Rapport de Stage

Au sein de la société
Compagnie Bureautique et Informatique
Du 18/07/2011 à 31/08/2011

Sujet :

Proposition d'une nouvelle architecture LAN et implémentation d'un réseau d'une entreprise

Réalisé par :
LABRIKI Issam
ELMANSOUR Mohamed

Encadré par :
Mr. Mohamed NSIRI
Chef de Section Réseaux

4ème année Système et Réseaux Informatique

Année universitaire 2010/2011

Remerciement

Au terme de notre travail, nous tenons à remercier M.Mohamed NSIRI chef de Projet pour son accueil chaleureux, ainsi que Mr Mohamed DINOURI, le directeur, de nous avoir acceptés en tant que stagiaires au sein de la société **CBI**.

Ensuite, on profite de lôoccasion pour exprimer notre profonde reconnaissance et gratitude envers lôensemble du corps professoral et administratif de **lôEcole Supérieure en ingénierie de lôinformation, Télécommunication Et Management** qui, sans leurs efforts désintéressés, notre intégration ne saurait avoir lieu.

Que toutes ces personnes trouvent ici lôexpression de nos sincères remerciements.

Résumé

De nos jours, les entreprises s'orientent de plus en plus à posséder leur propre parc de réseau informatique sous forme d'un LAN (Local Area Network) Ethernet permettant ainsi l'échange des données.

La haute disponibilité et l'efficacité de ces réseaux sont alors des facteurs déterminants dans le bon déroulement de l'activité de l'entreprise.

Par conséquent, dans la perspective de proposer aux entreprises des solutions adaptées à leurs besoins actuels et futurs, on a étudié durant notre stage au sein de **CBI** les architectures classiques déployées jusqu'à présent afin de relever leurs limitations et proposer par la suite une architecture offrant la disponibilité, l'évolutivité et la sécurité.

Et pour mettre en évidence les apports de cette nouvelle architecture proposée, une étude de cas réelle de déploiement d'un réseau d'entreprise a été faite.

PLAN

Sommaire

Introduction générale

De nos jours, les entreprises sôorientent de plus en plus à posséder leur propre parc de réseau informatique sous forme dôun LAN (Local Area Network) Ethernet permettant lôéchange des données et lôoptimisation du temps de travail. Les réseaux LANs sont de plus en évolution continue afin de supporter de nouvelles applications, notamment les applications temps réel distribuées, la téléphonie sur IP, la visioconférence, le E-commerceé .

Face à ces nouvelles applications, la haute disponibilité et lôefficacité de ces réseaux sont des facteurs déterminants dans le bon déroulement de lôactivité de lôentreprise, surtout face aux pannes imprévisibles. Pour assurer cette haute disponibilité, il sôavère nécessaire de procéder à la redondance des équipements et des liens constituant le réseau. Ce réseau peut également implémenter un ensemble de mécanismes de partage de charge pour mieux exploiter la bande passante disponible.

Côest dans ce cadre que sôinscrit notre projet de fin dôétudes au sein de la société **CBI**. Ce projet consiste à proposer une architecture LAN offrant surtout une haute disponibilité en réduisant la durée de convergence du réseau, et assurant un partage facile et dynamique de charge toute en gardant la configuration et lôadministration simple et facile à mettre en î uvre.

Le présent rapport est structuré comme suit :

Le premier chapitre comporte une étude théorique et pratique permettant la compréhension des VLANs, des protocoles VTP, Spanning Tree ainsi que lôHSRP. Ce qui sôavère nécessaire pour relever les limitations des réseaux commutés (ceux utilisant les protocoles niveau 2) en analysant les résultats des maquettes mises en place.

Le second chapitre donne un aperçu global sur les technologies et protocoles niveau 3 et propose une architecture reposant dessus. Il décrit ainsi les bénéfices importants apportés par une architecture dôaccès routé, où les commutateurs dôaccès sont des routeurs avec des liens « uplinks » en mode routé point à point vers les commutateurs de distribution.

Le troisième chapitre traite un exemple d'implémentation d'une solution mettant en œuvre les nombreux avantages qu'ont les protocoles de niveau 3. Il s'agit de mettre en place un réseau d'une entreprise dont les sites sont éparpillés sur tout le territoire national. Pour ce faire, un récapitulatif des besoins de cette entreprise est donné, suivi de la proposition des architectures physiques et logiques répondant aux besoins exprimés. Une justification des différents choix de mise en place est présentée avant de détailler la logique d'adressage utilisée, pour donner à la fin quelques éléments relatifs à l'évolution future du réseau.

Présentation de l'entreprise

La CBI (Compagnie Bureautique Informatique), entreprise 100% marocaine a été Fondée en 1970 sur la base dôun contrat de distribution avec TOSHIBA pour OFFICE AUTOMATION et RUF pour les machines mécanographiques. Depuis sa création, l'offre globale solutions (produits et services) de CBI est restée centrée sur les technologies de l'information et n'a cessé de s'enrichir en intégrant les innovations technologiques afin de pouvoir répondre aux besoins de ses clients et d'être toujours en avance dans un monde en perpétuelle mouvance.

L'offre solutions de la CBI couvre des produits et des marchés complémentaire (bureautique, informatique, systèmes d'information, télécommunications, Internet/Intranet) mais toujours orientés vers les nouvelles technologies et les outils de productivité.

Cette offre, constituée de produits de haute technologie leaders sur leurs marchés et construite grâce à des partenariats très étroits avec les fournisseurs internationaux (prises de, participations, contrats, partenariats, etc.), représente une consolidation continue de savoir faire et de compétences.

La CBI répond aux besoins du marché grâce à ses équipes propres et aux partenariats internationaux ou locaux passés avec les acteurs majeurs du marché.

Aujourdôhui la CBI est structurée en 4 pôles (business units):

1. Pôle Bureautique

2. Pôle Informatique

3. Pôle Intégration Systèmes

4. Pôle Réseaux et Télécoms

La division Réseaux et Télécoms, ou CBI Networks, dans laquelle jôai été intégré, a été impliquée très tôt dans la conception et la mise en place de réseaux privés chez des clients prestigieux. Elle a suivi lôévolution technologique en maintenant en permanence un savoir-faire et une compétence de très haut niveau. La plupart des ingénieurs et techniciens intervenants dans les projets dôétude et de déploiement de réseaux sont certifiés par les fabricants des matériels utilisés et ont plusieurs années dôexpérience sur le terrain.

Au fil des années, CBI Networks a su développer des partenariats avec les leaders mondiaux du secteur. Côest avec eux quôelle intervient sur lôensemble des projets quôelle développe. La veille technologique permanente ainsi que les relations avec ses partenaires sont une garantie de la qualité des solutions proposées et de leur adéquation aux objectifs définis par les utilisateurs

A ces divisions sôajoute une unité administrative et logistique qui supporte lôensemble des activités de lôentreprise.

Fin 2002, un centre de formation a également été mis en place de manière à avoir une structure permanente avec les équipements les plus modernes pour la formation aussi bien interne quôexterne.

Les principales activités de la CBI sont :

- La mise en î uvre
- Lôassistance technique
- La formation
- Lôintégration système
- La maintenance

1976	Introduction du premier photocopieur à papier ordinaire
1977	Introduction des mini-ordinateurs **RUF**
1981	Introduction des micro-ordinateurs **TOSHIBA**
1982	Connexion du PC site central en **BSC**
1986	Introduction des fax **TOSHIBA** Introduction des ordinateurs portables **TOSHIBA**
1987	Création de la division **DATACOM** pour introduction du réseau **X25** avec **TRT** Introduction du réseau local TenNet
1991	Introduction des systèmes dôexploitation **SCO UNIX**, **Novell** et du **SGBDR Informix**
1993	Introduction des plates-formes **INTEL**
1994	Introduction des systèmes de développement **MAGIC**
1995	Introduction des systèmes Multimédia
1996	Choisis par lô**ONPT** comme société de commercialisation des services Internet Centre de formation agréé **INFORMIX**, **UNIX**, **MAGIC**
1997	Partenaire direct des produits de **IBM** (Serveur, Poste de travail) et des produits **BayNetworks** (Switch, Hub et Routeur)
1998	Introduction du photocopieur numérique Partenaire **CS Telecom** et **CISCO** pour les solutions Télécommunication
1999	Partenaire solutions **ORACLE** et **Business Object** Lancement des copieurs numériques **TOSHIBA** multifonctions
2000	Partenaire **IBM** solutions **RISC 6000**
2002	Inauguration du Centre de Formation en Réseaux & Télécoms
2003	Partenariat avec **Filenet** (GED/Workflow)
2004	Partenariat avec **SSA Global** (ERP) Partenariat avec **Sonatel Multimedia** (Sénégal)
2005	Partenariat avec **Hyperion**

CHAPITRE 1
Etude des architectures LAN classiques

- VLANs et VTP
- Spanning-tree
- HSRP
- Limitations des protocoles de niveau 2.

Afin de proposer de nouvelles architectures en termes de réseaux LAN, une étude approfondie des architectures classiques de niveau 2 sôimpose. En effet, on sera amené à étudier profondément les réseaux VLAN, les protocoles VTP, Spanning Tree ainsi que lôHSRP afin de mettre le point sur les différentes faiblesses de ceux-ci.

Lœétude ainsi prévue sera théorique dôune part et pratique dôune autre part. En effet, pour relever les limitations des réseaux commutés (ceux qui utilisent les protocoles de niveau 2), on procédera dôabord par une étude théorique détaillée de ces dites technologies suivie par une manipulation de chacune dœelles sur maquette.

I. VLAN et VTP :

1. Généralité sur les VLANs :

La plupart des attaques sur les réseaux proviennent de l'intérieur de l'entreprise. Il est donc indispensable de garantir une certaine étanchéité entre les différents utilisateurs des services d'un réseau d'entreprise.

Un réseau local virtuel, ou VLAN, est une solution de niveau 2 qui permet de connecter avec un matériel adapté (Switch VLAN) un groupe logique de stations de travail, même si ces dernières ne sont pas géographiquement proches les unes des autres.

Un VLAN permet de partitionner un réseau local de manière logique, de telle sorte que le domaine de diffusion pour un VLAN soit limité aux nî uds et aux commutateurs membres du VLAN.

Les VLANs offrent les avantages suivants :

- ✓ Regroupement d'utilisateurs qui ont besoin d'accéder aux mêmes ressources.
- ✓ Plus de souplesse pour l'administration et les modifications du réseau car toute l'architecture peut être modifiée par un simple paramétrage des commutateurs.
- ✓ Gain en sécurité car les informations sont encapsulées dans un niveau supplémentaire et éventuellement analysées.
- ✓ Réduction de la diffusion du trafic sur le réseau : Un flux originaire d'un VLAN nommé n'est transmis qu'aux ports qui appartiennent à ce même VLAN

- ✓ Flexibilité et évolutivité : Les utilisateurs peuvent être groupés indépendamment de leurs emplacements physiques dans des segments virtuels. Aussi, on peut facilement créer dôautres segments ou diviser le segment contenant un grand nombre de machine.

2. Le mode trunk :

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

Les trunks peuvent être utilisés :

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

Il existe plusieurs protocoles dôétiquetage à savoir le 802.1Q, lôISL...etcé .Certains de ces protocoles sont propriétaires et ne fonctionnent que sur les équipements d'une seule marque.

- ➢ Inter-Switch Link (ISL)

Développé spécifiquement pour les équipements Cisco, lôISL est utilisé sur des ports FastEthernet et GigaBitEthernet et permet dôencapsuler les trames dôorigine dans des trames plus grandes. Les trames ISLs ont la forme suivante :

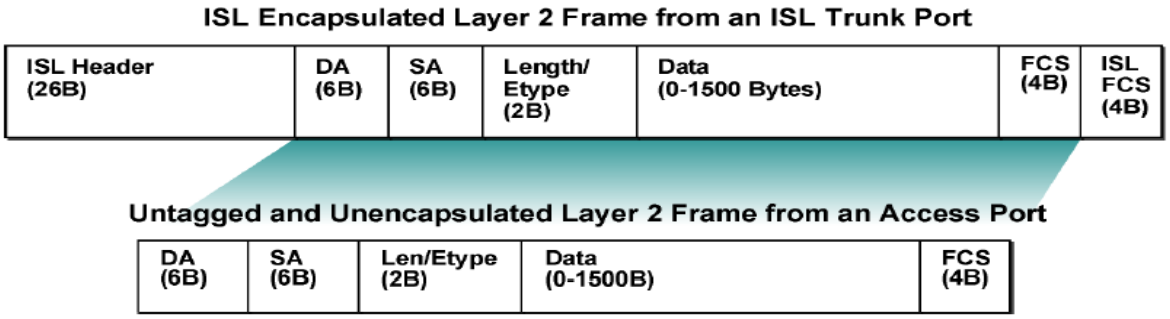

Figure 1:Trame ISL (Inter-Switch Link)

- IEEE 802.1Q

Le standard IEEE 802.1Q fournit un mécanisme d'encapsulation très répandu et implanté dans de nombreux équipements de marques différentes. Comme dans le cas de l'encapsulation ISL précédente, l'en-tête de trame est complété par une balise de 4 octets.

La forme de la trame dans ce cas est :

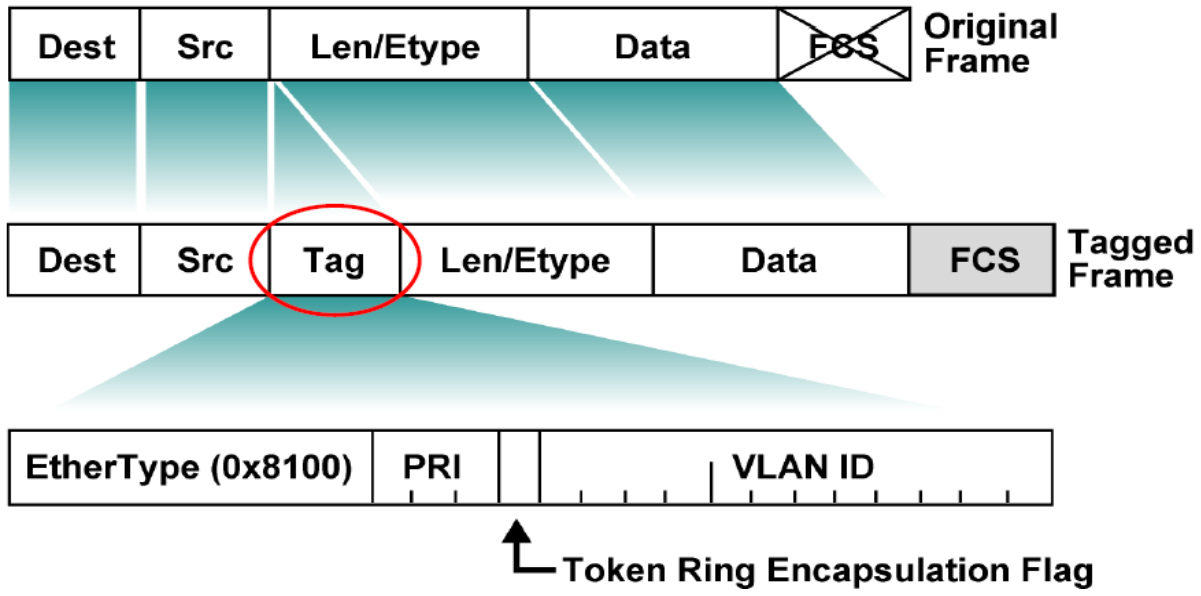

Figure 2:trame IEEE 802.1Q

Les champs qui composent le Tag IEEE 802.Q sont:

-Priorité (3bits): permet dôassigner 8 niveaux de priorité à une trame Ethernet (0 = priorité élevée et 7 la plus faible priorité)

-CFI (Canonical Format Indicator) 1bit: il est à 0 dans le cas de lôEthernet, et à 1dans le cas du TokenRing.

-VLAN ID (12 bits): identifiant du VLAN.

3. Routage inter-vlan

Pour assurer la communication entre différentes machines appartenant à différents VLANs, il est impératif de passer par la couche niveau 3 (un routeur). Côest ce quôon appelle routage Inter-VLAN.

Lôimplémentation du routage Inter-VLAN nécessite un dispositif de routage qui possède plusieurs interfaces (une par VLAN). Ces interfaces peuvent être physiques ou virtuelles. Les machines dans un VLAN auront comme passerelle lôinterface du VLAN.

Une illustration pratique de cette notion est donnée dans le paragraphe suivant.

4. Maquette VLANs

Afin dôassimiler la notion des VLANs et de lui donner un aspect plus pratique, une maquette illustrative est mise en place.

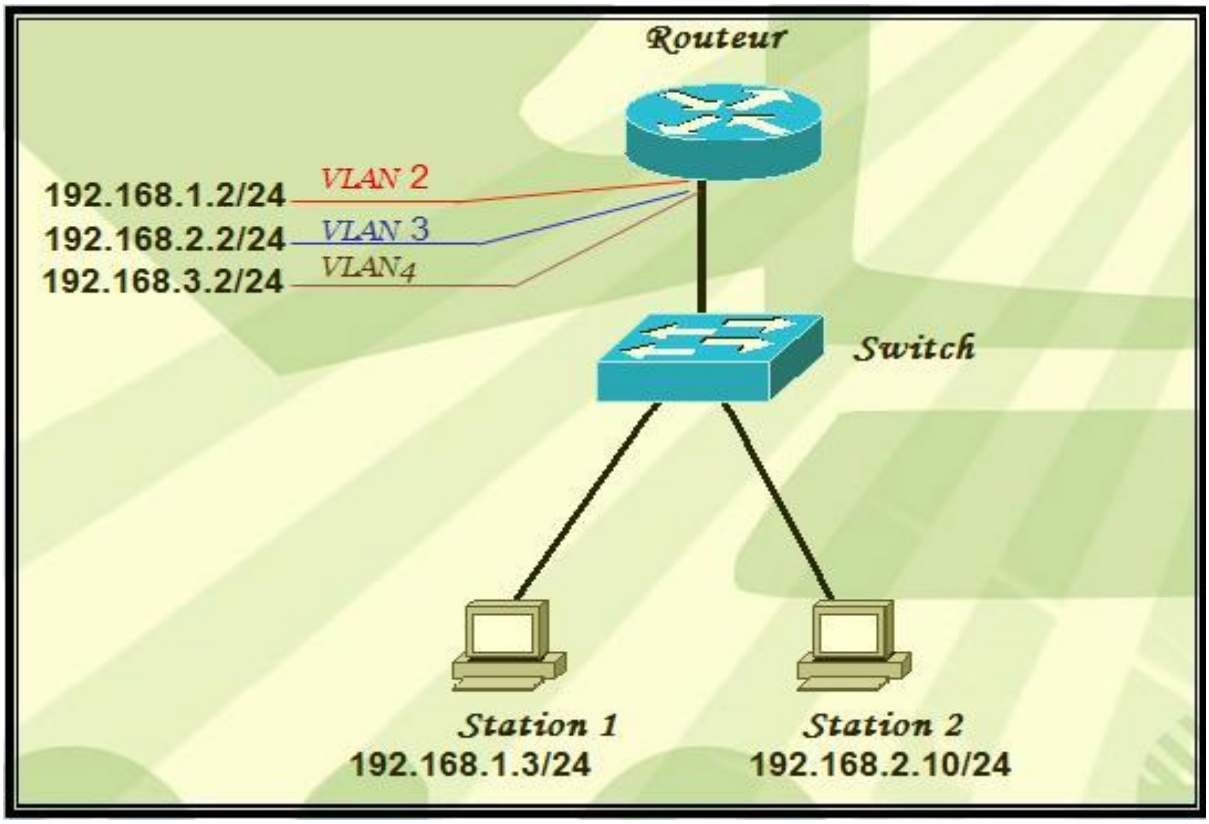

Figure 3: Maquette VLANs

Dans cette topologie, on a proposé un nombre de VLANS qui seront créés au niveau du switch. Ci-dessous la configuration qui permet de créer un VLAN, dôaffecter un port du switch et une adresse réseau à ce VLAN:

```
S#vlan database
S(vlan)#vlan 2
S(vlan)#exit

S(config)#interface fastEthernet 0/4
S(config-if)#switchport mode access
S(config-if)#switchport access vlan 2

S(config)#interface vlan 2
S(config-if)#ip address 192.168.1.1 255.255.255.0
S(config-if)#no shutdown
```

- Configuration dôun trunk :

Vu quôon dispose dôun ensemble de VLANs qui peuvent éventuellement communiquer entre eux, le port du switch auquel est relié le routeur doit être configuré en mode Trunk pour acheminer les trafics de ces différents VLANs.

Exemple de configuration dôun trunk :

```
S(config)#interface fastEthernet 0/1
S(config-if)#switchport mode trunk
S(config-if)#switchport trunk encapsulation dot1q
```

Au niveau du routeur, des sous-interfaces sont créées, chacune correspondant à un réseau VLAN :

```
R(config)#interface fastEthernet 0/0.2
R(config-subif)#encapsulation dot1Q 2
R(config-subif)#ip address 192.168.1.2 255.255.255.0
R(config-subif)#no shutdown
```

5. VLAN Trunking Protocol : VTP

VTP ou VLAN Trunking Protocol est un protocole utilisé pour configurer et faciliter lôadministration de VLANs dans un réseau commuté. Quand on configure un nouveau VLAN dans un serveur VTP, le VLAN est distribué à travers tous les commutateurs du domaine. Ceci réduit le nombre de configuration des VLANs dans les autres commutateurs. Le protocole VTP, disponible dans la plupart des produits des séries Catalyst, est une marque déposée de Cisco.

Le protocole VTP apporte les avantages suivants:

- configuration consistante des VLANs dans le réseau.
- gestion centralisée des VLANs.
- Facilité de gestion des VLANs.

Tous les commutateurs appartenant au même domaine VTP doivent partager les mêmes informations sur les VLANs. Chaque domaine VTP est identifié par un nom et chaque commutateur doit appartenir à un seul domaine VTP.

Un commutateur peut être configuré pour opérer dans un des modes suivants :

- Server: Dans ce mode, on peut créer, modifier, ou supprimer des VLANs. le serveur VTP génère et reçoit des annonces VTP et synchronise sa configuration avec les autres commutateurs du domaine. Le mode server est le mode par défaut.
- Client: les clients VTP traitent et transmettent les annonces reçues et synchronisent les informations de configuration VLAN avec les autres commutateurs.
- Transparent: Un commutateur VTP transparent n'annonce et ne synchronise pas sa configuration VLANs. il ne fait que transmettre les annonces VTP qu'il reçoit à son port trunk.

Du moment qu'on aura besoin de plusieurs VLANs dans la partie traitant le Spanning Tree (voir Figure 6 : Maquette STP), il est nécessaire d'assurer leur gestion à travers la configuration du protocole VTP.

Le switch S1 sera en mode serveur, et les autres switchs seront les clients VTP. Il est nécessaire que le serveur S1 et les clients VTP S2 et S3 soient inclus sous le même nom de domaine VTP. La configuration de ceux-ci est présentée ci dessous:

```
S1#vlan database
S1(vlan)#vtp domain Cisco
S1(vlan)#vtp server

S2#vlan database
S2(vlan)#vtp domain Cisco
S2(vlan)#vtp client

S3#vlan database
S3(vlan)#vtp domain Cisco
S3(vlan)#vtp client
```

II. Spanning Tree :

STP est un protocole de gestion de couche 2, qui fournit des chemins redondants dans un réseau tout en évitant les boucles de routages. Tous les protocoles STP utilisent un algorithme qui calcule le meilleur chemin sans boucle à travers le réseau.

Dans les réseaux Ethernets, un seul chemin actif peut exister entre deux stations. Plusieurs chemins actifs entre des stations causent inévitablement des boucles dans le réseau. Lorsque les boucles surviennent, certains commutateurs reconnaissent une même station sur plusieurs ports. Cette situation entraîne des erreurs au niveau de l'algorithme d'expédition et autorise la duplication de trames qui seront expédiées.

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

Tous les commutateurs dans un LAN étendu participant dans un arbre « spanning » assemblent des informations sur les autres commutateurs du réseau à travers des échanges de messages de données connues comme des messages BPDU (Bridge Protocol Data Unit).

Cet échange de message aboutit aux actions suivantes :

- Un commutateur Root unique est élu pour la topologie réseau spanning tree.
- Un commutateur désigné est élu par segment de LAN commuté.
- Toutes les boucles dans un réseau commuté sont éliminées en plaçant des ports redondants de commutateur à l'état Backup ; tous les chemins non nécessaires pour joindre le commutateur Root depuis n'importe où dans le réseau commuté sont placés en mode STP bloqué.

En général, chaque commutateur possède un identificateur Bridge ID. Le Bridge ID est une suite de 8 octets (Figure 4).

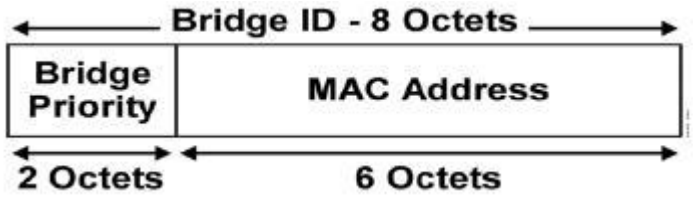

Figure 4:Bridge ID

Chaque commutateur envoie son Bridge ID dans un BPDU aux autres commutateurs et le compare avec ceux reçus. Le commutateur qui possède la plus petite priorité est le commutateur racine. Dans le cas dûne même priorité, lôadresse MAC est utilisée et le commutateur avec la plus petite adresse MAC dans le réseau devient le commutateur Root.

Des changements topologiques peuvent se produire dans les réseaux commutés suite au changement d'état d'une ligne (de up à down et inversement). Quand un port qui ne participait pas à la topologie passe directement à l'état d'acheminement, cela peut créer des boucles. Les ports doivent attendre la nouvelle information de topologie pour se propager par les commutateurs dans le LAN avant qu'ils ne puissent commencer à acheminer les trames. Aussi, ils doivent permettre à la durée de vie des trames d'expirer pour les trames qui ont été expédiés en utilisant l'ancienne topologie.

La figure suivante illustre le changement d'état dûun port

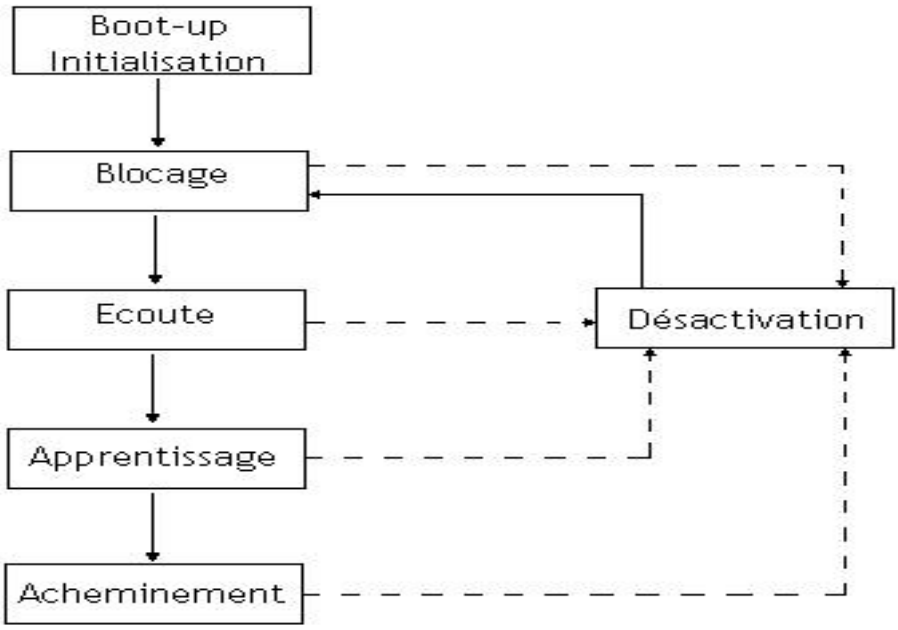

Figure 5: Etats des ports STP

Avant de passer à lôétat dôacheminement, le port reste dans lôétat bloqué 20 secondes, 15 secondes dans lôétat dôecoute et 15 secondes dans lôétat dôapprentisage avant de passer à lôétat dôacheminement.

Pour illustrer ce changement dôétat, la maquette suivante sôest avérée nécessaire.

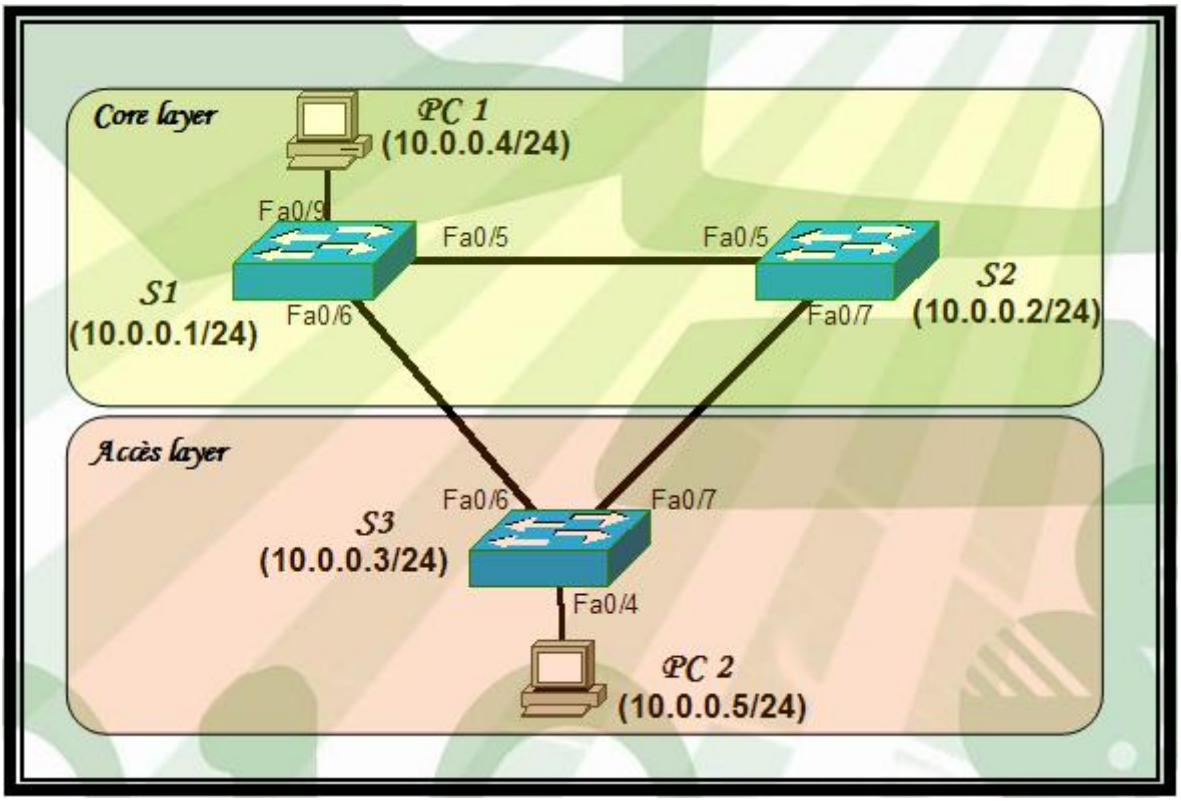

Figure 6:Maquette Spanning tree

La topologie ci dessus suit le modèle hiérarchique de Cisco. En effet, les commutateurs S1 et S2 font partie du Core layer alors que le commutateur S3 appartient à lôAccess layer. Le PC1 est considéré comme serveur.

Le protocole Spanning tree est activé par défaut dans les commutateurs Cisco, les Catalysts. Du fait, les 3 switchs ont la même priorité. La sélection de la racine dans se cas, se base sur la comparaison des adresses MAC. En effet, la racine est le nî ud dont lôadresse MAC est la plus petite.

Cependant, il est plus commode dôabandonner la configuration par défaut en faveur dôun choix dôune racine appartenant au backbone du réseau vu que ses switchs sont en général les plus puissants. Les commandes suivantes sont celles utilisées dans ce cas :

```
S1(config)#spanning-tree vlan 1 root primary
S2(config)#spanning-tree vlan 1 root secondary
```

S1 est désormais la racine et S2 est son backup. S2 deviendra le Root si S1 tombe en panne.

Suite à une défaillance dans une liaison désignée, lôalgorithme du Spanning Tree est réexécuté et le port de réserve transite par les différents états : 20 secondes dans lôétat blocking, 15 secondes dans lôétat listening et 15 secondes dans lôétat learning avant de passer à lôétat forwording.

Ce temps de transistion se traduit par la perte de 6 pings consécutifs comme le montre lôimage suivante :

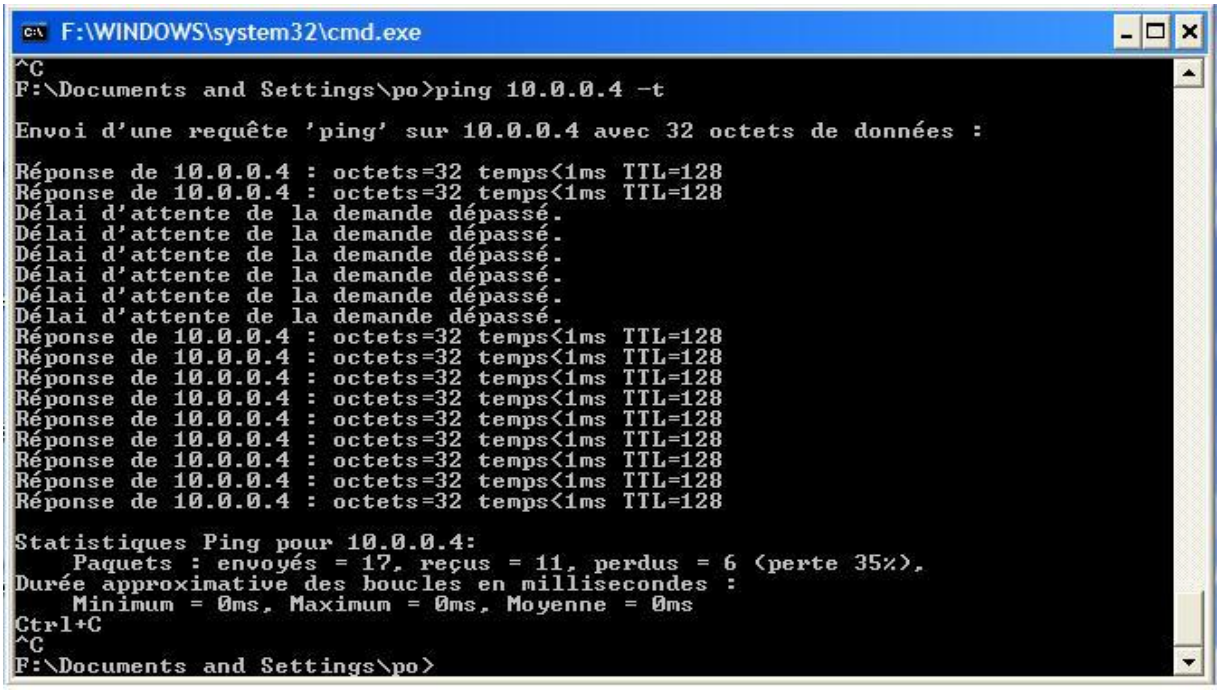

Figure 7: Temps de transition Spanning-tree

1. Les optimisations Cisco :

Pour optimiser le temps de convergence illustré dans la figure 7, Cisco a introduit quelques améliorations dont on cite :

- PortFast
- UplinkFast
- BackboneFast
- STP par VLAN (PVST: Per-VLAN Spanning Tree)
- Common Spanning Tree(CST)
- PVST+
- Multiple Spanning Tree(MST)

On se contente de détailler ci-dessous les deux premières optimisations.

- PortFast :

Si on connecte une station sur un port d'un commutateur, on est contraint d'attendre 50 secondes avant que la station puisse envoyer et recevoir des données. Ce délai pose un problème de timeout pour certaines applications, notamment dans le cas du DHCP. Aussi, si l'on connecte un simple PC à ce port, il n'introduira jamais de boucle comme c'est le cas pour un switch. Donc la configuration comme un PortFast est un moyen qui permet de réduire le temps nécessaire pour que le port passe à l'état forwarding.

- UplinkFast :

L'UplinkFast est une solution qui permet d'activer rapidement un port bloqué (port de backup) d'un switch d'accès au cas où son port racine principal (root port) tombe en panne, et ceci sans attendre la convergence du STP. Le port bloqué passe vers l'état forwarding dans 5 secondes alors qu'avec le STP, il lui faut une cinquantaine de secondes.

2. Rapid Spanning Tree Protocol (RSTP):

Le Rapid Spanning tree est défini par la norme IEEE 802.1w. Ce protocole propose une meilleure définition de l'état et des rôles des ports.

Le protocole RSTP spécifie un peu plus l'état «blocking» en lui donnant la possibilité d'être «alternate» ou «backup». Alternate signifie que le port peut passer rapidement à l'état de «designated» si 3 trames

BPDU consécutives ne sont pas reçues depuis le designated actuel. Lors de la connexion d'un commutateur au même segment via plusieurs interfaces, toutes ces interfaces passent vers l'état backup sauf une d'entre elles, qui reste dans l'état forwording. En cas de défaillance de l'interface principale (initialement en designated), ces ports pourront automatiquement basculer à l'état forwarding.

III. Protocole HSRP :

HSRP (Hot Standby Redundancy Protocol) est un protocole propriétaire Cisco, donc configurable uniquement sur des équipements Cisco, fournissant une connectivité ininterrompue dans un réseau exécutant le protocole IP. Ce système implique obligatoirement l'utilisation de deux ou plusieurs routeurs (passerelles), il consiste en l'utilisation partagée d'une adresse IP dite virtuelle (VIP) et une adresse MAC (couche 2) virtuelle entre les routeurs configurés pour l'HSRP. Ainsi, tous les autres hôtes distants et équipements réseau situés sur le LAN, auront comme passerelle par défaut ce routeur virtuel avec une adresse IP et MAC virtuelles.

VIP (Virtual Internet Protocol) est une adresse IP virtuelle représentée par le groupe HSRP. Tous les hôtes distants sur le réseau communiqueront avec le routeur actif avec son VIP. Cependant, les communications échangées entre les routeurs d'un même groupe se font avec leur adresse physique (propre à chaque routeur) pour pouvoir les identifier.

La VIP est configurée manuellement par l'administrateur, et l'adresse MAC est de la forme 0000.0c07.acXX, xx représentant le groupe HSRP en hexadécimal.

C'est cette adresse MAC virtuelle qui sera utilisée par les hôtes distants pour les résolutions d'adresses (ARP) et la VIP pour les adresses sources ou destinataires lors de l'acheminement des paquets. Cependant, lorsque les routeurs au sein d'un groupe HSRP « communiquent » entre eux, les adresses physiques sont utilisées pour pouvoir identifier chacun des routeurs.

Le protocole HSRP utilise les notions suivantes :

- Un routeur « Actif » est un routeur sélectionné pour acheminer les paquets. Tout le trafic réseau entre et sort de ce routeur.

- Un routeur « Standby » est un routeur de secours qui prendra le rôle de routeur actif si ce dernier est en panne, et si les conditions nécessaires à lœélection sont rassemblées. Bien que celui-ci ne participe pas

  à lœacheminement des paquets, il communique avec les routeurs de son groupe HSRP par lœenvoi périodique de paquets HSRP.
- Un groupe HSRP regroupe tout les routeurs participant à une même « jonction » du réseau de lœentreprise. Un réseau peut être composé de plusieurs groupes HSRP, et un routeur peut appartenir à plusieurs groupes HSRP.

Pour bien comprendre le fonctionnement du protocole HSRP, la maquette suivante a été mise en place:

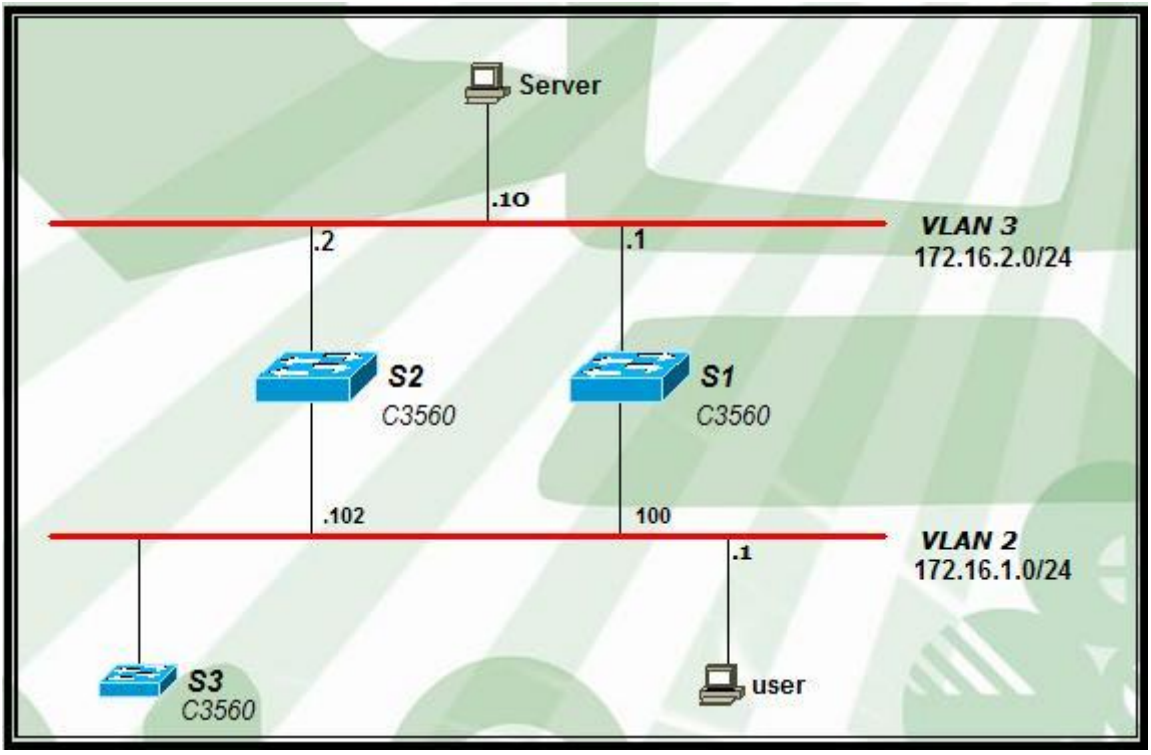

Figure 8:Maquette HSRP

Les switchs S1 et S2, dont les propriétés sont regroupées dans le tableau ci-dessus, appartiennent au même groupe HSRP.

	S1	S2
Etat	Active	Standby
Matériel	Cisco 3560	Cisco 3560
Interface HSRP	FastEthernet 0/2	FastEthernet 0/2
Adresse IP / masque	172.16.2.101/24	172.16.2.102/24
Priorité	105	Par défaut
VIP	172.16.2.100	
Adresse MAC virtuelle	0000.0c07.ac01	

La configuration du protocole HSRP dans les deux switchs se fait de la manière suivante :

```
S1(config)#interface fastEthernet 0/1
S1(config-if)#no switchport
S1(config-if)#ip address 172.16.2.1 255.255.255.0
S1(config-if)#no shutdown
S1(config)#interface fastEthernet 0/2     // mode de configuration interface
S1(config-if)#no switchport                // desactivation du switchport
S1(config-if)#ip address 172.16.1.101 255.255.255.0 //configuration adresse ip et masque
S1(config-if)#standby 1 ip 172.16.1.100 // configuration HSRP VIP
S1(config-if)#standby 1 priority 105   // configuration de la priorité
S1(config-if)#standby 1 preempt        // activation de preemption

S2(config)#interface fastEthernet 0/1
S2(config-if)#no switchport
S2(config-if)#ip address 172.16.2.2 255.255.255.0
S2(config-if)#no shutdown
S2(config)#interface fastEthernet 0/2
S2(config-if)#no switchport
S2(config-if)#ip address 172.16.1.102 255.255.255.0
S2(config-if)#standby 1 ip 172.16.1.100
S2(config-if)#standby 1 preempt
```

Dans son état actif, un routeur transmet les paquets envoyés à lôadresse MAC virtuelle du groupe. Il répond aussi aux messages ARP destinés à lôadresse IP virtuelle. Pour vérifier ceci on utilise la commande **tracert** :

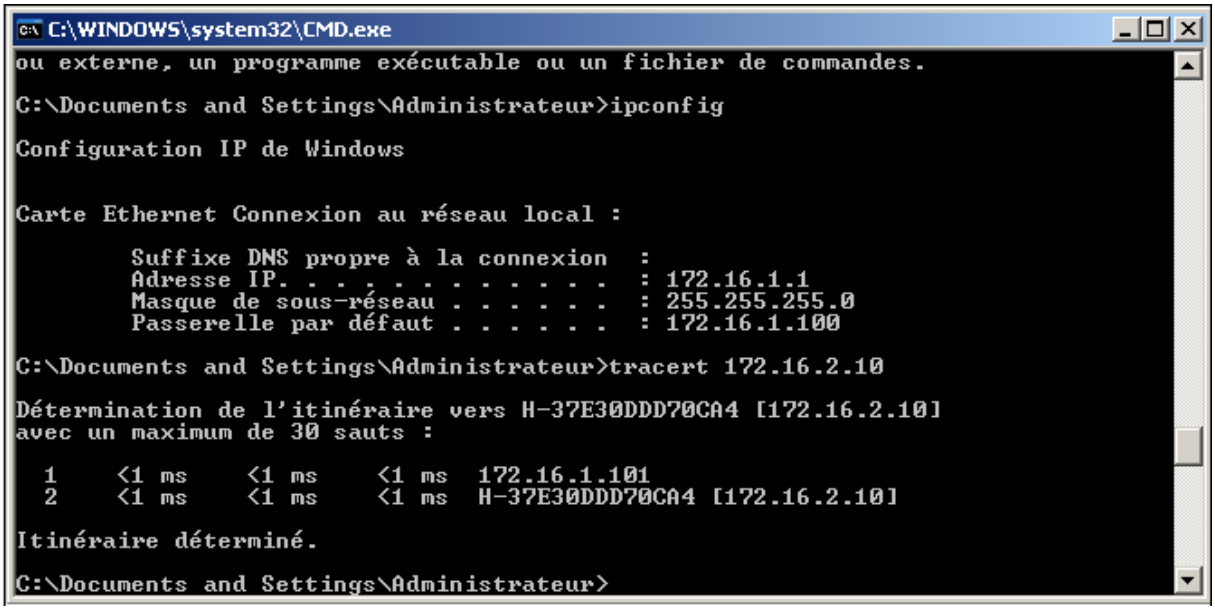

Figure 9:Transition par S1

Pour arriver à la destination 172.16.2.10 les messages transitent par le routeur S1.

Maintenant, on fait passer lôinterface fa 0/2 de S1 de lôétat up à lôétat down et on lance un ping continu à partir de lôadresse 172.16.1.1.

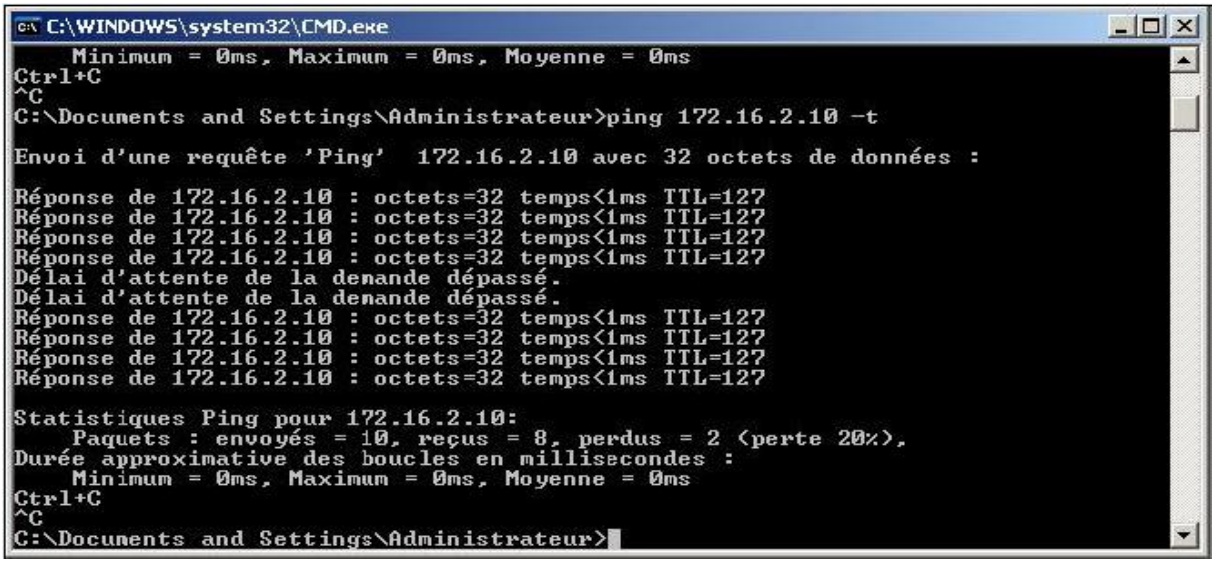

Figure 10: Temps de transition HSRP

On remarque que la destination 172.16.2.10 devient injoignable, et deux paquets du ping sont perdus avant de revenir à lôétat normal. Ceci se traduit par le fait que S1 devient inaccessible et que S2 ne reçoit plus les messages Hello envoyés par le routeur actif. Alors, S2 décide de passer à lôétat actif pour prendre le relais et transmettre les messages du user.

Pour vérifier que cêst S2 qui achemine les messages du user on retape la commande tracert qui donne les résultats suivants :

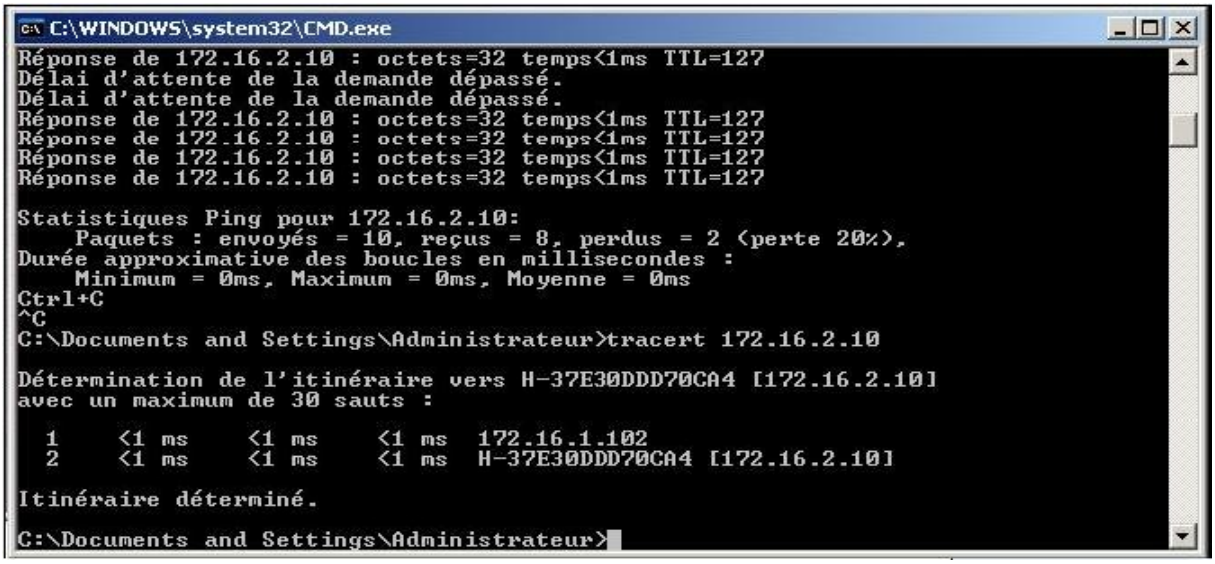

Figure 11:Transition par le routeur de backup

Ces résultats montrent bien que les messages transitent maintenant par le routeur S2.

IV. Limitation des protocoles niveau 2 :

Lôétude précédente et lôanalyse des résultats de lôensemble des maquettes mises en place, nous ont permis de dégager plusieurs limitations et inconvénients des architectures de niveau 2. Dans ce qui suit, on en cite quelques un:

- Temps de convergence important :

Les protocoles de niveau 2 (HSRP et Spanning Tree) présentent un délai de convergence très important. En effet, Des tests à base dôHSRP (voir paragraphe HSRP) ont montré que ce protocole nécessite, lors dôune défaillance dôun lien, au moins un temps de 10s avant de repasser à lôétat fonctionnel.

Dans le domaine Spanning Tree, La rupture dôun lien affecte tout le réseau. Et le temps de la reconstruction de lôarborescence dépasse les 30s. Ce temps de transition est souvent non transparent pour beaucoup dôapplications réseaux.

Malgré le fait que Cisco a introduit plusieurs optimisations pour améliorer le fonctionnement du Spanning Tree sur les liaisons qui ont en besoin, il en reste plusieurs problèmes intrinsèques.

- Administration complexe:

Lorsquôun réseau de grande taille subit un problème, il faut réagir rapidement. Pour cela, il faut disposer dôoutils simples permettant un diagnostic rapide de la panne. Or, lorsquôil sôagit dôun problème de spanning tree, il nôest pas question dôutiliser efficacement un ping ou autre traceroute puisque lôon agit au niveau 2.

- Partage de charge complexe :

Lôutilisation de protocoles de niveau 2 nôaboutit en général pas à une répartition optimale de trafic. En effet, le fonctionnement de Spanning-Tree repose sur la désactivation de ports,

ports réactivés avec la détection dûne défaillance sur les ports actifs. Atteindre un partage de charge avec Spanning-Tree réclame une configuration complexe (définition de plusieurs instances de Spanning-Tree, é) gourmande en mémoire et difficile à analyser en cas de problème.

Aussi, le partage de charge avec HSRP passe par lûutilisation de plusieurs groupes HSRP, chaque partie du trafic aura alors comme passerelle la VIP dûun groupe. Ce mode de partage de charge sûavère aussi complexe et difficile à mettre en î uvre.

- Problèmes dûintroduction dûun nouveau commutateur

Lûintroduction dûun nouveau commutateur engendre plusieurs problèmes. Parmi ces problèmes, on cite lûinstabilité de la topologie Spanning Tree, le changement de la racine de lûarbre Spanning tree et la modification indésirable des VLANs. Chacun de ces points sera détaillé ci-dessous :

- Chaque nouvelle connexion de commutateurs sur le réseau (par exemple dans les salles de réunion), déclenche un nouveau calcul de lûarborescence Spanning Tree. Un calcul lent qui va créer une période dûinstabilité.
- La position de la racine définit la base de lûarborescence du Spanning Tree à partir de laquelle sont calculés les différents chemins vers les commutateurs dûaccès, pour éviter les boucles de niveau 2. Cette racine doit alors être un équipement central du réseau avec une performance de commutation adaptée à la taille du réseau. Si un commutateur, mal configuré (ayant une priorité plus grande), connecté en extrémité prétend à ce rôle de racine, cela cause un changement de racine et perturbe le fonctionnement du réseau.
- Si on ajoute un commutateur avec un nombre de révisons de configuration supérieur, tous les commutateurs en mode Serveur ou Client synchronisent leurs informations VLAN avec ce commutateur, cette opération peut produire une suppression ou création indésirable des VLANs, dûoù un changement de topologie du réseau.

- Contraintes dûArchitecture Accès Layer2

Dans une architecture à couche d'accès niveau 2, Les blocs de base sont les couches Core, distribution et accès :

- ⇨ Le niveau accès fournit la connectivité niveau 2 (les vlans). Il est connecté au niveau distribution à travers des liens niveau 2.
- ⇨ Le niveau distribution fournit l'agrégation de route et représente la démarcation entre les vlans d'accès et le backbone routé. Le niveau distribution est connecté au niveau Core au travers de liens en mode routés point à point.
- ⇨ Le niveau Core fournit un transport haute performance et stable autour de liens GE/10GE en mode routés point à point.

Pour les campus exigeant beaucoup de flexibilité dans l'allocation des subnets et des VLANs (par exemple pour le cas ou les vlans demandent à être partagés entre plusieurs commutateurs d'accès), l'architecture utilisée (Figure 12) est d'établir un trunk Layer2 entre les commutateurs de distribution et donc d'avoir une topologie Spanning Tree en « triangle ».

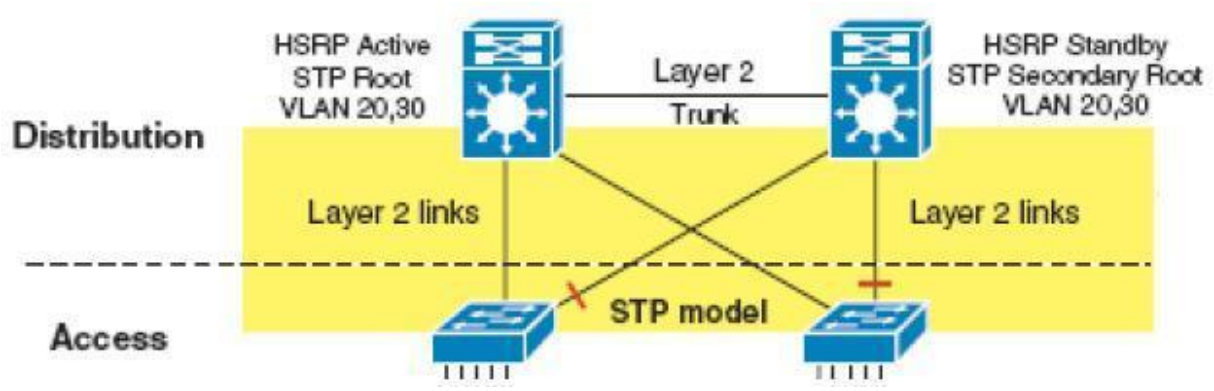

Figure 12:Architecture L3/L2 avec un lien trunk.

Ce modèle introduit des contraintes de Spanning Tree dans la disponibilité globale du réseau de campus. De plus il faudra s'assurer que la gateway HSRP est sur le même commutateur que le commutateur racine du domaine de Spanning Tree.

On peut faire en sorte que ces architectures (pour plus de performance en terme de convergence, de disponibilité et d'exploitation) n'implémentent pas de boucle niveau 2 et ne reposent pas sur le spanning tree. En règle générale, ce sont les architectures les plus déterministes et les plus recommandées (Figure 13). Dans ce cas, Les commutateurs d'accès sont configurés en tant que commutateurs de niveau2 et commutent

le trafic vers les interfaces uplinks. Ces deux liens uplinks sont « forwarding » car il n'y a pas de boucle L2 avec le niveau distribution.

Cependant, La contrainte principale dans le déploiement d'une telle architecture est que chaque vlan doit être localisé sur un seul commutateur.

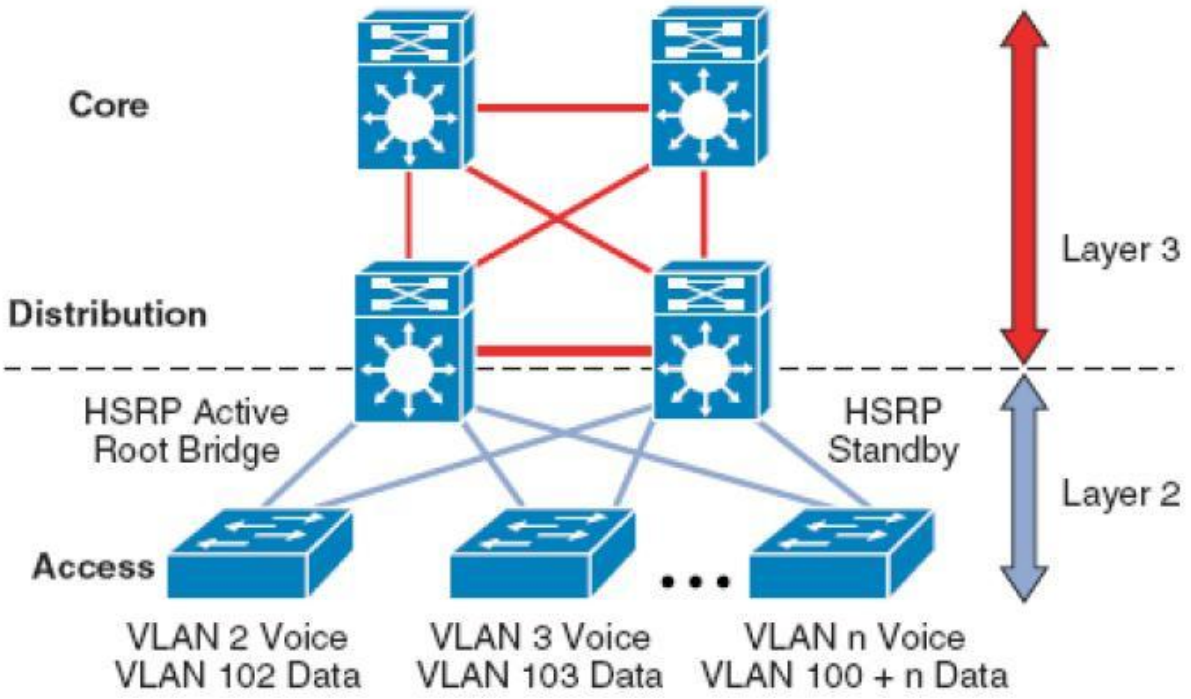

Figure 13: Architecture L3/L2 sans lien trunk.

V. Conclusion

A travers ce premier chapitre, on a donné un aperçu global sur les différents protocoles utilisés dans une architecture à réseaux commutés en analysant les résultats des maquettes mises en place. Cette analyse nous a permis de dégager un ensemble de problèmes et de limitations que nous tiendrons en compte lors de la présentation des nouvelles orientations en matière d'architecture LAN. Des architectures qui seront l'objet du chapitre suivant.

CHAPITRE 2
Proposition d'une nouvelle architecture LAN

- OSPF
- EIGRP
- VRF-Lite
- Avantage des architectures niveau 3

Si les technologies et protocoles LAN classiques en lôoccurrence Spanning tree et HSRP ont montré leur efficacité et ont optimisé lôinterconnexion pendant un certain temps, ils présentaient cependant certaines limitations, leur temps de convergence notamment restait assez long et nôétait pas parfois en faveur du taux de disponibilité requis.

Lôidée pour remédier à ces inconvénients fût dôutiliser des protocoles de niveau 3, des technologies qui ont été développées spécialement pour permettre un fonctionnement dynamique et fournir en conséquence des temps de réponse optimaux.

Dans ce chapitre on décrira ces nouvelles technologies et on essaiera de proposer une architecture reposant dessus en suivant la méthodologie décrite au chapitre précédent.

I. OSPF

Le protocole OSPF (Open Shortest Path First) est un protocole de routage à état de liens basé sur des normes ouvertes. Il est spécifié dans différentes normes du groupe IETF (Internet Engineering Task Force).

1. Design de l'OSPF :

Le routage OSPF est fondé sur la notion dôarea Chaque routeur contient une base de données complète des états de liens en vigueur dans une area spécifique. Tout nombre entre 0 et 4294967295 peut être affecté à une area dôun réseau OSPF. Cependant, le numéro 0 est affecté à une area unique, qui est identifiée en tant que area 0 ou area backbone. Dans les réseaux OSPF à areas multiples, toutes les areas doivent se connecter à lôarea 0.

LôOSPF peut être utilisé et configuré en tant que area unique pour les petits réseaux. Il peut également être utilisé pour les grands réseaux. Le routage OSPF peut évoluer vers les grands réseaux si les principes de conception de réseau hiérarchique sont appliqués.

2. Métrique OSPF :

LôOSPF utilise lôalgorithme du plus court chemin dôabord pour déterminer le meilleur chemin vers une destination. En vertu de cet algorithme, le meilleur chemin est celui de moindre coût.

LôOSPF détermine les meilleures routes en comparant leurs coûts, la meilleure route étant celle qui a le coût le plus faible. Si deux routes ont le même coût elles sont alors toutes les deux insérées dans la table de routage et le routeur effectuera un partage de charge entre ces deux chemins. (Voir maquette OSPF)

Le coût de traversée d'un lien est estimé par OSPF en fonction d'un calcul se basant sur le débit de celui-ci. La formule est la suivante :

Cost = bande passante de référence / bande passante de l'interface

Par défaut OSPF considère qu'un lien FDDI doit avoir un coût de 1, le débit d'un lien FDDI étant de 100MB le calcul du coût d'un lien est :

Cost = 10^8 / bande passante de l'interface

Chaque lien a un coût. Chaque nî ud a un nom (dans lôOSPF, un routeur est désigné par un identifiant sous la forme dôune adresse IP). Et chaque nî ud dispose dôune base de données complète de tous les liens, ce qui fait que des informations complètes sur la topologie physique sont connues. Les bases de données dôétat de liens de tous les routeurs dôune même area sont identiques.

3. Fonctionnement du protocole OSPF :

Quand un routeur démarre un processus de routage OSPF sur une interface, il envoie un paquet dôinvite "Hello" et continue dôenvoyer ces invites à intervalles réguliers. Lôensemble des règles qui gouvernent cet échange de paquets dôinvite OSPF est appelé le protocole «Hello».

Au niveau de la couche 3 du modèle OSI, des paquets HELLO sont adressés à lôadresse multicast 224.0.0.5. Cette adresse correspond à «tous les routeurs OSPF». Les routeurs OSPF utilisent des paquets HELLO pour initier de nouvelles contiguïtés et pour sôassurer que les routeurs voisins fonctionnent encore. Des HELLO sont envoyés toutes les 10 secondes par défaut sur les réseaux broadcast à accès multiple et sur les réseaux point-à-point.

Dans les réseaux à accès multiples, le protocole «Hello» élit un routeur désigné (DR acronyme de «Designated Router») et un routeur désigné de secours (BDR acronyme de Backup DR).

Le protocole «Hello» transporte les informations de ceux des voisins qui acceptent de former une adjacence et d'échanger leurs informations d'état de liens. Dans un réseau à accès multiples le DR et le BDR maintiennent les relations d'adjacence avec tous les autres routeurs OSPF du réseau.

Chaque routeur envoie des mises à jour de routage à état de liens (LSA) dans des paquets de mise à jour d'état de liens (LSU). Ces LSA décrivent toutes les liaisons du routeur. Chaque routeur qui reçoit une LSA de ses voisins l'enregistre dans la base de données d'état de liens. Ce processus est répété pour tous les routeurs du réseau OSPF.

Lorsque les bases de données sont complètes, chaque routeur utilise l'algorithme SPF pour calculer une topologie logique exempte de boucles vers chaque réseau connu.

4. Performance de l'OSPF :

En cas de changement de l'état de lien, les routeurs utilisent un processus de diffusion pour avertir tous les autres routeurs du réseau du changement qui est survenu. Sur réception de LSA, le routeur va très vite calculer un SPF de façon à construire le plus rapidement possible son shortest path tree.

Par contre si le routeur observe une augmentation du nombre d'évènement, les timers sont chaque fois multipliés par 2 jusqu'à arriver à un maximum, de façon à ralentir la fréquence de calcul et à revenir dans un mode ou l'on privilégie la stabilité et de façon à ne pas inonder l'aire de LSA.

Aussi, la configuration d'aires OSPF permet de réduire les temps de convergence en diminuant la taille de la Link State Database et en réduisant l'impact d'une modification dans une aire sur les autres aires.

5. Maquette OSPF :

Pour mettre en point le mécanisme de partage de charge dans le cas dôune architecture routée (utilisation du protocole OSPF dans notre cas), on a mis en place la maquette suivante: une topologie à liens redondants.

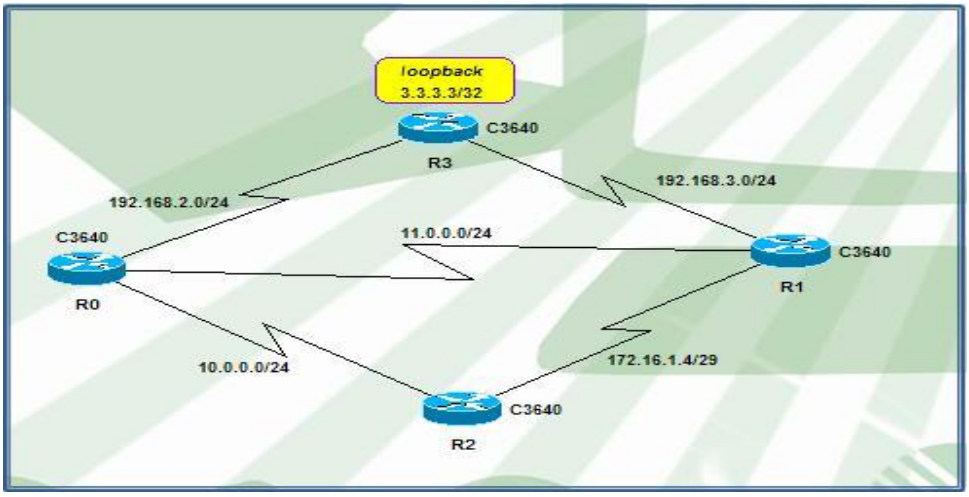

Figure 14: Maquette de routage

- Activation de l'OSPF :

Lôactivation du protocole OSPF se fait par la commande « *router ospf Process ID* ». Le process ID est un numéro unique et arbitraire qui identifie le processus de routage. Dans notre cas, on choisit le process ID 100. La commande network identifie les réseaux IP qui font partie du réseau OSPF. Le masque générique (wildcard-mask) représente lôensemble dôadresses hôtes que le segment prend en charge. Il est différent dôun masque de sous-réseau utilisé lors de la configuration des adresses IP sur les interfaces.

Pour chaque réseau, on doit préciser le domaine (area) auquel le réseau appartient. Dans notre cas on travaille dans lôarea 0.

```
R1(config)#router ospf ?
  <1-65535>  Process ID
R1(config)#router ospf 100
R1(config-router)#network 11.0.0.0 0.0.0.255 area 0
R1(config-router)#network 192.168.3.0 0.0.0.255 area 0
R1(config-router)#network 172.16.1.0 0.0.0.7 area 0
R1#write memory

Building configuration...
[OK]
```

- Partage de Charge :

LôOSPF autorise par défaut 4 chemins à coût égal, mais il peut en supporter jusquôà 16. Pour en fixer un nombre, on utilise la commande maximum-paths :

```
R0(config)#router ospf 100
R0(config-router)#maximum-paths ?
  <1-16>  Number of paths
R0(config-router)#maximum-paths 16
```

Par la commande « ip ospf cost », on impose un coût égal à 5 dans toutes les interfaces. Un exemple dôapplication de la commande sur lôinterface S0/1 du routeur R1.

```
R1(config)#interface serial 0/1
R1(config-if)#ip ospf cost 5
R1(config-if)#exit
```

La visualisation de la table de routage du routeur R1 montre lôexistence de deux entrées pour chacune des deux destinations : 10.0.0.0 et 192.168.2.0

```
R1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     3.0.0.0/32 is subnetted, 1 subnets
O       3.3.3.3 [110/6] via 192.168.3.2, 00:40:06, Serial0/3
     172.16.0.0/29 is subnetted, 1 subnets
C       172.16.1.0 is directly connected, Serial0/2
     10.0.0.0/24 is subnetted, 1 subnets
O       10.0.0.0 [110/10] via 172.16.1.4, 00:40:06, Serial0/2
                 [110/10] via 11.0.0.1, 00:40:06, Serial0/1
     11.0.0.0/24 is subnetted, 1 subnets
C       11.0.0.0 is directly connected, Serial0/1
O    192.168.2.0/24 [110/10] via 192.168.3.2, 00:40:06, Serial0/3
                    [110/10] via 11.0.0.1, 00:40:06, Serial0/1
C    192.168.3.0/24 is directly connected, Serial0/3
```

Il existe deux modes de partage de charge, par destination et par paquet. Dans le mode de partage de charge par destination, les paquets sont distribués en fonction de lôadresse de destination. Tous les paquets ayant la même destination transitent par le même chemin. Par contre, avec un partage de charge par paquets, les paquets de la même destination peuvent passer par plusieurs chemins. Ce mode permet une meilleure utilisation des liens redondants mais il présente lôinconvénient de ne pas garder la séquence des paquets (problème pour les applications de type VoIP).

CEF (Cisco Express Forwarding) est une technologie niveau 3 qui peut être exploitée pour faire le partage de charge dans les routeurs. Par défaut, CEF utilise un partage de charge par-destination. Avec la commande sh ip cef exact-route, on peut déterminer le chemin associé à une session :

```
R2>sh ip cef exact-route 10.10.0.1 3.3.3.3                    \\ session 1
10.10.0.1       -> 3.3.3.3       : Serial0/3 (next hop 172.16.1.5)
R2>sh ip cef exact-route 10.10.0.2 3.3.3.3                    \\ session 2
10.10.0.2       -> 3.3.3.3       : Serial0/2 (next hop 10.0.0.1)
```

Le tableau ci-dessus montre que tous les paquets de la première session (10.10.0.1 -> 3.3.3.3) sort par lôinterface serial 0/3 alors que les paquets de la deuxième session (10.10.0.2 -> 3.3.3.3) sort par lôinterface serial 0/2. Une session est déterminée par une adresse source et une adresse destination.

II. EIGRP

EIGRP (Enhanced Interior Gateway Routing Protocol) et un protocole de routage développé par Cisco dans le but dôaméliorer le protocole IGRP. EIGRP utilise lôalgorithme DUAL (Diffusing Update Algorithme), combinaison entre les protocoles à états de liens (OSPF/IS-IS) et à vecteurs de distance (RIP / IGRP).

1. Principe de base du protocole EIGRP :

Les mots clés du protocole EIGRP sont :

- ✓ Découverte du voisinage.
- ✓ Protocole de transport fiable.

La découverte du voisinage (neighbor discovery) est le processus par lequel un routeur prend connaissance de ses homologues avec lesquels il est en liaison direct. EIGRP utilise des petits paquets hello pour découvrir son voisinage. Tant quôun routeur reçoit un message hello dôun voisin, il considère que celui-ci est en état dôactivité correct et quôil peut échanger des informations avec lui. La particularité dôEIGRP réside dans le fait quôil effectue des mises à jour partielles. Lorsque lôétat dôune liaison ou dôun routeur change, le protocole EIGRP ne transmet immédiatement à ses voisins que lôinformation strictement nécessaire. Plutôt que leur envoyer la totalité de sa table de routage, seules les données modifiées sont communiquées. Cela soulage dôune façon substantielle lôoccupation de la bande passante. Il en va de même avec les mises à jour périodiques quôentreprend EIGRP. Lôefficacité est avérée, comparée à celle du protocole IGRP.

Au cî ur du protocole EIGRP, se trouve lôalgorithme DUAL (Diffusing Update Algorithm), basé sur un automate à nombre dôétats fini. Côest lui qui conduit le processus de décision du calcul des routes dans le réseau. DUAL exploite un vecteur de distance pour

choisir de manière efficace, en évitant toute boucle de routage, la meilleure route pour une destination particulière. Cette route est ensuite insérée dans la table de routage. DUAL détermine par ailleurs une route de secours. Cette dernière n'est envisagée (et choisie) que si la route principale se trouve indisponible pour une raison quelconque. Cela évite ainsi de recalculer en urgence une nouvelle route et permet de réduire fortement le temps de convergence du réseau. EIGRP utilise également un protocole de transport fiable, appelé RTP (Reliable Transport Protocol), pour garantir la bonne distribution des informations de mise à jour, plutôt que de s'en remettre au mécanisme de diffusion.

EIGRP jouit par ailleurs du point fort suivant : il peut servir de protocole de routage à des réseaux appliquant des protocoles de communication autres que IP, comme les protocoles IPX ou Appletalk. Il est particulièrement avantageux de pouvoir faire cohabiter des environnements réseaux hétérogènes, et de n'avoir à configurer qu'un seul protocole de routage dans le réseau.

2. Métrique EIGRP :

La formule globale donnant la métrique utilisée par le protocole EIGRP est la suivante :

Metric = [K1 x BW + (K2 x BW)/(256 - Load) + K3 x Delay] x [K5/(Reliability + K4)] x 256

Par défaut, les constantes Kn utilisées dans la formule sont les suivantes : K1 = 1, K2 = 0, K3= 1, K4 = K5 = 0. D'où la formule suivante utilisée par défaut par EIGRP pour calculer les meilleurs chemins :

Metric = BW + Delay

Où **BW = 10000000 / Bandwidth (Kbits/s)** et **Delay = Délai (microsecondes) / 10**

Bandwidth est la plus petite valeur de Bande Passante sur le chemin calculé.

Délai est la somme des délais le long du chemin calculé.

3. Fonctionnement de l'EIGRP :

Le protocole EIGRP repose sur plusieurs concepts de base ; parmi ceux-ci, on trouve la table de voisinage, la table de topologie et la table de routage :

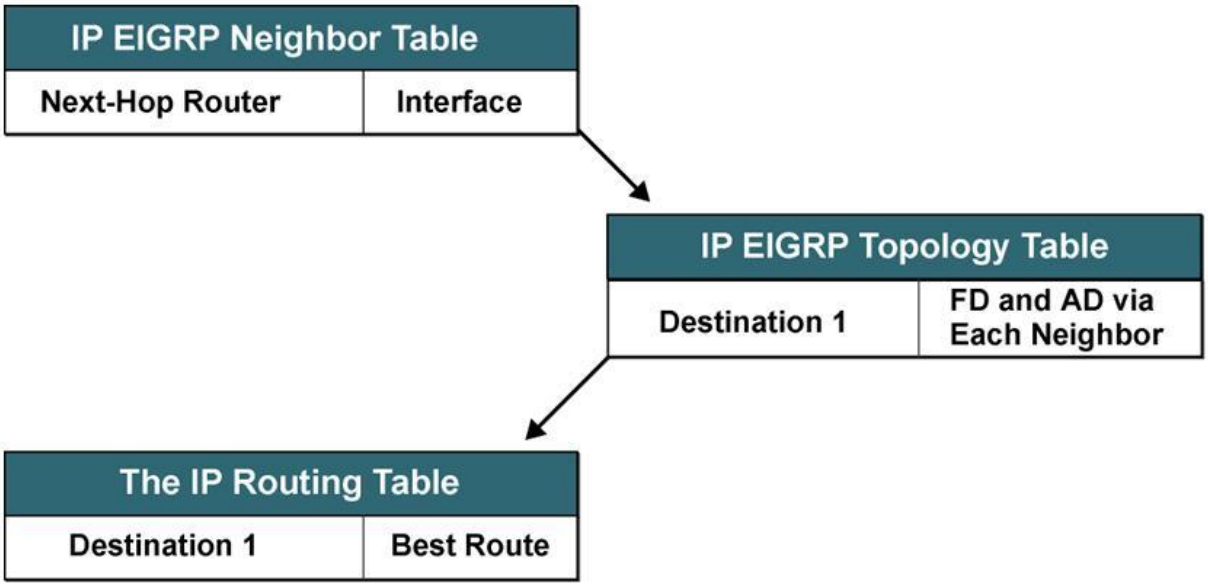

Figure 15: Les tables de lôEIGRP

Le premier élément que nous examinons, côest la table de voisinage (neighbor table). Comme nous lôavons dit, un routeur découvre son environnement grâce aux messages hello quôil reçoit de (et quôil envoie vers) ses routeurs voisins.

Lôassociation de tous les messages hello constitue la table de voisinage. Elle fournit au routeur des informations dôétat des liaisons avec ses routeurs adjacents. Les messages hello contiennent une information temporelle, correspondant au temps de maintien (hold time). Celui-ci exprime le temps durant lequel le routeur qui a reçu un message hello considère le routeur qui le lui a transmis comme étant valide et accessible.

Si aucun nouveau message hello nôapparaît à lôexpiration de ce temps, le processus DUAL est informé du changement dôétat probable survenu dans réseau. La table de voisinage conserve en outre la trace des numéros de séquences du protocole RTP, et permet dôestimer le temps approprié pour entreprendre les requêtes de retransmission des paquets RTP.

EIGRP a une table de topologie (topology table) qui contient toutes les destinations annoncées par les routeurs voisins, de même que la métrique associée à chacune. Cette table constitue la base d'information pour les calculs effectués par DUAL.

Les résultats des traitements effectués par DUAL alimentent la table de routage. Une entrée de la table de topologie, pour une destination donnée, peut se traduire par deux états : soit la destination est active, soit elle est passive (ce dernier état correspondant à la condition normale).

Une route peut être activée uniquement lorsque la survenue d'un événement nécessite un nouveau calcul de routage, en raison par exemple d'une soudaine indisponibilité d'un routeur ou d'une liaison de communication.

Une entrée de la table de topologie est introduite dans la table de routage, et validée, lorsque le routeur apprend qu'il peut s'en servir comme possible route de secours (feasible successor). Cette route est perçue comme la meilleure alternative possible vers une destination donnée, s'il advient que la route principale (la meilleure connue) tombe en panne.

Lorsqu'une route de secours existe pour une entrée donnée, dans la table de topologie, et que le routeur principal associé à cette entrée n'émet plus des paquets hello, l'entrée principale n'est plus activée dans la table de topologie. C'est alors l'entrée relative à la route de secours qui indiquera la destination.

4. Performance de l'EIGRP :

Le protocole EIGRP offre plusieurs avantages :

- ✓ Convergence rapide.
- ✓ Configuration simple.
- ✓ Agrégation des routes simple.
- ✓ Partage de charge sur des chemins à différente métrique.

- Convergence rapide :

La convergence rapide est obtenue par le fait que pour chaque réseau destination, un routeur EIGRP va calculer (dans la mesure du possible) un chemin de secours en plus du chemin optimal. Ainsi, dans le cas ou le meilleur chemin nôest plus disponible, le chemin de secours est quasi-immédiatement utilisé. Ce comportement est différent de celui de la majorité des autres protocoles de routage tels OSPF pour lesquels, dans le cas de la non disponibilité du chemin principal, il faut ré-exécuter lôalgorithme de routage pour déterminer le nouveau chemin optimal.

- Agrégation des routes :

Lôagrégation des routes permet dôalléger la table de routage, dôy faciliter la recherche des routes et dôéconomiser les échanges dôinformations de routage dans le réseau. Dans la partie configuration du protocole EIGRP, on donne un exemple dôagrégation de route.

- Partage de charge sur des chemins à différente métrique :

Le partage de charge permet d'augmenter l'utilisation effective de la bande passante. En plus du partage de charge sur des liens à coût égal, EIGRP permet aussi le partage de charge sur des chemins à différentes métriques. La commande variance permet au routeur d'inclure des routes avec une métrique plus grande par le biais d'un coefficient multiplicateur. La variance est un nombre entier n compris entre 1 et 128 (1 correspond au partage de charge à coût égal, valeur par défaut). Le coefficient multiplicateur définit la plage de métriques acceptables. Toutes les routes ayant une métrique inférieure à n fois la métrique de la meilleure route seront incluses dans la table de routage. Une petite démonstration est présentée dans la partie configuration.

5. Maquette EIGRP

Dans ce paragraphe, on donne une illustration des mécanismes dôagrégation des routes et de partage de charge avec le protocole EIGRP. Pour ce faire, on considère lôexemple suivant :

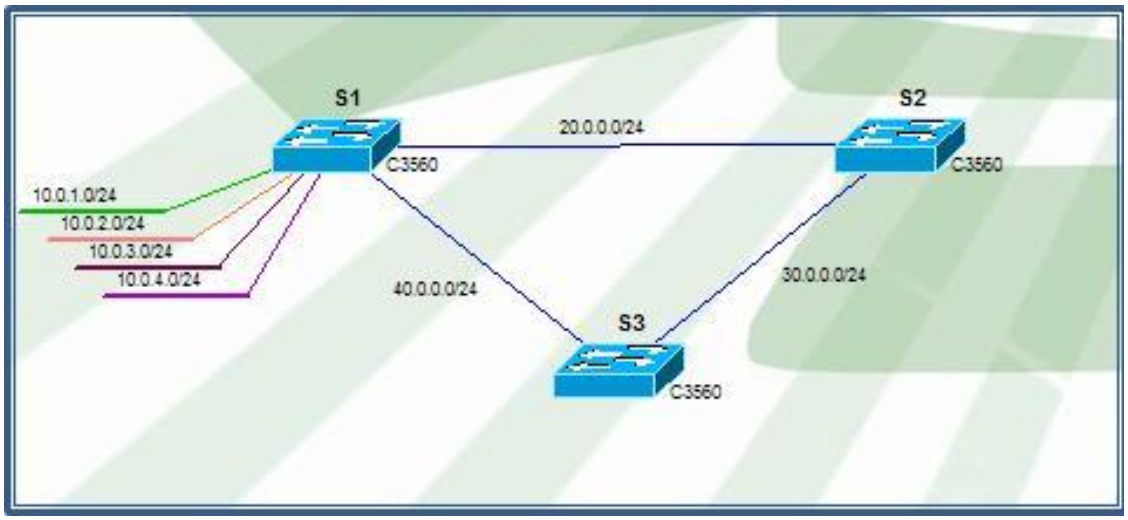

Figure 16: Maquette EIGRP

- Activation du protocole EIGRP

La commande « *router EIGRP* » permet de créer un processus de routage EIGRP. 100 est le numéro du système Autonome (AS : Autonomous System). Un système Autonome correspond à une entité dépendant de la même administration. Tous les routeurs du même autonomous système doivent utiliser le même numéro AS pour échanger les informations de routage.

Pour déclarer les différents réseaux auxquels le routeur est directement connecté, on utilise la commande « *network* ». Le protocole EIGRP cherche les interfaces appartenant à ces réseaux et y applique son processus.

```
S2(config)#router eigrp 100
S2(config-router)#network 20.0.0.0 0.0.0.255
S2(config-router)#network 30.0.0.0 0.0.0.255
S2(config-router)#no auto-summary
```

Par défaut, le protocole EIGRP autorise lôagrégation automatique. Avec cette option, le processus EIGRP ne supporte pas les sous réseaux. Pour désactiver lôagrégation automatique, on utilise la commande no « *auto-summary* ».

- Agrégation des routes

Les réseaux contigus : 10.0.1.0/24, 10.0.2.0/24, 10.0.3.0/24, 10.0.4.0/24 dérivent tous du réseau /16.

Donc il sera intéressant de regrouper tout ces subnets dans le même réseau. Pour atteindre cet objectif, une commande dôagrégation sera entrée au niveau des interfaces Fa0/5 et Fa0/6. Nous donnons ici lôexemple de configuration :

```
S1(config)#interface fastEthernet 0/5
S1(config-if)#ip summary-address eigrp 100 10.0.0.0 255.255.0.0
S1(config-if)#interface fastEthernet 0/7
S1(config-if)#ip summary-address eigrp 100 10.0.0.0 255.255.0.0
```

Lôagrégation est effectuée grâce à la commande « *ip summary-address* » qui a pour arguments le protocole de routage (EIGRP dans notre cas), le numéro du système autonome (100), lôadresse ip du réseau (10.0.0.0) et le masque (255.255.0.0).

On visualise la table de routage par la commande « *sh ip route* » :

```
S1#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     20.0.0.0/24 is subnetted, 1 subnets
C       20.0.0.0 is directly connected, FastEthernet0/5
     40.0.0.0/24 is subnetted, 1 subnets
C       40.0.0.0 is directly connected, FastEthernet0/7
     10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
D       10.0.0.0/16 is a summary, 00:03:23, Null0
C       10.0.1.0/24 is directly connected, FastEthernet0/1
C       10.0.4.0/24 is directly connected, FastEthernet0/4
     30.0.0.0/24 is subnetted, 1 subnets
D       30.0.0.0 [90/30720] via 40.0.0.3, 00:08:04, FastEthernet0/7
                 [90/30720] via 20.0.0.2, 00:08:05, FastEthernet0/5
```

Uptime

Dans les résultats affichés, on lit la distance administrative 90 du protocole EIGRP.

Le Uptime représente le temps écoulé à partir du moment où le routeur local a pris connaissance de cette entrée.

La ligne en gras rouge signifie que le routeur courant, le routeur S1, a regroupé les 4 réseaux dans une seule entrée. Null0 signifie que si les autres routeurs envoient des paquets à une destination non existante mais comprise dans le summary (par exemple 10.0.7.0), le routeur S1 ignore ces paquets.

Pour arriver à la destination 30.0.0.0, le routeur S1 dispose de deux chemins redondants. Un via lôinterface 40.0.0.3(Fa0/7) et lôautre via 20.0.0.2 (Fa0/5). Les deux chemins ont la même métrique. Il sôagit donc dôun partage de charge à égale métrique.

- Partage de Charge sur des chemins à différente métrique

Pour étudier le partage de charge via des routes à différent coût, on se place dans les conditions permettant cette situation. Dans la topologie proposée dans la maquette OSPF, on change la bande passante de lôinterface S0/3. Ici la configuration permettant ceci :

```
R0(config)#interface serial 0/3
R0(config-if)#bandwidth ?
  <1-10000000>  Bandwidth in kilobits
R0(config-if)#bandwidth 1000000
```

Ensuite, on met le multiplicateur « *variance* » à 2 :

```
R2(config)#router eigrp 100
R2(config-router)#variance 2
```

« Sh ip eigrp topology » pour visualiser le contenu de la table de topologie :

```
R2#sh ip eigrp topology
IP-EIGRP Topology Table for AS(100)/ID(172.16.1.4)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 3.3.3.3/32, 2 successors, FD is 2809856
        via 10.0.0.1 (2809856/896000), Serial0/2, serno 113
        via 172.16.1.5 (2809856/2297856), Serial0/3
P 10.0.0.0/24, 1 successors, FD is 2169856
        via Connected, Serial0/2
P 11.0.0.0/24, 2 successors, FD is 2681856
        via 10.0.0.1 (2681856/2169856), Serial0/2
        via 172.16.1.5 (2681856/2169856), Serial0/3
P 192.168.2.0/24, 1 successors, FD is 2681856
        via 10.0.0.1 (2681856/514560), Serial0/2
P 192.168.3.0/24, 1 successors, FD is 2681856
        via 172.16.1.5 (2681856/2169856), Serial0/3
P 172.16.1.0/29, 1 successors, FD is 2169856
        via Connected, Serial0/3
```

Il en ressort que le chemin via un 172.16.1.5 a une valeur FD inférieur à 2 fois la FD du meilleur chemin, en plus il est un feasible successor cêst à dire que sa valeur AD (advertised distance), la valeur après le slash, est inférieur à la valeur FD (feasible distance) du meilleur chemin via 10.0.0.1. Donc ce chemin va participer nécessairement dans le partage de charge.

Effectivement, la route est incluse dans la table de routage :

```
R2#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     3.0.0.0/32 is subnetted, 1 subnets
D       3.3.3.3 [90/2809856] via 172.16.1.5, 00:05:35, Serial0/3
                [90/2809856] via 10.0.0.1, 00:05:35, Serial0/2
     172.16.0.0/29 is subnetted, 1 subnets
C       172.16.1.0 is directly connected, Serial0/3
     10.0.0.0/24 is subnetted, 1 subnets
```

```
C       10.0.0.0 is directly connected, Serial0/2
    11.0.0.0/24 is subnetted, 1 subnets
D       11.0.0.0 [90/2681856] via 172.16.1.5, 00:05:35, Serial0/3
              [90/2681856] via 10.0.0.1, 00:05:35, Serial0/2
D    192.168.2.0/24 [90/2681856] via 10.0.0.1, 00:05:35, Serial0/2
D    192.168.3.0/24 [90/2681856] via 172.16.1.5, 00:05:35, Serial0/3
```

III. VRF-Lite

Une autre évolution en matière LAN consiste à utiliser une extension du protocole MPLS sans passer par ce dernier. Il s'agit de la technologie VRF-Lite (VPN Routing and Forwarding-Lite).

1. Généralités sur les VRF-Lite.

VRF-lite est utilisé sur un réseau sans WAN. Il est souvent utilisé sur des commutateurs de couche 3. Il s'agit d'une extension des fonctionnalités MPLS qui permet d'obtenir la segmentation d'un réseau en différents VPNs sans pour autant utiliser la « labellisation » des paquets avec des en-têtes MPLS. Quand on utilise VRF-lite, les équipements de couche 3 utilisent le tag 802.1q pour taguer les paquets, cela permet de garder la virtualisation entre les équipements de couche 3. Chaque liens physique 802.1q transportera donc plusieurs instances de routage et chaque instance VRF possèdera son propre process IGP (OSPF) ou 'adresse family' (EIGRP, RIPv2, MP-BGP).

Le schéma suivant illustre cette notion :

Note : Pour la lecture du schéma, il faut considérer que les éléments représentés en couleur jaune (utilisateurs, liens, routeurs) font partie d'un réseau indépendant de celui représenté avec les éléments colorés en rouge. Par exemple, on pourra noter que les liens entre routeurs sont constitués d'une succession de points rouge et jaune. Cela signifie qu'un unique lien physique est constitué de deux liens logiques, l'un propre au réseau « rouge », l'autre propre au réseau « jaune ».

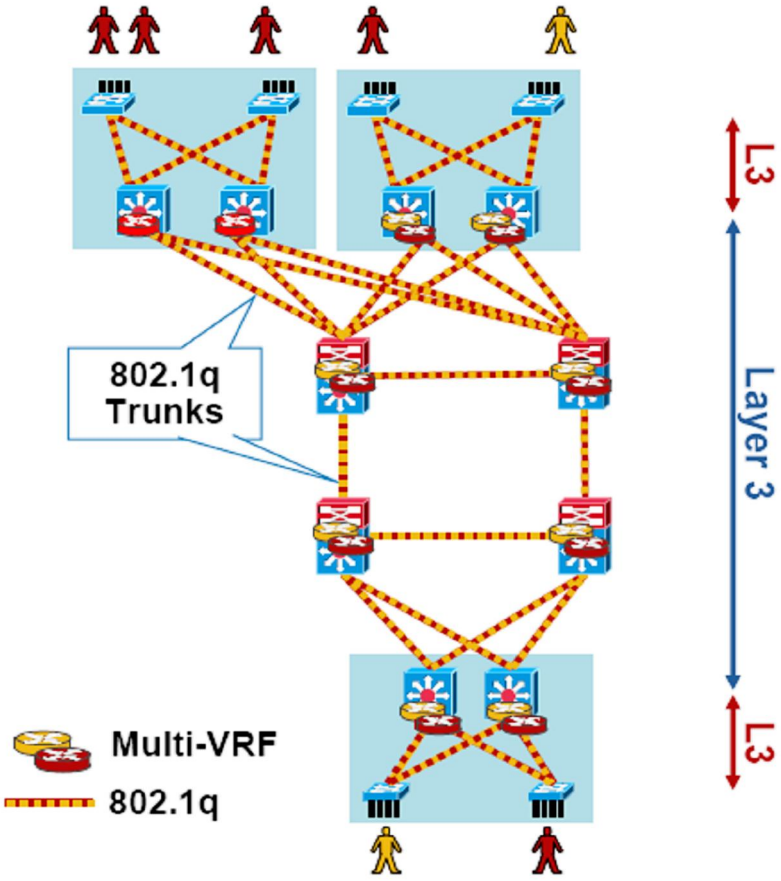

Figure 17: Notion de Multi-VRF CE (VRF-Lite) End-To-End

La notion de VRF-Lite permet de scinder un routeur donné en plusieurs routeurs logiques, plus souvent appelés instances VRF (VPN routing and forwarding).

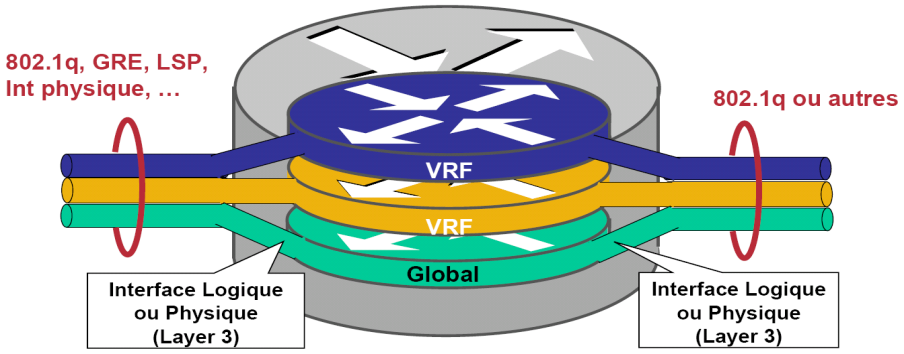

Figure 18: Virtualisation dûn équipement réseau

Lorsque l'on crée une VRF, le routeur va créer une table de routage, une FIB (Forwarding Information Base) et une instance CEF (Cisco Express Forwarding) spécifique à la VRF. Il y

aura donc autant de table de routage, FIB et CEF qu'il y a de VRF, plus une pour la fonction de routage global qui prendra en charge tout le trafic non tagué par une VRF.

Chaque VRF est désignée par un nom (par ex. RED, GREEN, etc.) sur les routeurs. Les noms sont affectés localement, et nôont aucune signification vis-à-vis des autres routeurs. Chaque interface de routeur reliée à un site client est rattachée à une VRF particulière. Lors de la réception de paquets IP sur une interface cliente, le routeur procède à un examen de la table de routage de la VRF à laquelle est rattachée lôinterface, et donc ne consulte pas sa table de routage globale. Cette possibilité dôutiliser plusieurs tables de routage indépendantes permet de gérer un plan dôadressage par sites, même en cas de recouvrement dôadresses entre VPN différents. Une illustration pratique est donnée au paragraphe Maquette VRF, on y donne un exemple de configuration des instances VRF en utilisant des plages dôadresses identiques et le protocole de routage OSPF.

Conceptuellement, il faut considérer que sur une même architecture physique, on développe plusieurs architectures virtuelles, suivant le schéma ci-dessous :

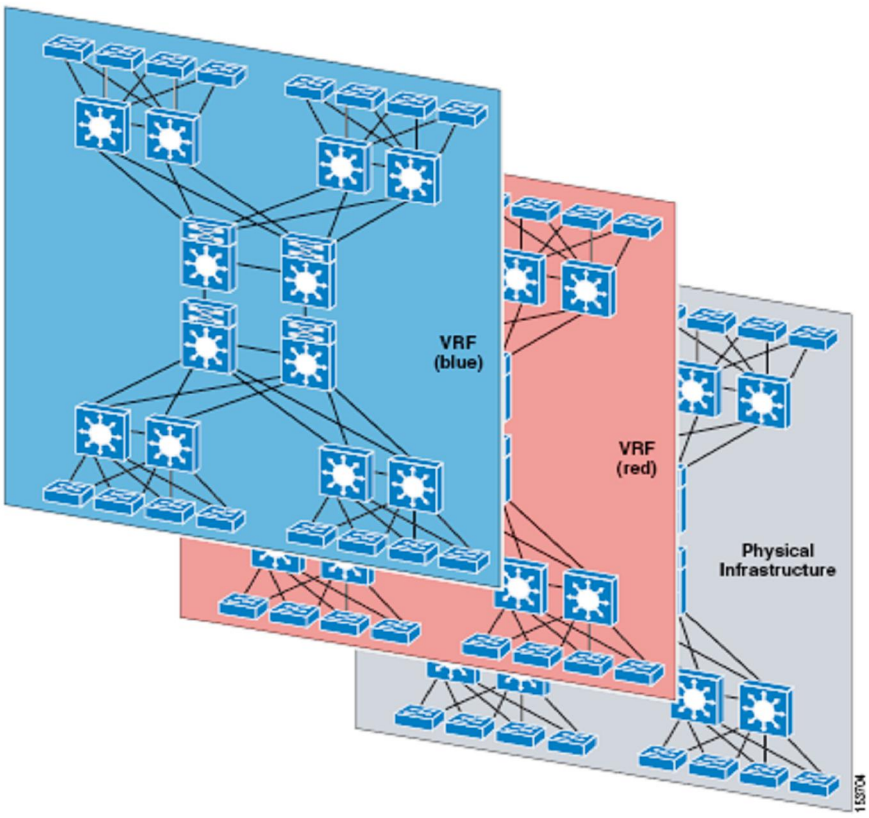

Figure 19: Virtualisation dôun réseau physique

Superposés sur une même architecture physique, on retrouve deux réseaux virtuels, l'un coloré en rouge, l'autre coloré en bleu.

2. Maquette VRF :

Pour comprendre la notion des VRF, la maquette suivante est mise en place :

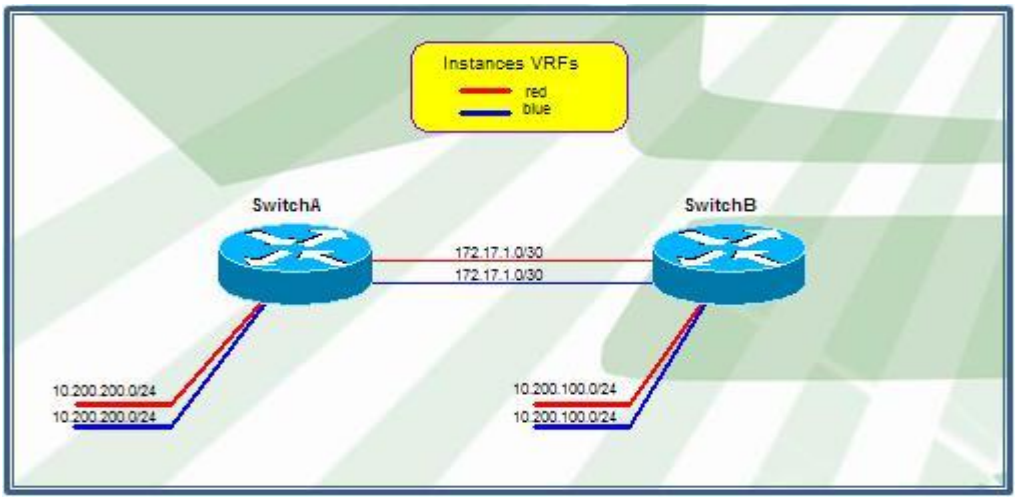

Figure 20: Maquette VRF

On définit le long de cette configuration, deux domaines VRFs : red et blue.

- Création des VRFs :

La création des instances vrf se fait par la commande ip vrf <nom_de_l'instance>

```
switchA(config)#ip vrf blue
switchA(config-vrf)#rd 20:20

switchA(config)#ip vrf red
switchA(config-vrf)#rd 30:30
```

Le paramètre rd est un identifiant de l'instance VRF.

- Assignation d'interface (interface physique ou logique) :

Dans le mode de configuration d'une interface (logique ou physique), on associe cette interface à une instance VRF :

```
switchA(config)#interface vlan 2
switchA(config-if)#ip vrf forwarding blue
switchA(config-if)#ip address 10.200.200.1 255.255.255.0
switchA(config-if)#no shutdown

switchA(config)#interface vlan 3
switchA(config-if)#ip vrf forwarding red
switchA(config-if)#ip address 10.200.200.1 255.255.255.0
switchA(config-if)#no shutdown
```

La commande « *ip vrf forwarding* » permet de placer une interface dans la VRF spécifiée. Comme le montre lœexemple ci-dessus, la même adresse IP peut être affectée plusieurs fois à différentes interfaces, car celles-ci sont placées dans des VRF différentes.

On vérifie dans le tableau ci-dessous les instances VRFs existantes ainsi que les interfaces qui leur sont associées :

```
switchA#sh ip vrf
  Name                 Default RD        Interfaces
  blue                 20:20             Vl2
                                         Vl4
  red                  30:30             Vl3
                                         Vl5
```

- Vérification et tests

Cœest dans le contenu des tables de routage que réside alors tout lœintérêt de lœutilisation des VRFs. En effet, si on visualise la table de routage globale du SwitchB, on a le résultat suivant:

```
SwitchB#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set
```

Il ressort que cette table de routage est vide. A priori ce routeur ne peut donc communiquer avec aucune adresse existante dans le réseau. La vérification avec un « *ping* » vers une adresse du réseau blue valide ce comportement :

```
switchA#ping 10.200.100.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.200.100.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

Effectivement dans cet exemple, le routage est effectué au niveau des instances VRF et non pas au niveau de la table de routage globale (on n'a pas configuré de processus OSPF global, qui ne soit associé à aucune instance VRF). Visualisons la table de routage associée à l'instance blue :

```
switchA#sh ip route vrf blue

Routing Table: blue
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     172.17.0.0/30 is subnetted, 1 subnets
C       172.17.1.0 is directly connected, Vlan4
     10.0.0.0/24 is subnetted, 2 subnets
C       10.200.200.0 is directly connected, Vlan2
O E2    10.200.100.0 [110/20] via 172.17.1.2, 00:06:32, Vlan4
```

Il apparaît que la table de routage contient tous les éléments nécessaires à la communication au sein de l'instance blue, aussi bien les interfaces directement connectées au switch que les adresses apprises par routage OSPF. Ces routes sont totalement cloisonnées par rapport à la table de routage de l'instance red.

On vérifie quôau sein de lôinstance blue, il y a communication IP :

```
switchA#ping vrf blue 10.200.100.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.200.100.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/8 ms
```

Par contre, il est impossible depuis lôinstance blue dôeffectuer un « *ping* » vers une adresse de lôinstance red.

La configuration de VRF vient donc naturellement compléter l'architecture des VLAN de couche 2. Cette solution permet de garder de la source jusqu'à la destination le tag de réseau virtuel et dôaméliorer la sécurité.

IV. Avantages des architectures niveau 3

Dans ce paragraphe, nous détaillerons une architecture qui met en relief les performances des protocoles et technologies vus précédemment.

1. Architecture niveau 3 globale

Après avoir étudié et assimilé les architectures niveau 2 dans le premier chapitre et celles du niveau 3 au début de ce chapitre, nous proposons donc une architecture LAN totalement routée depuis la couche accès jusquôà la couche backbone, une recommandation parmi celles les plus récentes de Cisco concernant les réseaux de campus.

Il sôagit dôune architecture où les liens entre commutateurs dôaccès et commutateurs de cî ur de réseau sont des liens de niveau 3 (avec leur segment dôadresses IP) et non plus des liens de niveau 2 (liens trunk regroupant plusieurs vlans) comme cela était généralement déployé jusquôà présent. Cette fonctionnalité est permise par le fait que les commutateurs dôaccès intègrent de plus en plus les fonctionnalités de niveau 3 habituellement présentes dans les commutateurs déployés dans les couches distribution/backbone.

Nous donnons dans la figure suivante lôarchitecture générique de ce type de déploiement :

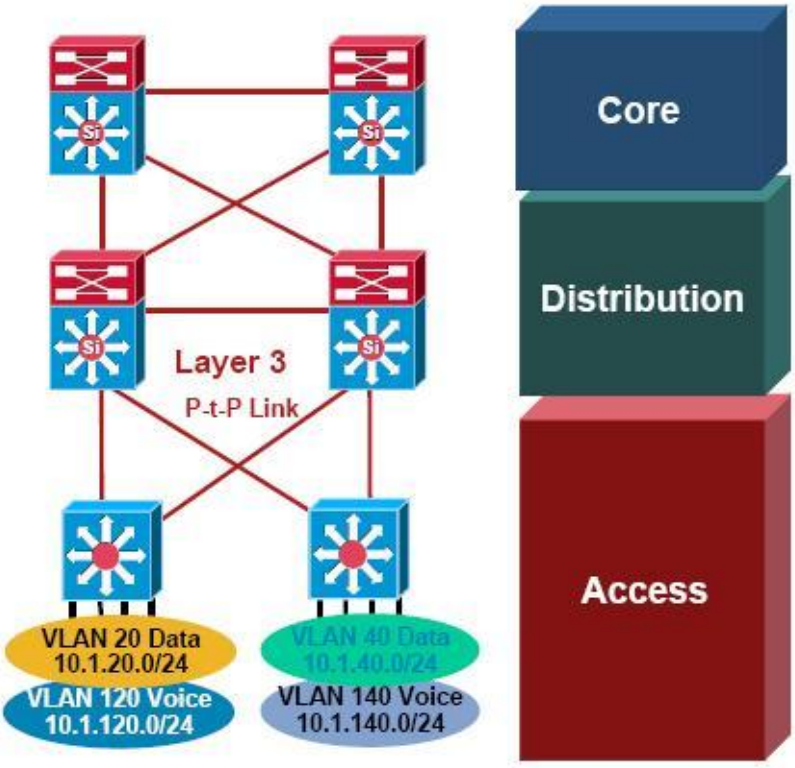

Figure 21: Architecture générique dôune solution totalement routée

Dans ce type dôarchitecture, les mécanismes de niveau 2 restent limités aux commutateurs dôaccès. Les mécanismes de niveau 3 prennent en charge le trafic à partir des liens « upstream» des commutateurs dôaccès, reliés aux commutateurs de distribution/backbone. Ces mécanismes de niveau 3 consistent en lôactivation dôun protocole de routage dynamique (EIGRP, OSPF,é) dans lôensemble du réseau, jusquôaux commutateurs dôextrémité.

Ce type de design a plusieurs avantages :

- Une durée de convergence en cas de défaillance dôun lien beaucoup plus courte quôavec lôutilisation de protocoles de niveau 2 (spanning-tree).
- Un partage de charge dynamique géré au niveau 3 grâce à lôutilisation de liens redondants ayant même métrique EIGRP ou OSPF.
- Un plan de contrôle unique (protocole de routage de niveau 3)
- Des outils de « troubleshooting » maîtrisés (ping, traceroute, ..).

- Une exploitation facilitée : Ce type de design permet aux administrateurs réseaux de s'affranchir des problèmes de boucles de spanning-tree (Il n'y a plus aucun besoin d'utiliser le protocole Spanning-Tree, vu que tous les liens inter-commutateurs sont des liens routés) généralement fastidieux à analyser.

Nous développerons par la suite certains de ces avantages de façon plus détaillée.

Nous donnerons également le point faible majeur de cette architecture, ainsi qu'un comparatif des performances offertes par les deux types d'architecture (Niveau 2 / Niveau 3)

1-1- Réduction de la durée de convergence

La réduction importante de la durée de convergence en cas de coupure d'un lien est l'un des avantages majeurs apporté par l'utilisation de protocole de routage au niveau de la couche d'accès.

A titre indicatif, nous donnons ci-après une comparaison des temps de convergence obtenus d'une part avec l'utilisation combinée de protocoles de niveau 2 et 3 (niveau 2 dans la couche accès et niveau 3 dans la couche distribution/backbone) et d'autre part avec l'utilisation exclusive de protocoles de niveau 3 dans les couches accès/distribution/backbone.

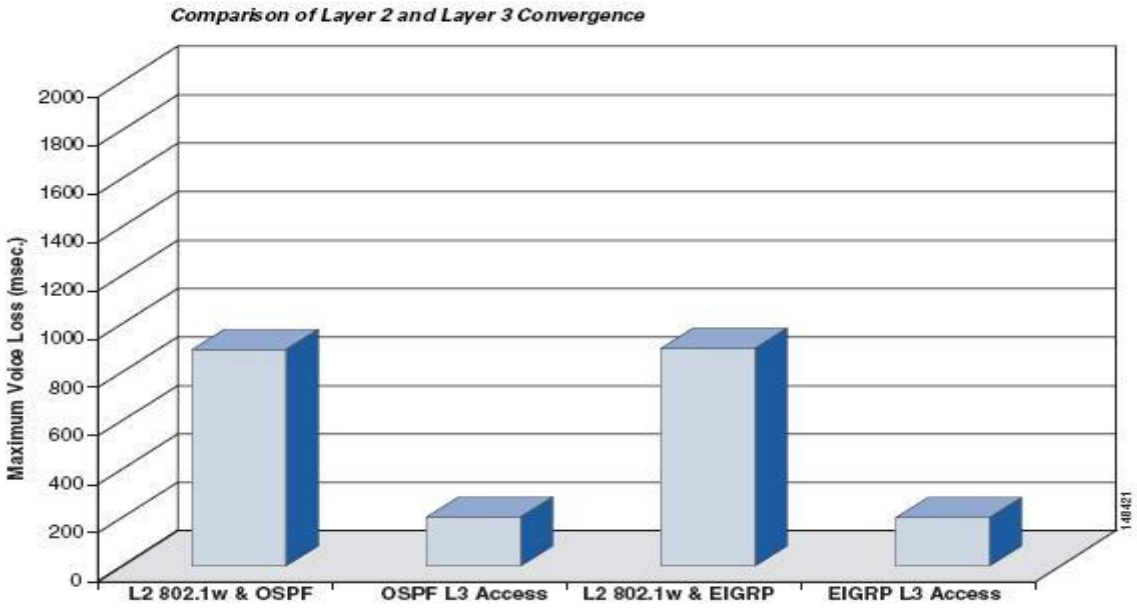

Figure 22: Temps de convergence en fonction des protocoles de haute disponibilité utilisés

Pour atteindre les temps de convergence liés à lôutilisation de protocoles de niveau 2 (800 ï 900 ms), il est nécessaire dôoptimiser les différents protocoles en vigueur au niveau de la couche dôaccès (timers du protocole HSRP, optimisation de Spanning-Tree, é) et cela tout en travaillant sur le routage au niveau des couches distribution/backbone.

Lôutilisation correcte de protocoles de routage dynamiques au niveau de la couche dôaccès permet dôatteindre des temps de convergence de lôordre de 200 ms, ce qui est un gain important en regard des applications ayant des contraintes « temps réel » (Téléphonie sur IP, Vidéoconférence, é).

1-2- Partage de charge dynamique

Lôutilisation de protocoles de routage au niveau de la couche dôaccès permet dôutiliser les liens « upstream » de façon optimisée.

Lôutilisation de protocoles de niveau 2 (Spanning-Tree) nôaboutit en général pas à une répartition optimale de trafic. En effet, le fonctionnement même de Spanning-Tree repose sur

la désactivation de ports, ports réactivés avec la détection dûne défaillance sur les ports actifs. Atteindre un partage de charge avec Spanning-Tree réclame une configuration complexe (définition de plusieurs instances de Spanning-Tree, é) difficile à analyser en cas de problème.

Les protocoles de routage permettent de réaliser le même objectif de partage de charge, avec une configuration beaucoup plus simple à mettre en î uvre et à exploiter. Lôéquilibrage de charge est obtenu en exploitant les fonctionnalités de routage et de commutation rapide des paquets (CEF : Cisco Express Forwarding).

Nous donnons ci-après une configuration type de double connexion Accès -> Distribution/Backbone.

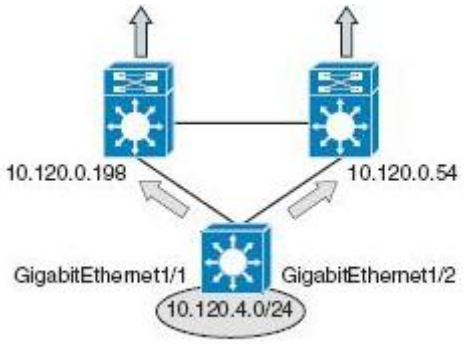

Figure 23: Exemple de double connexion dûun commutateur dôaccès avec la couche distribution

Le partage de charge est obtenu avec lôutilisation de liens redondants à coût égal. Cette configuration permet également dôobtenir les meilleurs temps de convergence.

En effet avec cette configuration, pour chaque réseau destination, chaque commutateur dispose de deux entrées dans sa table de routage et de deux entrées dans la table de commutation CEF. Le comportement normal (les deux liens « upstream » sont opérationnels) permet lôutilisation simultanée des deux liens. (Le partage de charge mis en place par CEF peut par la suite être implanté en mode partage par paquet ou par destination)

1-3- Facilité d'administration

Un réseau local totalement routé est d'une plus grande simplicité d'administration. Tous ses éléments fonctionnent de la même manière (Construction d'une table de routage, commutation rapide des paquets avec l'utilisation de CEF, les tables de commutation CEF étant générées à partir des tables de routage).

Les outils de niveau 3 généralement utilisés au niveau des routeurs (ping, traceroute, é) sont maintenant opérationnels pour diagnostiquer un éventuel problème réseau sur l'ensemble de l'architecture mise en place. On peut utiliser ces outils pour déterminer les points de congestion du réseau et rapidement prendre les mesures correctives nécessaires.

Cette simplicité d'administration apporte un avantage indéniable par rapport aux architectures de niveau 2 avec les problèmes de Spanning-Tree qui les accompagnent. Ces architectures réclament une sécurisation extrêmement rigoureuse pour que le simple ajout d'un commutateur dans le réseau n'entraîne pas de dysfonctionnements dans tout ce dernier. (Introduction de boucles, changement de la racine de l'arbre Spanning-Tree, é).

1-4- Point faible

Le point faible principal de cette architecture réside dans la difficulté d'implantation d'architectures complexes qui nécessitent absolument que des postes/serveurs situés dans des bâtiments/locaux différents soient dans le même vlan.

- Remarque : Cela n'implique pas nécessairement que des postes situés dans des vlans différents ne communiqueront pas ensemble, il s'agirait ici seulement de délimiter les domaines de broadcast.

Par exemple, une architecture de DataCenter distribué, pour laquelle une contrainte professionnelle serait que les serveurs constituant le DataCenter soient dans le même subnet, peut imposer l'utilisation des mécanismes de niveau 2 (trunk, Spanning-tree,é).

1-5- *Comparatif points forts / points faibles :*

Points forts	Points faibles
- Réduction de la durée de convergence - Partage de charge sur les liens accès -> backbone - Facilité dôadministration et de troubleshooting - Architecture simplifiée	- un même subnet ne pourra pas se retrouver sur plusieurs switchs dôaccès (pas de spanning de vlan).

2. Intérêt de la virtualisation

Lorsquôon est contraint dans une entreprise de construire plusieurs réseaux en fonction des utilisateurs, on doit multiplier les équipements réseaux. Mais créer plusieurs réseaux physiques pour répondre à cette attente demande un investissement bien trop coûteux. Il serait par contre judicieux de ce servir des équipements déjà en place et de les "virtualiser" de façon a obtenir plusieurs réseaux logiques avec un seul réseau physique.

La création de plusieurs réseaux virtuels viendra alors naturellement quand on aura mis en évidence des groupes d'utilisateurs ou de ressources, par exemple :

- Utilisateurs nomades extérieurs à l'entreprise qui pourraient corrompre volontairement ou involontairement tout le réseau de celle-ci. On pourra ainsi les mettre dans un réseau en quarantaine avec un accès très limité aux ressources.
- Mise en place d'outils dont le comportement n'est pas encore maîtrisé (nouvelle application, mise à jour, nouveaux serveurs,é) qui nécessite de faire des tests d'intégration. Ils pourront ainsi être testés dans un réseau virtuel qui les isolera du réseau de production.
- Mais aussi et tout simplement par département, services ou site.

Cela permettra de mettre en place une politique par groupe et donc de simplifier l'administration de ses groupes.

Un autre avantage de la virtualisation des réseaux est lôamélioration de la sécurité du réseau. En effet les différentes instances VRF sont totalement cloisonnées et aucune communication ne peut se produire entre des éléments appartenant à des instances VRF différentes (voir les tests effectués en paragraphe précédent).

V. Conclusion :

Si on a fait de la description des technologies de routage et de virtualisation niveau3 la vocation de ce chapitre, nous proposons plus dôéclaircissement sur leurs avantages grâce à une application sur projet réel dans le chapitre suivant.

CHAPITRE 3
Mise en place d'un réseau LAN d'entreprise

- Présentaion du projet d'implémentaion
- Choix de mise en place
- Implémentation et mise en œuvre
- Evolution du réseau

Suite à un appel d'offre, notre équipe a reçu la tâche de mettre en place le réseau d'une entreprise X tout en insistant sur l'utilisation des technologies précitées dans le chapitre précédent.

Ce chapitre a pour objectif de donner les éléments d'ingénierie pour la mise en place du réseau de transmission haut débit de cette entreprise. Il s'agit donc de réaliser l'infrastructure active du réseau à base de commutateurs réseau de la gamme Catalyst de Cisco Systems.

I. Présentaion du projet d'implémentaion:

1. Besoins exprimés :

Pour pouvoir répondre aux besoins de communication existants et futurs, l'entreprise désire, dans le cadre du présent projet, déployer un réseau Ethernet haut débit, pour l'interconnexion de son siège et ses différents sites distants répartis dans les principales villes marocaines.

Les besoins exprimés par les différentes entités techniques ont montré la nécessité d'avoir des liaisons permettant:

- Une haute disponibilité.
- Une évolutivité et une administration facile.
- L'utilisation du câblage en fibre optique existant.

2. Solution proposée :

➢ Architecture physique :

L'architecture physique découle directement des besoins exprimés et des contraintes de disponibilité de fibres. Pour la partie exploitation du réseau, elle tient compte des besoins en

haute disponibilité de celui-ci. Pour cela, nous sommes partis sur une architecture redondante en boucle où les équipements sont géographiquement séparés.

Les principaux concepts de lôarchitecture cible sont les suivants :

- ✓ **Hiérarchisation en deux niveaux :**
  - ⇨ Un niveau fédérateur, appelé backbone, qui permet en un minimum de bonds de converger vers le Siège (site principal).
  - ⇨ Un niveau de desserte assurant lôinterconnexion des sites secondaires.

- ✓ **Bande passante importante et disponibilité de bout en bout :** Par la mise en place de liaisons Gigabit Ethernet avec au moins deux chemins pour converger vers le site principal.

- ✓ **Temps de réponse maîtrisé et réduit** : dans lôaccessibilité du Siège (site de convergence de lôensemble des informations) :
  - En mode normal, au maximum 6 commutateurs sont traversés pour atteindre le site principal et ceci quelque soit la localisation du site distant,
  - En mode secours, suite à une panne (commutateur en panne, interface de lien hors service ou fibre coupée), au maximum 8 commutateurs sont traversés pour atteindre le site principal et ceci quelque soit la localisation du site distant,

Cette infrastructure physique permet de réaliser des liens redondants pour chacun des sites et reste toutefois modifiable et évolutive.

II. Choix de mise en place :

Nous détaillons ici les choix réalisés pour la mise en place de cette architecture logique. Nous avons été guidés dôune part, par la simplicité, et dôautre part par la standardisation des protocoles mis en î uvre.

1. Spanning tree :

Lôutilisation de cette technologie basée sur le niveau 2 ne nous a pas paru très performante pour deux raisons :

- Les temps de convergence sont parfois importants.
- Lôadministrabilité en cas de problème est quasi-inexistante.

Lôexpérience nous a montré que lorsquôun réseau, de la taille du nôtre, subit un problème, il faut réagir rapidement. Pour cela, il faut disposer dôoutils simples permettant un diagnostic rapide de la panne. Or, lorsque lôon est confronté à un problème de spanning tree, il nôest pas question dôutiliser efficacement un ping ou autre traceroute puisque lôon agit au niveau 2 ! Nous avons donc préféré suivre dôautres pistes.

2. HSRP :

Il existe une technologie permettant la gestion des équipements redondants. Il s'agit d'HSRP (« Hot Standby Routing Protocol »).

Une solution de ce type repose sur lôhypothèse dôavoir deux routeurs : lôun fonctionne, lôautre est en attente, prêt à prendre le relais en cas de problème sur le premier.

Cette technique peut être utilisée avec plus de deux routeurs, il est aussi possible, moyennant quelques particularités dans les configurations d'activer le partage de charge entre les routeurs.

HSRP est une solution idéale pour les routeurs d'accès, c'est-à-dire les routeurs immédiatement connectés aux hôtes.

Toutefois, cette technologie a une contrainte forte, il est nécessaire que tout les routeurs d'un groupe HSRP soient dans le même sous réseau (ainsi que l'adresse virtuelle), ce qui nôest pas dans notre cas. Donc, notre topologie réseau, ne peut se satisfaire d'HSRP.

3. Le routage dynamique :

Dans un premier temps, lôutilisation du routage statique paraît une solution possible. Le routage statique, en plus de sa simplicité et son déterminisme, assure une stabilité que les protocoles dynamiques ne pourront pas assurer.

Mais vu la taille du réseau déployé dans notre entreprise, le routage statique paraît de plus en plus difficile. Le nombre important de routeurs rend les routes statiques ingérables. Ainsi, lôutilisation dôun protocole de routage dynamique devient indispensable.

4. Le choix de l'OSPF :

Un certain nombre de critères doivent être pris en compte pour choisir le protocole de routage d'un réseau. Parmi ces critères, on trouve le support de ce protocole par les équipements, la simplicité de mise en î uvre, la stabilité et plusieurs dôautre fonctionnalité (vitesse de convergence, type de mise à jours, partage de charge, type de métrique, évolutivité,é).

Dans le cadre de ce projet, le client souhaitait également mettre en î uvre un protocole de routage standard, afin de pouvoir dans lôavenir envisager lôajout dôéquipements non Cisco. Opsf répond à ce critère.

Pour notre réseau le choix dôOSPF comme protocole de routage découle directement des fortes possibilités quôoffre ce protocole. En effet, OSPF est un protocole de routage dynamique, dont les principes de base imposent une topologie sur le modèle hiérarchique. Bien que contraignant, ce modèle assure la pérennité et l'efficacité du réseau dès lors qu'il est de taille importante.

La conception dôun réseau OSPF passe par la segmentation du domaine en sous-réseaux ou « area ». Cette segmentation est utile dans le sens ou un routeur OSPF ne va désormais plus faire les calculs OSPF sur lôensemble des LSAs du réseau, mais uniquement sur les LSAs propres à lôarea dôappartenance du routeur.

Un autre avantage de la segmentation en areas est la possibilité dôagréger les adresses (summarization) pour réduire la quantité de LSAs transitant par le réseau.

5. EIGRP et IS-IS

Au vu du paragraphe II-4 du chapitre 2, EIGRP semble être le protocole de routage interne disposant du plus grand nombre de fonctionnalités. En particulier son mode de calcul de métrique prenant en compte la charge, la latence et la fiabilité du lien lui donne un net avantage.

Mais deux problèmes d'EIGRP nous ont poussés à ne pas utiliser ce protocole. D'une part EIGRP ne permet pas de construire un routage hiérarchique comme le font IS-IS et OSPF, où les réseaux et la backbone servant au transit sont clairement définis, ce qui empêche de simplifier le routage en découpant le réseau en zones. D'autre part EIGRP est un protocole propriétaire Cisco et il n'existe donc aucun autre fabriquant de routeurs capables de dialoguer en EIGRP.

IS-IS s'il est performent, reste le protocole de routage natif OSI, l'utilisation de la suite de protocoles OSI pour les échanges de routage peut dérouter certains administrateurs et complexifier inutilement les configurations des routeurs.

Par conséquent OSPF reste le choix le plus cohérent pour ce réseau de grande taille non exclusivement composé de matériels Cisco dans le futur.

6. Besoin de virtualisation :

Après analyse des matrices de flux fournies par lôentreprise, Il sôest avéré nécessaire de séparer le trafic en trois domaines indépendants :

- **Administration** : Le PDG de l'entreprise veut disposer de ressources qui lui sont réservées. Ce domaine sera défini en plus des domaines existants dans le réseau de lôentreprise, et sera utilisé pour le trafic dôadministration et de supervision du réseau.

- **Exploitation** : Un simple employé ne devrait pas avoir accès à l'administration des équipements réseaux.
- **Utilisateurs Externes**: Une personne extérieure à l'entreprise souhaitant simplement se connecter au réseau pour accéder à Internet ne devrait pas avoir accès aux ressources vitales de l'entreprise.

Ce sont des domaines quôil faut considérer comme trois réseaux séparés. Pour assurer cette condition, plusieurs solutions se présentent.

Une première solution serait d'utiliser les VLANs et les ACLs pour contrôler chaque flux et gérer les restrictions d'accès. Cette solution peut convenir à de très petits réseaux mais devient très vite inadapté aux réseaux avec un nombre d'utilisateurs plus conséquent.

Les inconvénients de cette solution sont nombreux :

- × Sujet a beaucoup d'erreur de configuration
- × Très peu évolutive
- × Difficile à manager

Il ne nous reste donc que deux solutions : Soit multiplier les équipements réseaux, solution très coûteuse. Soit séparer le traitement de l'information dans les équipements réseau. On aura alors plusieurs routeurs virtuels sur un seul routeur physique.

L'intérêt est de :

- ✓ Mutualiser l'infrastructure : pas de nouvel achat.
- ✓ Conserver la hiérarchie : les réseaux virtuels garderont la hiérarchie des équipements déjà en place.
- ✓ Permettre une forte évolutivité du réseau : il sera très facile de modifier l'architecture réseau en fonction des différents événements de l'entreprise.

III. Implémentation et mise en œuvre :

1. Routage OSPF :

Lôutilisation dôinstances VRFs va introduire une particularité dans la configuration du routage OSPF. En effet, la configuration OSPF commence par la création dôun processus dédié aux opérations de routage. Dans un contexte classique (pas dôinstances VRFs), un processus OSPF unique prend en charge toutes les opérations de calcul de routage. Dans un contexte de VRFs, il faut maintenant créer un processus OSPF par instance VRF.

Le protocole OSPF est plus adapté aux contextes de VRFs. Par contre lôimplémentation du protocole EIGRP avec ce contexte nôest possible quôà partir dôune certaine gamme des Catalysts. Ce qui renforce encore le choix de protocole OSPF comme protocole de routage.

2. Proposition d'un plan d'adressage :

Dans ce paragraphe, on donne les détails de la politique dôadressage proposée. Pour des raisons de confidentialité, on utilise dans ce rapport une plage dôadresse (20.0.0.0/8), autre que celle proposée au client. On garde cependant la même logique dôadressage.

Le réseau 20.0.0.0/8 sera scindé en plusieurs sous réseaux /12, chaque sous réseaux /12 est dédié à un domaine VRF. On donne ci-dessous une illustration de cette subdivision :

Réseau 20.0.0.0/8	
Réseau Administration	20.0.0.0/12
Réseau Utilisateurs	20.16.0.0/12
Réseau Exploitation	20.32.0.0/11
-	20.64.0.0/12
-	20.80.0.0/12
-	20.96.0.0/12
-	20.112.0.0/12
-	20.128.0.0/12
-	20.144.0.0/12
-	20.160.0.0/12
-	20.176.0.0/12
-	20.192.0.0/12
-	20.208.0.0/12
-	20.224.0.0/12
-	20.240.0.0/12

Figure 24: Assignation des plages dôadresses en fonction des domaines existants

Chacun des domaines de lôentreprise disposera dôune plage /12, correspondant à un total de 1048576 adresses. Suite aux discussions avec les équipes techniques de lôentreprise, il sôest avéré que le réseau Exploitation pourra à lôavenir nécessiter plus dôadresses que les autres réseaux. Une plage /11 lui a donc été assignée par anticipation pour les besoins futurs.

Cette politique laisse de la marge pour encore 12 domaines supplémentaires. Chaque plage spécifique à un domaine sera ensuite scindée en fonction des areas OSPF.

La plage spécifique à une area OSPF sera de nouveau scindée en 3 sous-réseaux :

- Le sous-réseau utilisé pour les liens inter-switch.
- Le sous-réseau utilisé pour lôadressage Loopback.
- Le sous-réseau utilisé pour lôadressage des stations raccordées au switch. Ce sous-réseau sera de nouveau scindé à un niveau supplémentaire :
  - Sous-réseau des utilisateurs.
  - Sous-réseau des serveurs.

On donne ci-dessous le détail de lôadressage proposé pour le domaine des UTILISATEURS :

VRF UTILISATEURS 20.16.0.0/12					
Plages assignées aux Area OSPF		**Adressage liens WAN 1 réseau /24 = 128 réseaux /31 ou 64 réseaux /30**	**Adressage LAN (X représente un identifiant de switch). 254 adresses disponibles pour un switch.**		**Adressage Loopback**
Area 0	20.16.0.0/16	20.16.0.0/24	20.16.X.0/24		20.16.255.X/32
			20.16.X.0/25 (USERS)	20.16.X.128/25 (SERVERS)	
Area 1	20.17.0.0/16	20.17.0.0/24	20.17.X.0/24		20.17.255.X/32
			20.17.X.0/25 (USERS)	20.17.X.128/25 (SERVERS)	
Area 2	20.18.0.0/16	20.18.0.0/24	20.18.X.0/24		20.18.255.X/32
			20.18.X.0/25 (USERS)	20.18.X.128/25 (SERVERS)	
Area 3	20.19.0.0/16	20.19.0.0/24	20.19.X.0/24		20.19.255.X/32
			20.19.X.0/25 (USERS)	20.19.X.128/25 (SERVERS)	
Area 4	20.20.0.0/16	20.20.0.0/24	20.20.X.0/24		20.20.255.X/32
			20.20.X.0/25 (USERS)	20.20.X.128/25 (SERVERS)	
-	-	-	-		
-	-	-	-		
Area 15	20.31.0.0/16	20.31.0.0/24	20.31.X.0/24		
			20.31.X.0/25 (USERS)	20.31.X.128/25 (SERVERS)	20.31.255.X/32

Figure 25: Détail de lôadressage proposé pour le domaine des UTILISATEURS

Explication de lôadressage :

2 ème octet	Appartenance VRF + Area: -si valeur entre 16 et 31 -> c'est un adressage particulier à la VRF UTILISATEURS -Valeur 16 : Area 0 -Valeur 17: Area 1 -
3 ème octet	- 0 : Adressage utilisé pour les liens WAN - 255 : Adressage Loopback - valeur différente de 0 et 255 : Adressage LAN. La valeur de l'octet sera caractéristique d'un switch
4 ème octet	Dans le cas ou le 3 ème octet vaut 255 (loopback),la valeur du 4ème octet sera une valeur caractéristique du switch.

Figure 26: Explication de lôadressage du réseau utilisateurs

- Adressage des switchs

On aura noté dans le tableau précédent quôun switch donné est identifié avec un paramètre X. Ce paramètre X pourra être réutilisé entre plusieurs areas OSPF, la combinaison dôune area OSPF et dôune valeur X définissant en effet de manière unique un switch du réseau.

On pourra noter que le paramètre X s'incrémente avec un pas de 10. Cette politique a été mise en place afin de permettre l'insertion d'équipements réseaux dans les différents sites de l'entreprise, tout en permettant que l'ensemble des équipements soit numéroté de façon cohérente. (Numérotation croissante depuis l'origine des axes : Centre1 et Centre 180).

IV. Evolution du réseau :

Une contrainte initiale du projet était d'implanter OSPF comme protocole de routage. Cette contrainte vient du fait qu'au-delà des performances reconnues du protocole OSPF en termes de rapidité de convergence, il s'agit d'un protocole standardisé (RFC 2328), indépendant d'un constructeur donné (à la différence d'IGRP ou EIGRP propriétaires Cisco).

Une contrainte qui accompagne la mise en place d'un réseau OSPF est que toutes les « areas » qui composent le réseau doivent être raccordées à l'area 0. (Voir Figure 25 : Décomposition du domaine de l'entreprise en areas OSPF). Il n'est ainsi pas possible d'ajouter une area qui sera accolée par exemple à l'area 2 sans l'être à l'area 0.

Un autre protocole de routage, également standardisé et appartenant à la famille des protocoles à états de liens, est IS-IS (Intermediate System to Intermediate System). L'architecture d'un domaine IS-IS repose également sur la définition d'areas interconnectées entre elles. Cependant, une différence majeure par rapport à OSPF est que les areas d'IS-IS ne nécessitent pas d'être connectées à une area « backbone ». Les areas IS-IS peuvent être organisées avec une structure de chaîne. L'implantation d'IS-IS comme protocole de routage n'a cependant pas pu être envisagée car les équipements déployés dans le réseau de l'entreprise dans le cadre de ce projet ne supportent pas ce protocole.

L'évolution du réseau de l'entreprise peut consister en un ajout simple d'équipements à l'architecture existante, en l'extension d'une area OSPF existante (ou l'ajout d'une nouvelle area directement rattachée à l'area 0), ou encore en l'ajout d'un domaine non OSPF.

On se contente par la suite de donner quelques éléments relatifs à la première possibilité d'évolution.

- Ajout d'équipements à une area OSPF existante

Lôintégration de nouveaux routeurs (ou de switchs utilisés comme routeurs, comme cêst le cas pour ce projet) à une area OSPF est relativement simple. Il suffit de se maintenir à la même logique dôadressage, de configuration du routage OSPF, de définition des instances VRFs associées à cet équipementé

Lôajout dôun équipement nécessite au préalable de vérifier quôil supporte toutes les fonctionnalités à sa bonne intégration dans le réseau (OSPF, VRF-Lite,é).

V. Conclusion :

Lôélaboration de ce projet a mis en relief les nombreux avantages quôont les protocoles de niveau 3 et a permis de déduire en conséquent les tendances actuelles du marché en leur faveur.

Conclusion générale

Au cours de notre stage à CBI, on a été amené à étudier les technologies de réseaux classiques, mettre le point sur leurs différentes limites, étudier les technologies niveau 3 et dégager leurs avantages par rapport aux premières. Le but était de proposer une architecture reposant sur les nouvelles technologies étudiées précédemment.

Au terme de ce stage, on a pu proposer une architecture mettant en relief les différents points forts des protocoles et technologies niveau 3 à savoir une architecture LAN totalement routée depuis la couche accès jusquà la couche backbone qui permet de garantir à la fois une haute disponibilité et une administration facile, ce qui répond aux objectifs du projet.

On a pu également donner un exemple dimplémentation mettant en pratique les différentes technologies proposées.

Ce stage nous a été dun grand apport autant au niveau de mon expérience professionnelle quau niveau de mes connaissances concernant les réseaux LANs.

En effet, durant cette période de stage, on a pu développer nos capacités dadaptation, dorganisation, dinitiative et de travail en groupe.

Dautant plus, on a pu nous familiariser avec Dynamips et Dynagen, logiciels libres qui permettent l'émulation de machines virtuelles Cisco. En parallèle, on a assisté à une formation BSCI (Building Scalable Cisco Internetworks), formation axée sur les concepts et méthodes de configuration des protocoles de routage.

Dautre part, ce projet nous a offert loccasion dapporter une valeur ajoutée à léquipe dingénierie et de déploiement en participant à la mise en place de la politique dadressage et de routage et en préparant les configurations des équipements utilisés dans le réseau déployé de lentreprise.

Effectivement, le déploiement de la solution a commencé. Malgré les difficultés rencontrées lors des premières étapes dues à quelques instabilités du réseau de fibre optique, le client est actuellement satisfait du réseau mis en place. En effet ; malgré ces perturbations, les applications du client ont pu rester opérationnelles de façon transparente pour les utilisateurs grâce aux mécanismes de routage dynamique mis en place.

Ainsi, lôinfrastructure réseau déployée jusquôà présent est fonctionnelle et répond à tous les besoins exprimés par lôentreprise. Mais pourquoi ne pas la développer dôavantage et en tirer plus profit ?

Côest en essayant de répondre à cette question que nous avons décidé de suggérer plus de possibilités de communication future entre les différentes entités du réseau tout en gardant la démarcation offerte par les VRFs.

En effet, La notion dôinstances VRFs impose quôil nôy a en principe aucune communication possible entre des éléments appartenant à des instances VRFs différentes. (Voir les tests effectués en maquette VRFs). Cependant, il peut exister des besoins de communication entre des serveurs appartenant à des instances VRFs différentes, que cela soit au niveau dôun site distant donné, ou entre un site distant et le siège.

Pour obtenir cette communication inter-VRFs, on propose dôutiliser un mécanisme reposant sur lôutilisation dôun processus BGP qui se chargera dôéchanger les routes de table VRF à table VRF en fonction dôattributs spécifiques appelés Route-targets.

Dôautre part, une fois que cette technologie de virtualisation sera pleinement maitrisée par le client, on pourrait envisager lôutilisation dôun tel réseau comme un réseau dôopérateur. En effet, la disponibilité dôun réseau de fibre optique couvrant tout le territoire, et la possibilité de cloisonner le trafic permettrait de fournir des connexions au réseau à des entités extérieures, leur garantissant que leur trafic serait invisible à dôautres entités. Cette démarche permettrait au client de générer des revenus supplémentaires à partir de la bande passante inutilisée de son réseau mais implique une importante ingénierie et une administration du réseau encore plus poussée (garantie de la haute disponibilité du réseau aux entités tierces).

Bibliographie

Documentation CBI:

[1] Network Virtualization for the Campus, White Paper, Cisco Systems.
[2] Techniques for enterprise network virtualization.

Livres:

[1] Interconnecting Cisco Networking Devices, Part 2, Volume 1, Version 1.0
[2] Interconnecting Cisco Networking Devices, Part 2, Volume 2, Version 1.0
[3] Building Cisco Multilayer Switched Networks, Volume 1, Version 2.2
[4] Building Cisco Multilayer Switched Networks, Volume 2, Version 2.2

Sites Internet

[1] http://www.cisco.com
[2] http://www.supinfo-projects.com

URL

[1]http://www.cisco.com/web/FR/documents/pdfs/newsletter/ciscomag/2007/04/ciscomag_7_dossier_haute_disponibilite_dans_le_campus.pdf

Abréviation

A

ACL : Access Control List
AD : Advertised distance
ARP: Address Resolution Protocol
AS : Autonomous System

B

BDR : backup designated router
BGP : Border gateway protocol
BPDU : Bridge Protocol Data Unit
BSCI : Building Scalable Cisco Internetworks

C

FCS: Frame Check Sequence
CEF : Cisco Express Forwarding
CFI : Canonical Format Indicator
CST : Common Spanning Tree

D

DR : Designated Router
DUAL : Diffusing Update Algorithm

E

EIGRP: Enhanced Interior Gateway Routing Protocol

F

FD : Feasible Distance
FDDI : Fiber Distributed Data Interface
FIB : Forwarding Information Base

H

HSRP : Hot Standby Redundancy Protocol

I

IEEE : Institute of Electrical and Electronics Engineers
IETF: Internet Engineering Task Force
IGP : Interior Gateway Protocol
IGRP : Interior Gateway Routing Protocol
IS-IS : Intermediate System to Intermediate System
ISL : Inter-Switch Link

L

LAN: Local Area Network
LSA : Link State Advertissments
LSDB : Link-State DataBase
LSU : Link State Update

M

MAC: Medium Access Control address
MP-BGP: Multiprotocol Border Gateway Protocol
MPLS : Multi Protocol Label Switching

O

OSI : Open Systems Interconnection
OSPF : Open Shortest Path First

P

PVST: Per-VLAN Spanning Tree

R

RFC : Request For Comments
RIP : Routing Information Protocol
RSTP : Rapid Spanning Tree Protocol
RTP Reliable Transport Protocol

S

SPF : Shortest Path First
STP: Spanning Tree Protocol

V

VIP : Virtual Internet Protocol
VLAN: Virtual Local Area Network
VoIP : Voice-over-Internet protocol
VPN: Virtual Private Network
VRF : VPN Routing and Forwarding
VTP: VLAN Trunking Protocol

W

WAN: Wide Area Network