principe de type round-robin.

- Il contribue à améliorer la sécurité des réseaux internes puisqu'il les cache.

3.3.5 Limites

- Le NAT contredit le principe fondamental d'IP d'une communication de bout en bout (les stations d'extrémité établissent et gèrent elle-même leur communication). Le NAT pose donc des problèmes dans l'établissement de communications utilisant certains protocoles de sécurité assurant une authentification et une encryption, des applications peer-to-peer et autres tels que FTP (File Transfert Protocol).
- En matière de sécurité, il n'est jamais qu'une option qui ne remplace pas un filtrage IP pertinent.
- Par ailleurs, son utilisation répandue rend opaque l'étendue réelle de l'Internet.

3.3.6 Configurations

3.3.6.1 NAT statique

- Définition du NAT

(config)#ip nat inside source static local_inside_ip global_inside_ip

- Définition des interfaces Inside/Outside

(config)#interface type number
(config-if)#ip nat inside
(config)# interface type number
(config-if)#ip nat outside

3.3.6.2 NAT dynamique

- Adresses locales soumises au NAT

(config)#access-list access-list_number permit source_ip wildcard_mask

- Pool d'adresses globales

(config)#ip nat pool name start_ip end_ip

- Définition du NAT

(config)#ip nat inside source list access-list_number pool name

- Définition des interfaces Inside/Outside

(config)#interface type number
(config-if)#ip nat inside

(config)# interface type number

(config-if)#ip nat outside

3.3.6.3 NAT Overload

- Adresses locales soumises au NAT

(config)#access-list access-list_number permit source_ip wildcard_mask

- Définition du NAT

(config)#ip nat inside source list access-list_number interface type number Overload

- Définition des interfaces Inside/Outside

(config)#interface type number

(config-if)#ip nat inside

(config)# interface type number

(config-if)#ip nat outside

3.3.6.4 Diagnostic

#clear ip nat translation

#show ip nat translation [verbose]

#show ip nat statistics

#debug ip nat

3.4 Pare-feu

Un pare-feu (firewall en anglais) est une métaphore utilisée pour désigner un logiciel et/ou un matériel, qui a pour fonction de faire respecter la politique de sécurité du réseau, celle-ci définissant quels sont les types de communication autorisés ou interdits.

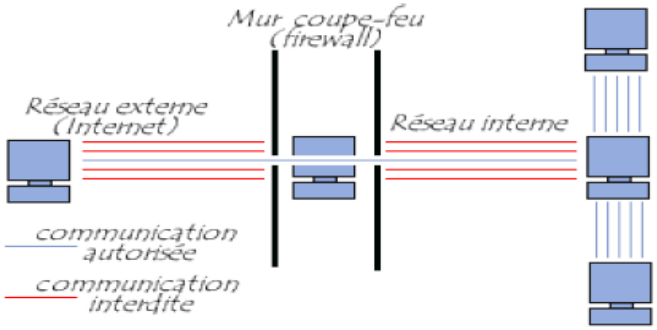


Figure 3.01 : *Représentation du système de pare-feu*

3.4.1 Principes de filtrage

Selon l'équipement, des informations sont extraites des flux réseaux depuis une ou plusieurs des couches 2 à 7 du modèle OSI, éventuellement corrélées entre elles, et comparées à un ensemble de règles de filtrage. Un état peut être mémorisé pour chaque flux identifié, ce qui permet en outre de gérer la dimension temporelle avec un filtrage en fonction de l'historique du flux. [21]
Les types de filtrage les plus courants sont :

- Liaison (adresse MAC Ethernet,...),
- Réseau (entêtes IP, IPX,... et type/code ICMP),
- Transport (ports TCP/UDP),
- Filtrage adaptatif (« stateful inspection ») ou dynamique,
- Session (« circuit level gateway », « proxys » génériques),
- Application : serveur(s) mandataire(s)/relais applicatifs (« proxys »),
- Dans la pratique une combinaison des types précédents est utilisée : un pare-feu protégeant un serveur http fera passer les requêtes clientes à travers un relais applicatif tandis que la réponse serveur ne sera analysée qu'au niveau transport pour mettre à jour l'état des sessions dynamiques.

Ce qui nous intéresse c'est ce qui concerne la couche 3 du modèle OSI.

3.4.2 ACL

Une ACL (Access Control List) permet d'autoriser ou de refuser des paquets en fonction d'un certain nombre de critères, tels que :
- L'adresse d'origine
- L'adresse de destination
- Le numéro de port.
- Les protocoles de couches supérieures
- D'autres paramètres (horaires par exemple)

Les listes de contrôle d'accès permettent à un administrateur de gérer le trafic et d'analyser des paquets particuliers.
Les ACL sont associés à une interface du routeur, et tout trafic acheminé par cette interface est vérifié afin d'y déceler certaines conditions faisant partie de la liste de contrôle d'accès.

Ils peuvent être créés pour tous les protocoles routés. Il faut donc définir une liste de contrôle d'accès dans le cas de chaque protocole activé dans une interface pour contrôler le flux de trafic acheminé par cette interface.
ACL a été inventé par Cisco, dans les autres constructeurs, ce type de filtrage prend d'autres appellations : pour Juniper c'est Policy…

3.4.2.1 Logique des ACL

Il est possible de résumer le fonctionnement des ACL de la façon suivante :

- Le paquet est vérifié par rapport au premier critère défini
- S'il vérifie le critère, l'action définie est appliquée
- Sinon le paquet est comparé successivement par rapport aux ACL suivants
- S'il ne satisfait aucun critère, l'action *deny* est appliquée

Les critères sont définit sur les informations contenues dans les en-têtes IP, TCP ou UDP
Des masques ont été définis pour pouvoir identifier une ou plusieurs adresses IP en une seule définition. Ce masque défini la portion de l'adresse IP qui doit être examinée

- 0.0.255.255 signifie que seuls les 2 premiers octets doivent être examinés
- deny 10.1.3.0 avec 0.0.0.255 : refus de toutes les IP commençant par 10.1.3

3.4.2.2 Fonctionnement des ACL

Il teste des règles les unes après les autres : si aucune règle n'est applicable, rejet du paquet.

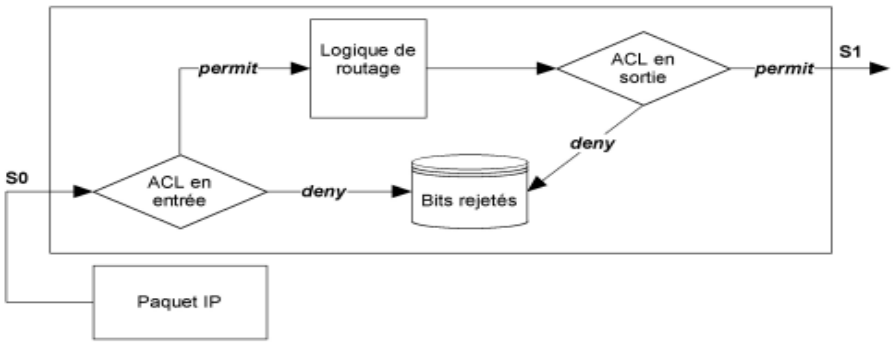


Figure 3.02 : *Organigramme du comportement des ACL dans un routeur*

3.4.2.3 Règles d'application

- Placer les listes d'accès aussi près de que possible de la source des paquets (au niveau de l'interface) s'il s'agit d'une ACL étendue. Par contre, s'il s'agit d'une ACL standard, il faut la placer au plus proche de la destination (puisque c'est ce qu'elle ne vérifie pas).
- Placer en tête de liste les règles (les instructions) qui font l'objet d'une correspondance la plus précise et les plus générales à la fin.
- Suivre ces deux recommandations tout en respectant les restrictions d'accès qui ont été identifiées.

3.4.2.4 Types

On a deux types d'ACL : étendue et standard. Leur différence c'est le mode de configuration.

3.4.2.5 Configurations

- ACL standard

Router(config)#access-list numéro-liste-accès {deny|permit} adresse-source [masque-source] [log]

Sur une interface on a :

Router(config-if)#ip access-group [number | name [in | out]]

- ACL étendue

Router(config)#access-list numéro-liste-accès {deny|permit} protocole adresse-source masque-source [opérateur port] adresse-destination masque-destination [opérateur port] [log]

Où "opérateur" peut prendre les valeurs suivantes :

- lt (less than)
- gt (greater than)
- eq (equal)
- neq (not equal)
- range (inclusive range).

Où le paramètre "port" peut prendre une valeur nominative ou numéraire : de 0 à 65535 ou, par exemple, http, telnet, ftp, …

- Liste d'accès nommée
  - Cas de liste standard :

Router(config)#ip access-list standard nom

Router(config-ext-nacl)#permit|deny

- Cas de liste étendue

Router(config)#ip access-list extended nom

Router(config-ext-nacl)#permit|deny

- Diagnostic

Router#show ip interface [type numéro]

Router#show access-lists [numéro-liste-accès|nom-liste-accès]

Router#show ip access-list [numéro-liste-accès|nom-liste-accès]

On pourra "logguer" le comportement d'une ACL en ajoutant le terme log à la fin d'une directive. Un show logging donnera le résultat.

3.4.3 DMZ

Lorsque certaines machines du réseau interne ont besoin d'être accessible de l'extérieur (comme c'est le cas par exemple pour un serveur web, un serveur de messagerie, un serveur FTP public, ...) il est souvent nécessaire de créer une nouvelle interface vers un réseau à part, accessible aussi bien du réseau interne que de l'extérieur, sans pour autant risquer de compromettre la sécurité interne. On parle ainsi de zone démilitarisé (souvent notée DMZ pour DeMilitarized Zone) pour désigner cette zone isolée hébergeant des applications mises à disposition du public. [22]
Ceci se crée en isolant les équipements du réseau (en restant connecté) et y assigné des commandes ACL pour régler ses communications avec le reste du réseau.

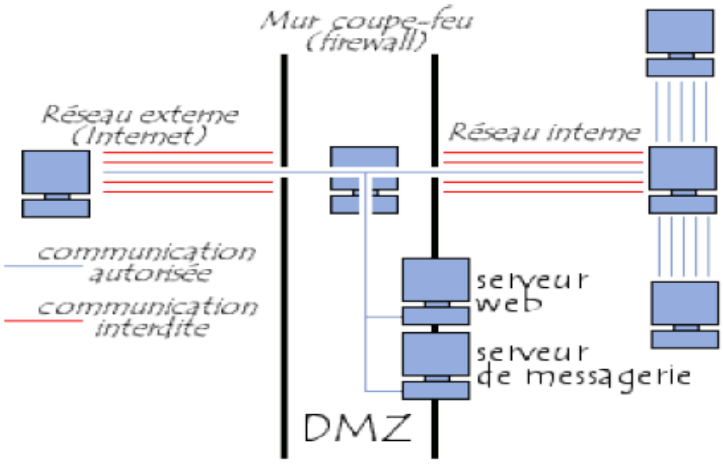


Figure 3.03 : *Zone démilitarisée*

Dans le cas de notre réseau campus, la zone démilitarisée sera situé sur un parc de serveurs qui sera protégée grâce à des pare-feu et des règles de filtrages tout prêt des serveurs internes.

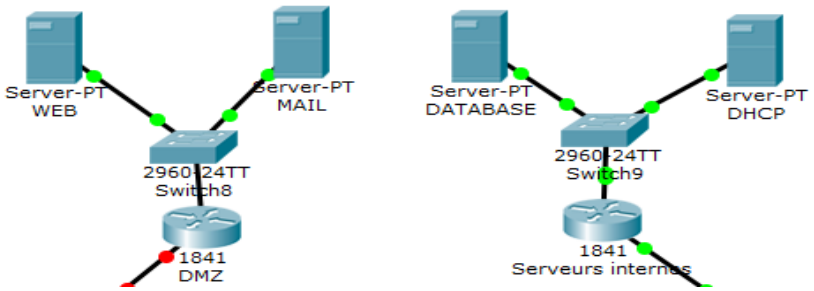


Figure 3.04 : *Piles de serveurs*

3.4.4 Serveurs internes

Ce sont ceux qui ne doivent pas être accessible qu'à l'intérieur du réseau. Ils sont la partie qui doit être le mieux protégé du réseau car ils contiennent les bases données de l'entreprise par exemple. Ils devraient être sécurisés à tous les niveaux du modèle OSI, dans notre cas, on s'en occupe des règles de filtrage et d'accès.

3.5 Sécurisation des VPN

3.5.1 Définition d'un VPN

Un VPN (Virtual Private Network) est un réseau virtuel s'appuyant sur un autre réseau (comme Internet). Il permet de faire transiter des informations, entre les différents membres de ce VPN, le tout de manière sécurisée.

On peut considérer qu'une connexion VPN revient à se connecter en réseau local mais en utilisant Internet. On peut ainsi communiquer avec les machines de ce réseau en prenant comme adresse de destination, l'adresse IP local de la machine que l'on veut atteindre. [23]

On parle alors de notion de tunnel : utiliser un protocole pour acheminer des messages d'un autre protocole. La différence entre l'encapsulation dans les tunnels et celle du modèle OSI c'est que dans le premier cas : encapsuler des messages d'un niveau donné dans des messages du même niveau ou de niveaux supérieurs alors que dans l'autre c'est l'inverse.

Voici les trois protocoles associés pour réaliser un tunnel :

- Le protocole 'porteur' utilisé ('Carrier Protocol') :

Le protocole d'un réseau existant permettant d'acheminer des informations : n'importe quel protocole robuste et répandu.

Exemples : les protocoles de l'Internet PPP/IP/TCP/HTTP mais aussi ATM (Asynchronous Transfert Mode).

- Le protocole d'encapsulation ('Tunneling Protocol'):

Le protocole qui est ajouté pour encapsuler les données usagers en les sécurisant c'est-à-dire qui réalise les objectifs VPN de sécurité.

Exemples : GRE, voir la liste sur le transparent suivant etc…

- Le protocole transporté ('Passenger Protocol'):

Le protocole utilisateur que l'on souhaite acheminer.

Exemples : un protocole Internet IP ou un protocole non Internet IPX, NETBIOS/NetBeui … dans le protocole IP.

3.5.2 Objectifs

Les motivations pour la conception d'un VPN sont :

3.5.2.1 Communications sécurisées sur une infrastructure partagée.

- Sécurité visée : mécanismes de protection

Par implantation en modifiant des protocoles de réseaux classiques.

D'où les solutions sont : adressage et routage privé offerts par des mécanismes de protection garantis par un constructeur de routeur et un fournisseur d'accès.

- Sécurité visée : mécanismes pour la confidentialité et l'intégrité

Par l'utilisation des protocoles de sécurité utilisant des techniques de cryptographie : authentification, chiffrement en confidentialité, signatures.

3.5.2.2 Economies de coûts en partageant des plates-formes de communication à haut débit.

Efficacité du partage de voies physiques à haut débit: coût des communications très réduit dans un réseau partagé (type Internet). Créé une liaison spécialisée comme Frame Relay est très cher. [24]

3.5.3 Classification des VPN

Il existe plusieurs types selon leur domaine opérationnel :

3.5.3.1 Classification selon le niveau du modèle OSI.

- VPN de niveau liaison (éventuellement même de niveau physique).

- VPN de niveau réseau.
- VPN de niveau transport.
- VPN de niveau application.

3.5.3.2 Classification selon l'approche de sécurité

- Protection: Solutions de niveau 3 en routage pair à pair ('VPN Peer to peer'), de niveau 1 ou 2 ou 3 en recouvrement (VPN 'overlay')
- Authentification, Confidentialité, Intégrité : Solutions de niveau quelconque (2, 3, 4,7) basées sur l'utilisation de tunnels ('Secure VPN Tunnelling').

Il existe de nombreux choix possibles selon des critères qualité :

- Analyse des risques couverts ou non par une implantation.
- Possibilités de passage à l'échelle de la solution.
- Complexité d'implantation puis de maintenance.

Nous allons spécialement nous intéressé au tunnel GRE ainsi qu'au VPN avec sécurisation IP ou IPsec.

3.5.4 GRE

GRE (Generic Routing Encapsulation) est d'origine Cisco, et normalisé par RFC 1701 (1994) puis modifiée RFC2784 (2000). L'objectif est de permettre d'encapsuler n'importe quel protocole sous le tunnel GRE. Ici, il n'y a pas encore de protocole de sécurité, juste une conception d'un tunnel sur un réseau public. Il travaille uniquement au niveau 3 du modèle OSI.

3.5.4.1 Paquet GRE

Voici la constitution d'un paquet GRE :

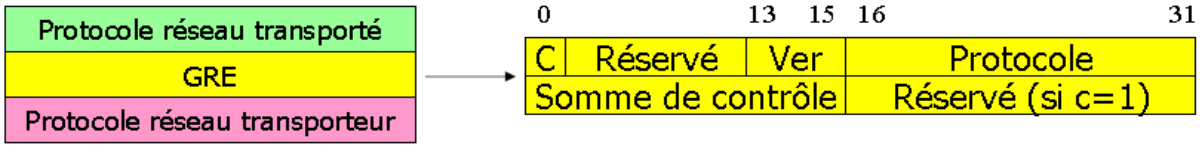


Figure 3.05 : *Paquet GRE*

Explications :

- C : Présence ou absence de la somme de contrôle (cheksum).
- Réservé : Bits réservés pour un usage futur.

- Ver : numéro de version (zéro actuellement).
- Protocole : contient un code numérique définissant le protocole transporté.
- Somme de contrôle : la même somme de contrôle que celle de IP portant sur l'entête GRE et le paquet transporté (si le bit c'est à 1).

C'est un protocole très simple compatible avec les tunnels L2TP ('Layer 2 Tunneling Protoclol') et peut être remplacé par l'obtention d'un code type protocole en IP.

3.5.4.2 Configurations

Nous avons ici un exemple de configuration de GRE :
R1(config)# int tunnel 0 // entrer dans la configuration du tunnel 0
R1(config-if)# ip address 192.168.2.1 255.255.255.0 // donner une adresse IP à ce tunnel
R1(config-if)# tunnel source g0/1//nommer l'interface source où s'applique le tunnel
R1(config-if)# tunnel destination 201.150.200.6 // adresse IP de l'interface de destination
R1(config-if)# tunnel mode gre ip // nommer le nom du protocole utiliser par le tunneling
*R1(config-if)# exit //*on sort de la configuration
Nous n'avons pas besoin d'allumer l'interface du tunnel mais il est actif au moment où il est configuré. Et les commandes sont les mêmes dans l'autre routeur (source ou destination) pour qu'il soit opérable de part et d'autre avec la même interface « tunnel 0 ».

3.5.5 VPN IPsec

3.5.5.1 Présentations

IPsec (Internet Protocol Security) est né du premier constat sur l'aspect critique de la sécurité dans internet en 1994 (RFC 1636) et des multiplications des attaques de type spoofing (usurpation d'identité) et d'écoute clandestine du contenu du trafic. Il y a aussi la nécessité de concevoir des mécanismes d'authentification et de chiffrement pour IP.
IPSec est décrit dans les RFC 2401, 2402, 2406 et 2408. Elle fournit les services suivants :

- Un protocole de d'authentification indiqué par l'en-tête d'authentification (AH (Authentication Header) : contrôle d'accès, authentification de l'origine des données, rejet de paquets rejoués.
- Un protocole combiné chiffrement authtification (ESP (Encapsulating Security Payload)) : confidentialités par chiffrement et limitée au flot du trafic.

	AH	ESP (chiffrement)	ESP (chiffrement + authentification)
Contrôle d'accès	x	x	x
Intégrité hors connexion	x		x
Authentication de l'origine des données	x		x
Rejet des paquets rejoués	x	x	x
Confidentialité		x	x
Confidentialité du flot du traffic		x	x

Tableau 3.01: *Les services d'IPsec*

3.5.5.2 Paramètres d'association de sécurité

Une connexion IPSec repose sur l'usage d'une association de sécurité (Security Association) unidirectionnelle (il en faudra donc deux par connexion, une pour chaque sens) préalablement établie entre les correspondants et qui va permettre aux deux parties de convenir des différents paramètres de la SA utilisés durant l'échange des données. Trois paramètres l'identifient :

- un index de paramètres de sécurité (SPI -Security Parameters Index).

Il s'agit d'une chaîne de 32 bits de signification locale (propre au système qui gère l'association), véhiculée en clair dans les en-têtes AH et ESP. Une SPI de valeur 0 est un cas particulier pour dire qu'aucune SA n'a été encore créée,

- l'adresse de destination, il peut s'agir d'un système d'extrémité ou d'un système intermédiaire (routeur, firewall ou poste de travail),
- l'identifiant de protocole de sécurité (SPId -Security Protocol Identifier-) qui indique la nature de la SA (AH ou ESP).

Plusieurs AS peuvent être combinés : les associations entre AS et type de trafic se font par le biais d'une base de données de politique de sécurité. [25]

3.5.5.3 Modes d'utilisation

IPsec peut être utilisée dans deux conditions de VPN :

- Mode transport :

Elle assure la protection pour les protocoles de la couche transport (information utile d'un paquet IP). ESP chiffre (et optionnellement authentifie) uniquement l'information utile du paquet IP (l'en-tête reste inchangé).AH authentifie l'information utile IP et des parties de l'en-tête IP.

- Mode tunnel.

Elle assure la protection du paquet IP tout entier. Après l'ajout des champs AH ou ESP le paquet entier est traité comme l'information utile du paquet IP externe. Une (ou les deux) extrémité de l'AS doit être une passerelle de sécurité (firewall, passerelle implémentant IPSec,...).

	Mode Transport	Mode Tunnel
AH	Authentifie l'information utile IP + certains champs de l'en-tête IP	Authentifie le paquet IP entier + certains champs de l'en-tête externe
ESP	Chiffre l'information utilse IP	Chiffre tout le paquet IP
ESP (avec authentification)	Chiffre l'information utile IP et authentifie l'information utile IP	Chiffre et authentifie le paquet tout entier

Tableau 3.02: *Fonctionnalités des modes tunnels et transport*

3.5.5.4 Authentification Header

L'en-tête d'authentification assure :

- l'intégrité des données
- l'authentification des paquets IP
- l'authentification est basée sur l'utilisation d'un code d'authentification de message (MAC, Message Authentication Code).

AH permet entre autre de détecter le rejeu et doit supporter HMAC-MD5-96 et HMAC-SHA-1-96.

Plusieurs algorithmes d'authentification de messages existent :

- Authentification à l'aide d'une clé secrète (MAC) : authentification du message basée sur une clé secrète partagée par l'émetteur et le récepteur. Ce mécanisme est coûteux pour des messages de petite taille.
- Fonctions de hachage : dont la fonction est de construire un résumé du message et l'envoyer.
- Fonctions de hachage sécurisées (SHA-1, MD5,…) : ce sont des fonctions vérifiant des propriétés de robustesse (telles que l'impossibilité de deviner le contenu d'un message à partir de son résumé).

La solution retenue est l'authentification à l'aide de HMAC : il s'agit de combiner MAC et des fonctions de hachage sécurisées (SHA-1).

Les avantages sont : la rapidité du mécanisme d'authentification, plusieurs algorithmes de hachages cryptographiques disponibles.

- Service anti rejeu :

Une attaque est dite par rejeu quand un attaquant obtient une copie d'un message valide et la transmet ultérieurement à la destination.
Lorsqu'une nouvelle AS est établi, l'émetteur initialise un numéro d'ordre à zéro. Chaque fois qu'un paquet est envoyé à cette AS, l'expéditeur incrémente la valeur et la place dans le champ numéro d'ordre de l'en-tête AH. Le destinataire ne doit pas permettre au numéro d'ordre d'effectuer un cycle de 232-1 à 0 (pour éviter d'avoir plus d'un paquet valide avec le même numéro d'ordre).
Au niveau du récepteur : AH Crée une fenêtre de réception des paquets IP (Les paquets peuvent arriver dans le désordre) de taille W. Le numéro d'ordre le plus élevé jusqu'ici (N) est noté à l'extrémité droite de la fenêtre. Pour n'importe quel paquet correctement reçu ayant un numéro d'ordre compris entre N-W+1 et N, la position correspondante est marquée.
À la réception d'un nouveau paquet :
1. Si le paquet est nouveau et si le code MAC est valide, la position correspondante est marquée.
2. Si le paquet reçu est à droite de la fenêtre et s'il est correctement authentifié, la fenêtre est avancée de sorte que le numéro d'ordre devienne la nouvelle valeur de N.
3. Si le paquet n'est pas correctement authentifié ou s'il a un numéro d'ordre à gauche de la fenêtre, il est détruit.

3.5.5.5 Encapsulating Security Payload

ESP fournit : des services de confidentialités, un mécanisme anti-rejeu., un mécanisme d'authentification. ESP supporte différents algorithmes de cryptage : DES, 3DES, CAST,…

3.5.5.6 Gestion des clés

La gestion des clés implique la détermination de la distribution des clés secrètes. Une transmission classique nécessite quatre clés : deux paires de transmissions et de réceptions pour AH et ESP. IPSec supporte deux types de gestions :

- Manuelle : un administrateur configure manuellement chaque système avec ses propres clés.

- Automatique : un système automatisé permet une création à la demande de clés pour les AS. Le protocole de gestion de clés automatisé pour IPSec est ISAKMP/Oakley.

ISAKMP est un protocole fournissant un cadre pour la gestion des clés, et des formats pour la négociation des attributs de sécurité.

3.5.5.7 Configurations

Il faut tout d'abord vérifier que l'IOS du routeur implémente VPN et sa sécurisation. Dans notre cas, on a le mode transport c'est-à-dire on va sécuriser une connexion existante sans créé de tunnel.

- Activation des fonctions crypto du routeur :

R1(config)#crypto isakmp enable

Configuration de la « politique de sécurité » ou « policy » qui détermine quelle encryptions on utilise, quelle Hash quelle type d'authentification, etc.

R1(config)#crypto isakmp policy 10
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#encryption 3des
R1(config-isakmp)#hash md5
R1(config-isakmp)#group 5
R1(config-isakmp)#lifetime 3600
R1(config-isakmp)#exit

  - group 5 : Spécifie l'identifiant Diffie-Hellman
  - lifetime : Spécifie le temps de validité de la connexion avant une nouvelle négociation des clefs.

- Configuration de la clef :

R1(config)#crypto isakmp key mot_de_passe address 10.2.2.1

- Configuration les options de transformations des données :

R1(config)#crypto ipsec transform-set 50 esp-3des esp-md5-hmac

Dans notre cas : encryption : 3des, hash : md5 qui doit être le même dans chaque routeur.

- Création d'une ACL qui va déterminer le trafic autorisé :

R1(config)#access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255

Dans cette dernière étape nous configurons la crypto map qui va associé l'access-list, le traffic, et la destination :

R1(config)#crypto map nom_de_map 10 ipsec-isakmp
R1(config-crypto-map)#set peer 10.2.2.1

R1(config-crypto-map)#set transform-set 50
R1(config-crypto-map)#set security-association lifetime seconds 900
R1(config-crypto-map)#match address 101
R1(config-crypto-map)#exit

- Application de la crypto map sur l'interface de sortie :

Dans notre cas FastEthernet 0/0 :

R1(config)#interface FastEthernet 0/0
R1(config-if)#crypto map nom_de_map
*Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
Un message indique que la crypto map fonctionne.

On reprend ces commandes sur l'autre routeur de destination pour établir une connexion sécurisée.

3.6 Explication des choix

Dans notre cas, voici notre politique de sécurité :

- On a utilisé NAT dynamique mélangé avec Overload afin de pallier le manque d'adresses publiques pour une future extension du réseau. Deux adresses locales auront accès à Internet : 10.0.5.0 du réseau interne et celle de la DMZ 172.16.3.0. Ceci permet aussi de protéger le réseau des attaques extérieures.
- Deux pare-feu pour filtrage des adresses IP au niveau des deux piles de serveurs :
  - Serveur interne : qui ne doit être accessible que de l'intérieur du réseau car il contient toutes les bases de données de l'entreprise.
  - DMZ : qui ne doit pas être accessible que de l'extérieur. Il contient les serveurs mail, DNS qui sont nécessaires pour l'attribution de la connexion internet.
- Un système de VPN mode transport sécurisé par IPsec pour la connexion à travers Internet pour les échanges avec un réseau externe. Pour avoir une connexion moins coûteuse que les lignes louées et plus sécuriser en tant que VPN.

3.7 Conclusion

Aucun réseau n'est à l'abri du danger. Une politique de sécurité bien établie au sein du réseau assure sa fiabilité et sa survie. Il faut quand même tenir compte des existants : chiffre d'affaire, expositions aux risques afin de ne pas gaspiller les ressources et faire un compromis. Il n'existe pas de modèle parfait pour une bonne sécurisation, tout dépend de plusieurs paramètres, ainsi, la politique de sécurité diffère selon les demandes et les réseaux à concevoir.

CHAPITRE 4

Conception d'interconnexions sécurisés et à haute disponibilité

4.1 Introduction

L'objectif est de mettre en évidence les différents protocoles cités ci-dessus dans un réseau campus. La simulation sous Packet Tracer sera divisé en fonction des éléments à présenter et la réalisation consistera à montrer la conception d'un VPN mode tunnel et son fonctionnement. On a trois grandes lignes : les hautes disponibilités, la sécurité et enfin le tunneling.

4.2 Outils utilisés

4.2.1 Logiciel Packet Tracer 6.2

Packet Tracer est un logiciel de CISCO permettant de construire un réseau physique virtuel et de simuler le comportement des protocoles réseaux sur ce réseau. L'utilisateur construit son réseau à l'aide d'équipements tels que les routeurs, les commutateurs ou des ordinateurs. Ces équipements doivent ensuite être reliés via des connexions (câbles divers, fibre optique). Une fois l'ensemble des équipements reliés, il est possible pour chacun d'entre eux, de configurer les adresses IP, les services disponibles.

4.2.1.1 Description générale

La figure 1 montre un aperçu général de Packet Tracer. La zone (1) est la partie dans laquelle le réseau est construit. Les équipements sont regroupés en catégories accessibles dans la zone (2). Une fois la catégorie sélectionnée, le type d'équipement peut être sélectionné dans la zone (3). La zone (6) contient un ensemble d'outils :

– Select : pour déplacer ou éditer des équipements

– Move Layout : permet de déplacer le plan de travail

– Place Note : place des notes sur le réseau

– Delete : supprime un équipement ou une note

– Inspect : permet d'ouvrir une fenêtre d'inspection sur un équipement (table ARP, routage). La zone (5) permet d'ajouter des indications dans le réseau. Enfin, la zone (4) permet de passer du mode temps réel au mode simulation.

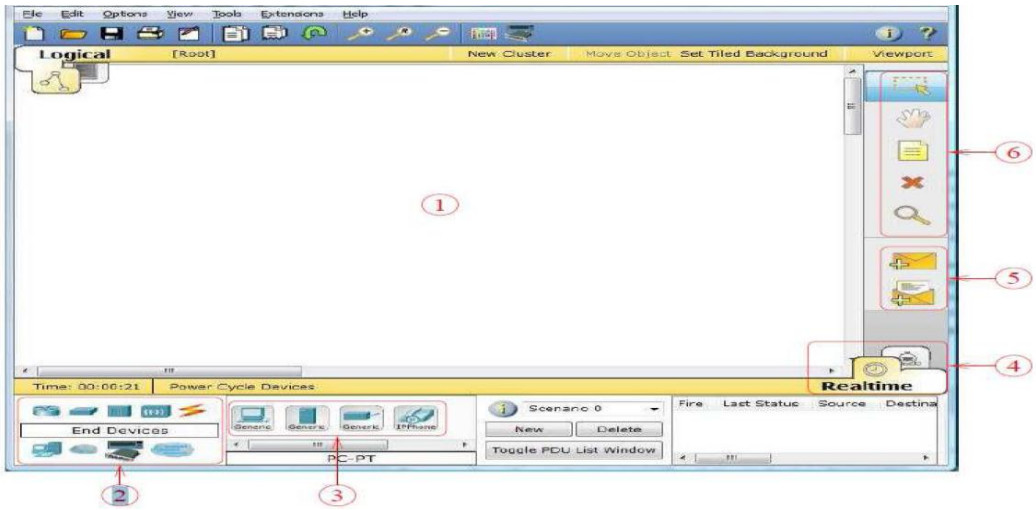


Figure 4.01 : *Espace de travail*

4.2.1.2 Construction un réseau

Pour construire un réseau, l'utilisateur doit choisir parmi les 8 catégories proposées par Packet Tracer : les routeurs, les switchs, les hubs, les équipements sans-fil, les connexions, les équipements dits terminaux (ordinateurs, serveurs), des équipements personnalisés et enfin, une connexion multi utilisateurs. Lorsqu'une catégorie est sélectionnée, l'utilisateur a alors le choix entre plusieurs équipements différents. Pour ajouter un équipement, il suffit de cliquer dessus puis de cliquer à l'endroit choisi. La figure 2 correspond à la zone décrite.

Figure 4.02 : *Barre d'outils*

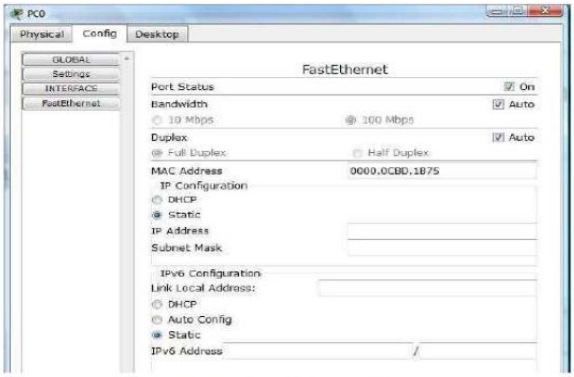
Pour relier deux équipements, il faut choisir la catégorie "Connections" puis cliquer sur la connexion désirée.

4.2.1.3 Configuration d'un équipement

Lorsqu'un ordinateur a été ajouté (appelé PC-PT dans Packet Tracer), il est possible de le configurer en cliquant dessus, une fois ajouté dans le réseau.
Une nouvelle fenêtre s'ouvre comportant trois onglets : Physical (aperçu réel de la machine et de ses modules), Config (configuration passerelle, DNS et adresse IP) et Desktop (ligne de commande ou navigateur Web).

Dans l'onglet Config, il est possible de configurer la passerelle par défaut, ainsi que l'adresse du serveur DNS (cliquez pour cela sur le bouton Settings en-dessous du bouton Global). Il est possible aussi de configurer l'adresse IP et le masque de sous-réseau (cliquez pour cela sur le bouton FastEthernet endessous du bouton INTERFACE).

Configuration passerelle et DNS

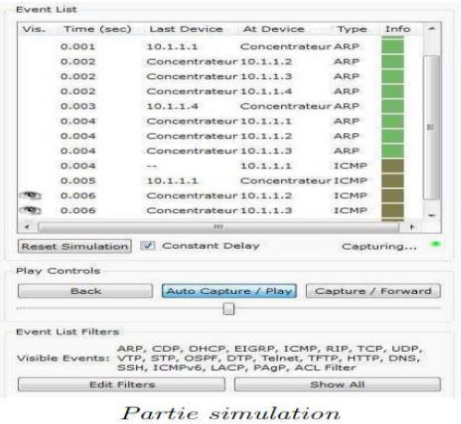


Configuration IP

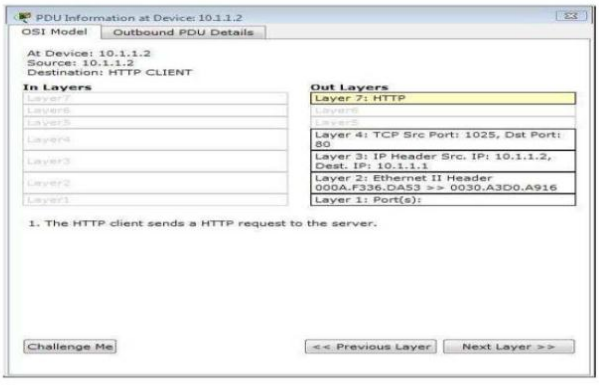
Figure 4.03 : *Interface graphique de configuration d'un PC*

4.2.1.4 Mode simulation

Une fois le réseau créé et prêt à fonctionner, il est possible de passer en mode simulation, ce qui permet de visualiser tous les messages échangés dans le réseau. En mode simulation, la fenêtre principale est scindée en deux, la partie de droite permettant de gérer le mode simulation : exécution pas-à-pas, vitesse de simulation, protocoles visibles. La partie gauche de lac figure 4 montre la partie simulation et sa partie droite montre les détails obtenus en cliquant sur un message (ici http : Hyper Text Transfert Protcocol).



Partie simulation



Détails sur un paquet

Figure 4.04 : *Etude d'un PDU mode simulation*

4.2.1.5 Invite de commandes

Il est possible d'ouvrir une invite de commandes sur chaque ordinateur du réseau. Elle est accessible depuis le troisième onglet, appelé Desktop, accessible lorsque l'on clique sur un ordinateur pour le configurer (mode sélection). Cet onglet contient un ensemble d'outils dont l'invite de commandes (Command prompt) et un navigateur Internet (Web Browser).
L'invite de commandes permet d'exécuter un ensemble de commandes relatives au réseau. La liste est accessible en tapant help. En particulier, les commandes ping, arp, tracert et ipconfig sont accessibles. Si Packet Tracer est en mode simulation, les messages échangés suite à un appel à la commande ping peuvent ainsi être visualisés.

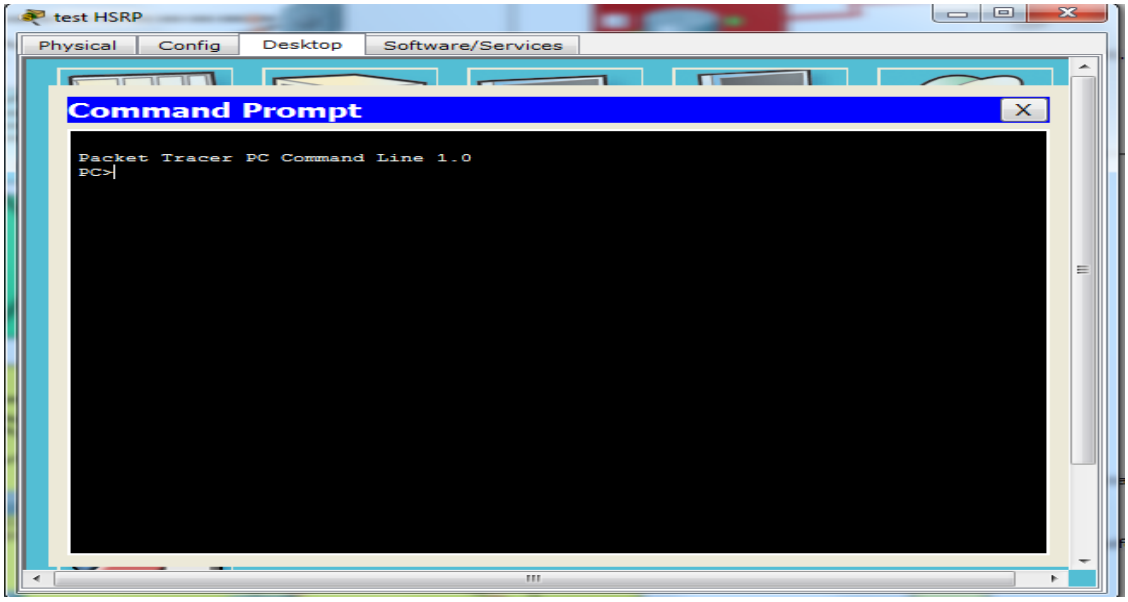


Figure 4.05 : *Invite de commande*

4.2.1.6 Cisco Packet Tracer 6.2

Cisco® a officiellement annoncé pour la communauté NetAcad le lancement de la nouvelle version de Cisco Packet Tracer Simulator 6.2 (6.2.0.0052), disponible en téléchargement sur le dépôt officiel de l'Académie Cisco Netspace. Dans la nouvelle version ont été corrigés plusieurs bugs et ajoute un support amélioré / pour certaines fonctionnalités pour mettre en évidence:

- Cisco Router 819
- Tour Mobile, Bureau Central Server, Sniffer
- JavaScript et CSS dans le support du serveur HTTP
- Importation FTP Server

- Gérer serveur FTP est Fichiers Able Serveur HTTP
- Autres améliorations en mode physique et soutien IOS

4.2.2 Wireshark

Wireshark est un analyseur de paquets libre utilisé dans le dépannage et l'analyse de réseaux informatiques, le développement de protocoles, l'éducation et la rétro-ingénierie. Son appellation d'origine (Ethereal) est modifiée en mai 2006 pour des questions relatives au droit des marques. Wireshark utilise la bibliothèque logicielle GTK+ pour l'implémentation de son interface utilisateur et pcap pour la capture des paquets ; il fonctionne sur de nombreux environnements compatibles UNIX comme GNU/Linux, FreeBSD, NetBSD, OpenBSD ou Mac OSX, mais également sur Microsoft Windows. Aujourd'hui, Wireshark reconnaît 1 515 protocoles.
Il sert à capturer les paquets transitant dans un réseau où se connecte la machine tout en explicitant automatiquement les adresses, les protocoles des échanges en temps réel.

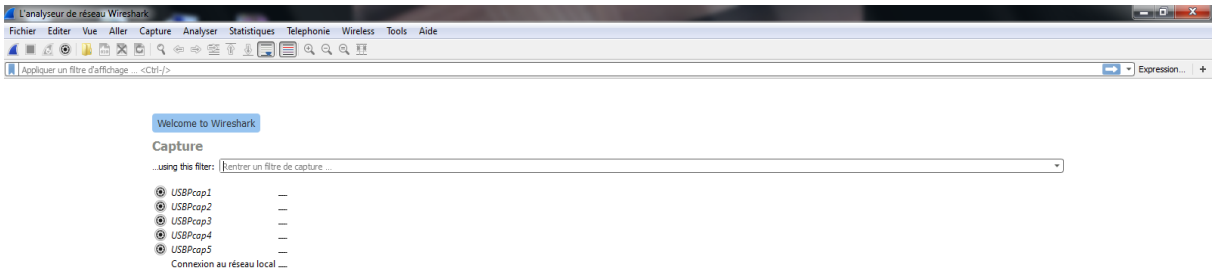


Figure 4.06 : *Environnement de Wireshark*

Il sera utilisé pour étudier les flux pour la réalisation.

4.2.3 Lecteur multimédia VLC

C’est un lecteur, encodeur et un diffuseur multimédia gratuit et libre fait par des volontaires de la communauté VidéoLAN.
VLC utilise ses propres codecs, fonctionne sur les plateformes les plus répandues, et peut lire quasiment tous les fichiers CD, DVD, flux réseau, cartes de capture et autres formats de médias.

4.2.4 Routeur 1800 series

Les routeurs à intégration de service de la gamme Cisco 1800 ont évolué à partir des routeurs d’accès modulaires mainte fois récompensés de la gamme Cisco 1700. Le routeur Cisco 1841 se caractérise par une importante valeur ajoutée par rapport aux générations précédentes de routeurs de la gamme Cisco 1700. Les principales caractéristiques différenciatrices sont : la multiplication

par cinq des performances sécurité ainsi qu'une augmentation considérable en terme de capacités et de densité d'emplacements d'interfaces.

Le routeur Cisco 1841 supporte plus de 30 cartes interfaces parmi les cartes interfaces déjà existantes pour les routeurs Cisco 1700. Cartes WIC (WAN Interface Card) et cartes multiflex (cartes Voix/WIC [VWIC] – pour les données seulement pour le routeur Cisco 1841. Le support des cartes WIC densité élevée (HWIC) est en option.

De plus, le routeur Cisco 1841 dispose en option d'un système de prévention des intrusions (IPS), de fonctions de pare-feu à inspection d'états, d'un renforcement des performances des réseaux privés virtuels (VPN) grâce à des fonctions de cryptage matériel embarquées, il dispose de nouvelles interfaces haute densité offrant au final un large choix d'options de connectivité Lan / Wan qui associé à une haute densité d'emplacements comme des interfaces commutateurs LAN multiports intégrés.

Garantissant une évolutivité maximum de la plateforme pour répondre aux besoins d'extension future du réseau.

4.2.5 Routeur 1900 series

1900 series offre une connectivité continue hautes performances avec services Intégrés permettant le déploiement dans les environnements WAN haut débit grâce à ses ports Gigabits Ethernet permettant de supporter des débits jusqu'à 10 gig/s selon le câble.

- Conception modulaire pour une souplesse de la maintenance optimale
- Modules EtherSwitch offrant des fonctionnalités de commutation intégrée
- Services Ready Engine (SRE) innovant (modèle 1941 uniquement)
- Sans point d'accès de fil 802.11n haut débit intégré (en option) pour une mobilité en toute sécurité
- Sécurité de pointe avec pare-feu, système de prévention des intrusions et du contenu ; filtrage pour une protection de meilleure contre les menaces et les attaques malveillantes
- Prise en charges VPN Assurant des collaborations de communications par GETVPN (Groupe Encrypted Transport VPN), DMVPN (Dynamic Multipoint VPN) ou Enhanced Easy VPN
- Redondance améliorée, diagnostics avec et alimentations de secours, la tolérance aux améliorant pannes et la disponibilité
- Simplicité opérationnelle

4.3 Simulation des protocoles de haute disponibilité et de sécurité dans un réseau campus

4.3.1 Présentation

On part des protocoles du bas vers le haut du réseau, commençant par la haute disponibilité jusqu'à la sécurité. On a créé un modèle de réseau campus et isoler les différentes zones pour mieux expliciter les fonctions de ces protocoles.

4.3.2 Déroulement

Voici l'architecture générale du réseau :

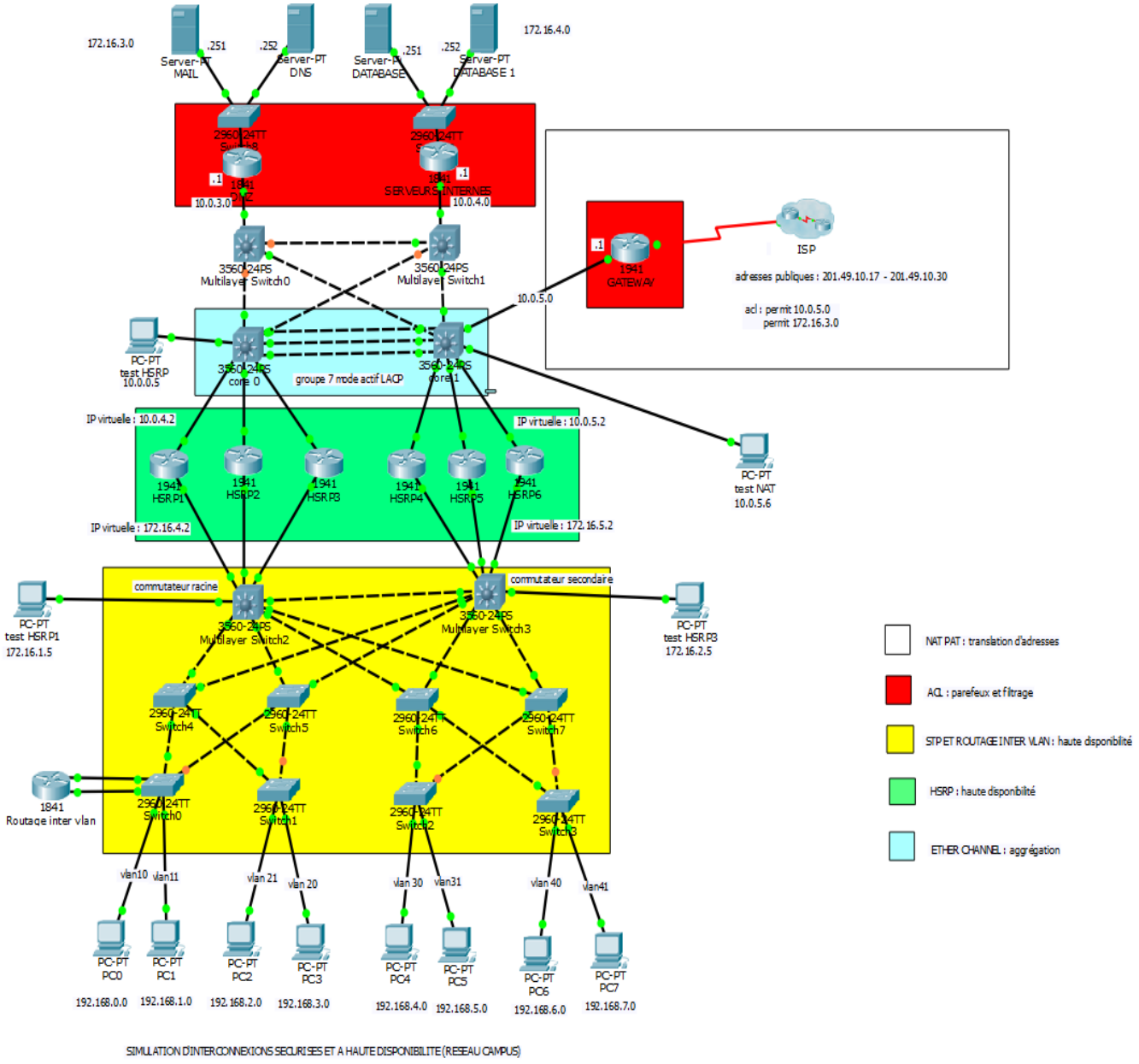


Figure 4.07 : *Topologie générale du réseau*

La simulation du VPN sera mise à part car il devrait se mélanger à la partie du NAT PAT, pour mieux voir ses fonctions de connexions avec le réseau externe.

4.3.2.1 Hautes disponibilités

Il s'agit de mettre en valeur les fonctionnalités de STP, HSRP et Etherchannel.

- STP

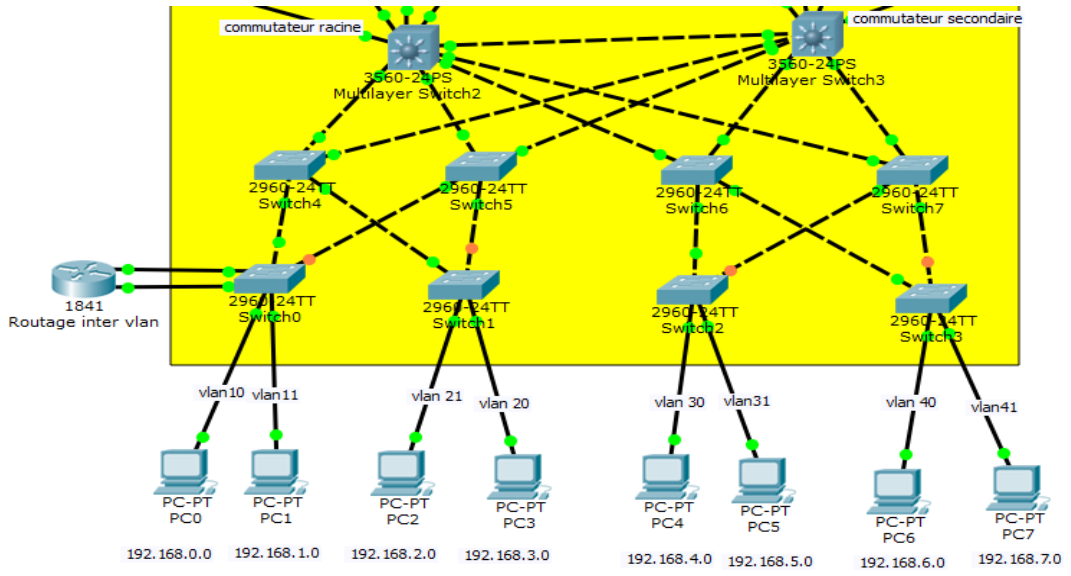


Figure 4.08 : *Partie STP*

La segmentation en vlan 10, vlan 11, vlan 20, vlan 21, vlan 30, vlan 31, vlan 40, vlan 41 permet une facilité dans la gestion du réseau et pour un routage inter vlan.
Les liaisons vers les terminaux (PC) seront mises en mode access et les liaisons entre commutateurs et routeurs seront en mode trunk c'est-à-dire découpées en liens logiques permettant de faire communiquer les VLAN.
La topologie utilisée est en étoile à maillage partiel pour créer les redondances et éviter les gaspillages à la fois. Elle permet aussi de faire gagner du temps de convergence en cas de coupure car si c'est en maillage globale ou totale, STP mettra beaucoup de temps pour rétablir les connexions.
Le Multilayer Switch2 est élu comme commutateur racine, c'est lui qui se chargera de gérer les redondances et les pannes. Le Multilayer Switch3 est le commutateur secondaire et remplacera la racine en cas de défaillance de ce dernier.
Le routeur offre un routage entre VLAN et leur connexion avec le reste du réseau.

Après avoir configuré les différents équipements, nous avons les états de la figure … STP va gérer les redondances en choisissant le meilleur chemin entre les VLAN. Dans ce cas, il va élire des ports à mettre en veille de couleur orange (figure). Un seul parcours sera destiné à relier deux VLAN.

Testons maintenant l'efficacité de STP en sectionnant un lien actif auprès de ceux en veille.

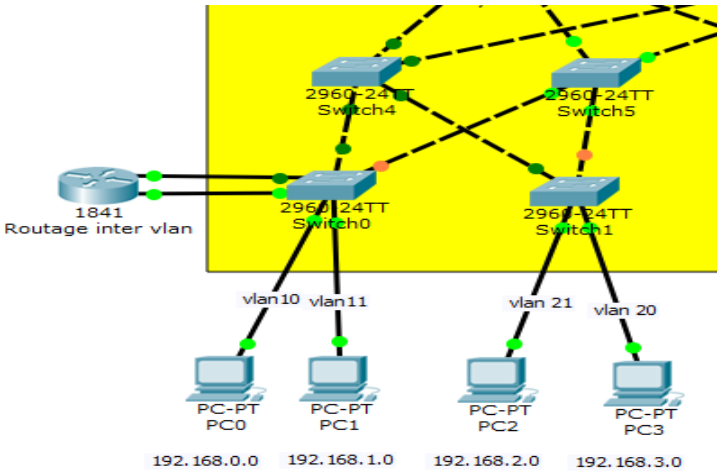


Figure 4.09 : *Avant section*

On envoi un ping de VLAN 10 vers VLAN 20 pour tester la connectivité. On a un succès :

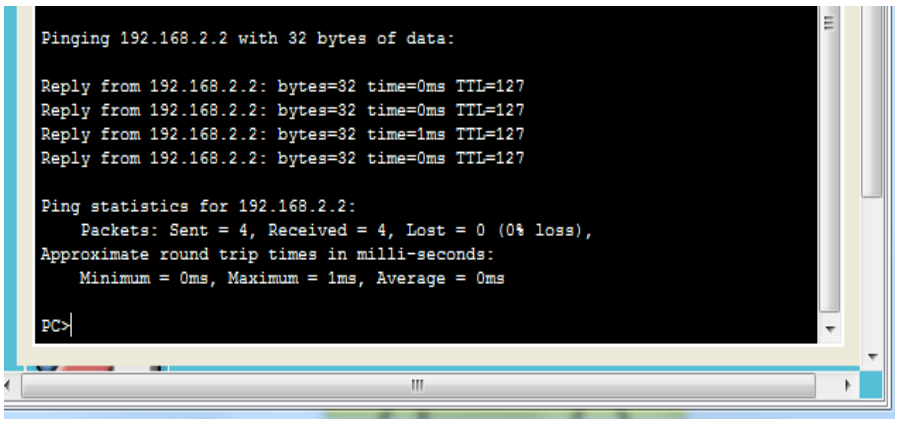


Figure 4.10 : *Envoi requête ping vers VLAN 21*

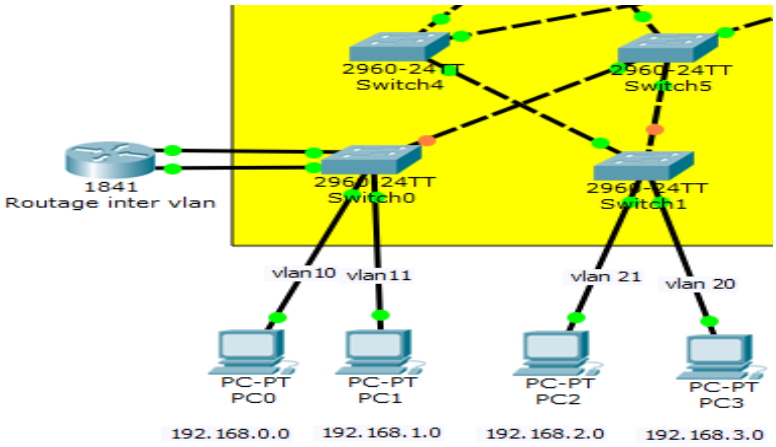


Figure 4.11 : *Après section*

Après ping, dans ce cas, les données n'arrivent pas à destination :

```
PC>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Figure 4.12 : *Echec d'envoi vers VLAN 21*

Quelques secondes après, l'autre lien s'active pour rétablir les échanges.

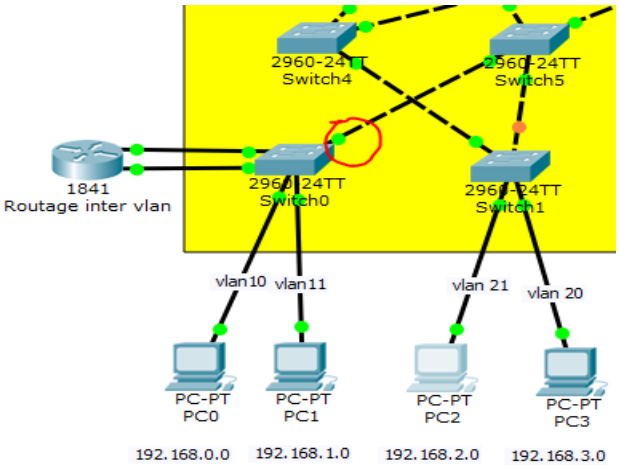


Figure 4.13 : *Démarrage d'un autre lien*

On refait le test de connectivité et on obtient de nouveau un succès :

```
PC>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Reply from 192.168.2.2: bytes=32 time=15ms TTL=127
Reply from 192.168.2.2: bytes=32 time=1ms TTL=127
Reply from 192.168.2.2: bytes=32 time=0ms TTL=127
Reply from 192.168.2.2: bytes=32 time=0ms TTL=127

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 15ms, Average = 4ms

PC>
```

Figure 4.14 : *Succès d'un envoi*

Ce test peut être effectué dans n'importe quel commutateur du réseau.

Comme on a vu dans le chapitre 2, STP a permis ici de gérer les redondances démontré par les tests de connectivités. Et en cas de panne de liens, il a permis au réseau de s'adapter en créant une nouvelle connexion entre les deux VLAN.

- HSRP

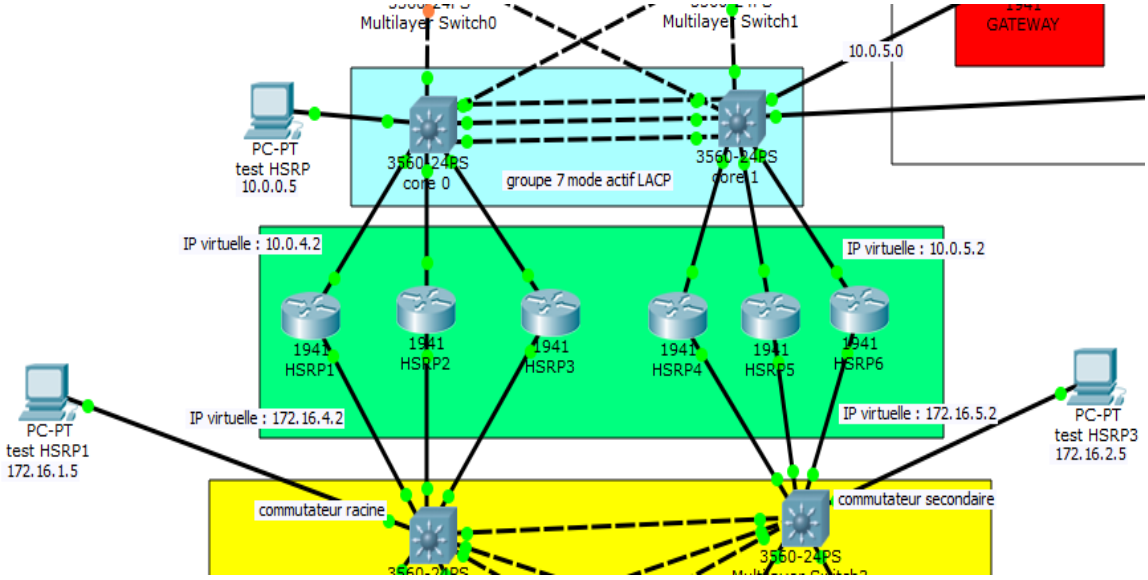


Figure 4.15 : *Architecture de la partie HSRP*

C'est dans les routeurs (la partie verte de la figure) qu'est contenue HRSP. Sa finalité est similaire à STP car elle permet aussi de gérer les redondances ainsi que les pannes mais au niveau routeur.

L'attribution des adresses IP virtuelles se fera de deux sens différents :

- Du commutateur racine (et secondaire) vers core 0 (et core 1) : 172.16.4.2 pour un groupe de HSRP et 172.16.5.2 pour l'autre groupe.

- De core 0 (et core 1) vers commutateur racine (et secondaire) : 10.0.4.2 pour l'un, et 10.0.5.2 pour l'autre.

Les routeurs HSRP1, HSRP2, HSRP3 font partie du groupe 10 du protocole HSRP tandis que HSRP4, HSRP5, HSRP6 appartiennent au groupe 11.

Les passerelles des PC nécessaires au test sont les adresses virtuelles des groupes et des interfaces auxquelles ils appartiennent.

Par exemple pour le PC « test HSRP » :

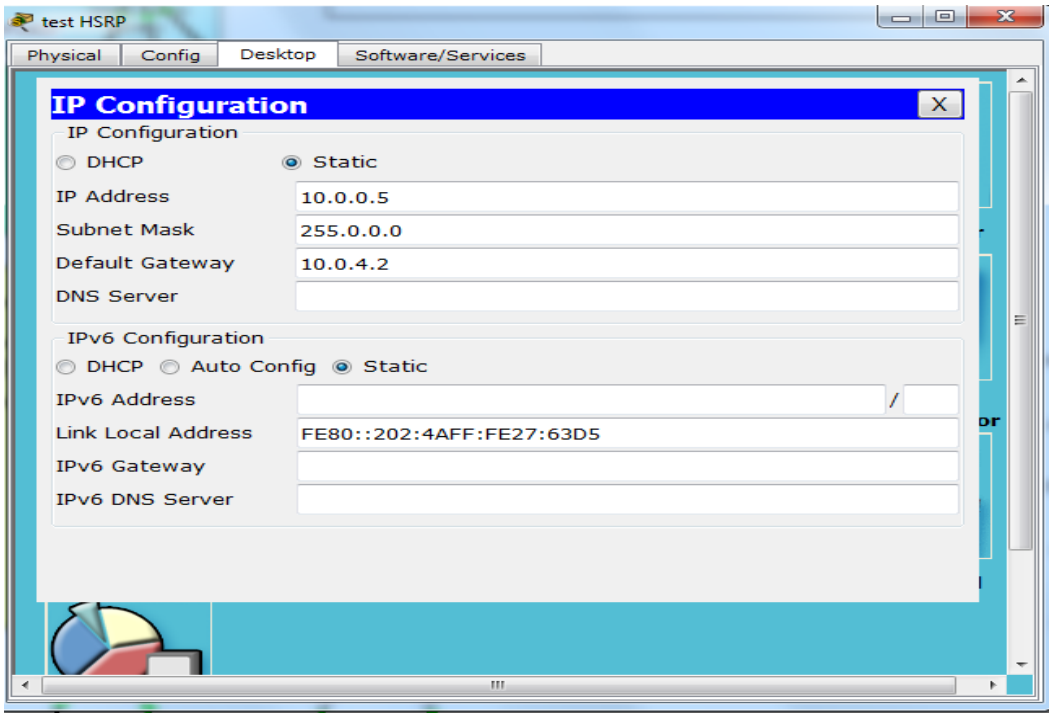


Figure 4.16 : *Configurations de PC-test HSRP*

La numérotation des priorités sont les suivantes :

- Pour le groupe 10 HSRP (routeurs HSRP1 HSRP2, HSRP3) :
  - Interface gig 0/1 : 10 pour HSRP1, 11 pour HSRP2, 12 pour HSRP3
  - Interface gig0/0 : 13 pour HSRP1, 14 pourHSRP2, 15 pour HSRP3
- Pour le groupe 11 HSRP (routeurs HSRP4 HSRP5, HSRP6) :
  - Interface gig 0/1 : 17 pour HSRP4, 18 pour HSRP5, 19 pour HSRP6
  - Interface gig0/0 : 20 pour HSRP4, 21 pourHSRP5, 22 pour HSRP6

D'où les interfaces des routeurs HSRP3 et HSRP6 sont en mode actif et les autres en veille (standby).

Afin de tester HSRP, nous allons couper un lien de HSRP3 permettant au PC test HSRP de communiquer avec PC test HSRP1. Un autre routeur ayant une priorité inférieure doit pouvoir prendre le relai et devenir le routeur actif, qui est dans notre cas HSRP2.

On va tout d'abord faire un test de connectivité pour voir si tout fonctionne en envoyant un ping de PC test HSRP vers l'autre:

```
PC>ping 172.16.1.5

Pinging 172.16.1.5 with 32 bytes of data:

Reply from 172.16.1.5: bytes=32 time=0ms TTL=127
Reply from 172.16.1.5: bytes=32 time=26ms TTL=127
Reply from 172.16.1.5: bytes=32 time=0ms TTL=127
Reply from 172.16.1.5: bytes=32 time=34ms TTL=127

Ping statistics for 172.16.1.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 34ms, Average = 15ms
```

Figure 4.17 : *Résultat du ping de test HSRP1*

Puis voir si les données transitent vraiment par le routeur HSRP3, grâce à la commande tracert :

```
Tracing route to 172.16.1.5 over a maximum of 30 hops:

  1    1 ms      0 ms      0 ms      10.0.0.4
  2    0 ms      0 ms      1 ms      172.16.1.5

Trace complete.
```

Figure 4.18 : *Traceroute vers test HSRP1*

L'adresse 10.0.0.4 est celle de l'interface gigabitethernet0/0 du routeur HSRP3 donc notre test a réussi.

Maintenant, on coupe la liaison en dessus du port gigabitethernet0/0 du routeur HSRP3 :

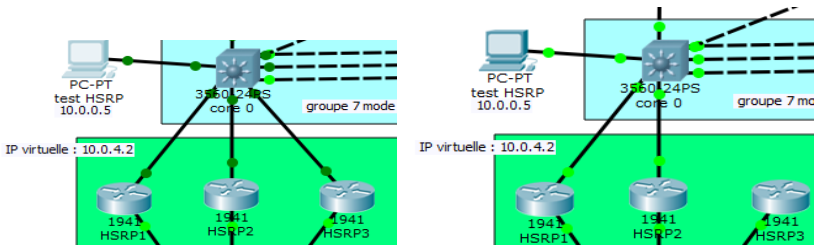


Figure 4.19 : *Etats avant et après section*

On teste la connectivité comme précédemment de test HSRP vers test HSRP1 :

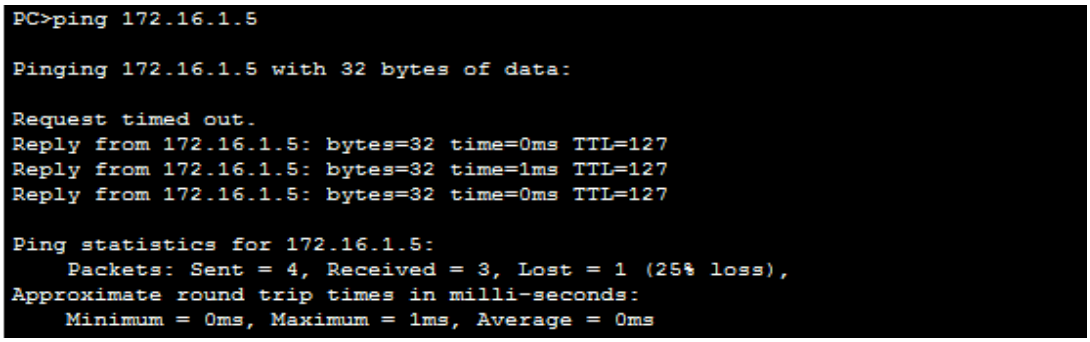


Figure 4.20 : *Nouveau résultat du ping*

Cette perte de donnée de 25% est due à la durée de convergence du routeur c'est-à-dire le temps pour que le routeur HSRP2 s'active et prend le relai. Mais si on refait le ping on a :

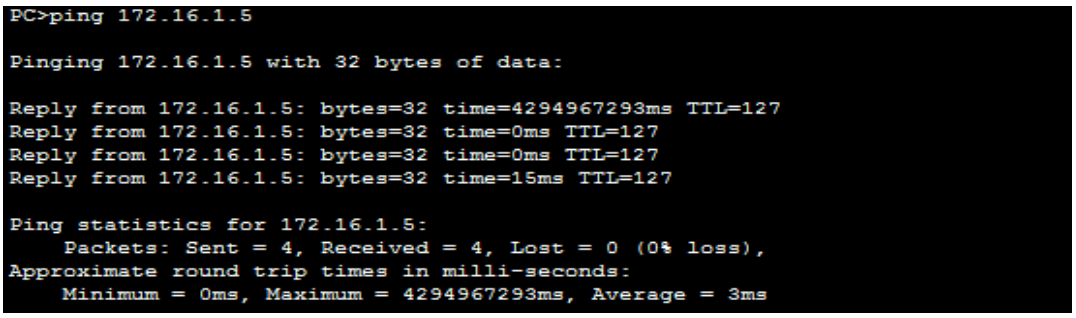


Figure 4.21 : *Succès total du ping*

Il n'y a plus de perte de données.

Maintenant nous allons voir lequel des deux routeurs HSRP1 et HSRP2 a pris le relai par la commande tracert vers la destination :

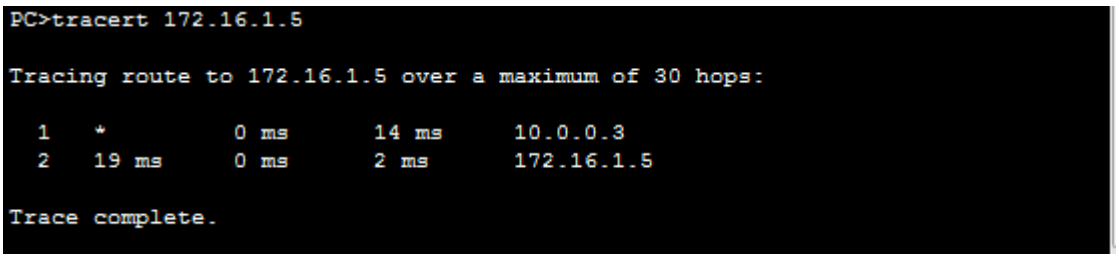


Figure 4.22 : *Traceroute vers test HSRP1*

L'adresse IP 10.0.0.3 est celle de l'interface gigabitethernet0/0 du routeur HSPR2. D' où on peut dire que HSRP2 a pris le relai dans la transmission des données de PC-test HSRP vers PC-test HSRP1.

Ce test est identique dans l'autre sens ou dans le groupe 11 HSRP.

On peut encore sectionner le lien du routeur HSRP2 et HRSP1 prendra le relai.

- Etherchannel

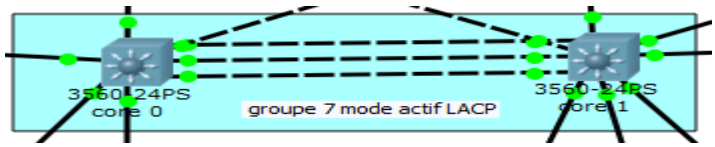


Figure 4.23 : *Commutateurs reliés par des liens agrégés*

Les commutateurs core0 et core1 sont configurés identiquement : protocole d'échange LACP et groupe 7. S'ils ne sont pas dans le même groupe ils ne peuvent pas communiquer.
Les liens agrégés doivent pouvoir transmettre les données comme un seul lien entre ces commutateurs. En cas de coupure, d'un ou de deux liaisons, les échanges doivent encore rester intacts.
On entre donc en mode simulation pour voir comment se passe ces échanges entre deux PC aux extrémités des commutateurs : de test HSRP vers test NAT. Tout d'abord sans coupure :

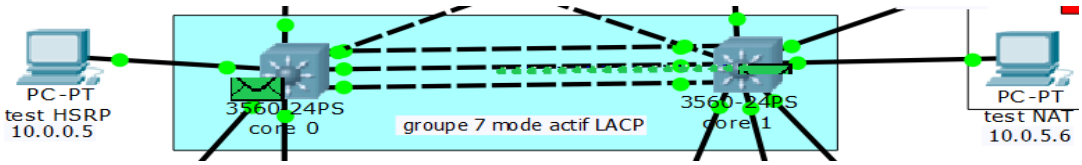
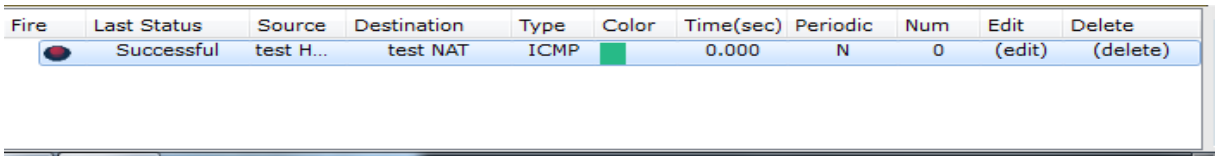


Figure 4.24 : *Echange de PDU à travers core0 et core1*



Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	test H...	test NAT	ICMP		0.000	N	0	(edit)	(delete)

Figure 4.25 : *Résultat de l'envoi*

On voit que l'enveloppe transite à travers les trois liens comme sur un seul et arrive bien à destination.
Après coupure d'un lien voyons le résultat en mode simulation :

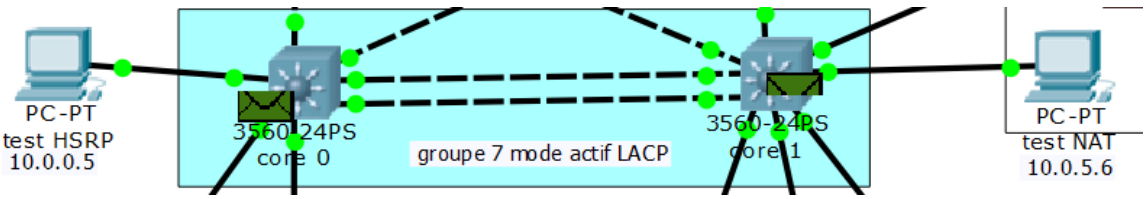


Figure 4.26 : *Echange de PDU à travers core0 et core1*

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	test H...	test NAT	ICMP		0.000	N	0	(edit)	(delete)

Figure 4.27 : *Résultat de l'envoi*

On a encore un succès. C'est-à-dire qu'Etherchannel assure vraiment la disponibilité de la communication entre ces commutateurs en maintenant les échanges intacts malgré les coupures. On sait aussi que grâce à Etherchannel, on augmente le débit au niveau de lignes agrégées. Malheureusement, il n'y a pas d'outil permettant d'évaluer cela sous Packet Tracer.

- Discussion

La combinaison des trois protocoles cités ci-dessus permet une véritable haute disponibilité et répartition de charge dans le réseau campus. Chacun joue un rôle primordial dans sa zone.

4.3.2.2 Sécurité

- Les translations d'adresses et de port (NAT/PAT)

Dans notre cas ils permettent à notre réseau campus de se connecter à internet.
Nous avons loués chez un fournisseur de service les adresses publiques : 201.49.10.17 jusqu'à 201.49.10.30 afin de se connecter à internet.
Le routeur GATEWAY fait partie du réseau interne et se charge des translations d'adresse et des filtrages.
Les connexions vers Internet sont simulées par l'envoi des requêtes ping vers le serveur WEB (10.0.6.2).
Internet a été représenté ici par un Cluster contenant un routeur et un serveur WEB.

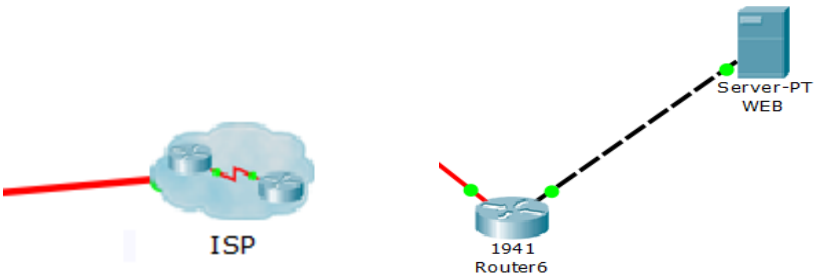


Figure 4.28 : *Cluster et son intérieur*

Nous avons choisi une configuration dynamique du NAT pour que chaque partie du réseau puisse se connecter à Internet en ayant chacun une adresse de navigation mais combiné à PAT pour prévoir un manque d'adresse publiques au sein du réseau. Dans ce cas, chaque utilisateur se connecte sur une même adresse mais un à un sur différents ports.

Ici, ce ne sera pas aisé pour un utilisateur malveillant de découvrir les adresses IP des utilisateurs internes et donc de les empêcher d'y accéder, car l'attribution des adresses publiques changent dynamiquement.

Le nom de notre pool est : campus.

Nous avons définis quelques politiques de sécurité assez simple pour mieux voir le fonctionnement des translations :

- Dans un premier temps, seul les terminaux ayant les adresses réseaux 10.0.5.0 et 10.0.3.0 auront accès à Internet.

Ils seront soumis à un même groupe de NAT (ACL 1) : ils seront attribués les uns après les autres une même adresse publique mais sous des ports différent lors des connexions (PAT).

Connexion de PC test NAT :

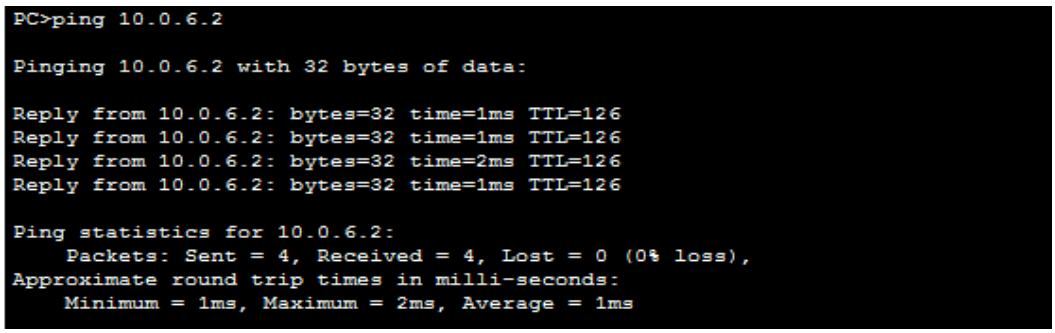


Figure 4.29 : *Résultats du ping*

Voyons les translations au niveau du routeur :

Router#sh ip nat translations

Pro	*Inside global*	*Inside local*	*Outside local*	*Outside global*
icmp	*201.49.10.17:10*	*10.0.5.6:10*	*10.0.6.2:10*	*10.0.6.2:10*
icmp	*201.49.10.17:11*	*10.0.5.6:11*	*10.0.6.2:11*	*10.0.6.2:11*
icmp	*201.49.10.17:12*	*10.0.5.6:12*	*10.0.6.2:12*	*10.0.6.2:12*
icmp	*201.49.10.17:9*	*10.0.5.6:9*	*10.0.6.2:9*	*10.0.6.2:9*

On remarque ici que la même adresse publique 201.49.10.17 est affecté à chaque requête mais avec des ports différents. Avec 10.0.3.0, on obtient le même résultat :

Router#sh ip nat translations

Pro Inside global	*Inside local*	*Outside local*	*Outside global*
icmp 201.49.10.17:13	*10.0.3.5:13*	*10.0.6.2:13*	*10.0.6.2:13*
icmp 201.49.10.17:14	*10.0.3.5:14*	*10.0.6.2:14*	*10.0.6.2:14*
icmp 201.49.10.17:15	*10.0.3.5:15*	*10.0.6.2:15*	*10.0.6.2:15*
icmp 201.49.10.17:16	*10.0.3.5:16*	*10.0.6.2:16*	*10.0.6.2:16*

Dans ce cas, si un terminal ayant l'adresse réseau 10.0.4.0 essaye de se connecter, il n'aura pas accès :

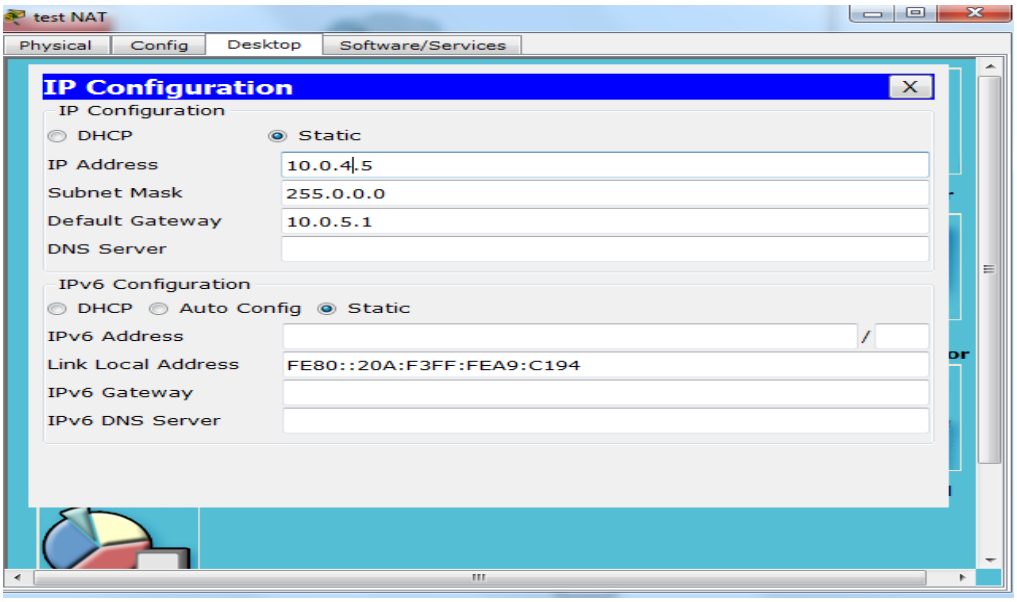


Figure 4.30 : *Nouvelle configuration du PC test NAT*

Après envoi d'une requête ping vers le serveur WEB, on a :

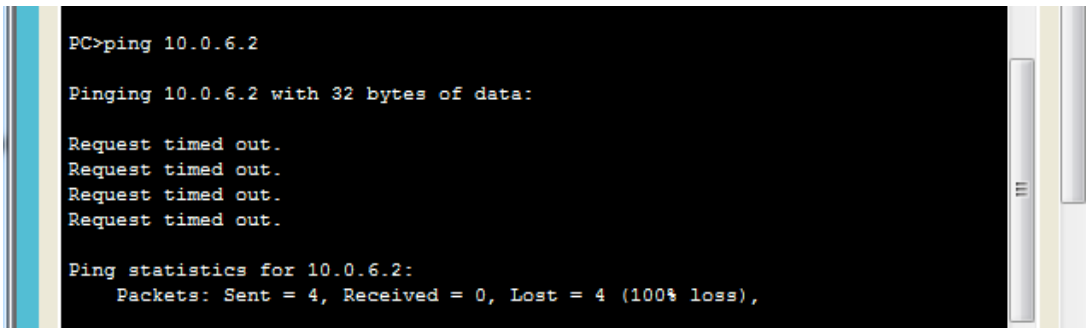


Figure 4.31 : *Echec de la connexion*

Le filtrage interne a été bien efficace car seul 10.0.5.0 et 10.0.3.0 auront accès à Internet.

- Les données provenant d'Internet transitent d'abord vers les serveurs de la DMZ, donc ces serveurs des DMZ doivent avoir accès à Internet. L'adresse réseau de ces serveurs : 172.16.3.0.

On les mettra dans un autre groupe de NAT (ACL2), donc ils auront une autre adresse publique différente de ce qu'on a vu précédemment.

On va tester cela en envoyant une requête d'un serveur vers l'adresse 10.0.6.2 :

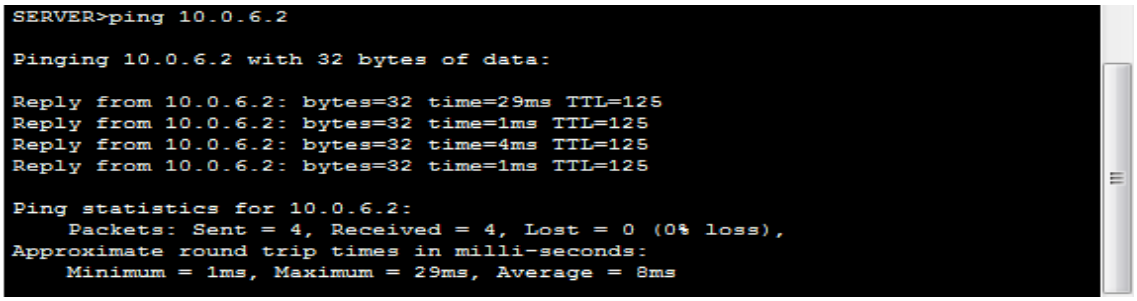


Figure 4.32 : *Envoi ping du serveur MAIL*

Pro Inside global	*Inside local*	*Outside local*	*Outside global*
icmp 201.49.10.18:25	*172.16.3.251:25*	*10.0.6.2:25*	*10.0.6.2:25*
icmp 201.49.10.18:26	*172.16.3.251:26*	*10.0.6.2:26*	*10.0.6.2:26*
icmp 201.49.10.18:27	*172.16.3.251:27*	*10.0.6.2:27*	*10.0.6.2:27*
icmp 201.49.10.18:28	*172.16.3.251:28*	*10.0.6.2:28*	*10.0.6.2:28*

On a vu ici que l'adresse publique attribué ici est 201.49.10.18 et est différent de précédemment.

- Les pare-feu : règles de filtrage

On y a déjà vu une partie à propos du NAT et PAT. L'établissement des règles dépendent des demandes en matière d'accès et de sécurité. Nous allons expliciter cela par notre politique de sécurité au niveau des routeurs d'accès aux serveurs.

- Seules les adresses 10.0.5.0 (adresse ayant accès à internet), 10.0.6.0 peuvent accéder aux serveurs DMZ. On les a regroupés sous le groupe 10 d'ACL. On a donc :

sh access-lists

Standard IP access list 10
10 permit 10.0.5.0 0.0.0.255
30 permit 10.0.6.0 0.0.0.255

Cette règle on l'a attribué à l'interface d'entrée du routeur sous fastethernet0/1 grâce à la commande : *Router(config-if)#ip access-group 10 in*

- Afin de protéger et de s'assurer de la sécurité du reste du réseau : seul le flux provenant des adresses 172.16.3.0 pourront sortir de la DMZ. On a attribué cette règle au groupe 11 de l'ACL pour mieux le discerner : *Standard IP access list 11 : 10 permit 172.16.3.0 0.0.0.255 (66 match(es)).* On a appliqué cette règle au niveau de l'interface fastethernet0/0 grâce à la commande : *Router(config-if)#ip access-group 11 in*
- Enfin, on renie tout flux provenant des serveurs internes pour mieux protéger ces derniers car ils contiennent les bases de données du réseau c'est-à-dire provenant de 172.16.4.0

Standard IP access list 10
10 permit 10.0.5.0 0.0.0.255
20 deny 172.16.4.0 0.0.0.255

On l'a mis dans groupe 10 car cette règle s'applique aussi à l'interface d'entrée fastethernet0/1.
Voici les différents essais pour voir l'application de ces règles.
On va transgresser les règles de l'ACL 10 en envoyant un ping du PC test HSRP (10.0.0.5) vers le serveur MAIL (172.16.3.251) par exemple.
Normalement les ping n'y arriveront pas à destination. Or, on a :

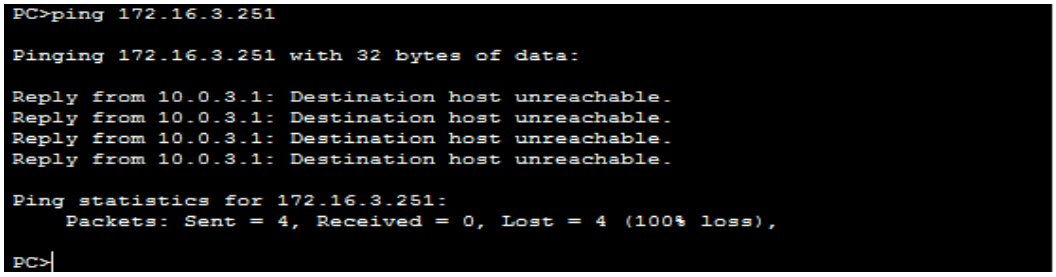


Figure 4.33 : *Echec de l'envoi*

Ceci dit que la destination vers l'hôte est introuvable, ce qui prouve que la règle est vraiment appliquée au niveau du routeur.
Les tests des autres règles se fait de la même manière.

- Pour les serveurs internes, on a établi que : tout élément du réseau interne peut y accéder sauf l'adresse 10.0.5.0 qui provient du routeur d'Internet dans le groupe 12 de l'ACL.

Standard IP access list 12
10 deny 10.0.5.0 0.0.0.255
20 permit any

- Discussion

Les translations d'adresses servent dans la sécurité à masquer les adresses IP des machines du réseau interne qui se connectent à Internet tandis que les ACL sécurisent les zones sensibles du réseau afin d'éviter une intrusion indésirable.

4.3.3 VPN IPsec

Notre réseau se connecte à travers Internet par l'intermédiaire d'un VPN en mode transport (pas de création de tunnel) et sécurisé par IPsec. On a séparé sa configuration du réseau en général.

Voici la topologie qu'on a choisie :

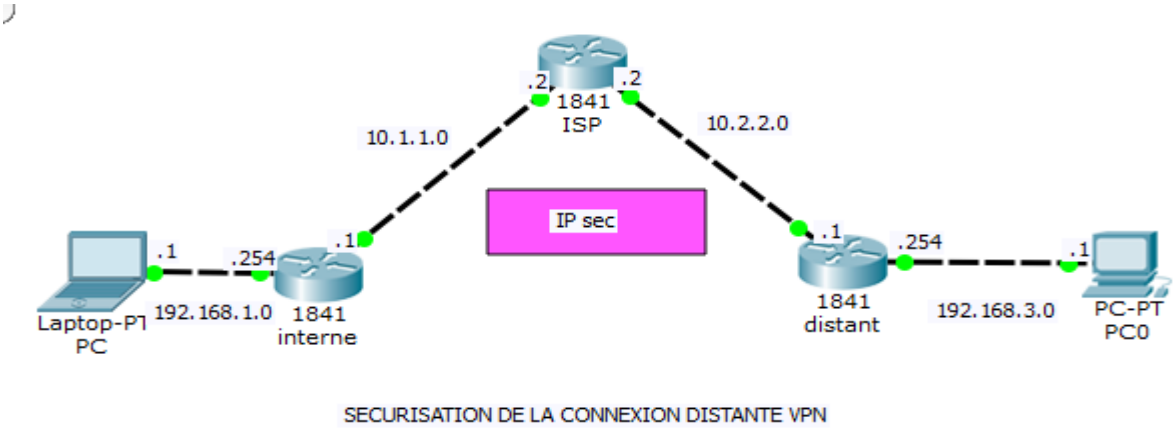


Figure 4.34 : *Architecture du VPN*

On test tout d'abord la connectivité entre les deux PC :

```
PC>ping 192.168.3.1

Pinging 192.168.3.1 with 32 bytes of data:

Reply from 192.168.3.1: bytes=32 time=11ms TTL=126
Reply from 192.168.3.1: bytes=32 time=0ms TTL=126
Reply from 192.168.3.1: bytes=32 time=0ms TTL=126
Reply from 192.168.3.1: bytes=32 time=0ms TTL=126

Ping statistics for 192.168.3.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 11ms, Average = 2ms
```

Figure 4.35 : *Ping de PC vers PC0*

Les configurations des clés ISAKMP sont programmées d'avance, négociés de part et d'autre dans chaque routeur.

Lorsqu'on regarde les fonctions de VPN grâce à *la* commande *show crypto map*, on ne retrouve plus les mots de passes d'IPsec et les différentes fonctions de cryptages utilisés.

Ces informations sont confidentielles entre les deux bouts.

On a :

- Routeur interne

R1#sh crypto map

Crypto Map vpn 10 ipsec-isakmp

Peer = 10.2.2.1

Extended IP access list 101

access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255

Current peer: 10.2.2.1

Security association lifetime: 4608000 kilobytes/900 seconds

PFS (Y/N): Y

Transform sets={

50,

}

Interfaces using crypto map vpn:

FastEthernet0/0

- Routeur externe

R3>en

R3#sh cr

R3#sh crypto map

Crypto Map vpn 10 ipsec-isakmp

Peer = 10.1.1.1

Extended IP access list 101

access-list 101 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255

Current peer: 10.1.1.1

Security association lifetime: 4608000 kilobytes/900 seconds

PFS (Y/N): Y

Transform sets={

50,

}

Interfaces using crypto map vpn:

FastEthernet0/0

La négociation des clés entre les routeurs se fait avant et après un échange d'un PDU par exemple. A l'entrée du routeur ISP, on peut apercevoir un paquet contenant la clé ISAKMP, envoyé par routeur externe vers routeur interne après que ce dernier a tenté d'accéder à l'autre bout.

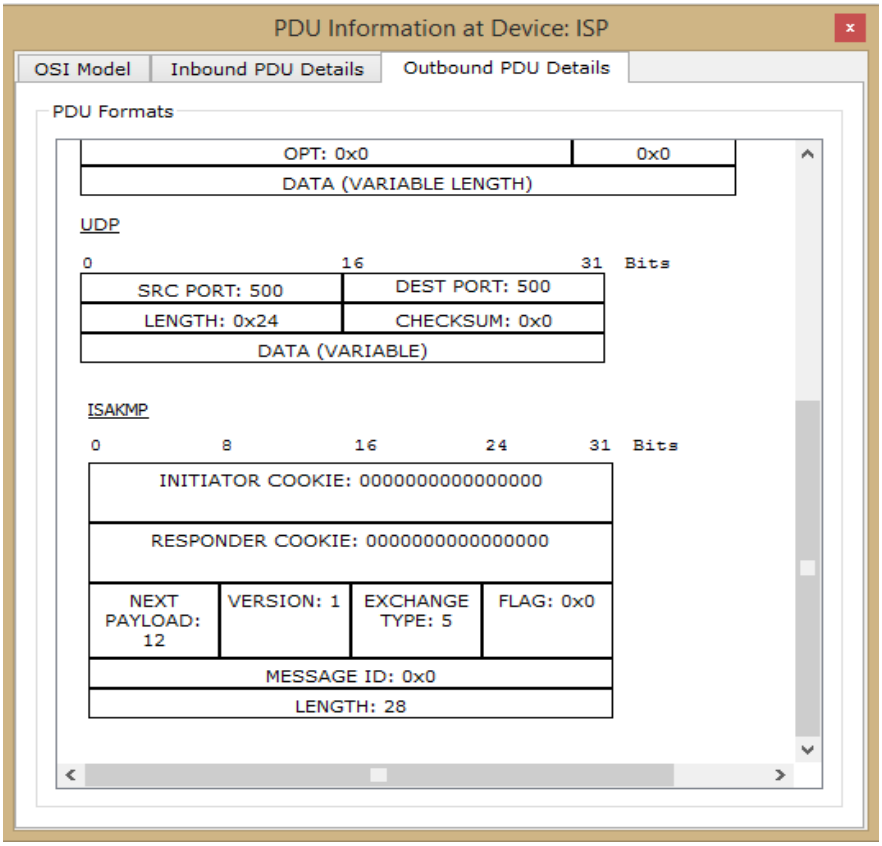


Figure 4.36 : *Contenu d'un PDU au niveau de ISP*

Si ces clés correspondent, la liaison est établie.

4.4 Réalisation d'un VPN mode tunnel

L'objectif ici est de mettre en évidence la nécessité de la création d'un tunnel pour la conception d'un réseau et d'en tirer les avantages.

Nous avons simulé la topologie du réseau à créer :

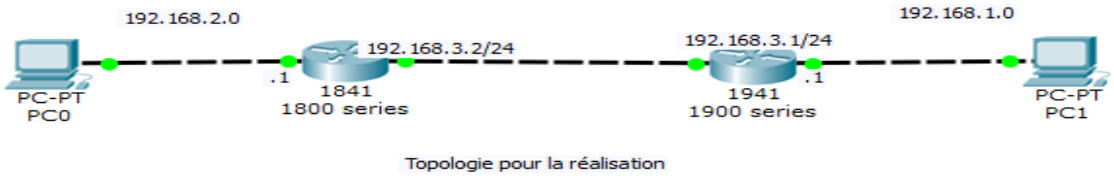


Figure 4.37 : *Architecture générale de la réalisation*

4.4.1 Configurations

4.4.1.1 Au niveau des PC

Equipements	Adresse IP	Passerelle	Masque
PC0	192.168.1.3	192.168.1.1	255.255.255.0
PC1	192.168.2.6	192.168.2.1	255.255.255.0

Tableau 4.01: *Configurations des PC*

- On y installe Wireshark pour voir les flux qui transitent.
- On y installe aussi VLC pour créer un flux multimédia échangé entre les deux PC.

Sur un des PC : on clique sur l'onglet média, puis ouvrir un flux réseau. On entre dans fichier puis on y ajoute une vidéo d'extension mp4. Puis on clique sur diffuser, on choisit le protocole des échanges : RTP/MPEG transport stream (voir annexe1). On clique sur ajouter et on configure l'adresse multicast et le port : 239.255.0.1, port : 5014.

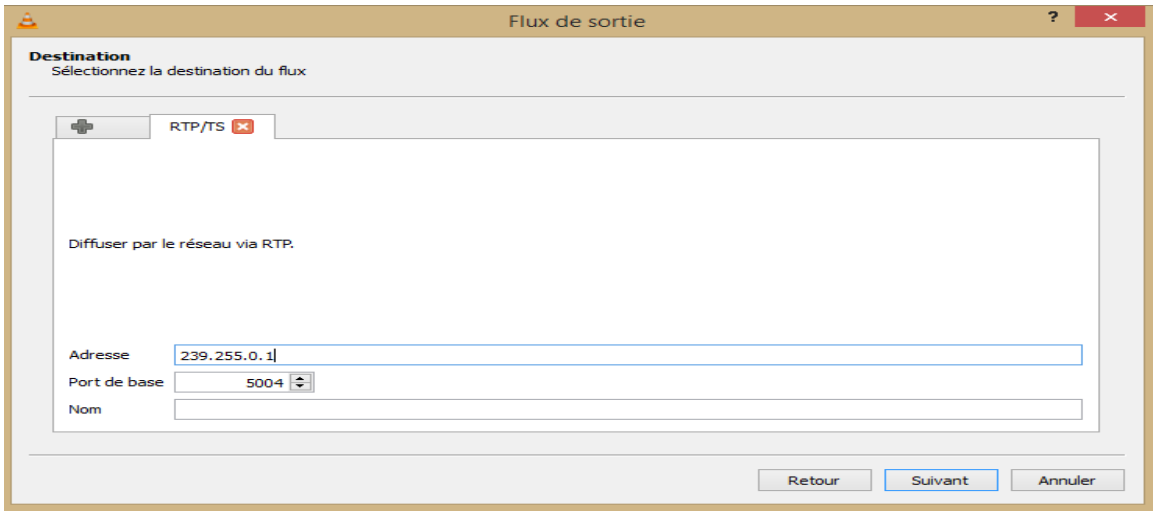


Figure 4.38 : *Réglages sur VLC*

C'est ce PC qui se chargera de diffuser le flux vidéo à travers le tunnel : le serveur.

Sur l'autre PC : il suffit de cliquer sur média, flux réseau et lire pour intercepter le flux.

On y entre évidemment l'adresse : 239.255.0.1, port 5014 pour qu'ils se connectent.

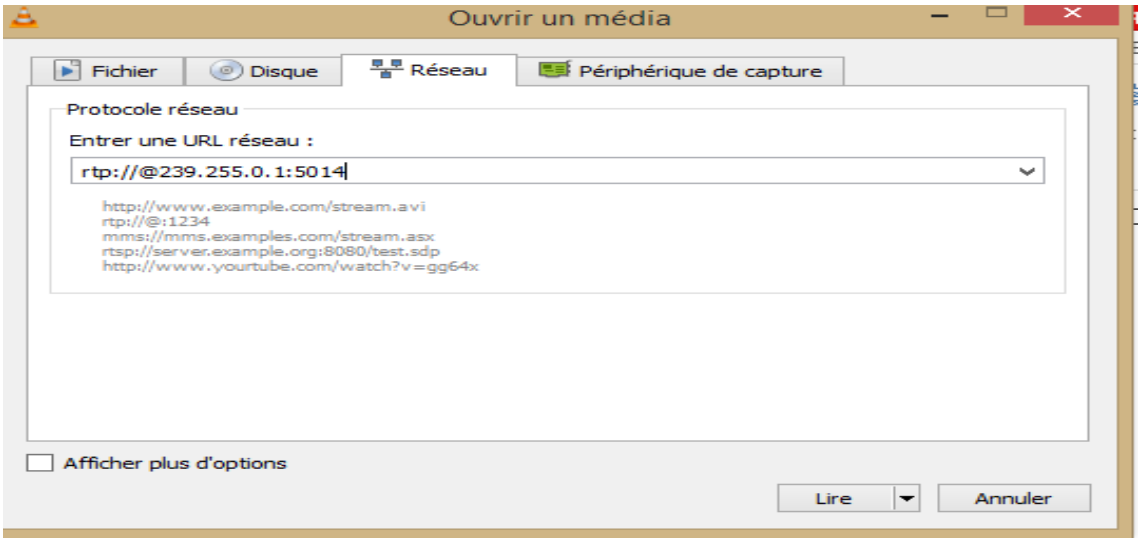


Figure 4.39 : *Configuration sur le PC client*

4.4.1.2 Au niveau des routeurs

Equipements	Adresse IP	Passerelle
Routeur 1800 series	Fa0/0 : 192.168.3.2 Fa0/1 : 192.168.1.1	255.255.255.0 255.255.255.0
Tunnel 0	10.0.0.2	255.0.0.0
Routeur 1900 series	Gig0/0 : 192.168.3.1 Gig0/1 : 192.168.2.6	255.255.255.0 255.255.255.0
Tunnel 0	10.0.0.1	255.0.0.0

Tableau 4.02: *Configurations des routeurs*

On crée un tunnel GRE entre les deux routeurs et on fait transiter dedans les flux. Par exemple sur series 1900 on a :

R1(config)# int tunnel 0
R1(config-if)# ip address 10.0.0.1 255.0.0.0
R1(config-if)# tunnel source gig0/0
R1(config-if)# tunnel destination 192.16.3.2
R1(config-if)# tunnel mode gre ip
R1(config-if)# exit
On fait de même sur series 1800.

4.4.2 Déroulement

On émet un flux vidéo du PC serveur vers le PC client. On doit voir en même temps la vidéo des deux bouts pour que le test fonctionne (streaming).

On lance Wireshark, et on commence la capture pour voir si les données transitent vraiment à l'intérieur du tunnel. RTP sera reconnu comme UDP sous Wireshark.

4.4.3 Résultats

4.4.3.1 Tests de connectivité des deux PC

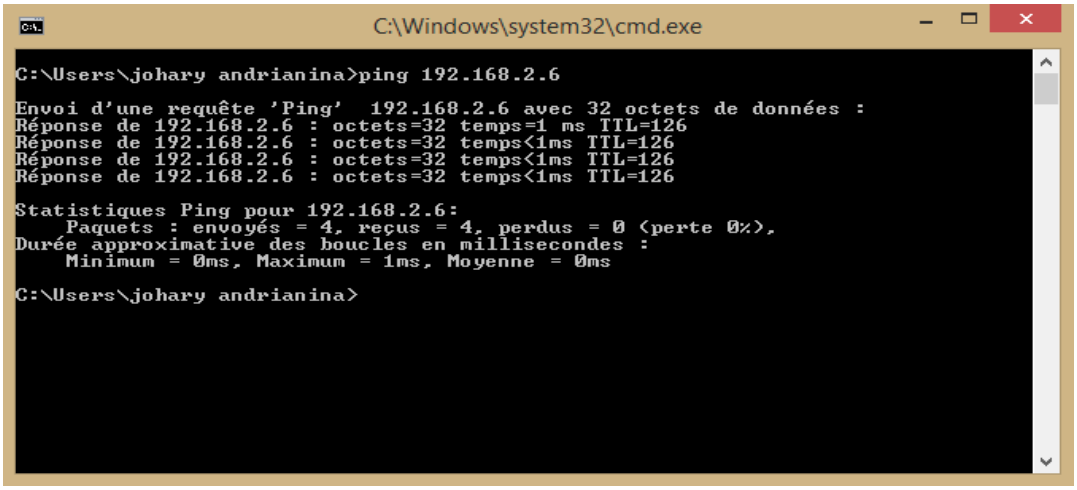


Figure 4.40 : *Envoi de ping PC0 vers PC1*

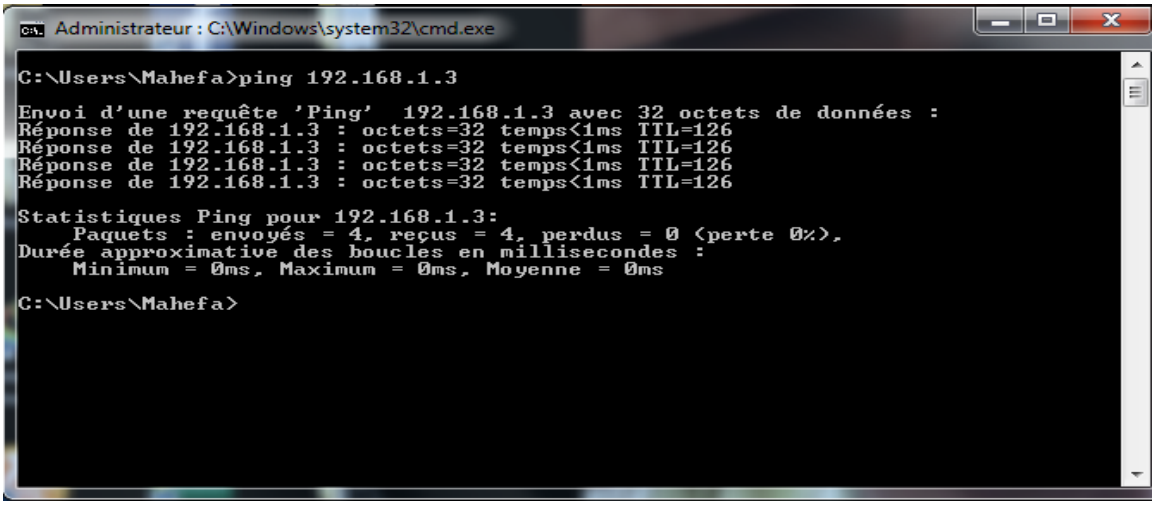
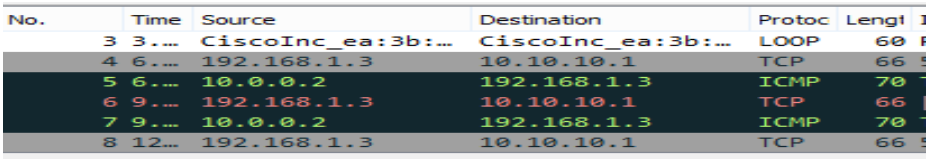


Figure 4.41 : *Envoi de ping PC1 vers PC0*

4.4.3.2 Analyse des flux vidéo

On voit bien que les PC sont vraiment aptes à s'échanger les données. Voyons l'état du tunnel sous Wireshark.

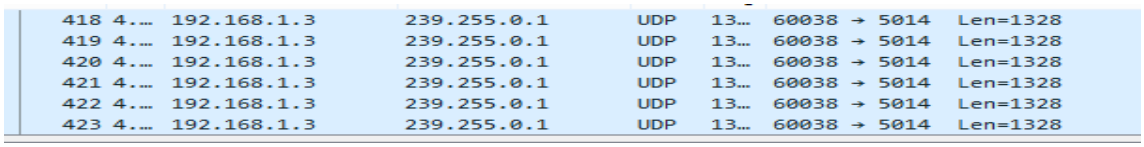


No.	Time	Source	Destination	Protoc	Lengt
3	3.…	CiscoInc_ea:3b:…	CiscoInc_ea:3b:…	LOOP	60
4	6.…	192.168.1.3	10.10.10.1	TCP	66
5	6.…	10.0.0.2	192.168.1.3	ICMP	70
6	9.…	192.168.1.3	10.10.10.1	TCP	66
7	9.…	10.0.0.2	192.168.1.3	ICMP	70
8	12…	192.168.1.3	10.10.10.1	TCP	66

Figure 4.42 : *Échange des paquets sous PC0*

On voit que le tunnel est fonctionnel car l'adresse 10.0.0.2 concerne l'interface connectée directement à PC0, de même pour PC1.

Nous allons maintenant observer le flux après diffusion de la vidéo par PC0 :



418	4.…	192.168.1.3	239.255.0.1	UDP	13…	60038 → 5014	Len=1328
419	4.…	192.168.1.3	239.255.0.1	UDP	13…	60038 → 5014	Len=1328
420	4.…	192.168.1.3	239.255.0.1	UDP	13…	60038 → 5014	Len=1328
421	4.…	192.168.1.3	239.255.0.1	UDP	13…	60038 → 5014	Len=1328
422	4.…	192.168.1.3	239.255.0.1	UDP	13…	60038 → 5014	Len=1328
423	4.…	192.168.1.3	239.255.0.1	UDP	13…	60038 → 5014	Len=1328

Figure 4.43 : *Flux RTP*

Pendant le streaming, les adresses IP des tunnels ne sont pas visibles, ce qui le rend intéressant du point de vue anonymat.

4.4.4 Discussion

Durant les échanges, on ne peut pas voir que les données transitent à travers le tunnel. Même en réalisant un « traceroute » de bout en bout, le tunnel reste indétectable.

On peut dire que GRE permet aussi le transport des données vidéo, multicast, c'est-à-dire des fichiers volumineux, mais cela dépend de la bande passante du support de transmission.

C'est seulement en « sniffant » les paquets par Wireshark qu'on a pu observer que les échanges se font vraiment à travers le tunnel créé avec les interfaces des deux routeurs.

L'intérêt du tunneling est donc la transparence et une confidentialité des échanges.

4.5 Conclusion

Ces différentes manipulations nous a permis de constater l'efficacité des protocoles de haute disponibilités que nous avons choisis sur le contrôle des redondances et résolutions en cas de panne. Les méthodes de sécurités intégrés dans les routeurs Cisco sont efficaces pour protégé le réseau interne de l'externe ou de lui-même. Et l'efficacité du tunneling dans les transmissions de données, nécessaire dans la conception des VPN.

CONCLUSION GENERALE

Le choix de la topologie est une des bases d'une bonne conception réseau : pour une transmission rapide, efficace, fiable et la sécurité des équipements.
La première partie nous montre l'intérêt de segmenter le réseau en LAN Virtuel (VLAN) et leur connexion utilisant le routage. Ainsi, les réseaux locaux (LAN) seront numérotés, donc plus facile à contrôler et faire communiqué entre eux et avec le reste du réseau. Combiné avec la structure hiérarchique, utilisé par la plupart des réseaux Métropolitains (MAN) et étendus (WAN), la segmentation nous montre de plus ses apports bénéfiques en termes de gestion.

Puis dans la seconde partie, on retrouve l'efficacité des protocoles de haute disponibilité : STP au niveau commutateur, HSRP et Etherchannel au niveau routeur qui gèrent en plus les partages de charge et les redondances. Ils permettent une fiabilité du réseau en cas de panne (coupure de lien, défaillance d'un équipement) tout en offrant un débit supérieur au cœur du réseau.

Enfin, un réseau disponible n'est pas à l'abri des attaques, ce qui nous conduit à la troisième partie qui est la conception et réalisation des politiques de sécurités. Ces attaques peuvent provenir de l'intérieur que de l'extérieur. Une application des règles de filtrages aux connexions internes et externes minimise les risques voir de les éradiqués. Le cryptage des données est un élément essentiel lorsqu'on transmet sur un réseau public des informations de valeurs (VPN IPsec).

Grâce à l'implémentation de toutes ces fonctions dans l'IOS de Cisco nous avons pu voir et analyser ces protocoles dans chaque branche du réseau campus.

Cependant, les qualités de services (Qos) dans les communications au niveau du réseau dépendent aussi de la sélection du routage, surtout dans les transmissions de longues distances. La vitesse ainsi que la convergence du réseau vont avec la rapidité du travail des nœuds qui le compose (commutateurs, routeurs…). Combiné à nos protocoles, on aura un Qos élevé au sein de notre conception.

Annexe 1 : Protocole RTP

A1.01 : Utilisation

RTP (Real time Transport Protocol) est à l'heure actuelle principalement utilisé comme transport de média pour les services de la voix sur IP ou de vidéo conférence, voire de *streaming*. En mode unidirectionnel, il est toujours associé avec un autre protocole de signalisation qui gère l'établissement de session et permet l'échange du numéro de port utilisé par les deux extrémités. On peut citer :

- le protocole SIP (Session Initial Protocol) pour les services de VoIP et de visioconférences ;
- le protocole H.323 pour les mêmes services (ancienne génération) ;
- le protocole RTSP (Real time Transport Streaming Protocol) pour le *streaming* bien que ce dernier possède un mode d'encapsulation TCP.

Le protocole ajoute un en-tête spécifique aux paquets UDP pour :

- spécifier le type et le format (codec) du média transporté ;
- numéroter les paquets afin de pouvoir gérer les pertes et les dé-séquencements ;
- fournir une indication d'horloge pour gérer la gigue.

RTP sera utilisé avantageusement sur un réseau temps réel (par exemple un réseau ATM à bande passante garantie, un canal optique, une radiodiffusion ou un canal satellite).
RTP est unidirectionnel mais peut être utilisé en mode diffusion (*multicast*) *via* satellite. Il est alors extrêmement économique en termes de ressources réseau pour servir un grand nombre de récepteurs, ce qui permet d'augmenter considérablement le débit utile et la qualité de codage du contenu.

A1.02 : Caractéristiques techniques

- Canal de retour

Bien qu'unidirectionnel, RTP peut toutefois être utilisé conjointement avec un canal de retour (*feedback*) sur la qualité de service (QoS) via RTCP(*Real-Time Transport Control Protocol*), négocié indépendamment Ce *feedback* peut par exemple informer l'émetteur sur les propriétés temps-réel du canal, l'état du tampon du récepteur, ainsi que demander des changements de

compression/débit pour les applications multimédia par exemple (dans ce cas, les données manquantes pourront être transmises via *Unicast*).
Pour la diffusion en masse cependant (flux en direct, radiodiffusé), cette voie de retour n'est généralement pas utilisée, mais le contenu est transmis plusieurs fois en parallèle avec un décalage temporel suffisant pour pallier les interruptions temporaires de qualité de réception, mais n'excèdent pas les limites des tampons des récepteurs (normalement pas plus d'une quinzaine de secondes d'écart). Le récepteur peut alors reconstituer et réordonner la séquence complète afin d'obtenir un flux continu sans perte.

- Mode multicast

La mise en œuvre de RTP en mode multicast requiert la configuration préalable de routage au niveau du récepteur, qui doit faire lui-même la demande de routage à ses routeurs hôtes, entre l'émetteur et le récepteur. L'émetteur quant à lui informe séparément les routeurs de diffusion auxquels il est directement connecté.
Pour les contenus protégés à valeur ajoutée, l'absence de voie de retour implique l'utilisation de clé de déchiffrement du contenu, que le récepteur doit négocier séparément avec l'émetteur (chacun peut recevoir facilement le contenu chiffré simplement en se connectant au routeur de diffusion). Mais RTP lui-même ne s'occupe pas du chiffrement et transporte le contenu de façon transparente.

Annexe 2 : Protocole SNMP

SNMP (Simple Network Management Protocol) est le protocole de gestion de réseaux proposé par l'IETF (Internet Engineering Task Force). Il est actuellement le protocole le plus utilisé pour la gestion, supervision et diagnostique des problèmes réseaux et matériels. Il travail dans la couche 7 du modèle OSI (couche application).

Fonctionnement du protocole SNMP

Le protocole SNMP constitué d'un ensemble de requêtes, de réponses et d'un nombre limité d'alertes. Le manager (la station de supervision) envoie des requêtes à l'agent (GetRequest : demande d'information, SetRequest : Affectation), qui retourne des réponses (GetResponse). Lorsqu'un événement anormal surgit sur l'élément réseau, l'agent envoie une alerte (trap) au manager.

Figure A2.01 : *Requêtes entre Manager et Client*

SNMP utilise le protocole UDP .L'agent reçoit les requêtes de la station de gestion sur le port 161. Le port 162 est réservé pour la station de gestion pour recevoir les alertes des agents.

SNMP permettra dans notre cas de gérer notre réseau à partir d'une machine administrateur et un serveur qui stockera les différents états du réseau.

Annexe 3 : Cisco ASA

Les Serveurs de Sécurité Adaptatifs Cisco ASA 5500 combinent les meilleurs services de VPN et de sécurité, et l'architecture évolutive AIM (Adaptive Identification and Mitigation), pour constituer une solution de sécurité spécifique. Conçue comme l'élément principal de la solution Self-Defending Network de Cisco (le réseau qui se défend tout seul), la gamme Cisco ASA 5500 permet de mettre en place une défense proactive face aux menaces et de bloquer les attaques avant qu'elles ne se diffusent à travers le réseau, de contrôler l'activité du réseau et le trafic applicatif et d'offrir une connectivité VPN flexible. Le résultat est une gamme de puissants serveurs de sécurité réseau multifonctions capables d'assurer en profondeur la protection élargie des réseaux des PME/PMI et des grandes entreprises tout en réduisant l'ensemble des frais de déploiement et d'exploitation et en simplifiant les tâches généralement associées à un tel niveau de sécurité. Réunissant sur une même plate-forme une combinaison puissante de nombreuses technologies éprouvées, la gamme Cisco ASA 5500 vous donne les moyens opérationnels et économiques de déployer des services de sécurité complets vers un plus grand nombre de sites. La gamme complète des services disponibles avec la famille Cisco ASA 5500 permet de répondre aux besoins spécifiques de chaque site grâce à des éditions produits conçues pour les PME comme pour les grandes entreprises. Ces différentes éditions offrent une protection de qualité supérieure en apportant à chaque installation les services dont elle a besoin. Chaque édition de la gamme Cisco ASA 5500 regroupe un ensemble spécialisé de services – firewall, VPN SSL et IPSec, protection contre les intrusions, services Anti-X, etc. – qui répondent exactement aux besoins des différents environnements du réseau d'entreprise.
Et lorsque les besoins de sécurité de chaque site sont correctement assurés, c'est l'ensemble de la sécurité du réseau qui en bénéficie.

Figure A3.01 : *Cisco ASA 5500*

- Des fonctionnalités éprouvées de sécurité et de connectivité VPN. Le système de prévention des intrusions (IPS) et de firewall multifonctions, ainsi que les technologies anti-X et VPN IPSec ou SSL (IP Security/Secure Sockets Layer) garantissent la robustesse de la sécurité des applications, le contrôle d'accès par utilisateur et par application, la protection contre les vers, les virus et les logiciels malveillants, le filtrage des contenus ainsi qu'une connectivité à distance par site ou par utilisateur.
- L'architecture évolutive des services AIM (Adaptive Identification and Mitigation).

Exploitant un cadre modulaire de traitement et de politique de services, l'architecture AIM de Cisco ASA 5500 autorise l'application, par flux de trafic, de services spécifiques de sécurité ou de réseau qui permettent des contrôles de politiques d'une très grande précision ainsi que la protection anti-X tout en accélérant le traitement du trafic. Les avantages en termes de performances et d'économies offerts par l'architecture AIM de la gamme Cisco ASA 5500, ainsi que l'évolutivité logicielle et matérielle garantie par les modules SSM (Security Service Module), permettent de faire évoluer les services existants et d'en déployer de nouveaux, sans remplacer la plate-forme et sans réduire les performances.

Fondement architectural de la gamme Cisco ASA 5500, AIM permet l'application de politiques de sécurité hautement personnalisables ainsi qu'une évolutivité de service sans précédent qui renforce la protection des entreprises contre l'environnement toujours plus dangereux qui les menace.

- La réduction des frais de déploiement et d'exploitation. La solution multifonctions

Cisco ASA 5500 permet la normalisation de la plate-forme, de la configuration et de la gestion, contribuant à réduire les frais de déploiement et d'exploitation récurrents.

Fonction	Description
Débit du firewall	Jusqu'à 150 Mbits/s
Débit du VPN	Jusqu'à 100 Mbits/s
Connexions	10 000 ; 25 000*
Homologues VPN IPSec	10 ; 25
Niveaux de licence des homologues VPN SSL	10, ou 25
Interfaces	Commutateur Fast Ethernet 8 ports avec groupage dynamique des ports (dont 2 ports PoE)
Interfaces virtuelles (VLAN)	3 (sans support de l'agrégation de VLAN)/20 (avec support de l'agrégation de VLAN)
Haute disponibilité	Non prise en charge ; mode actif/veille à inspection d'état et support ISP redondant

Tableau A3.01 : *Fonctionnalités et capacités du Serveur de Sécurité Adaptatif Cisco ASA 550*

BIBLIOGRAPHIE

[1] "Cisco CCNA Module 1", version 2.1.2, Inc 2000, version html

[2] A. Ratsimbazafy, "Réseaux Informatiques", cours L2-TCO, Dép TCO-ESPA, AU 2010-2011

[3] L.E. Randriarijaona, "Réseaux TCP/IP", cours L3-TCO, Dép TCO-ESPA, AU 2011-2012

[4] http://www.labo-cisco.com

[5] A. Ratsimbazafy, "Réseaux Téléinformatiques", cours L3-TCO, Dép TCO-ESPA, AU 2012-2013

[6] "Commutation, VLANs, VTP et STP", Chap6, documents publics de Cisco, ed 2013

[7] P. Hainaut, "LES VLAN", www.coursonline.te, 2013

[8] "Routage inter VLAN", Chap 6.2, documents publics de Cisco, ed 2013

[9] Zo A.F. Rabarijaona, « REDONDANCE D'UN RESEAU ET LE PROTOCOLE DE STP », mémoire de fin d'études, Dép TCO, 21 Mars 2011.

[10] J-L Montaignier, « RESEAU D'ENTREPRISE PAR LA PRATIQUE » , Eyrolles, ed 2006

[11] http://www.cisco.com, « Déploiement de réseau campus session 1.8 », ed 2002

[12] CCNA Discovery version 4.exe, « Conception et prise en charge des réseaux informatiques »

[13] A. Simon, « Keepalived : Haute disponibilité et répartition des charges enfin libérés », JRES, 22 Novembre 2011

[14] « TP mise en œuvre du Spanning Tree », BTS SIO-SISR 5, Lyvée du Grand Nouméa

[15] http://cisco.goffnet.org/leprotocolespanningtree

[16] C.D. Stefano et S. Wong, « Les protocoles de redondance HSRP, VRRP et CARP », 2007

[17] « Etherchannel Fundamentals no audio », documents publics de Cisco, ed 2013

[18] A.Vladimir, « Concevoir la sécurité informatiqueen entreprise », Creative Commons, 2014

[19] S. Ghernaouti, « Sécurité informatique et réseaux », ed DUNOD, 2013

[20] T. Delage, « Network Address Translation, Port Address Translation », GRETA VIVA5/IUT Valence, 2012

[21] http://www.certa.fr, « Filtrage et parefeux »

[22] C. Milard, « Cours pare-feu », comment ça marche, licence GNU FDL, ed 2003

[23] http://idum.fr/spip.php?article214, « VPN site to site IPsec », ed 2010

[24] G. Florin, « Sécurité des niveaux liaisons et réseaux privés virtuels, VPN », CNAM, Laboratoire Cédric, ed 2007

[25] B. Martin, « IPsec : Techniques », haking9 N 3, 2006

[26] G. Clugnac, « Réseaux de campus », 2013

[27] R. Abdelli, « Audit et Sécurité Informatique d'un Réseau Local D'entreprise », AU 2010-2011

FICHE DE RENSEIGNEMENTS

Nom : RAJAONASON

Prénoms : Johary Andrianina

Adresse : Lot B75P Andafiavaratra Ankadikely Ilafy

Antananarivo – Madagascar

Tel : +261346484537

E-mail: joharyrajaonasonm2@gmail.com

Titre du mémoire :

« MISE EN EVIDENCE DES PROTOCOLES DE HAUTE DISPONIBILITE ET DE SECURITE DANS UN RESEAU CAMPUS »

Nombre de pages : 102

Nombre de tableaux : 8

Nombre de figures : 82

Encadreur de mémoire : Monsieur RABEMANANTSOA Josh

Tel : +261341400620

Mail : rabejosh@yahoo.fr

RESUME

Le concept de VLAN est né de l'augmentation considérable de la taille des réseaux et de la volonté de les segmentés. En parallèle, il y eu apparition des topologies modèles comme l'architecture campus. Le routage inter VLAN permet une connexion entre ces éléments de la couche inférieure du modèle OSI (2) vers les plus hautes. Cette prolifération cause une interconnexion avec d'autres réseaux comme Internet afin de transporter des données à longue distance, d'où la sécurité devient obligatoire. En effet, des utilisateurs ou logiciels malveillants peuvent nuire aux informations confidentielles de son propriétaire. Les pannes sont fréquentes, et les réseaux volumineux qui subissent une défaillance mettent beaucoup de temps à détecter les anomalies. Alors, il faut que le réseau soit capable de contourner afin de garder les échanges avant les réparations : haute disponibilité.

Mots Clés : Réseau de campus, Hiérarchique, Haute disponibilité, Sécurité, Cisco.

ABSTRACT

The concept of VLAN born of the considerable increase in the size of the networks and the control of the segmented. In parallel, there was appearance of models topologies like the campus architecture. Inter VLAN routing allows a connection between the lower layer of the OSI model elements (2) to the highest. This proliferation causes an interconnection with other networks such as the Internet to transport long distance data, where security becomes mandatory. Indeed, users or malware can harm the confidential information of its owner. Breakdowns are frequent and large networks which undergo failure takes a long time to detect anomalies. So we need the network to be able to work around in order to keep the exchange before repairs: high availability.

Keywords: Campus network, Hierarchical, High availability, Security, Cisco.