N° d'ordre : 02/TCO/M2 Pro 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 à visée PROFESSIONNELLE

Domaine : Science de l'ingénieur

Mention : Télécommunications

Parcours : Système de traitement d'informations (STI)

Par : **ANDRIANTSALAMA Nomentsoa Nampoina**

CONCEPTION ET MISE EN PLACE DU RESEAU HIERARCHIQUE A HAUTE DISPONIBILITE AU SEIN DU MFB

Soutenu le 06 Mai 2016 devant la Commission d'Examen composée de :

Président :

M. ANDRIAMIASY Zidora

Examinateurs : M. RATSIHOARANA Constant

M. RAKOTONDRAINA Tahina Ezechiel

Mme ANDRIANTSILAVO Haja

Encadreur : M. RANDRIARIJAONA Lucien Elino

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 le Professeur ANDRIANAHARISON Yvon Responsable du domaine de l'ingénieur.

Mes remerciements s'adressent également à Monsieur RAKOTOMALALA Mamy Alain, Maître de Conférences, Chef de Département.

Je tiens à témoigner ma reconnaissance et ma gratitude les plus sincères à Monsieur RANDRIARIJAONA Lucien Elino, Enseignant au sein du Département Télécommunication, mon encadreur pédagogique pour sa volonté et ses conseils qui m'ont aidé à la conception et l'élaboration de cet ouvrage. Je tiens à aussi à remercier Monsieur LALA ARISON Zo Ny Aina, Ingénieur réseau au MFB qui, en tant que Encadreur professionnel, s'est toujours montré à l'écoute et très disponible tout au long de sa réalisation.

J'exprime ma gratitude aux membres de jury, présidés par Monsieur ANDRIAMIASY Zidora ; qui ont voulu examiner ce travail :

- Monsieur RAKOTONDRAINA Tahina Ezéchiel, Docteur et Enseignant-Chercheur en Télécommunication à l'ESPA.
- Monsieur RATSIHOARANA Constant, Maître de Conférences, enseignant au sein du département Télécommunication à l'ESPA.
- Madame ANDRIANTSILAVO Haja, Assistante 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

AAA	Authentication Authorization and Accounting
ARP	Address Resolution Protocol
ASCII	American Standard Code for Information Interchange
ATM	Asynchronous Transfer Mode
CLI	Command Line Interface
CRC	Contrôle de Redondance Cyclique
DHCP	Dynamic Host Configuration Protocol
DLCI	Data-Link Connection Identifier
DNS	Domain Name System
DTP	Dynamic Trunking Protocol
EIGRP	Enhanced Interior Gateway Routing Protocol
FAI	Fournisseur d'Accès Internet
HDLC	High-Level Data Link Control
HTML	Hypertext Markup Language

HTTPS	HyperText Transfert Protocol Secure
ICMP	Internet Control Message Protocol
IOS	Interface Operating System
IP	Internet Protocol
IPSec	Internet Protocol Security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISO	International Organization for Standardization
ISO	International Organisation for Standardization
LACP	Link Aggregation Control Protocol
LAN	Local Area Network
MFB	Ministère des Finances et du Budget
NAT	Network Basic Input/output System
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First

PC	Personnal Computer
PDU	Protocol Data Unit
POP	Point Of Presence
PPDIOO	Prepare, Plan, Design, Implement, Operate Optimize
PPP	Point to Point Protocol
PPPoE	Point to Point Protocol of Ethernet
RIP	Routing Information Protocol
SLIP	Serial Line Internet Protocol
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SSH	Secure Shell
STP	Shield Twisted-Pair
STP	Spanning Tree Protocol
TCP	Transmission Control Protocol

TSAP	Transport Service Access Point
UDP	User Datagram Protocol
UTP	Unshield Twisted-Pair
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
VTP	Vlan Trunking Protocol
WAN	Wide Area Network

INTRODUCTION GENERALE

Les réseaux informatiques et les ordinateurs constituent aujourd'hui des outils essentiels au succès d'une entreprise, peu importe sa taille. Au début, les entreprises exploitaient les réseaux de données pour enregistrer et gérer en interne des informations financières, des renseignements sur les clients et des systèmes de paie des employés.

Ces réseaux d'entreprise ont ensuite évolué pour permettre le transfert de nombreux types de services d'informations différents, parmi lesquels les courriels, la vidéo, les messageries et la téléphonie. Pour répondre aux besoins quotidiens des entreprises, les réseaux eux-mêmes deviennent de plus en plus complexes. 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.

Les réseaux se doivent donc d'être bien conçus pour répondre à toutes les attentes et imprévus pouvant se produire. 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.

Ainsi dit, l'objectif de ce mémoire de fin d'études intitulé : « CONCEPTION ET MISE EN PLACE DE RESEAU HIERARCHIQUE A HAUTE DISPONIBILITE AU SEIN DU MFB» est de présenter et d'étudier les bonnes pratiques et les étapes à suivre pour réaliser la meilleure conception d'un réseau qui répond aux exigences en matière de réseau d'entreprise. Elle se portera donc sur quatre chapitres dont le premier se focalise sur la généralité sur les réseaux informatiques. Ensuite, dans le second chapitre, nous étudierons les différentes étapes pour la conception d'un réseau d'entreprise. Le troisième chapitre parlera de l'étude et conception du réseau d'entreprise du Ministère des Finances et du Budget. Et enfin, le dernier chapitre sera consacré à la simulation sur Packet Tracer et sera donc une réalisation de ces études théoriques citées dans les chapitres précédentes.

CHAPITRE 1
GENERALITES SUR LE RESEAU INFORMATIQUE

1.1 Définitions

Un réseau informatique est un ensemble d'ordinateurs reliés entre eux grâce à des lignes physiques et échangeant des informations sous forme de données numériques (valeurs binaires, c'est-à-dire codées sous forme des signaux pouvant prendre deux valeurs : 0 et 1). Un système informatique est un ensemble de matériels et de logiciels destinés à réaliser des tâches mettant en jeu le traitement automatique des informations.

1.2 Les différents types des réseaux

On distingue différents types de réseaux selon leur taille, leur vitesse de transfert des données ainsi que leur étendue. On fait généralement trois catégories de réseaux:

- LAN (Local Area Network)
- MAN (Metropolitan Area Network)
- WAN (Wide Area Network)

1.2.1 Les LAN

LAN signifie *Local Area Network* (en français *Réseau Local*). Il s'agit d'un ensemble d'ordinateurs appartenant à une même organisation et reliés entre eux dans une petite aire géographique par un réseau, souvent à l'aide d'une même technologie (la plus répandue étant Ethernet). La vitesse de transfert de données d'un réseau local peut s'échelonner entre 10 Mbit/s (pour un réseau Ethernet par exemple) et 1 Gbit/s (en Gigabit Ethernet par exemple). La taille d'un réseau local peut atteindre jusqu'à 100 voire 1000 utilisateurs.[1]

1.2.2 Les MAN

Les MAN (*Metropolitan Area Network*) interconnectent plusieurs LAN géographiquement proches (au maximum quelques dizaines de km) à des débits importants.

Ainsi un MAN permet à deux nœuds distants de communiquer comme si ils faisaient partie d'un même réseau local. Un réseau MAN est formé de commutateurs ou de routeurs interconnectés par des liens hauts débits (en général en fibre optique).

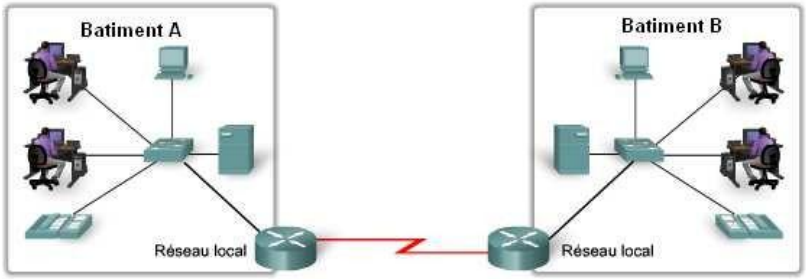


Figure 1.01 : *Schéma d'un MAN*

1.2.3 Les WAN

Un WAN (Wide Area Network ou réseau étendu) interconnecte plusieurs LAN à travers de grandes distances géographiques. Les débits disponibles sur un WAN résultent d'un arbitrage avec le coût des liaisons (qui augmente avec la distance) et peuvent être faibles.

Les WAN fonctionnent grâce à des routeurs qui permettent de "choisir" le trajet le plus approprié pour atteindre un nœud du réseau. [1]

Le plus connu des WAN est Internet

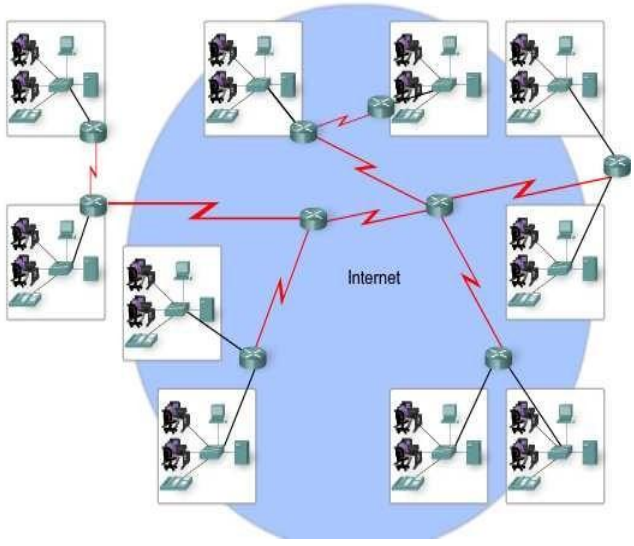


Figure 1.02 : *Schéma d'un WAN*

1.3 Les différentes catégories des réseaux

On distingue également deux catégories de réseaux :

- Réseaux poste à poste (Peer to Peer= P2P).
- Réseaux avec serveur dédié (Server/client).

1.3.1 Le réseau P2P

Chaque poste ou station fait office de serveur et les données ne sont pas centralisées, l'avantage majeur d'une telle installation est son faible coût en matériel (les postes de travail et une carte réseau par poste). En revanche, si le réseau commence à comporter plusieurs machines (>10 postes) il devient impossible à gérer.

Par exemple : Si on a 4 postes et 10 utilisateurs, chaque poste doit contenir les 10 mots de passe afin que les utilisateurs puissent travailler sur n'importe lequel des postes. Mais si maintenant il y a 60 postes et 300 utilisateurs, la gestion des mots dépasse devient périlleuse.

1.3.2 Le réseau Server/Client

Il ressemble un peu au réseau poste à poste mais cette fois-ci, on y rajoute un poste plus puissant, dédié à des tâches bien précises. Cette nouvelle station s'appelle serveur. Le serveur centralise les données relatives au bon fonctionnement du réseau.

Dans l'exemple précédant, c'est lui qui contient tous les mots de passe. Ainsi ils ne se trouvent plus qu'à un seul endroit. Il est donc plus facile pour l'administrateur du réseau de les modifier ou d'en créer d'autres. L'avantage de ce type de réseau est sa facilité de gestion des réseaux comportant beaucoup de postes. Son inconvénient majeur est son coût souvent très élevé en matériel.

En effet, en plus des postes de travail il faut se procurer un serveur qui coûte cher car c'est une machine très puissante et perfectionnée. De plus la carte réseau que l'on y met est de meilleure qualité que celle des postes de travail.

1.4 Le modèle OSI

1.4.1 Définitions

Le modèle OSI a été conçu par l'ISO (International Organization for Standardization) pour fournir un cadre dans lequel concevoir une suite de protocoles pour système ouverts. L'idée était que cet ensemble de protocoles serait utilisé pour développer un réseau international qui ne dépendrait pas de systèmes propriétaires.

Ce modèle est un modèle de référence en ce qui concerne les réseaux, il décrit les concepts et les démarches à suivre pour interconnecter des systèmes, il est composé de 7 couches : physique, liaison, réseau, transport, session, présentation, application.[2]

1.4.2 Architecture du modèle OSI

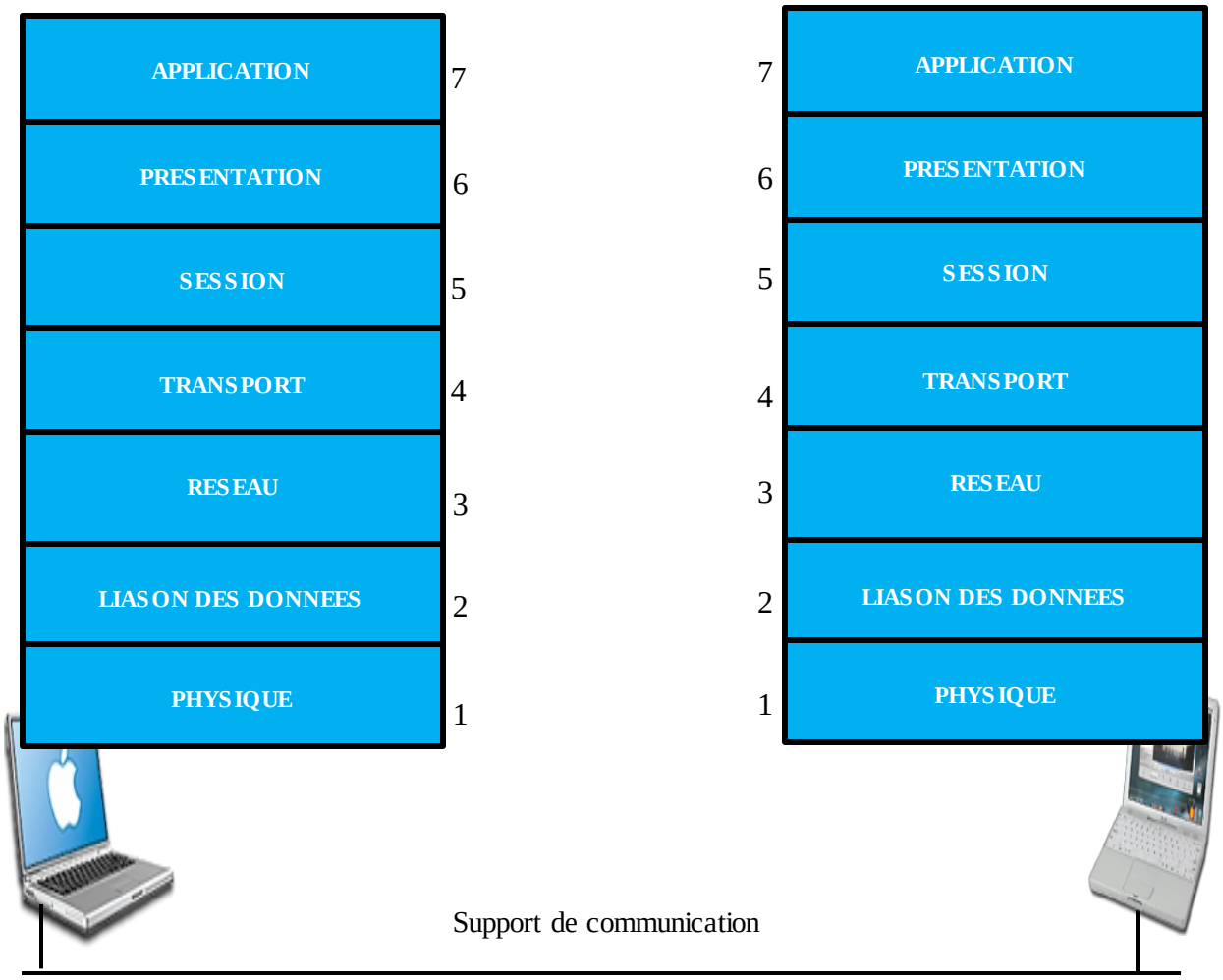


Figure 1.03 : *Architecture du modèle OSI*

Le modèle comporte sept couches succinctement présentées ci-dessus de bas en haut. Ces couches sont parfois réparties en deux groupes.

On distingue :

- Les couches basses (1-4) relatives au transfert de l'information ;
- Les couches hautes (5-7) relatives au traitement réparti de l'information ;

Les couches basses sont plutôt orientées communication et sont souvent fournies par un système d'exploitation c'est-à-dire que les couches hautes sont plutôt orientées application et réalisées par des bibliothèques ou un programme spécifique. Dans le monde IP, ces trois couches sont rarement distinguées que toutes ses fonctions sont considérées comme partie intégrante du protocole applicatif. [1][2]

1.4.3 Présentation des couches

1.4.3.1 La couche physique

La couche physique fournit les moyens (mécaniques, électrique, . . .) pour transmettre des éléments binaires entre entités de liaisons sur un circuit de communication.

Elle reçoit les signaux et les convertit en bits de données qu'elle délivre à la couche supérieure.

Cette couche transmet donc les bits à travers un canal de communication. Les bits représentent des enregistrements de base de données ou des fichiers à transférer, mais la couche physique ignore ce que ces bits représentent.

Ces bits peuvent être encodés sous forme de 0 et 1 ou sous forme analogique. La couche physique fait intervenir alors les interfaces mécaniques et électriques sur le média physique.

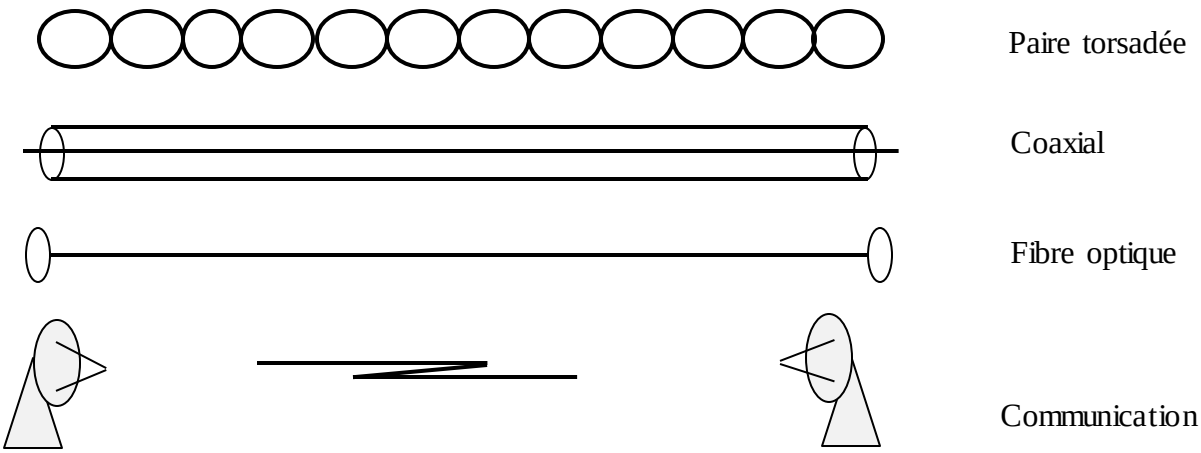


Figure 1.04 : *Quelques interfaces physiques de transmission*

1.4.3.2 La couche liaison de données

La couche liaison de données fournit une ligne qui paraît exempte d'erreurs de transmission à la couche réseau à partir de la couche physique. Elle prend les données de la couche physique et fournit ses services à la couche réseau. Les bits reçus sont groupés en unités logiques appelées trame. Dans le contexte d'un réseau, une trame peut être une trame Token Ring ou Ethernet, ou un autre type de trame réseau. Pour les liens des réseaux étendus, ces trames peuvent être des trames SLIP, PPP, X25, ATM ou Frame Relay. La couche liaison de données est la première couche qui gère les erreurs de transmission en utilisant un contrôle de redondance cyclique (CRC) présente dans le champ de contrôle d'erreurs.

1.4.3.3 La couche réseau

La couche réseau permet de gérer l'acheminement correct de paquets de la source à destination.

Elle a trois grandes fonctions :

- le contrôle de flux ; la couche réseau sert à éliminer les congestions et à réguler le flot de données.
- le routage ; la couche réseau gère les connexions entre les nœuds du réseau. Un service supplémentaire, fourni par la couche réseau, concerne la façon de router les paquets entre les nœuds d'un réseau.

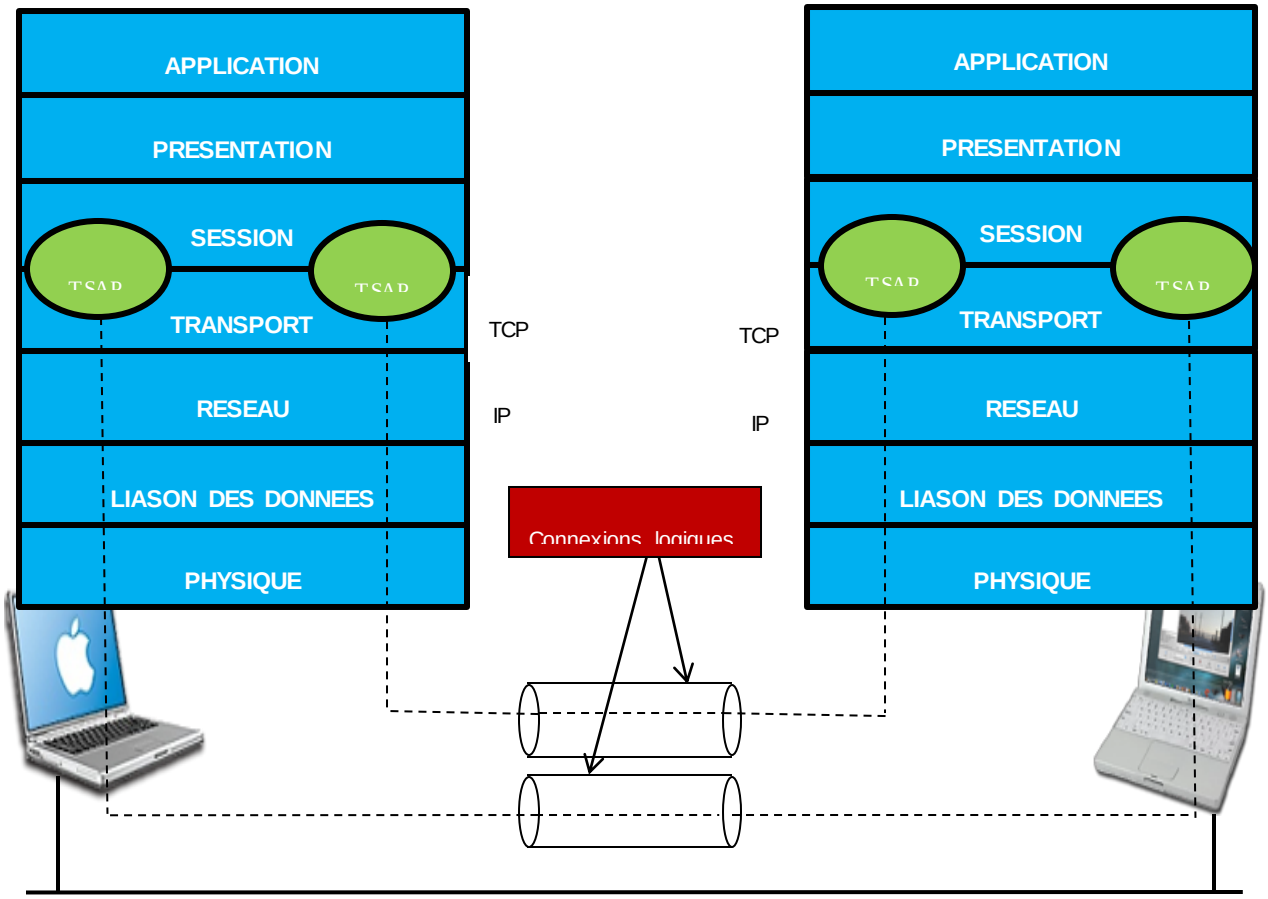
- l'adressage ; cette couche permet aussi à deux réseaux différents d'être interconnectés en implémentant un mécanisme d'adressage uniforme. Token Ring et Ethernet possèdent, par exemple, différents types d'adresses. Pour interconnecter ces réseaux, on a besoin d'un mécanisme d'adressage compréhensible par les deux réseaux.

1.4.3.4 La couche transport

La fonction de la couche transport est d'accepter des données de la couche session, de les découper éventuellement en plus petites unités et de s'assurer que tous les morceaux arrivent à destination. Cette couche garantit que les données reçues sont telles qu'elles ont été envoyées. Pour vérifier l'intégrité des données, cette couche se sert des mécanismes de contrôle des couches inférieures.

Elle est aussi responsable de la création de plusieurs connexions logiques par multiplexage sur la même connexion réseau quand plusieurs connexions logiques partagent la même connexion physique.

Elle implémente le multiplexage dans lequel plusieurs éléments logiciels partagent la même adresse de la couche réseau. Pour identifier sans erreur l'élément logiciel dans la couche transport, une forme plus spécifique d'adresse est nécessaire. Ces adresses, appelées adresses de transport, sont fournies par une combinaison de l'adresse de la couche réseau et d'un numéro TSAP (Transport Service Access Point). Cette adresse est appelé numéro de port dans les réseaux TCP/IP.



TSAP= Transport Service Access Point

Figure 1.05 : *Multiplexage de plusieurs connexions logiques*

1.4.3.5 La couche session

La couche session fournit aux entités de présentation les moyens nécessaires pour organiser et synchroniser leur dialogue. C'est-à-dire que la couche session gère les connexions entre les applications coopérants. Un utilisateur peut se connecter à un hôte avec cette couche, à travers un réseau où une session est établie pour transférer des fichiers.

La couche session offre les fonctions suivantes :

- Contrôle du dialogue ;
- Gestion des jetons ;
- Gestion de l'activité.

En général, une session permet des communications full duplex. La couche session peut fournir une ou deux voies de communication (contrôle de dialogue).

Pour certains protocoles, il est essentiel qu'un seul côté lance une opération critique. Pour éviter que les deux côtés lancent la même opération, un mécanisme de contrôle, comme l'utilisation de jetons, doit être implémenté. Avec la méthode du jeton, seul le côté qui possède le jeton peut lancer une opération. La détermination du côté qui doit posséder le jeton et son mode de transfert s'appellent la gestion du jeton.

1.4.3.6 La couche présentation

Pour que deux systèmes puissent se comprendre, ils doivent utiliser le même système de représentation des données. La couche présentation se charge de la syntaxe des informations que les entités d'application se communiquent. Il existe plusieurs façons de représenter des données, par exemple, l'ASCII pour les fichiers texte. La couche présentation utilise un langage commun compréhensible par tous les nœuds du réseau.

Cette couche gère donc le chiffrement et le déchiffrement des données et convertit les données machine en données exploitables par n'importe quelle autre machine.

1.4.3.7 La couche application

C'est la dernière couche du modèle OSI. Cette couche donne au processus d'application le moyen d'accéder à l'environnement OSI. Elle fournit les protocoles et les fonctions nécessaires aux applications utilisateurs qui doivent accomplir des tâches de communication. [2][3]

Les fonctions que la couche application peut fournir :

- Les protocoles pour les services de fichiers distants tels que l'ouverture, la fermeture, la lecture, l'écriture et le partage des fichiers.
- Les services de transfert de fichiers et d'accès aux bases de données distantes.
- Les services de gestion des messages des applications de messagerie.
- Les services de répertoires pour localiser les ressources d'un réseau.
- La gestion des périphériques.
- L'exécution de travaux distants.

1.5 Les équipements réseau

L'interconnexion de réseaux peut être locale: les réseaux sont sur le même site géographique. Dans ce cas, un équipement standard (répéteur, routeur …etc.) suffit à réaliser physiquement la liaison. L'interconnexion peut aussi concerner des réseaux distants. Il est alors nécessaire de relier ces réseaux par une liaison téléphonique (modems, etc..).

1.5.1 Le répéteur (Repeater)

Le répéteur permet d'interconnecter deux segments d'un même réseau :

- il est passif au sens où il ne fait qu'amplifier le signal.
- il ne permet pas de connecter deux réseaux de types différents
- il travaille au niveau de la couche 1 de model OSI.

1.5.2 Le pont (Bridge)

Les ponts ne peuvent connecter que deux réseaux utilisant le même protocole. Ils reconnaissent la provenance des données qui leur parviennent, et ne traitent que celles qui transitent d'un réseau à un autre, les trames échangées au sein d'un même réseau n'étant pas transmises, ce qui assure une confidentialité accrue entre les réseaux reliés.

1.5.3 Le routeur (Router)

Les routeurs peuvent être comparés à des "carrefours" de réseaux, n'étant pas, contrairement aux deux dispositifs précédents, limités à la connexion de deux réseaux au maximum (ils comportent généralement de 4 à 16 ports).
Le chemin emprunté par les données est prédéfini dans une table de routage, et optimisé selon des critères de longueur de chemin (nombre de sauts pour atteindre la machine visée), ou de temps (encombrement du réseau).

1.5.4 Le concentrateur (HUB)

Le concentrateur est un boîtier qui a la fonction de répéteur. Mais sa fonction principale, est de pouvoir concentrer plusieurs lignes en une seule. On peut y connecter plusieurs stations, dont le nombre dépend du type de HUB. Un HUB sera connecté sur un autre HUB ou sur un serveur qu'avec une seule et unique ligne.

1.5.5 Le commutateur (Switch)

Le commutateur (ou Switch) est un système assurant l'interconnexion de stations ou de segments d'un LAN en leur attribuant l'intégralité de la bande passante, à l'inverse du concentrateur qui la partage. Les commutateurs ont donc été introduits pour augmenter la bande passante globale d'un réseau d'entreprise et sont une évolution des concentrateurs Ethernet (ou HUB).

1.5.5.1 Commutateur niveau 2

Un commutateur niveau 2 agit au niveau des couches physique et logique (niveau 1 et niveau 2). Il ne traite que les trames MAC. On parle de commutation de niveau 2 ou layer 2 switching.

1.5.5.2 Commutateur niveau 3

Un commutateur niveau 3 agit au niveau de la couche réseau (niveau 3). Il ne traite que les paquets IP. C'est l'équivalent d'un routeur mais en beaucoup performant. On parle de commutation niveau 3 ou layer 3 switching.

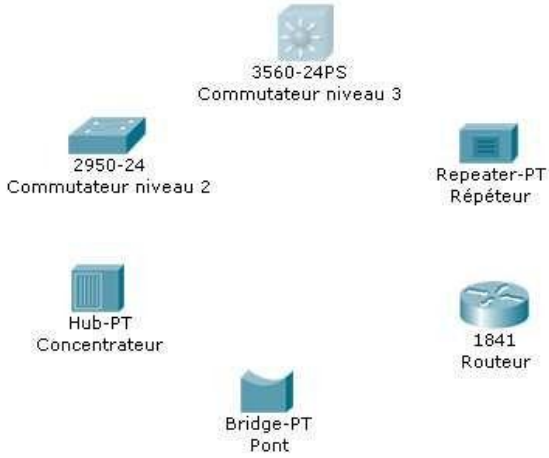


Figure 1.06 : *Symboles des équipements réseau*

1.6 Les techniques de commutation

Pour transporter des informations, il faut déterminer une technique de transfert. En d'autres termes, il faut savoir comment transférer un paquet depuis la machine source jusqu'à la machine réceptrice. La commutation est l'établissement d'une connexion temporaire entre deux points d'un réseau. On peut faire de la commutation de circuit qui utilise le réseau téléphonique (RTC), et de la commutation de paquets qui utilise le réseau (IP) Internet….

1.6.1 La commutation de circuits

Elle consiste à créer dans le réseau un circuit particulier entre l'émetteur et le récepteur avant que ceux-ci ne commencent à échanger les informations. Ce circuit est propre aux deux entités communicantes et sera libérer en fin de communication. Si pendant un certain temps les deux entités ne s'échangent pas de données, le circuit reste quand même attribué.
Toutes les données suivent le même chemin tout au long de la communication.
Exemple : Le réseau RTC.

1.6.2 La commutation de messages

Un message est une suite d'informations formant un tout, par exemple un fichier ou une ligne de commande tapée au clavier d'un ordinateur. La commutation de message consiste à envoyer un

message de l'émetteur jusqu'au récepteur en passant de nœuds de commutation à un nœud de commutation. Chaque nœud de commutation attend d'avoir reçu complètement le message avant de le réexpédier au nœud suivant.

Cette technique nécessite de prévoir de grandes zones mémoire dans chaque nœud du réseau ou un contrôle de flux pour ne pas saturer le réseau.

1.6.3 La commutation de paquets

Un paquet est une suite d'octets, dont le contenu n'à pas forcément une signification et ne pouvant pas dépasser une taille fixée par avance .Apparu dans les années 70 pour résoudre le problème d'erreur de commutation de messages.

Un message émis est découpé en paquets. On parle de segmentation du message, les paquets sont commutés dans le réseau comme dans le cas des messages. La bonne liaison vers le destinataire est trouvée grâce à une table dite de commutation (ou de routage pour la couche 3). Le message est reconstitué à partir du réassemblage des paquets reçus par le destinataire.

1.7 Les types de supports

1.7.1 Le câble à paires torsadées blindées

Un câble à paires torsadées blindées (ou câble STP) est un média utilise deux paires de fils enveloppées dans un revêtement tressé ou un film métallique.

Le câble STP protège le faisceau entier de fils à l'intérieur du câble ainsi que les paires de fils individuelles. Le câblage STP offre une meilleure protection parasitaire que le câblage UTP, mais à un prix relativement plus élevé. [1]

1.7.2 Le câble à paires torsadées non blindées

Le câblage UTP, terminé par des connecteurs RJ-45, est un support en cuivre courant pour l'interconnexion de périphériques réseau, tels que des ordinateurs, avec des périphériques intermédiaires, tels que des routeurs et commutateurs réseau.

Des situations différentes peuvent exiger des câbles UTP répondant à différentes conventions de câblage. Ceci signifie que les fils individuels du câble doivent être connectés dans des ordres différents à diverses séries de broches des connecteurs RJ-45.

1.7.3 Le câble coaxial

Un câble coaxial se compose d'un conducteur de cuivre entouré d'une couche de matériau isolant flexible. Sur ce matériau isolant, une torsade de cuivre ou un film métallique constitue le second fil du circuit qui agit comme protecteur du conducteur intérieur. Cette seconde couche, ou blindage, réduit également les interférences électromagnétiques externes. La gaine du câble enveloppe le blindage. Tous les éléments du câble coaxial entourent le conducteur central. Comme ils partagent tous le même axe, cette construction est dite coaxiale.

1.7.4 La fibre optique

Le câblage en fibre optique utilise des fibres de verre ou de plastique pour guider des impulsions lumineuses de la source à la destination. Les bits sont codés sur la fibre comme impulsions lumineuses. Le câblage en fibre optique prend en charge des débits de bande passante de données brutes très élevés. La plupart des normes de transmission actuelles n'approchent cependant pas encore la bande passante potentielle de ce support.

1.7.5 Les supports sans fils

Les supports sans fil transportent des signaux électromagnétiques à des fréquences radio et micro-ondes qui représentent les chiffres binaires des communications de données. En tant que support réseau, la transmission sans fil n'est pas limitée aux conducteurs ou voies d'accès, comme les supports en cuivre et à fibre optique.

Les technologies de communication de données sans fil fonctionnent bien dans les environnements ouverts. Cependant, certains matériaux de construction utilisés dans les bâtiments et structures, ainsi que le terrain local, limitent la couverture effective. De plus, la transmission sans fil est sensible aux interférences et peut être perturbée par des appareils aussi courants que les téléphones fixes sans fil, certains types d'éclairages fluorescents, les fours à micro-ondes et d'autres communications sans fil.

1.8 Conclusion

Dans ce chapitre on a vu les grands principes d'un réseau informatiques. Nous y avons étudié les différents types de réseau, les équipements réseau, les types de supports ainsi que le modèle OSI. Pour échanger des données il faut donc des équipements matériels et des équipements logiciels. Dans la partie suivante, nous allons intéresser un peu plus sur la conception d'un réseau d'entreprise et les étapes clés pour une bonne conception du réseau.

.

CHAPITRE 2
CONCEPTION DE RESEAU D'ENTREPRISE

2.1 Conception d'un réseau viable

Un réseau viable et de qualité ne se crée pas par accident. Il est le fruit du travail des concepteurs et des techniciens réseau, qui identifient les besoins de l'entreprise et choisissent les solutions les mieux adaptées pour y répondre.

Les utilisateurs d'un réseau ne se rendent généralement pas compte de la complexité que compose le réseau. Pour eux, le réseau n'est rien d'autre qu'un moyen d'accéder aux applications dont ils ont besoin, au moment où ils en ont besoin. [5][6]

2.2 Besoins des entreprises et objectifs de conception fondamentaux

Les entreprises ont chacun leur besoin particulier pour leur réseau. Chacun d'entre eux a leurs exigences mais, en générale, ils sont classés dans les catégories suivantes : [7][8]

- **Disponibilité** : Le réseau doit être disponible et fonctionnel en permanence, même en cas de rupture de liaison, de panne matérielle ou de surcharge.
- **Fiabilité** : Il doit offrir un accès fiable aux applications et des temps de réponse raisonnables d'un hôte à l'autre.
- **Sécurité** : Il doit être sécurisé. Les données transmises sur le réseau doivent être protégées, de même que celles stockées sur les périphériques qui y sont connectés.
- **Extensibilité** : Le réseau doit être facile à modifier pour pouvoir s'adapter à la croissance et aux besoins de l'entreprise.
- **Facilité de gestion** : Les pannes occasionnelles étant inévitables, le dépannage du réseau doit être facile. La détection et la résolution des problèmes ne doivent pas prendre trop de temps.

2.3 Conception de réseau hiérarchique

2.3.1 Modèle de réseau hiérarchique

Le modèle de conception hiérarchique est un outil pour la conception d'une infrastructure de réseau fiable. Il fournit une vue modulaire d'un réseau, simplifiant ainsi la conception et la construction d'un réseau extensible.

Une conception hiérarchique permet de regrouper des périphériques en un certain nombre de réseaux distincts qui sont alors organisés en couches.

Cela se fait donc en divisant un réseau en trois couches :

- **Couche d'accès** : permet à un utilisateur d'accéder aux périphériques réseau. Dans un campus de réseau, la couche d'accès intègre généralement des périphériques de réseau local commutés présentant des ports qui fournissent une connectivité aux stations de travail et aux serveurs. Dans l'environnement de réseau étendu, elle peut permettre à des télétravailleurs ou des sites distants d'accéder au réseau d'entreprise grâce à la technologie de réseau étendu.
- **Couche de distribution** : agrège les locaux techniques, en utilisant des commutateurs pour segmenter des groupes de travail et pour isoler les problèmes de réseau au sein d'un environnement de campus. De même, la couche de distribution agrège des connexions de réseau étendu à la périphérie du campus et fournit une connectivité basée sur des stratégies.
- **Couche cœur de réseau** (également appelée réseau fédérateur) : réseau fédérateur à haut débit conçu pour commuter des paquets le plus rapidement possible. Le cœur de réseau étant un élément essentiel pour la connectivité, il doit fournir une disponibilité élevée et s'adapter très rapidement aux changements. Il offre également des capacités d'évolutivité et de convergence rapide.

2.3.2 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.

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.[7]

2.3.3 Les architectures d'entreprise Cisco :

Les architectures d'entreprise Cisco permettent de diviser une conception hiérarchique à trois couches en différentes zones modulaires. Les modules représentent des zones possédant une connectivité physique ou logique différente. Ils indiquent où ont lieu les différentes fonctions au sein du réseau. Cette modularité accroît la flexibilité dans la conception du réseau et facilite la mise en œuvre et le dépannage. Il existe trois centres majeurs dans la conception de réseau modulaire :

- *Campus d'entreprise* : cette zone contient les éléments de réseau nécessaires à une exploitation indépendante, au sein d'un réseau de campus ou de filiale.

- *Batterie de serveurs* : composant de campus d'entreprise ; la batterie de serveurs du centre de calcul protège les ressources de serveur et fournit une connectivité haut débit fiable et redondante.

- *Périphérie du réseau* d'entreprise : lorsque le trafic de données arrive au réseau campus, cette zone le filtre et le sépare des ressources extérieures, pour l'acheminer vers le réseau d'entreprise. Elle contient tous les composants nécessaires à une communication efficace et sécurisée entre le campus d'entreprise et les sites distants, les utilisateurs distants et Internet.

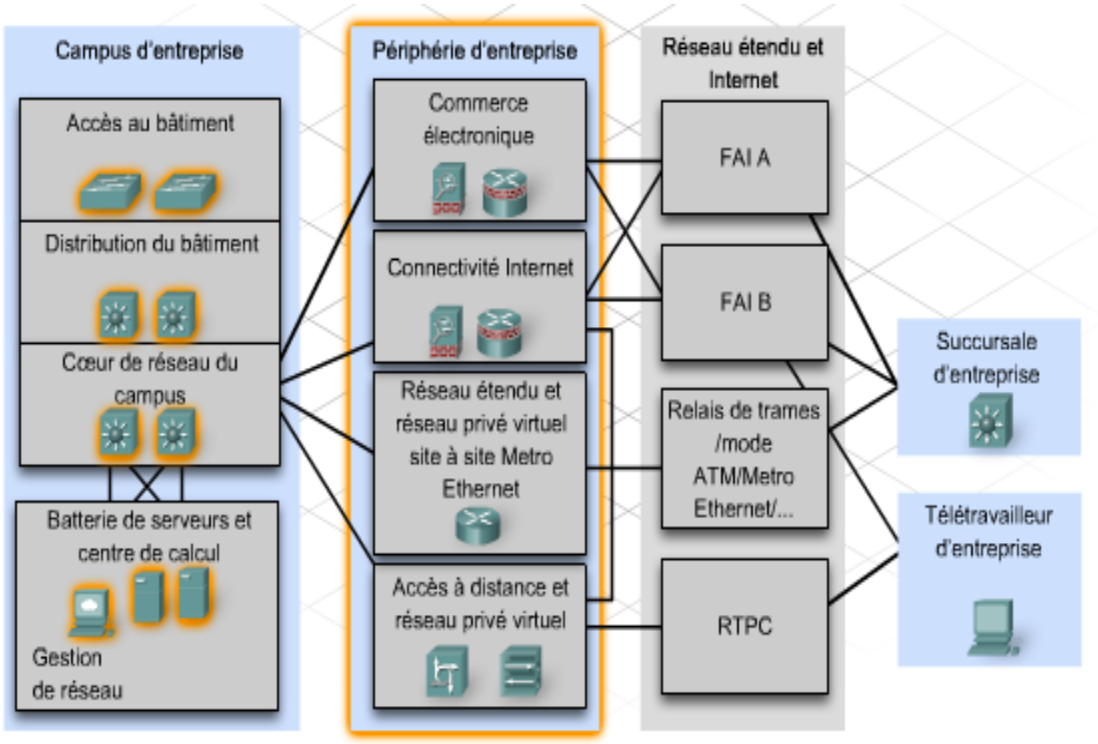


Figure 2.01 : *Architecture d'entreprise cisco*

La structure modulaire des architectures d'entreprise Cisco offre les avantages suivants en termes de conception :

- Elle crée un réseau déterministe doté de frontières clairement définies entre les modules. Ces points de démarcation clairs permettent au concepteur du réseau de savoir exactement d'où vient le trafic et où il va.
- Elle facilite le travail de conception en rendant chaque module indépendant. Le concepteur peut alors se concentrer sur les besoins de chaque zone, de manière individuelle.
- Elle améliore l'extensibilité du système en permettant à l'entreprise de rajouter facilement de nouveaux modules. Lorsque la complexité du réseau augmente, il suffit au concepteur d'ajouter de nouveaux modules fonctionnels.
- Elle permet au concepteur d'ajouter des services et des solutions sans avoir à modifier la structure sous-jacente du réseau.

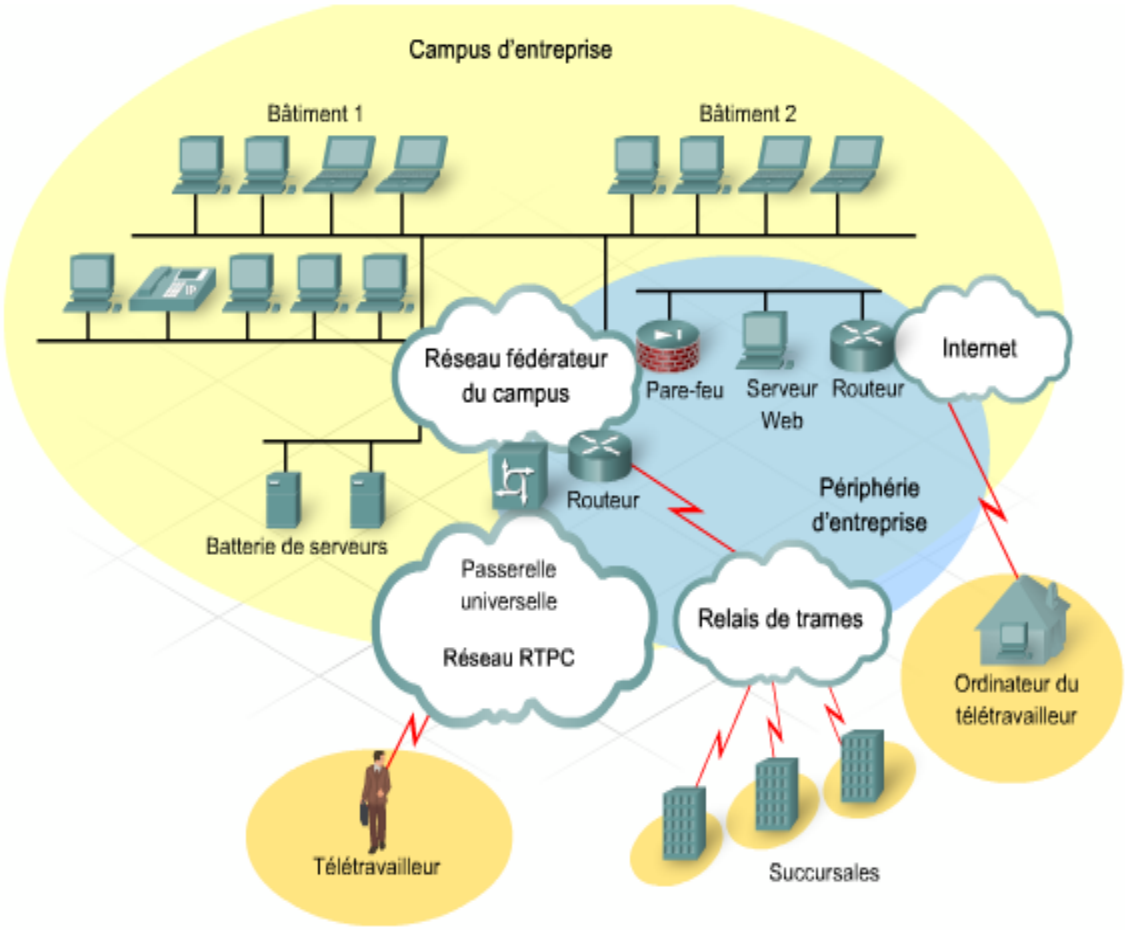


Figure 2.02 : *Architecture du réseau*

2.4 Méthodologie de conception

Les projets de conception de réseaux de grande envergure se divisent généralement en trois étapes distinctes :

Étape 1 : identification des besoins du réseau.

Étape 2 : caractéristiques du réseau actuel.

Étape 3 : conception de la topologie et des solutions de réseau.

2.4.1 Identification des besoins du réseau

Le concepteur travaille en étroite collaboration avec le client afin de documenter les objectifs du projet. Ceux-ci se divisent généralement en deux catégories :

- Objectifs commerciaux : de quelle façon le réseau peut-il contribuer au succès de l'entreprise ?
- Spécifications techniques : de quelle façon la technologie est-elle mise en œuvre au sein du réseau ?

2.4.2 Caractéristiques du réseau actuel

L'équipe réunit des informations sur le réseau et les services existants, puis les analyse. La fonctionnalité du réseau existant doit être comparée aux objectifs définis pour le nouveau projet. Le concepteur détermine quels équipements, infrastructures et protocoles existants peuvent être réutilisés, le cas échéant, puis quels nouveaux équipements et protocoles doivent être ajoutés en complément.

2.4.3 Conception de la topologie du réseau

L'approche descendante constitue l'une des stratégies les plus courantes de la conception de réseau. Selon cette méthode, le concepteur détermine tout d'abord les besoins en matière d'applications et de services réseau, puis conçoit un réseau capable de les prendre en charge.

Une fois la conception terminée, un prototype est créé ou un test de faisabilité est réalisé. Cette approche garantit que le nouveau réseau est conforme aux attentes du client et ce, avant la mise en œuvre.

L'une des erreurs les plus courantes des concepteurs de réseau est leur incapacité à évaluer correctement l'envergure du nouveau réseau.

- Définition de l'étendue du projet

Lorsqu'il définit les besoins de la nouvelle structure, le concepteur identifie les problèmes pouvant affecter l'ensemble du réseau et ceux affectant uniquement certaines sections. Une évaluation incorrecte de l'impact d'un besoin donné a tendance à accroître l'étendue du projet, par rapport aux

estimations initiales. Cette erreur peut avoir des conséquences graves sur la mise en œuvre du nouveau réseau, en termes de coût et de respect des délais.

- Conséquences sur l'ensemble du réseau

Les besoins ayant un impact sur l'ensemble du réseau incluent :

- ajout de nouvelles applications réseau et modification majeure des applications existantes, tels les changements de base de données ou de structure DNS
- amélioration de l'efficacité de l'adressage réseau ou modification des protocoles de routage ;
- intégration de nouvelles mesures de sécurité
- ajout de nouveaux services réseau, tels que le trafic vocal, la mise en réseau de contenu et le réseau de stockage
- déplacement physique des serveurs, dans une batterie de serveurs de centre de calcul.

2.4.4 Préventions de pannes

Le concepteur du réseau doit faire en sorte de créer un réseau résistant aux défaillances et permettant une reprise rapide en cas de panne. Les principaux routeurs et commutateurs peuvent être équipés des éléments suivants :

- ventilateurs et alimentations doubles ;
- conception à châssis modulaire ;
- modules de gestion supplémentaires.

Bien qu'ils augmentent le coût du réseau, les composants redondants représentent généralement un investissement très utile. Lorsque cela est possible, les périphériques de la couche cœur de réseau doivent être dotés de composants remplaçables à chaud, qui peuvent être installés ou démontés sans avoir à mettre le périphérique hors tension. La durée de réparation et les temps d'interruption des services réseau s'en trouvent ainsi réduits.

Les grandes sociétés installent souvent des générateurs et des systèmes ASC puissants. Ces systèmes évitent qu'une coupure d'électricité mineure n'entraîne des pannes importantes sur l'ensemble du réseau.

2.4.5 La prise en charge des réseaux étendus :

Lorsqu'une entreprise s'agrandit pour inclure des succursales, des services de commerce électronique ou des activités globales, un réseau local (LAN) peut s'avérer insuffisant pour satisfaire ses besoins commerciaux. L'accès de réseau étendu (WAN) est devenu aujourd'hui essentiel dans la plupart des grandes entreprises.

De nombreuses technologies de réseau étendu permettent de répondre aux différents besoins des entreprises et de nombreuses méthodes permettent de faire évoluer le réseau. L'ajout d'un accès de réseau étendu implique des aspects supplémentaires, notamment la sécurité du réseau et la gestion des adresses. Ainsi, il n'est pas toujours simple de concevoir un réseau étendu et de sélectionner des services de réseau d'opérateur appropriés.

Dans cette partie de la conception, il faut déterminer les options suivantes :

- Option de liaison de connexion dédiée
- Option de connexion à commutation de circuits
- Option de connexion à commutation de paquets
- Option de connexion internet

2.5 Cycle de vie d'un réseau

Le monde des réseaux est aujourd'hui en pleine évolution. La mise en réseau dépasse le simple raccordement d'ordinateurs entre eux. Il s'agit aujourd'hui d'une approche intelligente, jouant un rôle clé dans l'amélioration des performances d'une entreprise. Les sociétés cherchent à étendre toujours plus leurs réseaux. Grâce aux avancées technologiques, elles peuvent offrir de nouveaux services et améliorer leur productivité.

2.5.1 Cycle PPDIOO

Le cycle PPDIOO a été conçu pour accompagner l'évolution des réseaux. Il s'agit d'une approche en six phases. Chacune de ces phases définit les activités requises pour déployer et faire fonctionner sans soucis les technologies Cisco. Cette méthode indique également comment optimiser les performances d'un réseau, tout au long de son cycle de vie.[7] [8]

Les six phases de Cisco Lifecycle Services sont les suivantes :

- Phase de préparation
- Phase de planification
- Phase de conception
- Phase d'implémentation
- Phase d'exploitation
- Phase d'optimisation

2.5.1.1 Phase de préparation

Lors de la phase de préparation, on définit les objectifs commerciaux attendus par le client. On peut donc y trouver le fait de :

- améliorer l'expérience du client
- réduire les coûts
- ajouter des services supplémentaires
- prendre en charge l'évolution de l'entreprise.

Ces objectifs offrent un cadre pour monter le dossier commercial. Ce dossier permet de justifier l'investissement financier requis pour l'implémentation de la nouvelle infrastructure. L'entreprise prend ainsi en compte les contraintes commerciales possibles, notamment en termes de budget, de personnel, de stratégie et de planification.

Ces objectifs commerciaux fixés, le concepteur du réseau propose alors les solutions adéquates à chacun d'entre eux et la stratégie à suivre pour la nouvelle concéption.

Cette stratégie identifie :

- les technologies avancées prenant en charge la nouvelle solution de réseau ;
- les applications et services de réseau, actuels et planifiés, ainsi que leur niveau de priorité en fonction des objectifs commerciaux ;
- le personnel, les processus et les outils requis pour prendre en charge l'exploitation et la gestion de la nouvelle solution technologique.

La phase de préparation a généralement lieu avant que l'entreprise émette une demande de proposition ou une demande de devis, qui définissent les conditions requises pour le nouveau réseau. Ils contiennent des informations sur les méthodes d'achat et d'installation des technologies de réseau, auxquelles l'entreprise a recours.

2.5.1.2 Phase de planification

Lors de la phase de planification, le concepteur du réseau effectue une évaluation complète du site et de son fonctionnement. Cette évaluation permet de déterminer l'état actuel des infrastructures de réseau, d'exploitation et d'administration du réseau.

Le concepteur identifie toutes les modifications à effectuer, qu'elles soient physiques, environnementales ou électriques. Elle évalue également la capacité de l'infrastructure actuelle d'exploitation et de gestion de réseau à prendre en charge la nouvelle solution technologique. Tous les changements apportés à l'infrastructure, au personnel, aux processus et aux outils doivent être terminés avant l'implémentation de la nouvelle solution.

Cette phase permet également de déterminer les applications personnalisées requises, qui amélioreront la fonctionnalité du nouveau réseau. Le concepteur du réseau crée un document contenant tous les éléments requis en termes de conception.

2.5.1.3 Plan de projet

Lors de cette phase, le concepteur du réseau et le client mettent au point un plan qui permettra de gérer l'ensemble du projet. Ce plan de projet inclut les éléments suivants :

- tâches à réaliser
- calendrier et échéances clés
- risques et contraintes
- responsabilités
- ressources requises.

Le plan doit être conforme aux objectifs commerciaux précédemment établis, en termes d'étendue, de coût et de ressources.

2.5.1.4 Phase de conception

Lors de la phase de conception, le concepteur oriente son travail sur les exigences initialement définies durant la phase de planification.

Le document de conception est créé conformément aux spécifications identifiées lors des phases de préparation et de planification, en termes de :

- Disponibilité
- Évolutivité
- Sécurité
- Facilité de gestion

La conception doit être suffisamment flexible pour permettre d'effectuer les modifications ou les ajouts nécessaires si les besoins ou les objectifs évoluent. La nouvelle technologie doit être intégrée à l'infrastructure d'exploitation et de gestion de réseau existante.

À la fin de la phase de conception, le concepteur du réseau met au point des plans pour guider l'installation et garantir que le résultat final soit conforme aux souhaits du client. Ces plans incluent :

1. la configuration et le test de la connectivité
2. l'implémentation du système proposé
3. la démonstration de la fonctionnalité du réseau
4. la migration des applications de réseau
5. la validation du fonctionnement du réseau
6. la formation des utilisateurs finaux et du personnel d'assistance.

La conception du réseau est finalisée lors de la phase de conception. Les nouveaux équipements et technologies choisis sont testés. Une étude de la conception proposée permet de confirmer que les objectifs commerciaux sont remplis. Une proposition finale est créée, pour passer à la phase d'implémentation.

2.5.1.5 Phase d'implémentation

La phase d'implémentation commence après la conception et que le client l'a approuvée. Le réseau est alors construit conformément aux spécifications de conception prédéfinies. La phase d'implémentation permet de vérifier si la conception de réseau est viable ou non.

On passe alors au test de la nouvelle solution réseau dans un environnement contrôlé. Ce qui permet d'identifier et de résoudre les éventuels problèmes d'implémentation avant l'installation réelle.

Une fois les problèmes éventuels résolus, on intègre la nouvelle solution au réseau existant. Lorsque l'installation est terminée, des tests complémentaires sont effectués.

Le test d'acceptation du système permet de vérifier que le nouveau réseau est conforme aux objectifs commerciaux et aux spécifications de conception requises. Le résultat de ce test est consigné et intégré à la documentation fournie au client. Si une formation est requise pour le personnel du stade, elle doit être effectuée durant cette phase.[12]

2.5.1.6 Phase d'exploitation

Les phases d'exploitation et d'optimisation sont permanentes. Elles correspondent à l'exploitation quotidienne du réseau. Elle permet à l'entreprise d'obtenir des performances optimales en termes d'évolutivité, de disponibilité, de sécurité et de facilité de gestion.

Une fois le nouveau réseau installé, le personnel du stade assure l'administration du réseau afin de vérifier que celui-ci fonctionne conformément aux spécifications de conception définies lors des phases de préparation et de planification.

a. Définition des stratégies et des procédures

Les stratégies et les procédures sont des éléments nécessaires à la gestion des problèmes de réseau, notamment :

- les incidents de sécurité ;
- les changements de configuration ;
- l'achat d'équipement.

2.5.1.7 Phase d'optimisation

L'optimisation du réseau est un processus continu et permanent. Elle a pour objectif d'améliorer les performances et la fiabilité du réseau, en identifiant et en résolvant les problèmes potentiels avant qu'ils ne se concrétisent. Ceci garantit la réalisation des objectifs commerciaux et la conformité aux spécifications définies par l'entreprise. [13] Voici quelques-uns des problèmes de réseau les plus courants détectés lors de la phase d'optimisation :

- incompatibilité entre fonctions
- nombre de liaisons insuffisant
- problèmes de performances au niveau des périphériques, lorsque plusieurs fonctions sont activées
- évolutivité des protocoles.

La stratégie technologique et le fonctionnement du réseau doivent s'adapter à mesure que les objectifs commerciaux évoluent. Il peut même parfois être nécessaire de passer par une nouvelle étape de conception, en répétant le cycle PPDIOO.

2.6 Importance des performances des applications

La plupart des utilisateurs de services réseau disposent de très peu d'informations à propos du réseau sous-jacent ou de la conception du réseau. Leur expérience est basée sur leur interaction avec les applications exécutées sur le réseau.

La collecte de données statistiques en provenance de routeurs, de serveurs et d'autres périphériques réseau permet de déterminer si un système fonctionne conformément aux spécifications du fabricant. Toutefois, les considérations techniques seules ne garantissent pas la réussite sur le marché.

La réussite dépend de la manière dont le client, les fournisseurs et les prestataires considèrent les performances du réseau.

Pour les utilisateurs finaux, les performances des applications sont basées sur :

- La disponibilité
- La réactivité

2.7 Caractéristiques des applications réseaux

2.7.1 Caractéristiques des différentes catégories d'applications

Dans un réseau existant, la définition des caractéristiques d'une application permet au concepteur du réseau d'incorporer des objectifs commerciaux et des spécifications techniques à sa conception.

La définition des caractéristiques des applications implique l'examen des aspects suivants des applications réseau :

- fonctionnement des applications sur le réseau ;
- spécifications techniques de l'application ;
- interaction des applications entre elles sur le réseau.

À partir des données collectées lors des premières phases du processus de conception, le concepteur détermine les applications stratégiques. Il évalue le fonctionnement de ces applications avec le réseau proposé. Le processus de définition des caractéristiques fournit des informations sur l'utilisation de la bande passante du réseau et les temps de réponse pour les applications spécifiques. Ces paramètres influent sur les décisions de conception, notamment :

- la sélection du support de transmission
- les estimations de bande passante requise.

Le trafic des différents types d'applications génère des demandes de réseau variées. Le concepteur de réseau reconnaît quatre principaux types de communication d'application :

- Client à client
- Client à serveur distribué
- Client à batterie de serveurs
- Client au périmètre d'entreprise

Sur un réseau existant, la première étape de la définition des caractéristiques des applications consiste à collecter autant de données que possible à propos du réseau. Cela inclut la collecte de données liées à l'organisation, l'audit du réseau, l'analyse du trafic.

2.7.1.1 Données organisationnelles

Les données organisationnelles se composent de la documentation existante relative au. Lors des premières phases de conception, l'obtention de données est facile mais pas toujours fiable. Par exemple, les modifications des applications (mises à niveau ou logiciels installés par l'utilisateur) peuvent être dépourvues de documentation ou passer inaperçues.

2.7.1.2 Audit du réseau

Un audit de réseau rassemble des informations sur les périphériques réseau, surveille le trafic et révèle les détails de la configuration actuelle du réseau.

2.7.1.3 Analyse du trafic

L'analyse du trafic fournit des informations sur l'utilisation du réseau par les applications et les protocoles. Elle peut dévoiler des défaillances dans le réseau. Par exemple, plusieurs applications à bande passante élevée utilisant le même support peuvent générer des données très volumineuses, ce qui pourrait devenir une faiblesse dans la conception actuelle.

2.7.2 Impact des caractéristiques d'applications sur la conception réseau

Les performances des applications dépendent des types de matériel installés sur un réseau. Un réseau complexe contient plusieurs types de matériel. Chacun de ces types de périphériques peut retarder la réponse de l'application aux requêtes de l'utilisateur. Ce retard affecte la satisfaction du client quant aux performances de l'application. Par exemple, des retards dus au matériel peuvent affecter les applications utilisées pour l'audio et la vidéo, ce qui entraîne une dégradation des performances. Voici ce qui peut causer ces retards :

1. temps de traitement d'un routeur pour acheminer le trafic
2. commutateurs anciens ne pouvant pas traiter les charges de trafic générées par les applications modernes.

L'une des meilleures façons de garantir des performances élevées est d'utiliser l'approche descendante. Cette approche adapte la conception de l'infrastructure physique aux besoins des applications réseau. Les périphériques réseau sont choisis uniquement après une analyse approfondie des spécifications techniques.

Les applications sur un réseau moderne produisent une gamme de paquets. Ces paquets sont de tailles variées et présentent divers groupes de protocoles, différentes tolérances aux retards ainsi que d'autres caractéristiques. Lorsque les exigences de service de ces différentes applications entrent en conflit, des problèmes de performances peuvent s'ensuivre. Lors de l'ajout d'une nouvelle application, le concepteur du réseau doit envisager l'impact des applications existantes sur les performances, ainsi que les performances prévisibles de l'application dans différentes configurations et conditions de réseau.

2.8 Conclusion

Nous avons vu que pour mettre un place un projet de conception de réseau, il faut définir les objectifs commerciaux voulu par le client. Ensuite, faire en sorte que ces objectifs qu'on a recensé soit prise en charge par la nouvelle conception. Dans ce long processus de conception, on doit tenir compte des objectifs et exigences, de la capacité du réseau déjà en place et aussi des nouvelles technologies qu'on doit intégrer. La phase de conception du réseau doit se faire en six étapes appelées cycle PPDIOO. Un point très important sur la conception du réseau est aussi la sécurité sur le réseau. Dans le prochain chapitre, nous allons appliquer ces études au sein d'une entreprise.

CHAPITRE 3
CONCEPTION DU RESEAU DU MFB

3.1 Présentation du MFB

3.1.1 Rôle du MFB

Le MFB (Ministère de Finances et des Budgets) est le ministère qui a pour rôle :

- d'élaborer et de mettre en œuvre la politique financière, fiscale et budgétaire de l'Etat comprenant: l'élaboration des projets de Lois de Finances, le contrôle et la synthèse de l'exécution des Lois de Finances, les travaux d'assiette, de contrôle et de recouvrement des ressources fiscales et douanières, la gestion et le contrôle du patrimoine de l'Etat et des collectivités locales, la gestion de la trésorerie et des dettes intérieure et extérieure de l'Etat.
- de partager avec d'autres entités le pilotage de l'économie et la maîtrise des grands équilibres économiques, financiers et monétaires qui consistent en l'établissement, le suivi et le perfectionnement du tableau de bord et la conduite des travaux et d'analyses susceptibles d'éclairer les choix et décisions du Gouvernement en matière budgétaire et financière.
- d'assurer la gestion et le suivi-évaluation des aides extérieures et contribue à l'harmonisation de la coopération avec les bailleurs de fonds.
- d'assurer la tutelle des institutions financières et des établissements publics. [14]

3.1.2 Organisation du MFB

L'organisation générale du Ministère des Finances et du Budget est fixée comme suit :

- le Cabinet du Ministre
- le Secrétariat Général
- la Direction Générale de l'Audit Interne placée sous l'autorité directe du Ministre
- la Direction Générale du Contrôle Financier placée sous la tutelle et le contrôle technique du Ministre
- l'Autorité de Régulation des Marchés Publics placée sous la tutelle technique du Ministre
- la Cellule de Coordination des Projets de Relance Economique et d'Actions Sociales.[14]

Organigramme du Ministère des Finances et du Budget - République de Madagascar - 2015

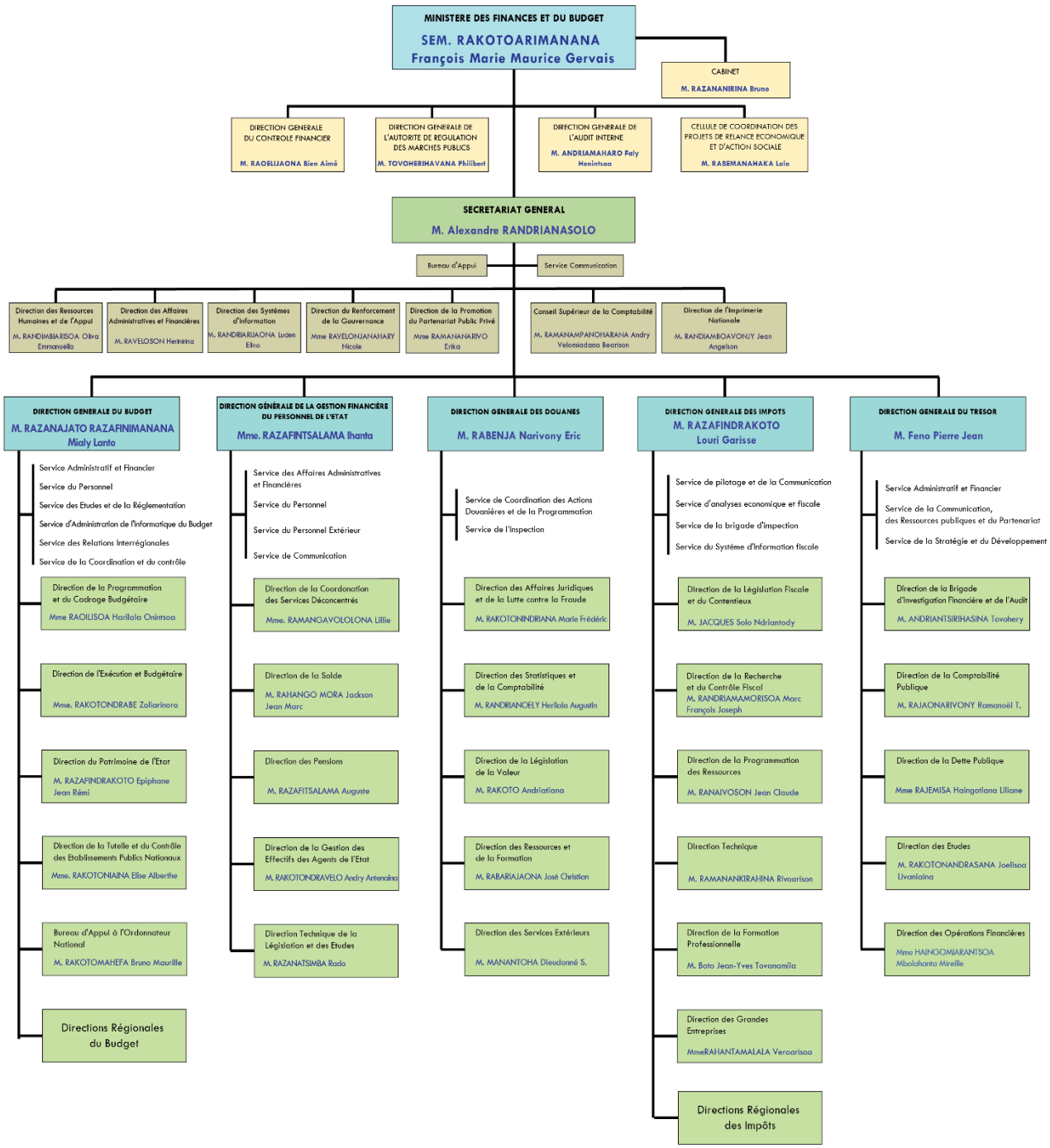


Figure 3.01 : *Organigramme MFB*

3.2 Réseau actuel du MFB

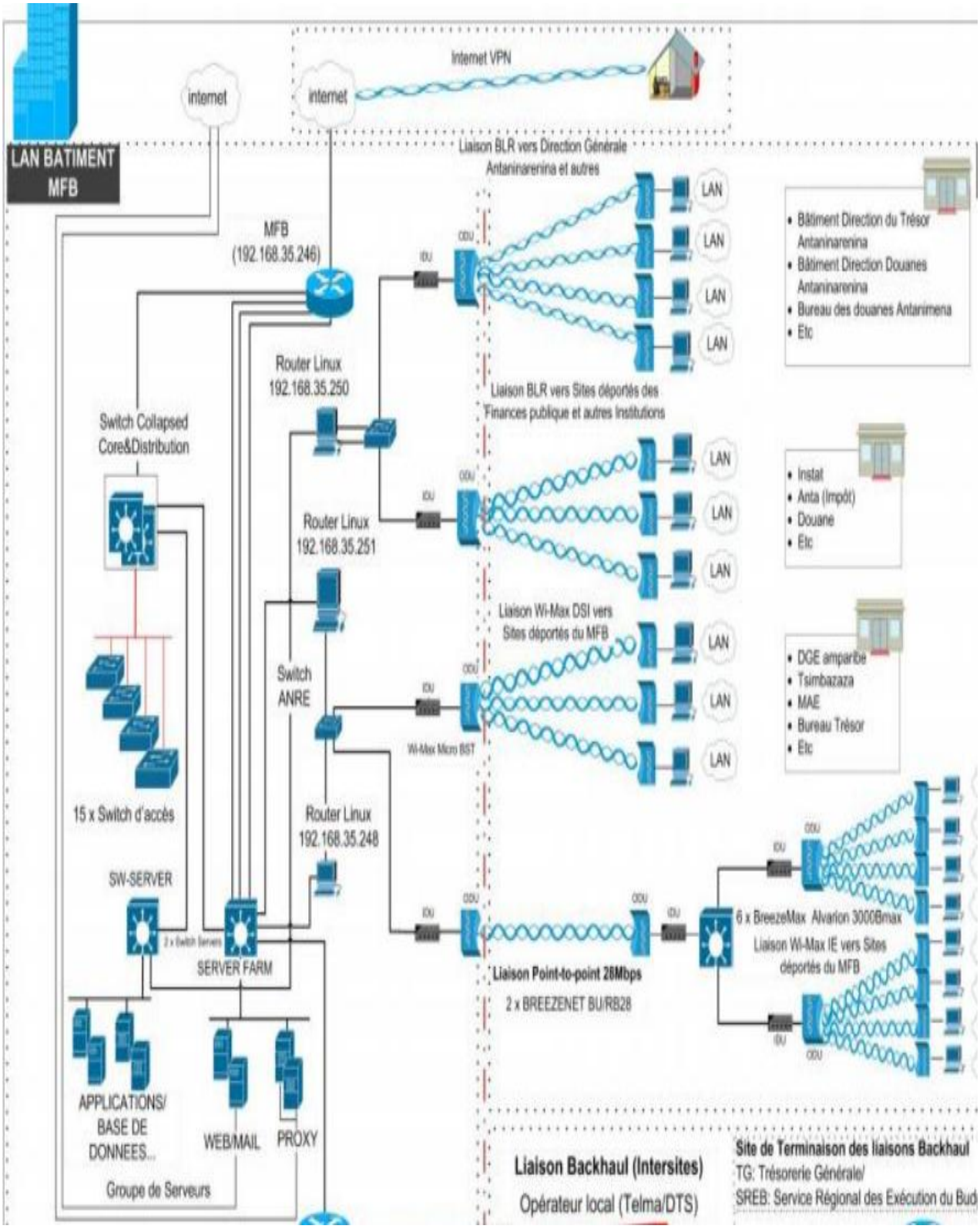


Figure 3.02 : *Architecture global du MFB*

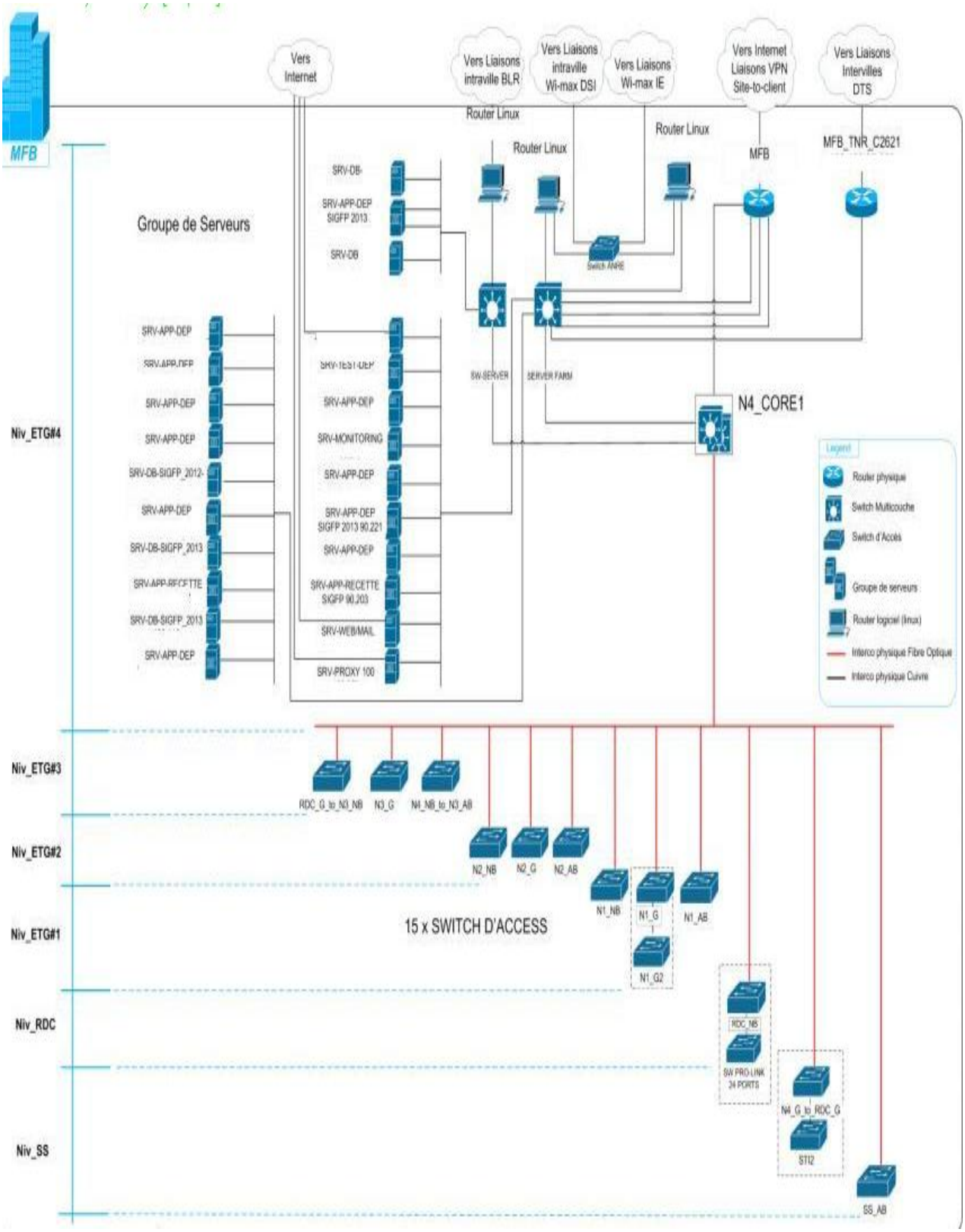


Figure 3.03 : *Architecture globale du réseau LAN*

3.3 La conception du réseau du MFB :

Comme précédemment vu dans le chapitre 2, la conception se fait en 3 étapes : identification des besoins du réseau, caractéristiques du réseau actuel, conception de la topologie et des solutions de réseau.

3.3.1 Identifications des besoins du réseau :

3.3.1.1 Disponibilité :

Le réseau doit être disponible 24 heures sur 24, 7 jours sur 7. Les pannes et les ruptures de liaison ne doivent en aucun cas avoir de l'impact sur la disponibilité du réseau.

Afin de répondre à cette exigence de temps de fonctionnement de près de 100 % des applications réseau, on doit implémenter des caractéristiques de disponibilité et de redondance élevées dans la nouvelle conception.

3.3.1.2 Performances:

La performance est l'une des clés de la réussite de la conception d'un réseau. Il faut créer une liste de considérations et d'objectifs de conception qui pourraient affecter les performances de ces applications prioritaires. Il doit offrir un accès fiable aux applications et des temps de réponse raisonnables d'un hôte à l'autre.

3.3.1.3 Sécurité :

La sécurité est un domaine de la conception de réseau qu'il ne faut pas négliger. Bien qu'il soit parfois nécessaire de trouver des moyens moins coûteux ou plus complexes de sécuriser un réseau, il est inacceptable d'ignorer la sécurité pour ajouter d'autres fonctionnalités au réseau.

3.3.1.4 Extensibilité :

L'ajout de nouvelle fonctionnalité sur la nouvelle conception ne doit pas être complexe. Le réseau doit être facile à modifier pour pouvoir s'adapter à la croissance et aux besoins de l'entreprise.

3.3.1.5 Facilité de gestion

L'un des objectifs principaux de la nouvelle conception doit être la facilité de maintenance du réseau et la détection des pannes ne doit pas être trop difficile à trouver.

3.3.2 Caractéristiques du réseau actuel

3.3.2.1 Les points faibles :

Avant d'intégrer de nouvelles fonctionnalités et de nouvelles technologies, la nouvelle conception doit d'abord palier toutes les faiblesses identifiées du réseau actuel.

- Conception de réseau linéaire :

Ce type de conception ne permet pas d'extensibilité : le réseau ne peut donc pas s'étendre sans que cela ait un impact sur les performances.

Il n'y a pas aussi de segmentation du réseau, donc impossible d'isoler ou filtrer le trafic.

- Pas de redondance :

Une panne sur un matériel du réseau peut entrainer la non-disponibilité d'une partie du réseau. De plus, on a des domaines défaillants étendus c'est-à-dire que les défaillances de liaisons et de périphériques affectent de vastes zones du réseau.

- Faiblesse de la sécurité :

La sécurité déployé est trop faible, il n'y a pas de pare-feu dynamique donc il ne fait que le filtrage et n'empêche pas tout le trafic non autorisé ou indésirable. Il n'y a pas aussi de système IDS ou IPS implémenté sur le réseau.

3.3.3 Conception de la topologie et les solutions proposées

Le réseau local existant présente une topologie linéaire, sans liaison redondante et offrant très peu de sécurité. Nous allons alors concevoir un nouveau réseau répondant aux exigences de l'entreprise. Pour cela, on va concevoir la topologie des différentes couches d'un réseau hiérarchique et le schéma logique montrant l'interconnexion entre les différentes couches et les périphériques.

3.3.3.1 Conception de la topologie de la couche d'accès

Les exigences répertoriées sur la couche d'accès du nouveau réseau sont les suivantes :

- connectivité pour les périphériques réseau existants
- ajout d'un accès sans fil
- ajout de téléphones IP
- liaisons redondantes vers le réseau de la couche de distribution
- utilisation de VLAN

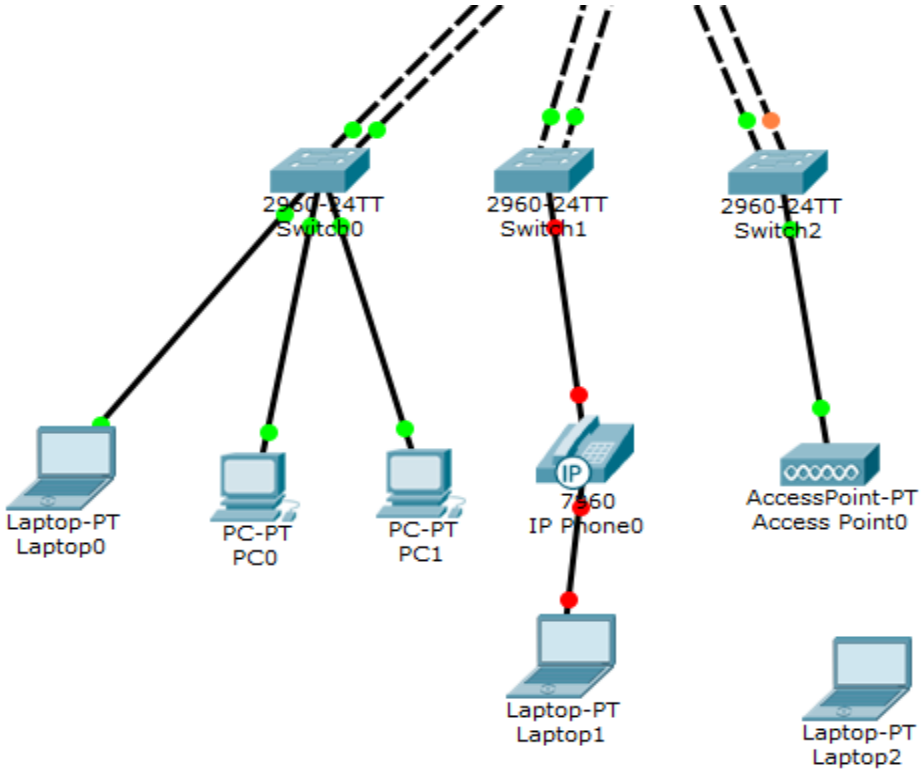


Figure 3.04 : *Topologie de la couche d'accès*

Sur la figure ci-dessus, on peut voir que les PC sont directement connectés au Telephone Ip. Ceci est possible parce que les téléphones IP et d'autres périphériques incluent un commutateur intégré qui permet le raccordement direct d'un PC sur le téléphone. Ce commutateur réduit le nombre de ports nécessaires dans le local technique pour le raccordement de périphériques supplémentaires.

a. Création de VLAN

On va créer des VLAN pour les différents départements comme la DSI, la DRH ou le DAAF. Les réseaux locaux virtuels permettent de segmenter le réseau.

Un VLAN permet à un administrateur réseau de créer des groupes de périphériques en réseau logique qui se comportent comme s'ils se trouvaient sur un réseau indépendant, même s'ils partagent une infrastructure commune avec d'autres réseaux locaux virtuels. [9]

b. Avantages d'un réseau local virtuel

La productivité des utilisateurs et l'adaptabilité du réseau sont des facteurs clés de croissance et de réussite de l'entreprise. L'implémentation de la technologie VLAN permet à un réseau d'assurer une prise en charge plus souple des objectifs de l'entreprise. Les principaux avantages des VLAN sont les suivants :

- **Sécurité :** les groupes contenant des données sensibles sont séparés du reste du réseau, ce qui diminue les risques de violation de confidentialité. Les ordinateurs de la faculté se trouvent sur le VLAN 10 et sont complètement séparés du trafic des données des étudiants et des invités.
- **Réduction des coûts :** des économies sont réalisées grâce à une diminution des mises à niveau onéreuses du réseau et à l'utilisation plus efficace de la bande passante et des liaisons ascendantes existantes.
- **Meilleures performances :** le fait de diviser des réseaux linéaires de couche 2 en plusieurs groupes de travail logiques (domaines de diffusion) réduit la quantité de trafic inutile sur le réseau et augmente les performances.
- **Atténuation des tempêtes de diffusion :** le fait de diviser un réseau en plusieurs réseaux VLAN réduit le nombre de périphériques susceptibles de participer à une tempête de diffusion. Comme l'explique le chapitre « Concepts et configuration de base de la commutation », la segmentation d'un réseau LAN empêche une tempête de diffusion de se

propager dans tout le réseau. Dans la figure, vous pouvez voir que bien que ce réseau comporte six ordinateurs, il n'y a que trois domaines de diffusion : Faculté, Étudiant et Invité.

- **Efficacité accrue du personnel informatique :** les VLAN facilitent la gestion du réseau, car les utilisateurs ayant des besoins réseau similaires partagent le même VLAN. Lorsque vous configurez un nouveau commutateur, toutes les stratégies et procédures déjà configurées pour le VLAN correspondant sont implémentées lorsque les ports sont affectés. Le personnel informatique peut aussi identifier facilement la fonction d'un VLAN en lui donnant un nom approprié. Dans la figure, pour être facilement identifiables, le VLAN 20 a été nommé « Étudiant », le VLAN 10 « Faculté » et le VLAN 30 « Invité ».
- **Gestion simplifiée de projets ou d'applications :** les VLAN rassemblent des utilisateurs et des périphériques réseau pour prendre en charge des impératifs commerciaux ou géographiques. La séparation des fonctions facilite la gestion d'un projet ou l'utilisation d'une application spécialisée, comme une plateforme de développement d'e-learning pour l'administration de la faculté. Il est également plus facile de déterminer la portée des effets de la mise à niveau des services réseau.

c. Communication inter-VLAN

Contrairement aux communications intra-vlan, c'est-à-dire la communication entre les mêmes vlans, l'inter-Vlan nécessite l'utilisation de couche 3 du modèle OSI avec les routeurs.[9] [13]

Il existe 3 façons de faire l'inter-Vlan :

- La legacy VLAN
- Router on a stick
- Multilayer Switch

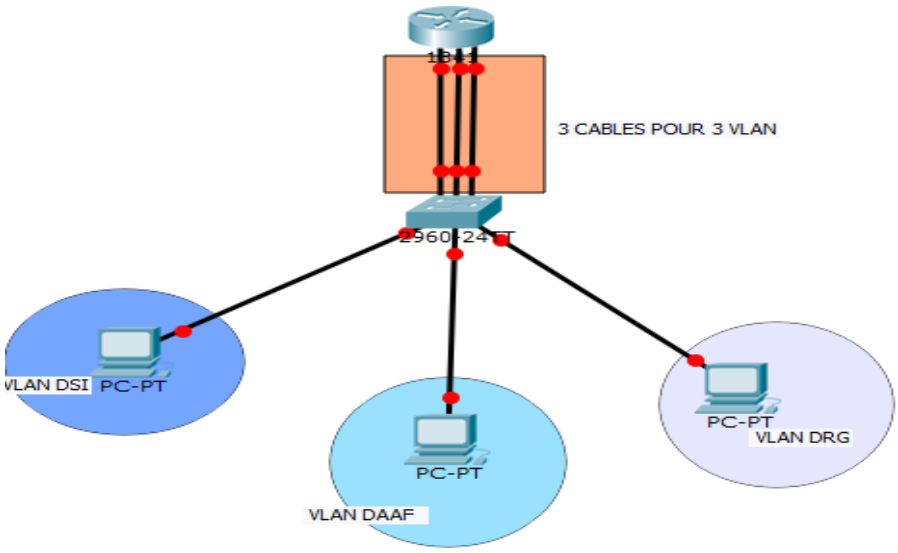


Figure 3.05 : *La legacy VLAN*

La legacy VLAN se fait en attachant chaque VLAN créé aux intérfaces du routeur. Il y a donc autant de connexions entre le switch et le routeur que de VLAN. Cette methode est très couteuse et également pas très pratiques. Ce n'est donc pas une solution adéquate.

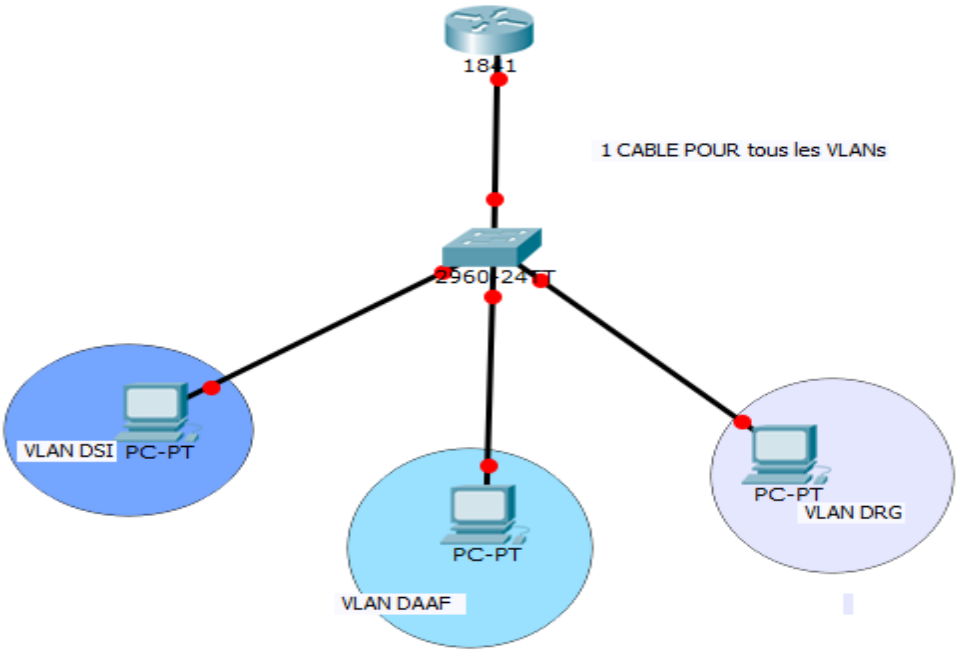


Figure 3.06 : *Router on a stick*

Pour trouver une solution à cette gaspillage, le router on a stick parait être une évidence à notre réseau. Cette technique permet d'utiliser qu'une seul interface pour gérer les communications entre les différents VLAN.

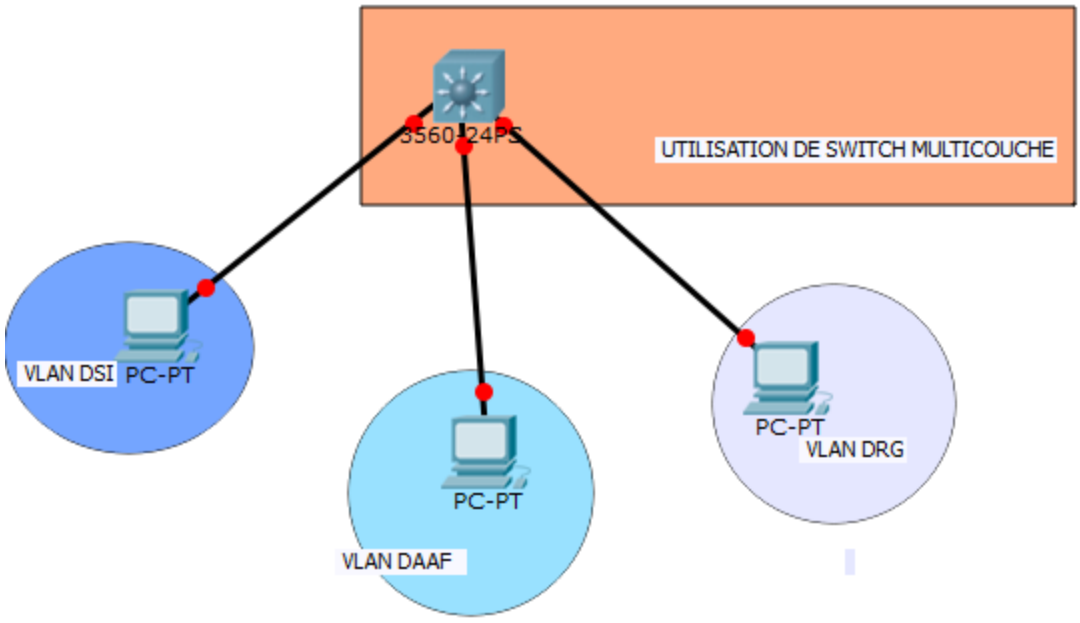


Figure 3.07 : *INTERVLAN par SWICH multicouche*

Mais nous allons utiliser une technique encore plus évolué que le router on-a-stick. Celle-ci consiste à unifier l'equipement switch et le router. Pour cela, on utilise le switch multicouche pour faire la communication intra-vlan et inter-vlan.

Elle nécessite la création des interfaces SVI sur le switch. Une interface SVI est une interface logique configurée pour un VLAN spécifique. Vous devez configurer une interface SVI pour un VLAN si vous voulez assurer le routage entre des VLAN ou fournir une connectivité d'hôte IP au commutateur. Par défaut, une interface SVI est créée pour le VLAN par défaut (VLAN 1) pour permettre l'administration à distance du commutateur.

d. Agrégation VLAN :

Il est difficile de décrire les VLAN sans parler des agrégations de VLAN. Nous avons expliqué que la segmentation en VLAN permet de contrôler les diffusions réseau et nous avons vu comment les agrégations de VLAN transmettent le trafic à différentes parties du réseau configurées dans un même VLAN. Dans la figure, les liaisons entre les commutateurs Comm1 et Comm2, et Comm1 et Comm3 sont configurées pour transmettre le trafic provenant des VLAN 10, 20, 30 et 99. Ce réseau ne peut tout simplement pas fonctionner sans agrégations de VLAN. Sachez que la plupart des réseaux que vous allez rencontrer comportent des agrégations de VLAN. Cette section regroupe les connaissances que vous possédez sur l'agrégation des réseaux locaux virtuels et vous donne les informations dont vous avez besoin pour pouvoir la configurer dans un réseau.

Une agrégation est une liaison point à point entre deux périphériques réseau qui porte plusieurs VLAN. Une agrégation de VLAN vous permet d'étendre les VLAN à l'ensemble d'un réseau. Cisco prend en charge la norme IEEE 802.1Q pour coordonner les agrégations sur les interfaces Fast Ethernet et Gigabit Ethernet. Vous en apprendrez plus sur cette norme plus loin dans cette section.

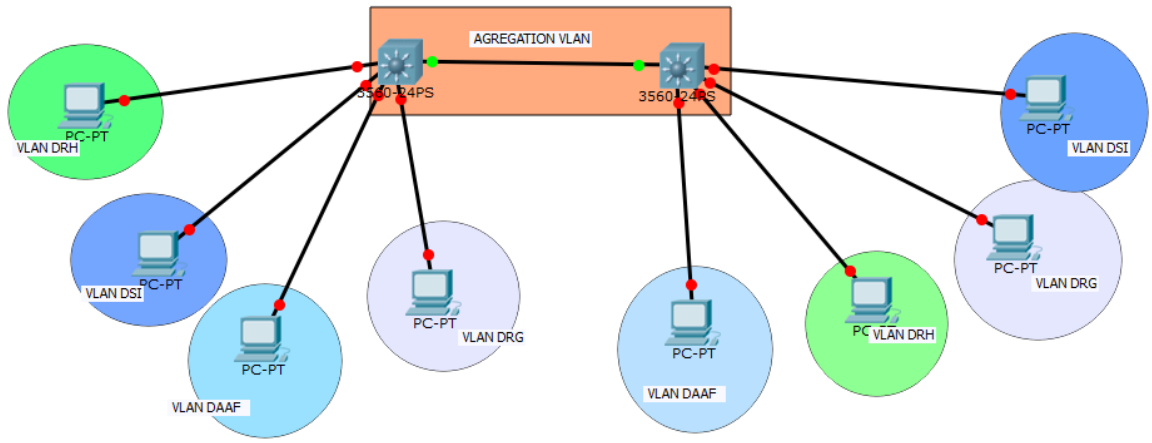


Figure 3.08 : *Agrégation VLAN*

e. *VTP :*

Le protocole VTP permet de configurer un commutateur pour qu'il propage des configurations VLAN à d'autres commutateurs du réseau. Le commutateur peut être configuré dans le rôle d'un serveur VTP ou d'un client VTP. Le protocole VTP détecte uniquement les réseaux locaux virtuels

de plage normale (ID de VLAN de 1 à 1 005). Les réseaux locaux virtuels de plage étendue (ID supérieur à 1 005) ne sont donc pas pris en charge par le protocole VTP.

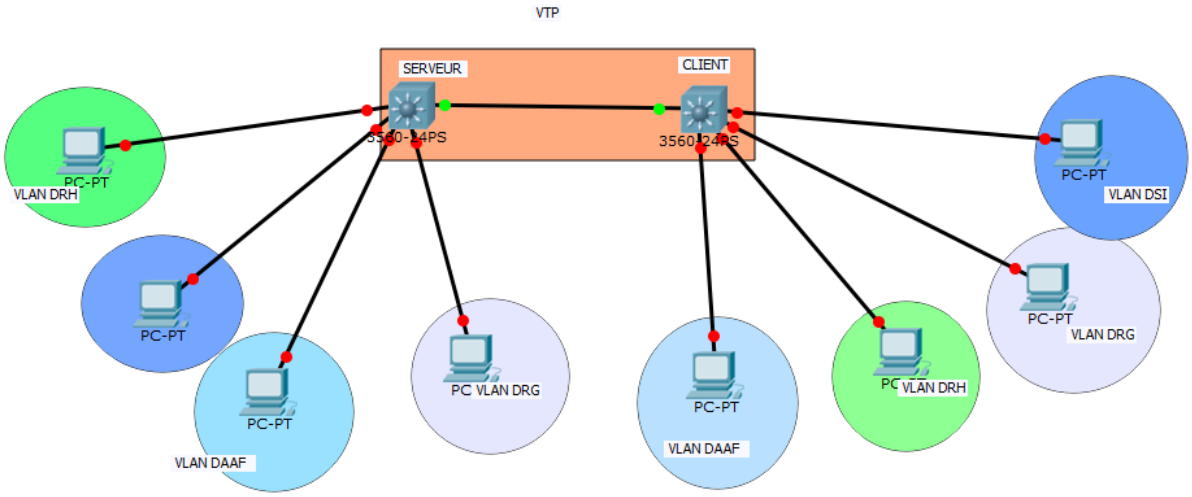


Figure 3.09 : *Mise en place VTP*

Le protocole VTP assure la cohérence de la configuration VLAN en gérant l'ajout, la suppression et le changement de nom des réseaux locaux virtuels sur plusieurs commutateurs Cisco d'un réseau. Le protocole VTP offre un certain nombre d'avantages pour les administrateurs réseau, comme l'illustre la figure.

- Configuration VLAN homogène sur le réseau
- Surveillance et suivi précis des VLAN
- Signalement dynamique des VLAN ajoutés à l'ensemble du réseau
- Configuration dynamique d'agrégations lors de l'ajout de VLAN au réseau

3.3.3.2 Conception de la topologie de la couche de distribution

Les exigences sur la couche de distribution sont nombreuses, dont les plus importantes sont :

- des liaisons et des composants redondants pour éviter les pannes
- fournir des fonctions de filtrage du trafic
- fournir une connectivité à large bande passante
- implémenter un protocole de routage à convergence rapide

- regrouper le trafic

Pour répondre à toutes ces exigences, les commutateurs multicouches sont les choix les plus adéquats puisqu'ils offrent une densité de port élevée et prennent en charge les fonctions de routage nécessaires. De plus ils permettent le filtrage par liste d'accès, la sécurité des ports et les fonctions de pare-feu

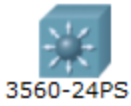


Figure 3.10 : *Switch multicouche*

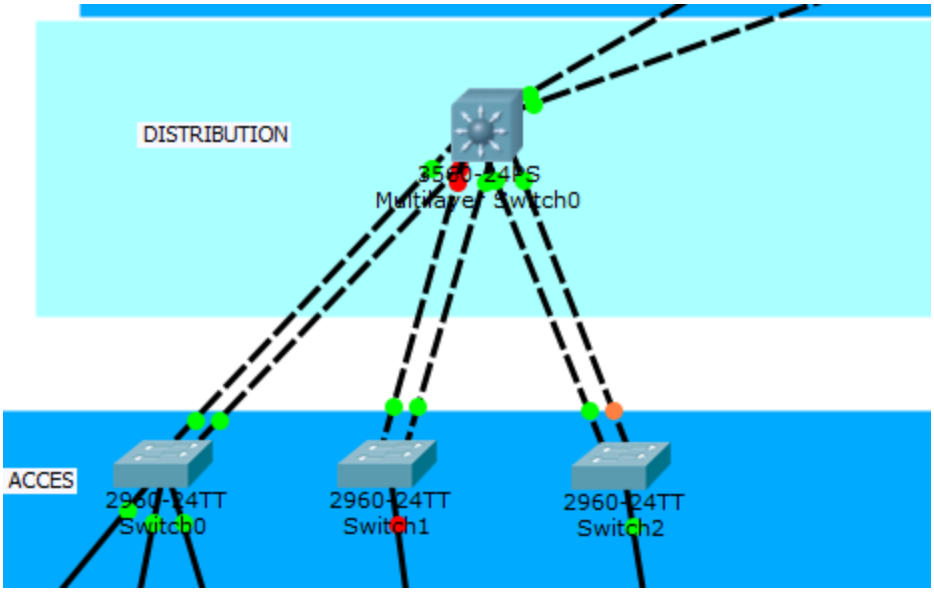


Figure 3.11 : *Topologie de la couche distribution*

a. HSRP :

On utilise le protocole HSRP sur la couche de distribution pour avoir une assurance en cas de panne de l'un des routeurs.

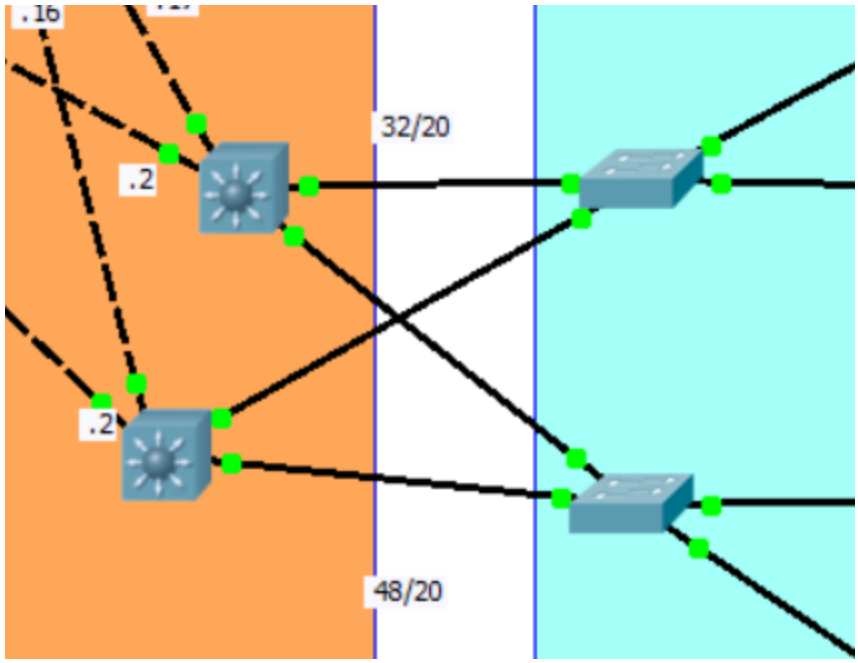


Figure 3.12 : *Les routeurs de la couche DISTRIBUTION*

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 :[18]

- 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)

b.Fonctionnement du HSRP :

Le HSRP permet que les deux routeurs de la couche distribution fonctionnent 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. [18]

Cet état de repos est appelé aussi standby.

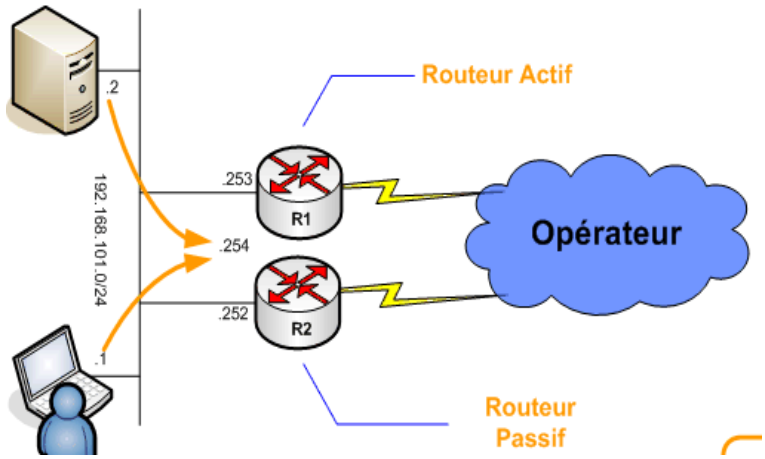


Figure 3.13 : *Etat initial des routeurs*

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.[18]

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.

3.3.3.3 Conception de la topologie de la couche cœur du réseau

La couche cœur est très importante dans la conception. Elle doit donc fournir une large bande passante et une haute disponibilité.

La vitesse est une des priorités car la quasi-totalité du trafic de l'entreprise doit circuler dans la couche cœur du réseau. On va donc utiliser les interfaces haut-débit et la technologie Etherchannel.

La disponibilité est l'autre priorité lors de la conception du cœur du réseau. Elle peut être reglé en utilisant des liaisons redondantes entre la couche cœur et la couche de distribution. L'utilisation de protocole de routage comme EIGRP et OSPF réduit aussi la reprise après l'échec d'une liaison favorisant le temps de disponibilité.

Les exigences de conception du réseau de la couche cœur de réseau sont donc les suivantes :

- connectivité haut débit aux commutateurs de la couche de distribution
- disponibilité 24h/24, 7 j/ 7
- interconnexions routées entre les périphériques de cœur de réseau ;
- liaisons haut débit redondantes entre les commutateurs de cœur de réseau et les périphériques des couches cœur de réseau et de distribution.

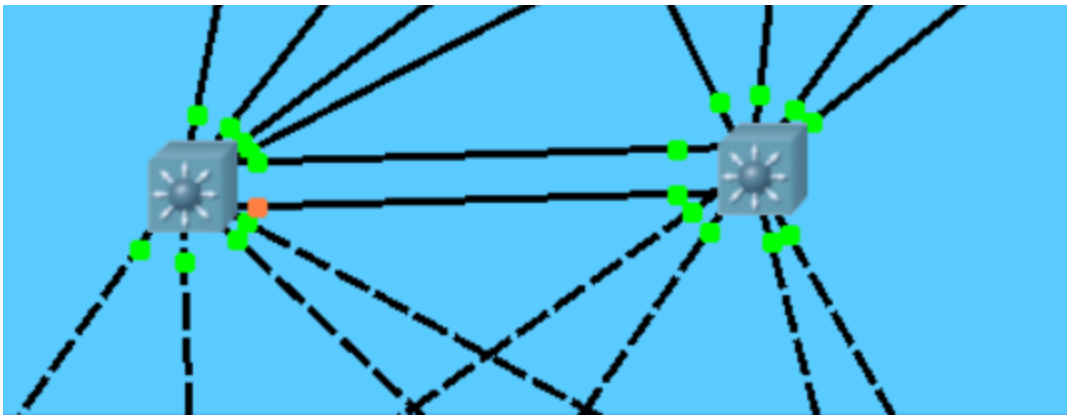


Figure 3.14 : *Topologie de la couche cœur du réseau*

a.Etherchannel :

Pour avoir une connexion haute débit entre les routeurs de la couche cœur du réseau, on utilise le protocole Etherchannel qui est une agrégation de liens. 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**.[19]

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.

b.LACP

L'etherChannel utilise le protocole LACP ou PAGP. C'est un protocole standard 802.3AD.

Nous retrouvons deux modes de ports sur l'equipement :

- Passive
- Active

Passive: création d'une agrégation si le port en face est en Active.

Active: 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 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.

c. Routage EIGRP :

Enhanced Interior Gateway Routing Protocol (EIGRP) est un protocole de routage sans classe à vecteur de distance. L'EIGRP propose une meilleur performance que les routages à vecteur de distance traditionnels que les RIP. Son seul incovénient est qu'il est un protocole proprétaire CISCO (voir Annexe 2).

3.3.3.4 Conception du réseau logique du MFB

Le schéma logique est le schéma qui montre l'interconnexion des différentes couches et des différents périphériques.

Les serveurs sont groupés en un seul lieu protégé par des matériels de sécurité CISCO ASA (voir Annexe 1) pour l'importance de ces contenus.

Les serveurs Web et Mails sont quant à eux, mis dans des Zones Démilitarisés ou DMZ pour pouvoir être accédés par les réseaux distants. Le niveau de sécurité dans cette zone est moyen dans ce cas pour simplifier l'accès. Seuls les serveurs qui n'ont aucun impact sur le fonctionnement du réseau interne seront donc mis dans cette zone.

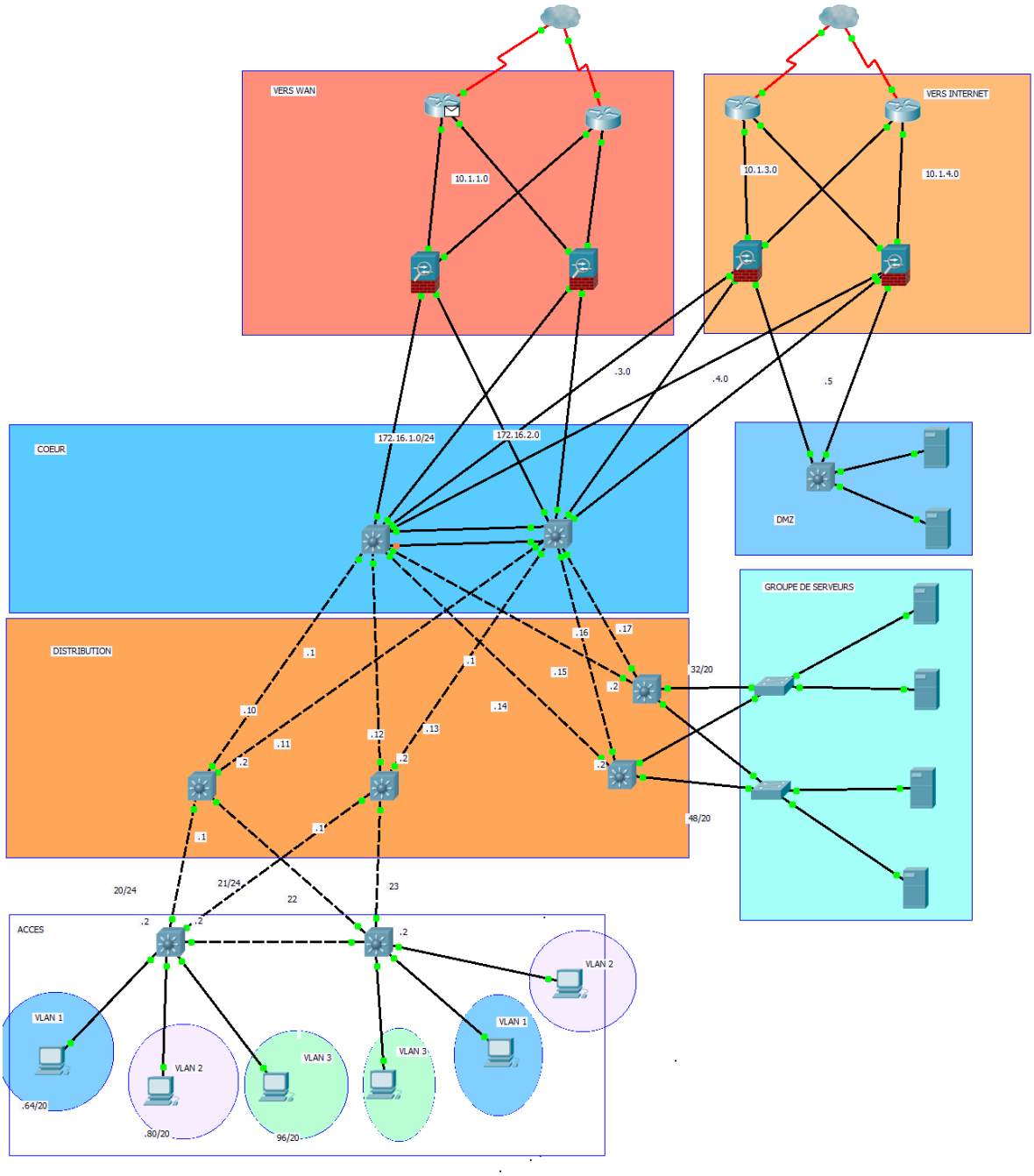


Figure 3.15 : *Schéma logique du réseau*

3.4 Conclusion

On a vu dans ce chapitre que le réseau actuel du MFB ne correspond plus aux exigences du réseau, que ce soit au niveau de la performance, de la disponibilité, de la sécurité ou de la facilité de gestion.

On a donc vu, après, les différentes étapes nécessaires à la conception du nouveau réseau de la MFB. On a alors parlé des topologies sur les différentes couches du réseau de la modélisation de réseau hiérarchique et les solutions proposées pour satisfaire les exigences du réseau. Sur la couche d'accès, on utilise des VLANS, les protocoles VTP et l'interconnexion INTERVLAN switch Multicouche. Sur la couche Distribution et cœur du réseau, on utilise HSRP, ETHERCHANNEL et le protocole de routage EIGRP. La prochaine chapitre, quant à elle, permettra de mettre en pratique l'utilisation de ces solutions en les simulant sous Packet Tracer.

CHAPITRE 4

SIMULATION DU RESEAU DU MFB SOUS PACKET TRACER

4.1 Présentation de Packet Tracer

4.1.1 Présentation de l'écran principal

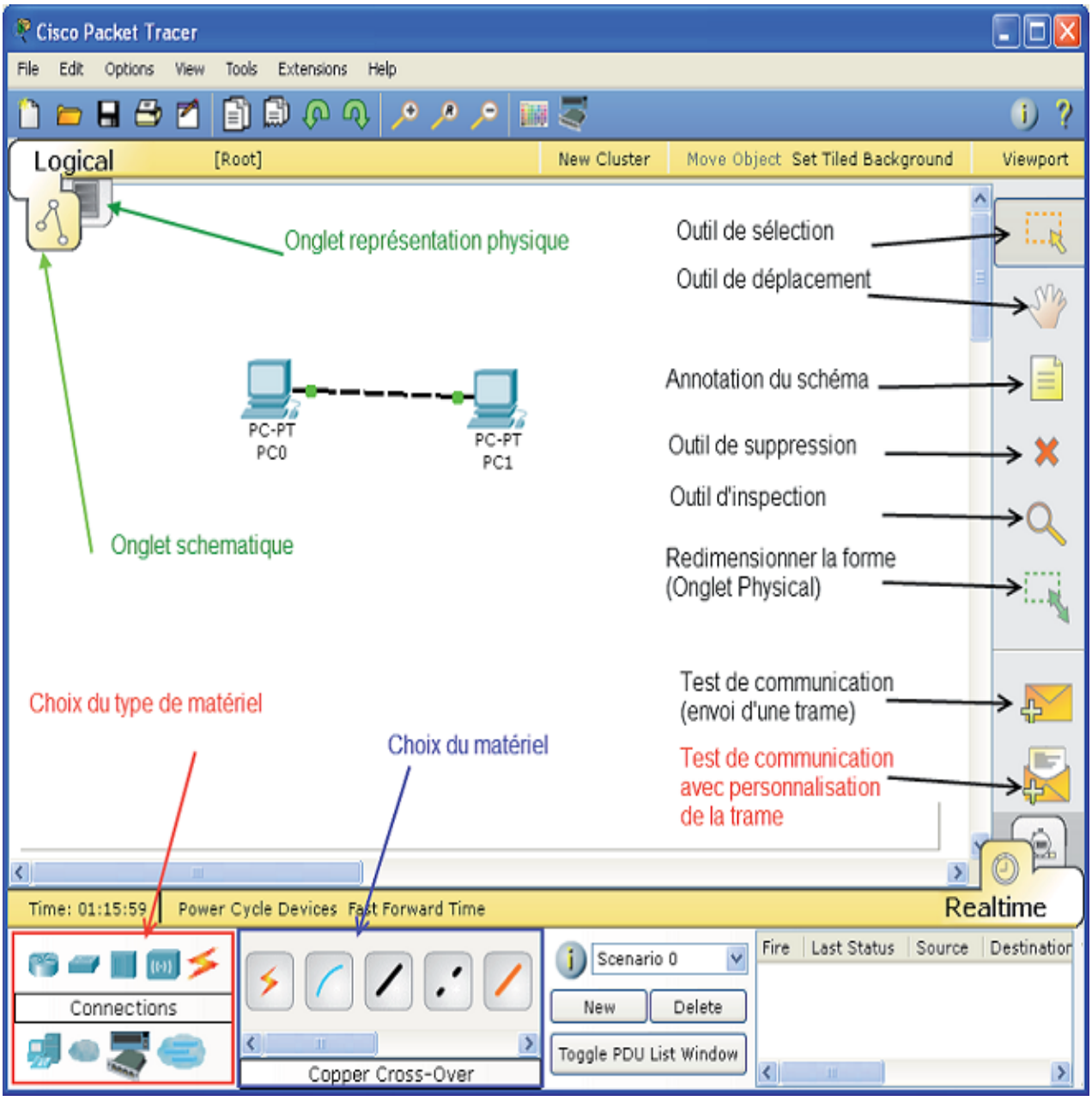


Figure 4.01 : *Ecran principale de packet tracer*

Il dispose d'une barre de menu classique ;

D'une barre d'outils principale comportant les fonctionnalités de base de gestion de fichier, d'impression, etc....

D'une barre d'outils à droite comportant les outils minimaux nécessaires.

Ainsi que trois boites à outils : choix du type de matériel, choix du matériel en fonction du type, résultats de l'échange de données.

4.1.2 Les principaux protocoles

Ce tableau présente les différents protocoles disponibles dans Packet Tracer selon les couches du modèle OSI.

Couches	Protocoles
Physique	Pas d'objet
Liaison	Ethernet (802.3), 802.11, HDLC, Frame Relay, PPP STP, VTP, DTP, CDP, 802.1q, LACP , … L2 QoS, SLARP, Auto Secure Wifi: simple WEP, WPA
Réseau	IPv4, ICMP, ARP, IPv6, ICMPv6, IPSec, GRE, Routage: RIPv1/v2/ng, Multi-Area OSPF, EIGRP, Static Routing Sécurité: Context Based Access Lists, Zone-based policy firewall et intrusion Protection System (sur certain routeur) Multilayer Switching, L3 QoS, NAT
Transport	TCP and UDP, TCP Nagle Algorithm & IP Fragmentation
Session	Pas d'objet
Présentation	Pas d'objet
Application	HTTP, HTTPS, TFTP, Telnet, SSH, DNS, DHCP, NTP, SNMP, AAA, Radius, Syslog, …

Tableau 4.01: *Récapitulatifs des principaux protocoles*

4.1.3 Spécification des équipements disponibles

Packet Tracer propose les principaux équipements réseaux composant nos réseaux actuels. Chaque équipement possède une vue physique comprenant des modules à ajouter, une vue configuration pour configurer les principales options via une interface graphique et une vue permettant la configuration via CLI (Command Line Interface).

- Routeur,
- Commutateur Terminaux (ordinateur, portable, serveur, imprimante et téléphone IP),
- Point d'accès Modem,
- Concentrateur.

Sachant que chaque équipement se voit attribuer un certain nombre de modules, permettant d'ajouter soit des ports supplémentaires, soit des nouveaux types de port. Les équipements propriétaires Cisco ont la possibilité de se voir attribuer les nouveaux IOS disponibles sur le site Cisco.

4.1.4 Paramétrage des appareils

Pour accéder au paramétrage d'un appareil, il faut cliquer, dans l'affichage physique (Physical) ou

Schématique (Logical), sur la représentation de l'appareil. Deux ou Trois onglets sont accessibles avec cette fenêtre.

4.1.4.1 Installation de nouveaux matérielles physiques

Elle consiste à placer les bonnes cartes dans l'appareil. Les cartes disponibles se trouvent à gauche de l'écran.

- Pour le placer, commencer par éteindre l'appareil avec le bouton Marche/Arrêt (M/A),
- Si besoin retirer la carte en place, par glisser-déplacer de l'appareil vers la liste des cartes,
- Appuyer à nouveau sur le bouton M/A.

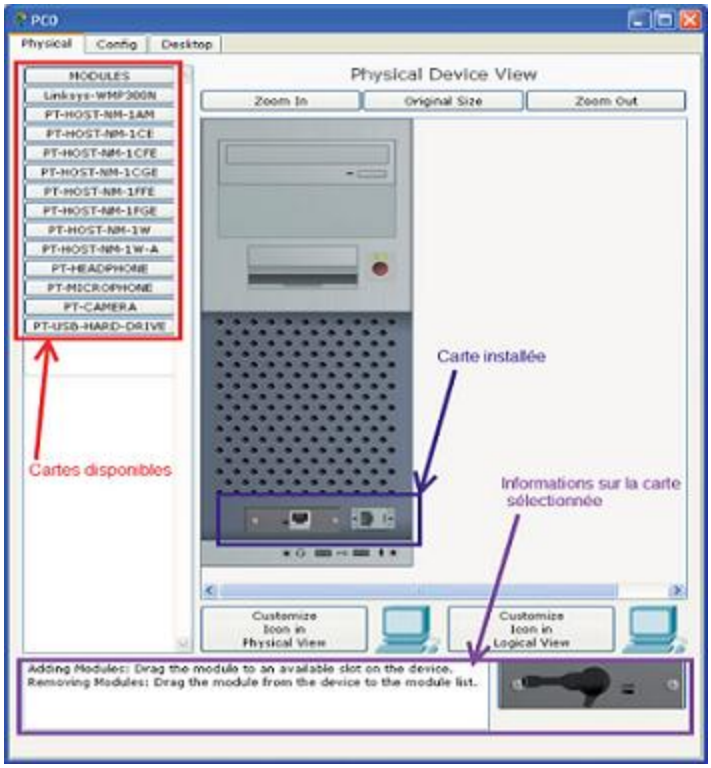


Figure 4.02 : *Installation d'une nouvelle carte*

4.1.4.2 Configuration

L'onglet Config permet de configurer l'équipement sélectionné.

Les boutons situés à gauche de la fenêtre déterminent le groupe de paramètres à configurer.

Par exemple: si une carte réseau FastEthernet équipe l'appareil, il sera possible de définir les paramètres de la carte en sélectionnant celle-ci avec le bouton FastEthernet et en renseignant les champs et cases à cocher de la partie droite de la fenêtre.

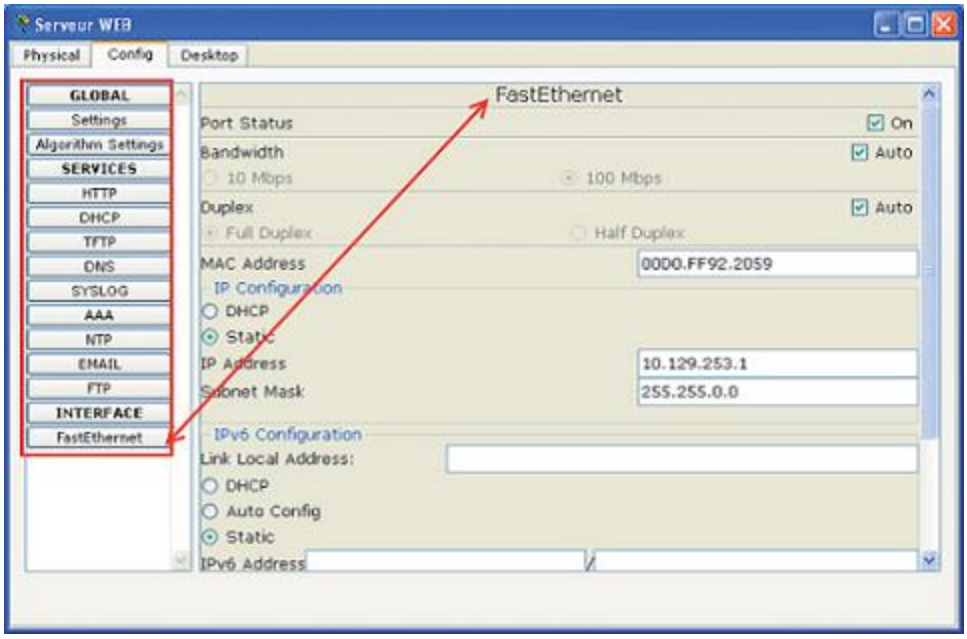


Figure 4.03 : *Paramétrage dans l'onglet configuration*

4.1.4.3 Remarque

Certains paramètres peuvent être définis par l'onglet Desktop.Cet onglet met à la disposition de l'utilisateur les outils logiciels habituels des équipements.

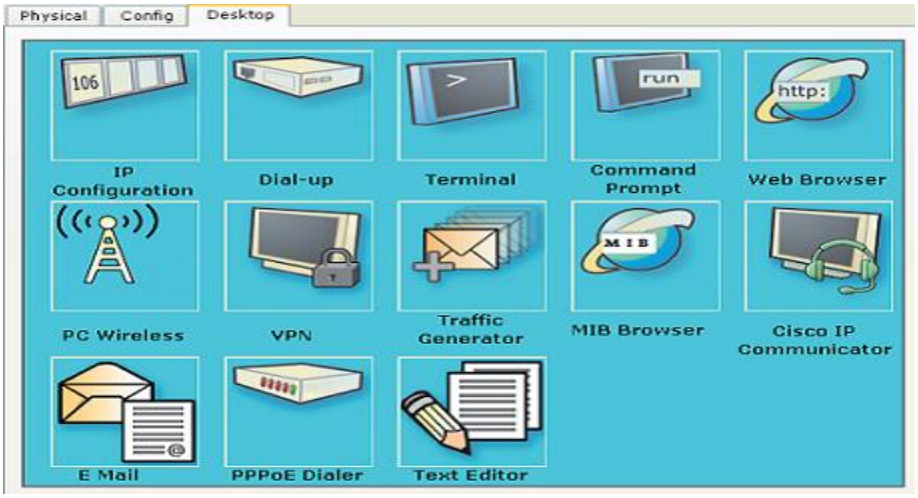


Figure 4.04 : *L'onglet desktop*

- IP configuration : permet de configurer les paramètres réseau de la machine.
- Dial-Up : permet de configurer un modem s'il est présent dans l'équipement.
- Terminal : permet d'accéder à une fenêtre de programmation (HyperTerminal).
- Command prompt : est la fenêtre DOS classique permettant de lancer des commandes en ligne de commande (PING, IPCONFIG, ARP, etc...).
- WEB Browser : il s'agit d'un navigateur Internet.
- PC Wireless : permet de configurer une carte WIFI si elle est présente dans l'équipement.
- VPN : permet de configurer un canal VPN sécurisé au sein du réseau.
- Traffic generator : permet pour la simulation et l'équipement considéré de paramétrer des trames de communications particulières (exemple : requête FTP vers une machine spécifiée).
- MIB Browser : permet par l'analyse des fichiers MIB d'analyser les performances du réseau.
- CISCO IP Communicator : Permet de simuler l'application logicielle de téléphonie développée par CISCO.
- E Mail : client de messagerie.
- PPPoE Dialer : pour une liaison Point à Point (Point to Point Protocol). [18] [20]

4.1.5 Simulation

Packet Tracer permet de simuler le fonctionnement d'un réseau par l'échange de trames Ethernet et la visualisation de celles-ci.

Il existe deux modes de simulation :

- la simulation en temps réel (REALTIME): elle visionne immédiatement toutes les séquences qui se produisent en temps réel,
- la simulation permettant de visualiser les séquences au ralenti entre deux ou plusieurs équipements comme la figure 4.06 nous montre.

4.1.5.1 Simulation en temps réel

- Réalisation d'un PING

Un ping fait appel au protocole ICMP avec le message numéro 8. Packet Tracer permet de faire un ping rapidement avec l'outil « Add Single PDU » représenté sous forme de petite enveloppe.

- Sélectionner l'outil,
- Cliquer sur l'ordinateur émetteur du PING,
- Cliquer ensuite sur l'ordinateur Destinataire du PING.

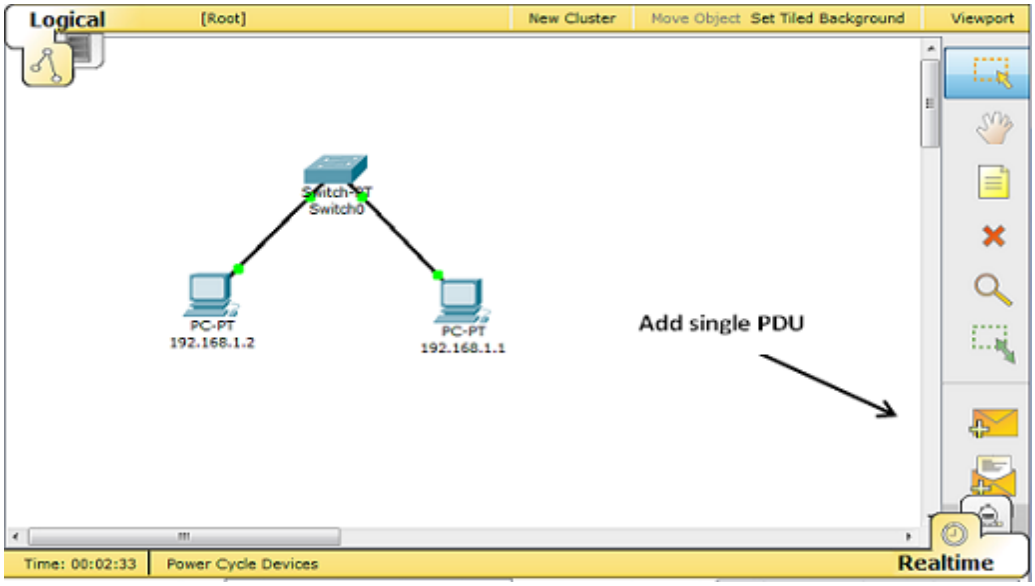


Figure 4.05 : *L'outil de réalisation d'un ping rapide*

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

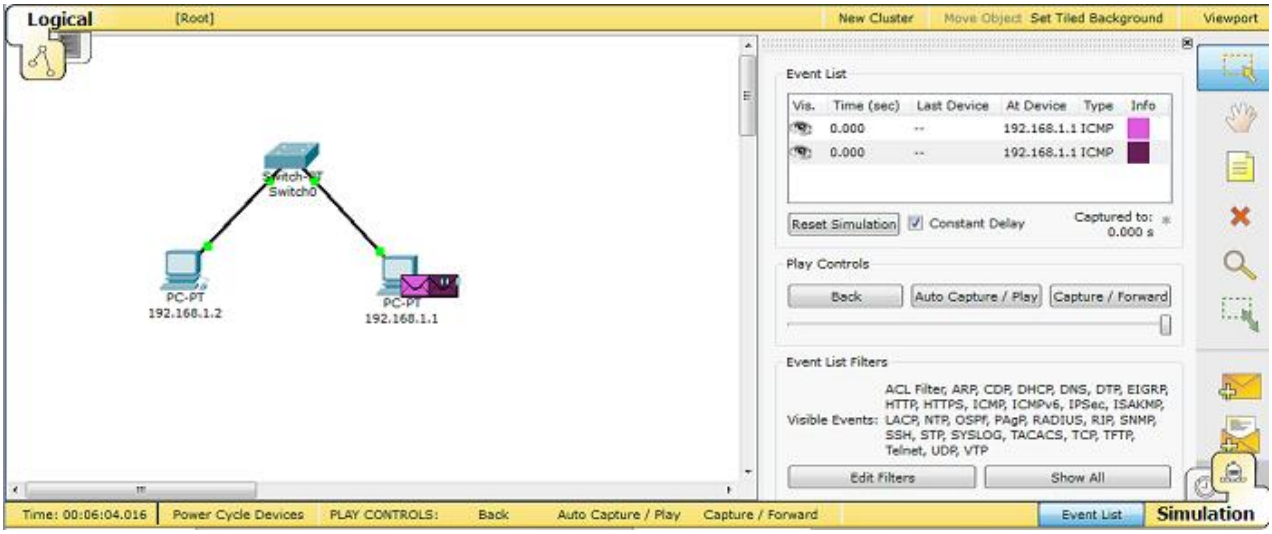


Figure 4.06 : *La fenêtre d'état de la transaction*

- Simulation en ligne de commande

Comme sur un vrai ordinateur, il est possible par ligne de commande de saisir des commande réseau (IPCONFIG, PING, ARP...).

- Ouvrir la fenêtre de configuration de l'ordinateur en cliquant sur sa représentation,
- Choisir l'onglet Desktop,
- Sélectionner l'outil Command Prompt,
- Saisir la commande souhaitée,
- Valider par la touche ENTREE.

La figure 4.07 suivante montre un test de connectivité avec la commande « ping ».

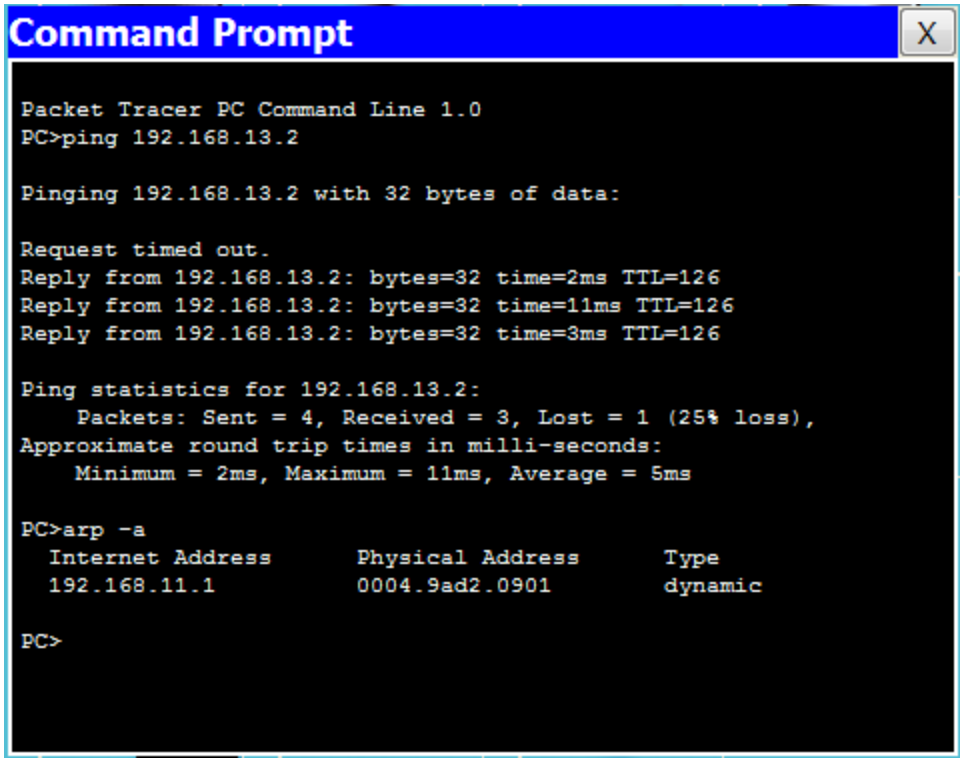


Figure 4.07 : *Test de connectivité en ligne de commande*

Les commandes disponibles dans la fenêtre Command prompt :

- arp : affiche la table arp.
- delete : permet de supprimer les fichiers se trouvant dans c : directory.
- dir : affiche les listes des fichiers dans c : directory.
- ipconfig : affiche la configuration logique et physique du matériel.

- netstat : affiche les protocoles statiques et celles du réseau TCP/IP.
- nslookup : vérification du DNS.
- ping : envoi de requêtes.
- snmpget : permet de visualiser la configuration snmp.
- telnet : permet de voir les clients telnet.
- tracert : permet de tracer la route de destination.
- help : affiche les listes des commandes disponibles,
- etc…

4.2 SIMULATION du Réseau du MFB

4.2.1 Architecture globale du réseau :

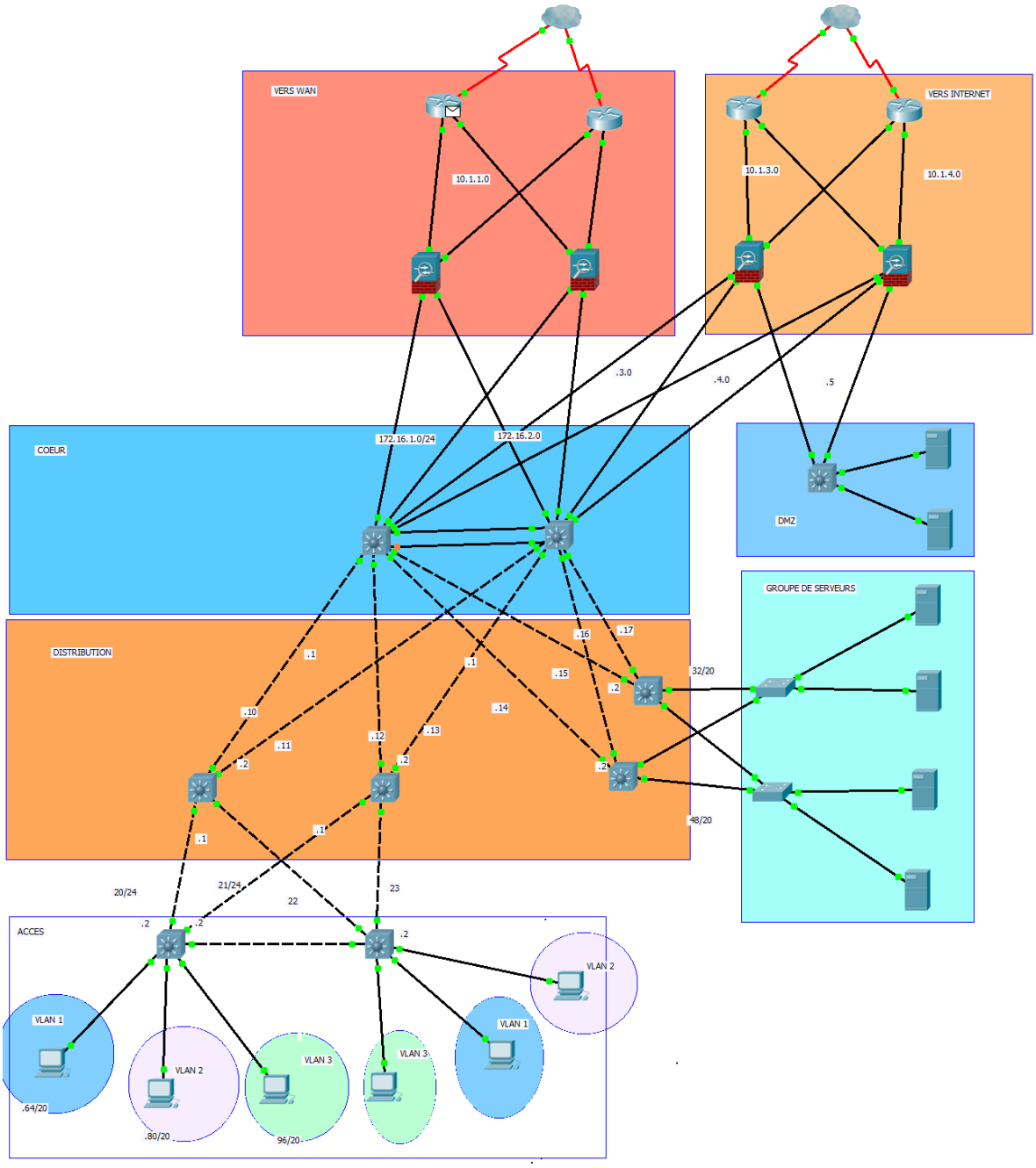


Figure 4.08 : *Schéma logique du Réseau*

4.2.2 Configurations des équipements utilisés

4.2.2.1 La couche de distribution:

D'abord on configure les liens entre le commutateur multicouche de la couche distribution (switch D) et le commutateur (switch 2) de celle de l'accès. On utilise l'agrégation de lien avec le protocole LACP avec la technologie Etherchannel sur les commutateurs CISCO.

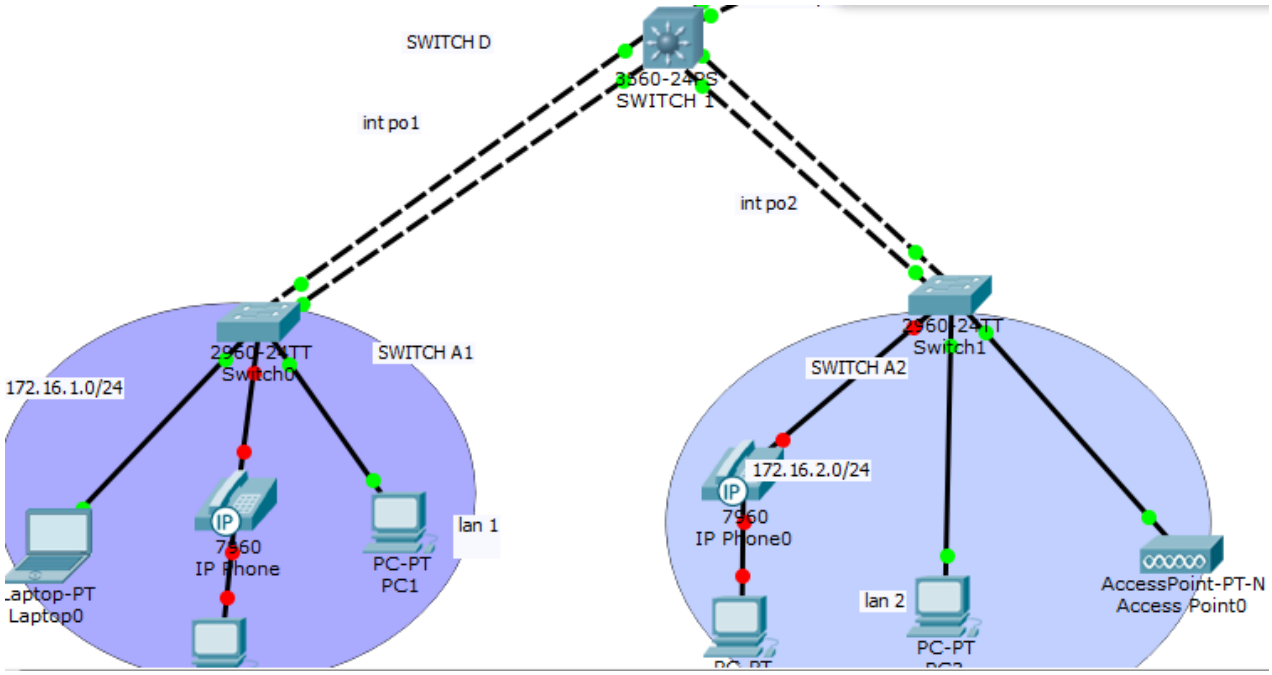


Figure 4.09 : *La couche d'accès et de distribution*

Sur le switch D, on regroupe les interfaces Fa0/1 et Fa0/2 pour ne faire qu'un :

```
Switch1> en

switch1# configure terminal

switch1(config)# interface range fastethernet 0/1 - 2

switch1(config-range-if)# switchport mode trunk
```

```
switch1(config-range-if)# channel-protocol lacp
switch1(config-range-if)# channel-group 1 mode active
switch1(config-range-if)# no shut
switch1(config-range-if)# exit
switch1(config)#exit
switch1#
```

Le commutateur D est en mode active tandis que le commutateur switch A1 est configuré en mode passive.

```
switch2> en
switch2# configure terminal
switch2(config)# interface range fastethernet 0/1 - 2
switch2(config-range-if)# switchport mode trunk
switch2(config-range-if)# channel-protocol lacp
switch2(config-range-if)# channel-group 1 mode passive
switch2(config-range-if)# no shut
switch2(config-range-if)# exit
switch2(config)#exit
switch2#
```

Ensuite on fait l'adressage dynamique des terminales des VLAN des différents départements DSI, DRH, DAAF, …. La configuration se fait sur le commutateur D :

```
>Conf t

>Ip dhcp pool LAN1

>Network 172.16.1.0 255.255.255.0

>Default-router 172.16.1.1

>Config interface

>Int f0/0

>no switchport

>Ip address 192.168.1.1 255.255.255.0
```

La commande *no switchport* est très importante pour un commutateur multicouche pour pouvoir faire l'addressage du port fastethernet.

4.2.2.2 La couche d'accès :

Pour la mise en place des VLANS sur la couche d'accès, on a utilisé la methode INTERVLAN par SWICH multicouche. Voici les configurations nécessaires pour la mise en place de ce réseau :

Tout d'abord la création des vlans :

- vlan 10
- name DSI
- VLAN 20
- name DAAF
- int f0/10
- swi mode access
- swit acc vlan 10
- int f0/20
- swi mode access

- swit acc vlan 20

Ensuite la configuration des interfaces SVI nécessaires pour la communication inter-vlan :

- INT VLAN 10
- IP ADD 192.168.10.1 255.255.255.0
- INT VLAN 20
- IP ADD 192.168.20.1 255.255.255.0

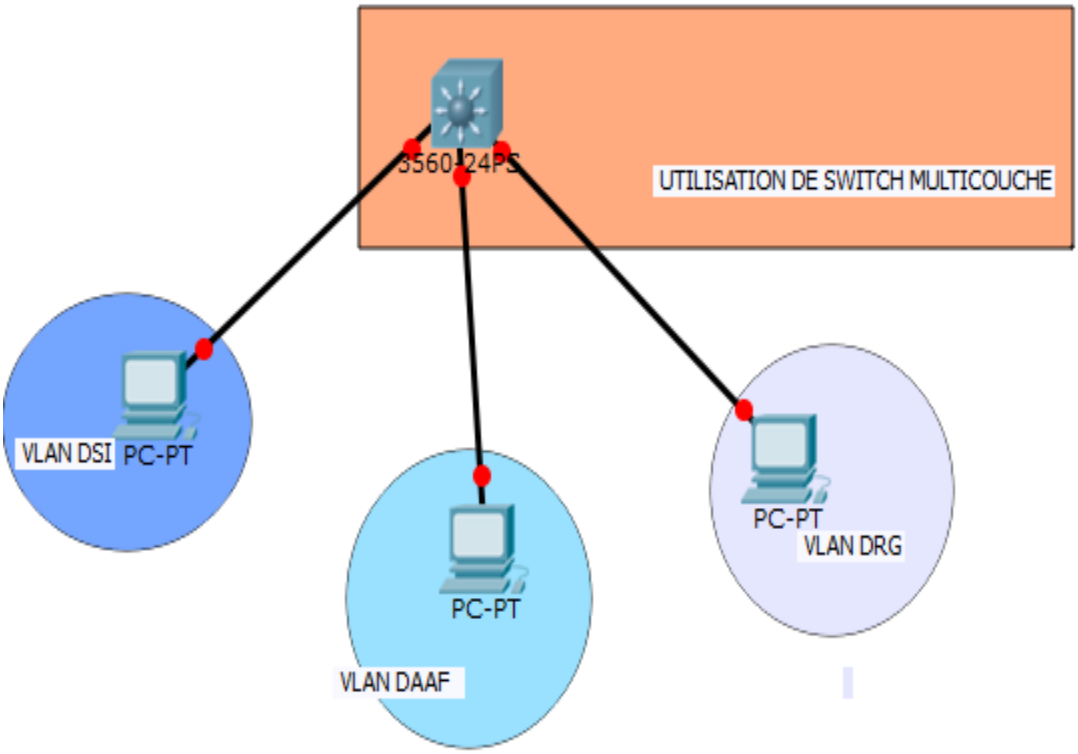


Figure 4.10 : *Création VLAN*

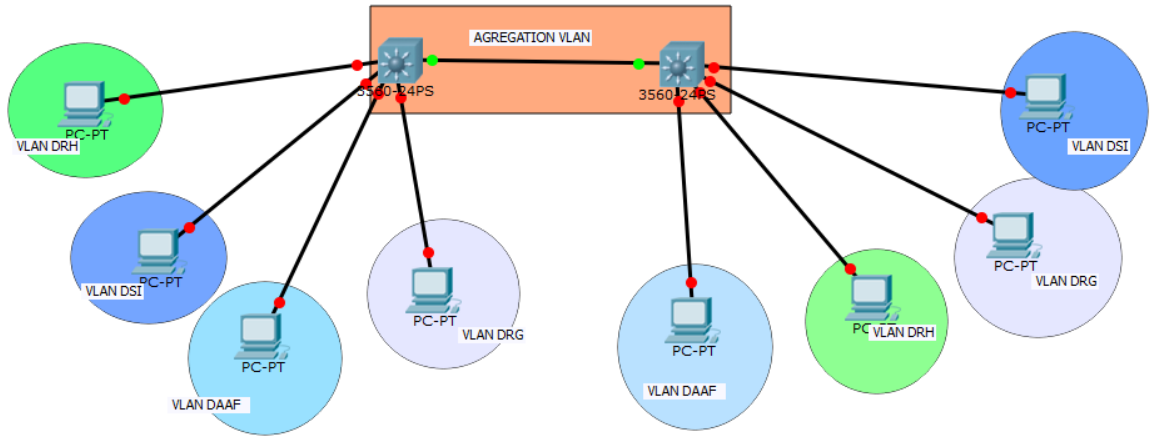


Figure 4.11 : *Agrégation VLAN*

Par la suite, pour relier deux switchs de la couche d'accès, on utilise le protocole vtp dont l'un qu'on configure en mode serveur et l'autre en mode client. Le serveur propage alors les vlans sur les autres switch clients.

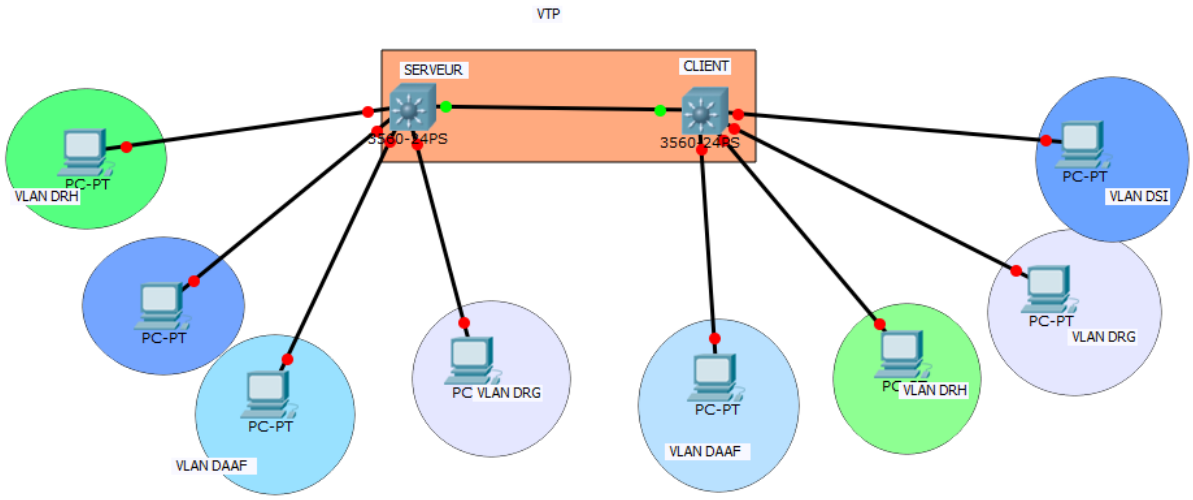


Figure 4.12 : *Mise en place VTP*

Voici les commandes à faire pour la mise en place de VTP sur les switchs d'accès :

- vtp domain domain1
- vtp mode <client,server,transparent>

sur le switch 1 :

- INT F0/1
- SWITCHPORT MODE TRUNK
- SWITCHPORT TRUNK ALLOWED VLAN 1-99

Et sur le switch 2, le trunk change automatiquement en mode trunk.

4.2.2.3 Sur la couche distribution :

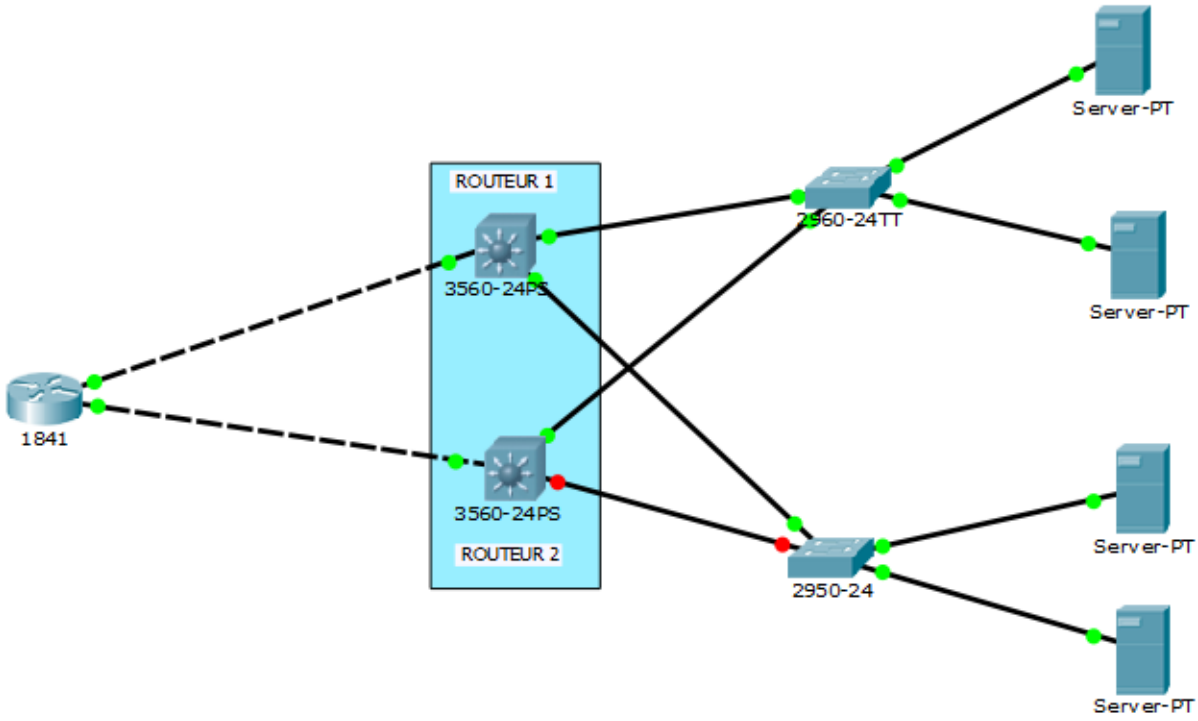


Figure 4.13 : *Les 2 routeurs de la couche distribution côté groupe de serveurs*

Pour permettre une haute disponibilité envers les serveurs, on utilise le protocole HSRP dans les routeurs. La commande qui suit permet d'activer ce protocole :

Sur le router 1 :

- INT F0/0

- STANDBY 1 IP 10.1.1.10
- STANDBY 1 PRIORITY 110
- STANDBY 1 PREEMPT

Et de même pour le routeur 2 :

- INT F0/0
- STANDBY 1 IP 10.1.1.10
- STANDBY 1 PREEMPT

4.2.2.4 Routage sur la couche distribution et cœur du réseau :

On utilise ici le protocole de routage EIGRP. Sa simplicité a fait pencher la balance par rapport aux autres protocoles OSPF et RIP. Tout d'abord il faut activer le routage sur le commutateur multicouche avec la commande IP ROUTING . On peut ensuite configurer le routage :

>router eigrp 1

>network 172.16.1.0 0.0.0.255

>network 10.1.1.0 0.0.0.255

>no auto-summary

>redistribute static

>int fa0/6

>no switchport

>ip address 10.1.1.1 255.255.255.0

On fait de même sur tous les routeurs de la couche d'accès avec la table d'adressage suivante :

Périphérique	Interface	Adresse IP	Masque de sous-réseau
Routeur R1 Acces	Fa0/2	172.16.20.2	255.255.255.0
	Fa0/3	172.16.21.2	255.255.255.0
RouteurR2 Acces	Fa0/2	172.16.22.2	255.255.255.0
	Fa0/3	172.16.23.2	255.255.255.0
Distribution1	Fa0/1	172.16.20.1	255.255.255.0
	Fa0/2	172.16.21.1	255.255.255.0
	Fa0/3	172.16.10.1	255.255.255.0
	Fa0/4	172.16.11.1	255.255.255.0
Distribution2	Fa0/1	172.16.21.1	255.255.255.0
	Fa0/2	172.16.23.1	255.255.255.0
	Fa0/3	172.16.12.1	255.255.255.0
	Fa0/4	172.16.13.1	255.255.255.0
Distribution3	Fa0/1	172.16.32.1	255.255.255.0
	Fa0/2	172.16.48.1	255.255.255.0
	Fa0/3	172.16.14.2	255.255.255.0

	Fa0/4	172.16.15.2	255.255.255.0
Distribution 4	Fa0/1	172.16.32.1	255.255.255.0
	Fa0/2	172.16.48.1	255.255.255.0
	Fa0/3	172.16.16.2	255.255.255.0
	Fa0/4	172.16.17.2	255.255.255.0
Core 1	Fa0/1	172.16.10.1	255.255.255.0
	Fa0/2	172.16.12.1	255.255.255.0
	Fa0/3	172.16.14.1	255.255.255.0
	Fa0/4	172.16.1.2	255.255.255.0
	Fa0/5	172.16.1.3	255.255.255.0
	Fa0/6	172.16.2.2	255.255.255.0
	Fa0/6	172.16.2.3	255.255.255.0
	Fa0/7	172.16.3.1	255.255.255.0
	Fa0/8	172.16.4.1	255.255.255.0
Core 2	Fa0/1	172.16.11.1	255.255.255.0
	Fa0/2	172.16.13.1	255.255.255.0
	Fa0/3	172.16.16.1	255.255.255.0

	Fa0/4	172.16.17.1	255.255.255.0
	Fa0/5	172.16.2.1	255.255.255.0
	Fa0/6	172.16.3.1	255.255.255.0
	Fa0/7	172.16.4.1	255.255.255.0
WAN ROUTER 1	Fa0/1	10.1.1.1	255.255.255.0
	Fa0/2	10.1.2.1	255.255.255.0
WAN ROUTER 2	Fa0/1	10.1.1.2	255.255.255.0
	Fa0/2	10.1.2.2	255.255.255.0
INTERNET ROUTER 1	Fa0/1	10.1.3.1	255.255.255.0
	Fa0/2	10.1.4.1	255.255.255.0
INTERNET ROUTER 1	Fa0/1	10.1.3.2	255.255.255.0
	Fa0/2	10.1.4.2	255.255.255.0

Tableau 4.02: *Adressage du réseau*

4.2.2.5 Configuration du cisco ASA :

La configuration du cisco ASA diffère sur la simulation sous Packet Tracer et sur la réalisation. Tout simplement parcequ'on utilise le ASA 5525 alors que sur Packet il n'y a que la série 5505. La différence se trouve sur l'adressage : les series 5510 permettent de configurer les adresses physiquement, alors que sur le 5505 on doit créer des VLANS.

Configuration sous 5505 : on crée donc 2 vlans, l'un pour l'interface public et l'autre pour le privé.

```
ASA5505(config)#  interface vlan 1
ASA5505(config)#  description Private-Interface
ASA5505(config-if)#  ip address 10.1.9.1 255.255.255.0
ASA5505(config-if)#  no shutdown

ASA5505(config)#  interface vlan 2
ASA5505(config)#  description Public-Interface
ASA5505(config-if)#  ip address 192.168.2.1  255.255.255.0
ASA5505(config-if)#  no shutdown

ASA5505(config)#  interface ethernet 0/0
ASA5505(config-if)#  switchport access vlan 2
ASA5505(config-if)#  no shutdown
```

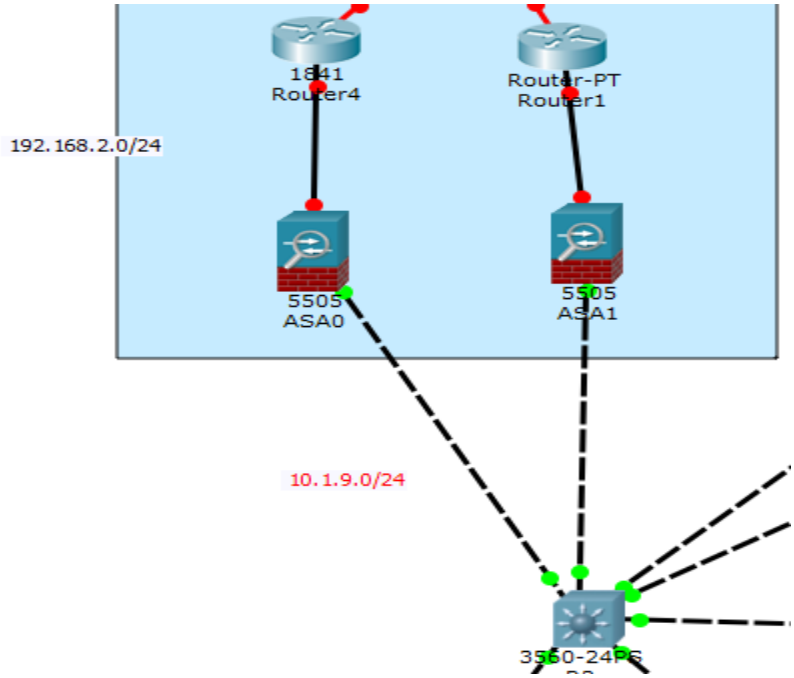


Figure 4.14 : *ASA sur le WAN*

Ensuite il faut configurer les interfaces allant de ethernet 0/1 à 0/7 avec la commande no shutdown et la route par défaut :

```
ASA5505(config-if)#  interface ethernet 0/1
ASA5505(config-if)#  no shutdown
ASA5505(config-if)#  interface ethernet 0/2
ASA5505(config-if)#  no shutdown
```

Et après designer les interfaces vlan public et privé :

```
ASA5505(config)# interface vlan 1
ASA5505(config-if)# nameif inside

ASA5505(config)# interface vlan 2
ASA5505(config-if)# nameif outside
ASA5505(config)# route outside 0.0.0.0 0.0.0.0 192.168.2.1
```

Et enfin on peut configurer les NAT, les ACL, les pare-feu, le serveur DHCP sur le cisco ASA.
Les ACL sont configurés comme suit :

```
access-list outside extended permit icmp 10.1.1.0 255.255.255.0 172.16.1.0 255.255.255.0 echo-reply
access-list outside extended permit icmp 10.1.1.0 255.255.255.0 172.16.1.0 255.255.255.0 echo
access-list outside extended permit icmp 10.1.1.0 255.255.255.0 any echo
access-list outside extended permit icmp 10.1.1.0 255.255.255.0 any echo-reply
access-list outside extended permit icmp 10.1.1.0 255.255.255.0 172.16.11.0 255.255.255.0 echo-reply
access-list outside extended permit icmp 10.1.1.0 255.255.255.0 172.16.11.0 255.255.255.0 echo
access-list outside extended permit icmp 10.1.1.0 255.255.255.0 172.16.21.0 255.255.255.0 echo
access-list outside extended permit icmp 10.1.1.0 255.255.255.0 172.16.21.0 255.255.255.0 echo-reply
access-list outside extended permit icmp 10.1.1.0 255.255.255.0 172.16.20.0 255.255.255.0 echo-reply
access-list outside extended permit icmp 10.1.1.0 255.255.255.0 172.16.20.0 255.255.255.0 echo
```

La configuration des parties DMZ est impossible sur la partie simulation car packet Tracer ne permet pas la mise en place d'une nouvelle interface SVI à part les Inside et Outside.

4.3 Conclusion

Ce chapitre nous a montré la simulation du réseau réalisé au sein du MFB. Il nous a permis de survoler toutes les configurations nécessaires pour la réalisation du projet. Nous avons utilisé ici le logiciel Packet Tracer comme outil de simulation car de nos jours il faisait partie des outils de simulation de réseau puissant et indispensable. On a pu voir qu'il y a quand même des différences entre la réalisation et la simulation avec les manques d'option et d'équipements du logiciel de simulation.

CONCLUSION GENERALE

Pour conclure, nous avons vu que pour mettre un place un projet de conception de réseau, il faut définir les objectifs commerciaux voulu par l'entreprise. Ensuite, faire en sorte que ces objectifs qu'on a recensé soit prise en charge par la nouvelle conception.

Dans ce long processus de conception, on doit tenir compte des objectifs et exigences, de la capacité du réseau déjà en place et aussi des nouvelles technologies qu'on doit intégrer. La phase de conception du réseau doit se faire en six étapes appelées cycle PPDIOO. Un point très important sur la conception du réseau est aussi la sécurité sur le réseau. 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.

On a aussi pu voir que le réseau du MFB ne répond plus aux besoins du réseau de nos jours et qu'il fallait donc un renouvellement de l'ensemble de celui-ci. La disponibilité, la sécurité, la facilité de gestion et la performance sont les principales exigences de cette nouvelle infrastructure. Le concept de VLAN est né de l'augmentation considérable de la taille des réseaux et de la volonté de les segmentés Le routage inter VLAN permet une connexion entre ces éléments de la couche inférieure du modèle OSI vers les plus hautes.

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.

Cependant, un réseau disponible n'est pas à l'abri des attaques. Ces attaques peuvent provenir de l'intérieur que de l'extérieur. Donc il faut mette en place de systèmes de sécurité qui sera pris en charge par le cisco ASA.

Annexe 1

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 A1.01 : *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 A1.01 : *Fonctionnalités et capacités du Serveur de Sécurité Adaptatif Cisco ASA 550*

Annexe 2

PROTOCOLE EIGRP

Enhanced Interior Gateway Routing Protocol (EIGRP) est un protocole de routage sans classe à vecteur de distance mis sur le marché en 1992, avec le système d'exploitation Internet IOS 9.21. Comme son nom l'indique, EIGRP est une amélioration du protocole IGRP (Interior Gateway Routing Protocol) de CISCO. Les deux sont des protocoles propriétaires et ne fonctionnent que sur des routeurs Cisco.

En développant EIRGP, Cisco avait pour objectif principal la création d'une version sans classe du protocole IGRP. EIGRP comprend plusieurs fonctions peu répandues dans les autres protocoles de routage par vecteur de distance (RIP - RIPv1 et RIPv2 et IGRP), Ces fonctions comprennent :

- protocole RTP (Reliable Transport Protocol) ;
- mises à jour limitées ;
- algorithme DUAL ;
- établissement de contiguïtés ;
- tables de voisinage et de topologie.

Bien qu'EIGRP puisse se comporter comme un protocole de routage d'état des liaisons, il s'agit toujours d'un protocole de routage à vecteur de distance.

A2.1 EIGRP : Protocole de routage à vecteur de distance amélioré

Bien que le protocole EIGRP soit décrit comme un protocole de routage à vecteur de distance amélioré, il s'agit d'un protocole de routage à vecteur de distance à part entière. Cela peut quelquefois engendrer la confusion. Pour être en mesure d'en apprécier les améliorations et de dissiper toute confusion, commençons par étudier son prédécesseur, IGRP.

A2.2 Les origines du protocole EIGRP : IGRP

Cisco a développé le protocole propriétaire IGRP en 1985, pour pallier certaines des limites du protocole RIPv1, notamment l'utilisation du nombre de sauts comme mesure et la taille maximale du réseau égale à 15 sauts.

Les protocoles IGRP et EIGRP n'utilisent pas le nombre de sauts, mais des mesures complexes comprenant la bande passante, le délai, la fiabilité et la charge. Par défaut, les deux protocoles de routage utilisent seulement la bande passante et le délai. Cependant, comme IGRP est un protocole de routage par classe utilisant l'algorithme Bellman-Ford et les mises à jour périodiques, son utilité est limitée sur bon nombre de réseaux actuels.

A2.3 L'algorithme

Les protocoles de routage à vecteur de distance traditionnels utilisent tous des variantes des algorithmes Bellman-Ford ou Ford-Fulkerson. Ces protocoles, par exemple, RIP et IGRP, affecte un délai aux entrées de routage individuelles, et nécessitent donc l'envoi périodique de mises à jours de la table de routage.

EIGRP utilise l'algorithme DUAL (Diffusing Update Algorithm). Bien qu'il reste un protocole de routage à vecteur de distance, le protocole EIGRP avec DUAL met en œuvre des fonctions qu'on ne trouve pas dans les protocoles traditionnels de ce type. Le protocole EIGRP n'envoie pas des mises à jour périodiques et les entrées de routage n'ont pas de délai de validité. Au lieu de cela, EIGRP utilise un protocole Hello léger pour contrôler l'état de la connexion avec ses voisins. Seules les modifications des données de routage, par exemple un nouveau lien ou un lien devenant indisponible, déclenchent une mise à jour de routage. Les mises à jour de routage EIGRP sont néanmoins des vecteurs de distance transmis aux voisins directement connectés.

C'est pour cette raison que Cisco a amélioré IGRP en utilisant un nouvel algorithme, DUAL, ainsi que d'autres fonctions. Les commandes des protocoles IGRP et EIGRP sont similaires, et dans bien des cas.

A2.3 Détermination du chemin

Les protocoles de routage à vecteur de distance traditionnels tels que RIP et IGRP conservent uniquement les routes préférées, le meilleur chemin vers un réseau de destination. Si la route devient indisponible, le routeur attend alors une autre mise à jour de routage, avec un chemin vers ce réseau distant.

L'algorithme DUAL du protocole EIGRP garde une table topologique et une table de routage distinctes. La table topologique inclut à la fois le meilleur chemin vers le réseau de destination et

tous les chemins de secours que DUAL a déterminés comme étant sans boucle. Sans boucle signifie qu'aucune route du voisin vers le réseau de destination ne passe par ce routeur.

Plus loin dans ce chapitre, vous verrez que l'algorithme DUAL considère un chemin de secours sans boucle valide si ce chemin respecte un critère appelé condition de faisabilité. Tout chemin de secours conforme à la condition de faisabilité est garanti exempt de boucle. EIGRP étant un protocole de routage à vecteur de distance, il est possible qu'il existe des chemins de secours sans boucle vers un réseau de destination ne respectant pas la condition de faisabilité. L'algorithme DUAL n'inclut donc pas ces chemins dans la table topologique en tant que chemins de ecours sans boucle valides.

Lorsqu'une route devient indisponible, DUAL recherche un chemin de secours valide dans la table topologique. S'il en existe un, il est immédiatement intégré à la table de routage. S'il n'en existe pas, DUAL lance un processus de détection sur le réseau pour voir s'il existe un chemin de secours ne satisfaisant pas à la condition de faisabilité. Ce processus est traité de façon plus complète, plus loin dans ce chapitre.

A2.4 Convergence

Les protocoles de routage à vecteur de distance traditionnels tels que RIP et IGRP utilisent des mises à jour périodiques. En raison de la nature non fiable de ces mises à jour périodiques, les protocoles de routage à vecteur de distance traditionnels peuvent être affectés par des problèmes de boucles de routage et de comptage à l'infini. Les protocoles RIP et IGRP utilisent différents mécanismes pour éviter ces problèmes, notamment les minuteurs de mise hors service, qui génèrent des délais de convergence élevés.

Le protocole EIGRP, lui, n'utilise pas les minuteurs de mise hors service. En revanche, il obtient des chemins sans boucle grâce à un système de calcul de route (calculs de diffusion) effectués de façon coordonnée parmi les routeurs. Le détail de ces calculs dépasse le cadre de ce cours, mais il en résulte des délais de convergence inférieurs à ceux des protocoles de routage à vecteur de distance traditionnels.

A2.5 ID de processus

EIGRP et OSPF utilisent tous les deux un ID de processus pour représenter une instance de leur protocole de routage respectif s'exécutant sur le routeur.

Router(config)#router eigrp autonomous-system

Bien qu'EIGRP appelle ce paramètre un numéro de « système autonome », celui-ci fonctionne en fait comme un ID de processus. Ce numéro n'est pas associé au numéro de système autonome étudié précédemment et toute valeur de 16 bits peut lui être attribuée.

Router(config)#router eigrp 1

Dans cet exemple, le nombre 1 désigne le processus EIGRP particulier s'exécutant sur ce routeur. Pour établir des contiguïtés de voisinage, le protocole EIGRP requiert que tous les routeurs du même domaine de routage soient configurés selon le même ID de processus. En général, un seul ID de processus de n'importe quel protocole de routage est configuré sur un routeur.

A2.6 Les commandes EIGRP

La commande network, dans le protocole EIGRP, a la même fonction que dans les autres protocoles de routage IGP :

Toute interface sur ce routeur qui correspond à l'adresse réseau dans la commande network est activée pour envoyer et recevoir des mises à jour EIGRP.

Ce réseau (ou sous-réseau) sera inclus dans les mises à jour de routage EIGRP.

La commande network est utilisée en mode de configuration du routeur.

Router(config-router)#network network-address

Les protocoles de routage à vecteur de distance traditionnels tels que RIP et IGRP utilisent des mises à jour périodiques. En raison de la nature non fiable de ces mises à jour périodiques, les protocoles de routage à vecteur de distance traditionnels peuvent être affectés par des problèmes de boucles de routage et de comptage à l'infini. Les protocoles RIP et IGRP utilisent différents mécanismes pour

éviter ces problèmes, notamment les minuteurs de mise hors service, qui génèrent des délais de convergence élevés.

Le protocole EIGRP, lui, n'utilise pas les minuteurs de mise hors service. En revanche, il obtient des chemins sans boucle grâce à un système de calcul de route (calculs de diffusion) effectués de façon coordonnée parmi les routeurs.

BIBLIOGRAPHIE

[1] W. R. Stevens, G. Pujolle, P. Rolin, « *Réseaux et principes fondamentaux* », Cours Master Informatique 2ème Année, Université d'Angers, France, A.U : 1999-2000.

[2] A. Ratsimbazafy, « *Réseaux Informatiques* », Cours L2-TCO, Dép. TCO-E.S.P.A., A.U. : 2010-2011.

[3] L.E. Randriarijaona, « *Réseaux TCP/IP* », Cours L3-TCO, Dép. TCO-E.S.P.A., A.U. : 2011-2012.

[4] B. Cousin, « *Réseaux et généralités* », Université IRISA-Campus de Beaulieu-Rennes, 2002.

[5] A. Aoun, « *Réseaux informatiques* », Université Paul Sabatier, Toulouse III, 2005.

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

[7] « Cisco CCNA Discovery 4 », « Conception et prise en charge des réseaux informatiques » version 4, CCNA 2002

[8] « Cisco CCNA Exploration 3 », version 4, CCNA 2002

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

[10] http://cisco.goffinet.org

[11] K. Trabelsi, H. Amara « *Mise en place des réseaux LAN interconnectés en redondance par deux réseaux WAN* », Université virtuelle de Tunis, A.U. : 2010-2011.

[12] B. Feneuil, « *Réseaux* », Université Louis Rascol, 1998.

[13] P. Nicolas, « *Cours de réseaux* », Master 1 informatique, Université d'Angers, 2006.

[14] http://mfb-mg.gov, 2016

[15] B. Cousin, « *Réseaux et généralités* », Université IRISA-Campus de Beaulieu-Rennes, 2002.

[16] A. Aoun, « *Réseaux informatiques* », Université Paul Sabatier, Toulouse III, 2005.

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

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

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

PAGE DE RENSEIGNEMENTS

Nom : ANDRIANTSALAMA

Prénoms : Nomentsoa Nampoina

Adresse de l'auteur : 193 Manjaka Ilafy

Téléphone : +261 32 49 838 30

E-mail : noments77@gmail.com

Titre du mémoire :

«CONCEPTION ET MISE EN PLACE DU RESEAU HIERARCHIQUE A HAUTE DISPONIBILITE AU SEIN DU MFB »

Nombre de pages : 85

Nombre de tableaux : 3

Nombre de figures : 37

Encadreur : Monsieur RANDRIARIJAONA Lucien Elino

Email : elrandria@yahoo.fr

Tel : 032 04 747 95

RESUME

La conception de réseau dépend des objectifs voulus, des exigences et les attentes des entreprises. Par rapport à ces objectifs, la nouvelle conception doit les implémenter. La topologie ainsi créé doit aussi répondre aux points suivants : la disponibilité, une transmission rapide, efficace, fiable et la sécurité des équipements. La création de VLAN est nécessaire pour un réseau de grande envergure. Au sein du MFB, les exigences mis en priorité sont la disponibilité, la sécurité, la facilité de gestion et la performance. La conception de réseau Hiérarchique est retenue pour la topologie du réseau. On a pu aussi faire connaissance des protocoles utilisés pour de la haute disponibilité tel que les STP, HSRP et Etherchannel. Pour la sécurité du réseau, on a choisi l'équipement Cisco ASA qui a l'avantage d'intégrer les différentes solutions nécessaire pour protéger le réseau.

Mots clés : Hierarchique, Vlan, EtherChannel, Cisco ASA, Disponibilité

ABSTRACT

The design of network depends on the wanted objectives, the requirements and waitings of the companies. Compared to these objectives, the new design must implement them. Topology thus created must also answer the following points: the availability, a fast, effective, reliable transmission and the safety of the equipment. The creation of VLAN is necessary for a network of great scale. Within the MFB, the requirements put in priority are the availability, safety, the facility of management and the performance. The design of Hierarchical network is retained for the topology of the network. One also could become acquainted with the protocols used for high availability such as the STP, HSRP and Etherchannel. For the safety of the network, one chose the equipment Cisco ASA which with the advantage of integrating different the solutions necessary to protect the network.

Key words : Hierarchical, Vlan, EtherChannel, Cisco ASA, Availability