REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITEYAHIA FARES DE MEDEA



Faculté de **T**echnologie

Mémoire de fin d'études de Master

Filière : Génie Électrique
Spécialité : Automatique des systèmes

Amélioration des performances des réseaux industriels : Étude du protocole d'agrégation de liens EtherChannel

---

Présenté par :

HAMRANI Abdelmoumin

Proposé et Dirigé par :

DR. ABBADI Amel

M^{me}. AMRI Amel

Promotion 2020

Remerciements

D'abord, Je remercie ***Allah*** *le tout puissant et miséricordieux, qui m'a donné la force et le courage pour terminer mes études et qui m'a permet d'achever ce modeste travail.*

Je tiens à exprimer toute ma reconnaissance à ma directrice de mémoire, ***Madame ABBADI Amel*** *professeur à l'université de Médéa ainsi qu'à ma co-directrice,* ***Madame AMRI Amel*** *professeur au INSFP de Médéa pour m'avoir proposé ce sujet et pour toute la confiance qu'elles m'ont accordé, pour leurs souci permanent, pour leurs conseils et suggestions et surtout pour leurs critiques qui ont été toujours positive. Je les remercie de m'avoir encadré, orienté, aidé et conseillé.*

Je tiens aussi à adresser mes remerciements aux membres de jury pour avoir accepté de juger et examiner mon travail.

Je tiens également à remercier l'ensemble de mes enseignants, qui sont à l'origine de tout mon savoir.

En fin, je remercie toutes les personnes qui ont contribué de près ou de loin, au bon déroulement de mon travail et de mes études.

DEDICACES

Je dédier cette thèse…

À ma très chère mère

Autant de phrases aussi expressives soient-elles ne sauraient montrer le degré d'amour et d'affection que j'éprouve pour toi. Tu représentes pour moi le symbole de la bonté par excellence, la source de tendresse et l'exemple du dévouement qui n'a pas cessé de m'encourager et de prier pour moi.

Je te dédie ce travail en témoignage de mon profond amour.

À mon père

À mes frères et mes sœurs

En témoignage de l'amour, et de l'attachement que je porte pour vous. Je vous dédie ce travail avec tous mes vœux de bonheur, de santé et de réussite.

À toute ma famille

À mes amis

Oussama, Foudhil, Belkacem, Riadh, Mohammad, Khiro, Yasser,Walid, Younes, Raouf, Hamid, Abdennour Rafik,Djilali, Hadji, Houssam

Je vous dédie ce travail et vous souhaite un avenir à la hauteur de vos ambitions. Que notre amitié dure
Et enfin, à tous ceux que j'aime et qui m'aiment.

Moumene

ملخص– الهدف من هذه المذكرة هو دراسة وضبط تكنولوجية قناة الأثير التابعة لشركة سيسكو والتي تقدم حلا مهما لمشاكل تعدد الروابط بين جهازين داعمين لهذه التقنية من جهة و من جهة أخرى تقدم إمكانية رفع عرض النطاق الترددي (السرعة) وعدم السماح بالوقوع في الأعطال بين المبدلات، الموجهات و الخوادم كما أنها تقوم بتوزيع الشحنة بين الروابط المادية.

في هذا العمل قمنا بضبط بروتوكولات قناة الأثير : بروتوكول تجميع البوابات PAgP و بروتوكول مراقبة تجميع الروابط LACP بإستعمال المحاكي Cisco Packet Tracer و هذا مكننا من إدراك كيف أن قناة الأثير تسمح بتجميع الكثير من روابط الأثير المادية و المتشابهة في رابط منطقي واحد مع منع بروتوكول الشجرة الممتدة STP من إيقاف رابط أو أكثر.

كلمات مفتاحية: قناة الأثير, سيسكو, تعدد الروابط, عرض النطاق الترددي ,بروتوكول مراقبة تجميع الروابط, بروتوكول تجميع البوابات, بروتوكول الشجرة الممتدة.

Résumé. — L'objectif poursuivi dans cette mémoire porte sur l'étude et configuration de la technologie EtherChannel de Cisco qui apporte une solution intéressante aux problèmes de redondance des liens entre deux périphériques EtherChannel-enabled d'une part et d'autre part elle offre la possibilité d'augmenter la bande passante (vitesse) et la tolérance aux pannes entre les commutateurs, les routeurs et les serveurs et de partager la charge entre les liaisons physiques. Dans ce travail nous avons configuré les protocoles d'EtherChannel : le protocole d'agrégation des ports PAgP et le protocole de contrôle d'agrégation des liens LACP en utilisant le simulateur Cisco Packet Tracer et cela nous a permis de voir comment EtherChannel permet d'assembler plusieurs liens physiques Ethernet identiques en un seul lien logique. Toute en évitant que le protocole de l'arbre étendu STP bloque une ou plusieurs liaisons.

Mots clés : EtherChannel, Cisco, redondance des liens, bande passante, protocole de contrôle d'agrégation des liens, protocole d'agrégation des ports, protocole de l'arbre étendu.

Abstract. — The objective of this memory concerns the study and configuration of the EtherChannel technology from Cisco which provides an interesting solution to the problems of redundancy of the links between two EtherChannel-enabled devices on the one hand and on the other hand it offers the ability to increase bandwidth (speed) and fault tolerance between switchs, routers and servers and to share the load between physical links. In this work we have configured the EtherChannel protocols: the PAgP port aggregation protocol and the LACP link aggregation protocol using the Cisco Packet Tracer simulator and this allowed us to see how EtherChannel allows assembling several Identical Ethernet physical links in a single logical link. While avoiding that the Spanning Tree Protocol blocks one or more links.

Key words: EtherChannel, Cisco, redundancy of links, bandwidth, spanning tree protocol, port aggregation protocol, link aggregation control protocol.

Table des matières

INTRODUCTION GÉNÉRALE 1

CHAPITRE I: GÉNÉRALITÉS SUR LES RÉSEAUX INFORMATIQUES 3

I.1 Introduction 3

I.2 Définition d'un réseau 3

I.3 Composants réseau 3

I.3.1 Présentation des composants réseau 3

I.3.2 Périphériques finaux 4

I.3.3 Périphériques intermédiaires 4

I.3.4 Supports réseau 5

I.3.5 Représentations du réseau 6

I.4 Classification des réseaux 7

I.4.1 Par étendu 7

I.4.2 Par relation fonctionnelle entre les composants 8

I.4.3 Par topologie 8

I.5 Réseaux locaux virtuels 11

I.5.1 Définition 11

I.5.2 Avantages des réseaux locaux virtuels 11

I.5.3 Types des réseaux locaux virtuels 12

I.6 Modèle de référence 13

I.6.1 Modèle de référence OSI 13

I.6.2 Le modèle de référence TCP/IP 16

I.6.3 Comparaison des modèles OSI et TCP/IP 17

I.7 Adresses de communication 17

I.7.1 Adresses IP 17

I.7.2 Adresse MAC 19

I.8 Conclusion 20

CHAPITRE II: PROTOCOLES DE GESTION DE LIENS.....21
II.1 Introduction.....21
II.2 Le protocole spanning tree.....21
II.2.1 Introduction au protocole spanning tree.....21
II.2.2 Problèmes majors de la redondance des liens.....21
II.2.3 Définition.....22
II.2.4 Fonctionnement du protocole STP.....22
II.2.5 Mode des ports sur les commutateurs.....25
II.2.6 Rôles des ports :.....25
II.2.7 Exemple de STP :.....26
II.2.8 Variantes STP.....28
II.3 Le protocole EtherChannel.....30
II.3.1 Introduction.....30
II.3.2 Définition.....30
II.3.3 Avantages d'EtherChannel.....30
II.3.4 Fonctionnement d'EtherChannel.....31
II.3.5 Les composants de l'EtherChannel.....32
II.3.6 Restrictions de mise en œuvre d'EtherChannel :.....32
II.3.7 Protocoles EtherChannel.....33
II.3.8 Dépannage de la fonctionnalité EtherChannel.....36
II.4 Conclusion.....37
CHAPITRE III: CONFIGURATION ET SIMULATION.....38
III.1 Introduction.....38
III.2 Présentation du simulateur « Cisco Packet Tarcer ».....38
III.2.1 Définition.....38
III.2.2 Présentation de l'interface.....38
III.2.3 Modes de fonctionnement.....42

III.2.4 Connexions / Liens 42
III.2.5 Statut du lien 44
III.3 Système d'exploitation réseau Cisco IOS 44
III.3.1 Méthodes d'accès à la CLI 45
III.3.2 Programmes d'émulation de terminal 45
III.3.3 Principaux modes de commande 45
III.3.4 Touches d'accès rapides et raccourcis 46
III.4 Configuration du protocole EtherChannel : 47
III.4.1 Partie 1 : Configuration des paramètres de base du commutateur 48
III.4.2 Partie 2 : Configuration de PAgP 52
III.4.3 Partie 3 : Configuration de LACP 56
III.4.4 Partie 4 : Configurer On 58
III.4.5 Test et vérification 60
III.5 Conclusion 63
CONCLUSION GÉNÉRALE 64
BIBLIOGRAPHIE 65

Liste des figures

Figure I-1 : Symboles utilisées dans les schémas de réseau. 6
Figure I-2 : Diagramme d'un réseau. 6
Figure I-3 : Topologie en bus. 9
Figure I-4 : Topologie en étoile. 9
Figure I-5 : Topologie en anneau. 10
Figure I-6 : Topologie maillée. 10
Figure I-7 : Topologie arborescente. 11
Figure I-8 : VLAN Voice Cisco. 13
Figure I-9 : Modèle OSI. 14
Figure I-10: Modèle TCP/IP. 16
Figure I-11 : Comparaison entre le modèle TCP/IP et le modèle OSI. 17
Figure I-12 : Propriété de protocole IPv4. 18
Figure II-1 : Topologie en arbre étendu. 23
Figure II-2 : Champs BID. 23
Figure II-3 : Topologie redondante. 26
Figure II-4 : Élection du commutateur racine. 27
Figure II-5 : Sélection des ports racines. 27
Figure II-6 : Sélection des ports désignés et blocage des autres ports. 28
Figure II-7 : Agrégation des liens. 31
Figure II-8 : Protocole EtherChannel PAgP. 34
Figure II-9 : Topologie EtherChannel LACP. 36
Figure III-1 : Interface de Packet Tracer. 39
Figure III-2 : La fenêtre de paquet créé par l'utilisateur (UCPW). 41
Figure III-3 : Topologie. 47
Figure III-4 : Câblage du réseau. 49
Figure III-5 : Initialisation et redémarrage des commutateurs. 49
Figure III-6 : Désactivation de la recherche DNS. 49
Figure III-7 : Configuration de nom du périphérique. 50
Figure III-8 : Désactivons de tous les ports exceptés celles connectés à des PC. 50
Figure III-9 : Configuration de VLAN 99. 50
Figure III-10 : Configuration de VLAN 10. 50

Figure III-11 : Configuration de port f0/6 en tant que ports d'accès au VLAN 10. 50
Figure III-12 : Configuration des adresses IP. 51
Figure III-13 : Enregistrement de la configuration. 51
Figure III-14 : Configuration d'adresse IP. 51
Figure III-15 : Configuration des ports sur S1 avec le mode PAgP desirable. 52
Figure III-16 : Configuration des ports sur S3 avec le mode PAgP auto. 52
Figure III-17 : Topologie du réseau après avoir configuré PAgP sur S1 et S3. 53
Figure III-18 : Vérification de la configuration sur les ports. 53
Figure III-19 : Vérification du port-channel 1 en S1 54
Figure III-20 : Vérification du port-channel 1 sur S3 54
Figure III-21 : Configuration des ports trunks. 55
Figure III-22 : Vérification du port-trunk et VLAN natif. 55
Figure III-23 : Configuration de LACP entre S1 et S2. 56
Figure III-24 : Topologie su réseau après avoir configuré LACP entre S1 et S2. 56
Figure III-25 : Vérification de protocole EtherChannel utilisé par Po2 sur S1. 57
Figure III-26 : Vérification de protocole EtherChannel utilisé par Po2 sur S2. 57
Figure III-27 : Configuration de mode ON entre S2 et S3. 58
Figure III-28 : Vérification de protocole EtherChannel utilisé par Po3 sur S2. 59
Figure III-29: Vérification de protocole EtherChannel utilisé par Po3 sur S3. 59
Figure III-30 : Test de connectivité entre PC-A et PC-C. 60
Figure III-31: Résumé de STP en S3. 61
Figure III-32 : Topologie du réseau après avoir configuré l'EtherChannel 62
Figure III-33 : Résumé de STP en S1. 62
Figure III-34 : Résumé de STP en S2. 63

Liste des tableaux

Tableau II-1 : Couts des liens. 24
Tableau II-2 : Réglage de modes PAgP. 34
Tableau II-3: Réglages de mode LACP. 36
Tableau III-1 : Table d'adressages. 48

Liste des abréviations

ARP	**A**ddress **R**esolution **P**rotocol
BID	**B**ridge **ID**entifier
BPDU	**B**ridge **P**rotocol **D**ata **U**nit
CCNA	**C**isco **C**ertified **N**etwork **A**ssociate
CLI	**C**ommand **L**ine **I**nterface
DNS	**D**omain **N**ame **S**ystem
IEEE	**I**nstitute of **E**lectrical and **E**lectronics **E**ngineers
IETF	**I**nternet **E**ngineering **T**ask **F**orce
IOS	**I**nternetwork **O**perating **S**ystem
IP	**I**nternet **P**rotocol
LACP	**L**ink **A**ggregation **C**ontrol **P**rotocol
LAN	**L**ocal **A**rea **N**etwork
MAC	**M**edia **A**ccess **C**ontrol
MAN	**M**etropolitan **A**rea **N**etwork
MOTD	**M**essage **O**f **T**he **D**ay
MSTP	**M**ultiple **S**panning **T**ree **P**rotocol
NAT	**N**etwork **A**ddress **T**ranslation
OSI	**O**pen **S**ystem **I**nterconnection
OUI	**O**rganizationally **U**nique **I**dentifier
PAgP	**P**ort **Ag**gregation **P**rotocol
PAN	**P**ersonal **A**rea **N**etwork
PING	**P**acket **In**ternet **G**roper
PVRST+	**P**er **V**irtual local area network **R**apid **S**panning **T**ree plus
PVST	**Per V**irtual local area network **S**panning **T**ree
RSTP	**R**apid **S**panning **T**ree **P**rotocol
STP	**S**panning **T**ree **Pr**otocol
TCP	**T**ransmission **C**ontrol **P**rotocol
VLAN	**V**irtual **L**ocal **A**rea **N**etwork
VOIP	**V**oice **O**n **I**nternet **P**rotocol
WAN	**W**ide **A**rea **N**etwork

INTRODUCTION GÉNÉRALE

INTRODUCTION GÉNÉRALE

Dans le monde industriel, la communication de données passe traditionnellement par les bus de terrain. La diversité des types et des standards complique l'interopérabilité et en accroit les couts. C'est pourquoi Ethernet a petit à petit été envisagé pour les applications industrielles. En effet, Ethernet est un standard ouvert bien défini qui simplifie l'interopérabilité et accepte des composants provenant de sources multiples (Fiabilité), il est rapide (le débit peut atteindre 12 Mbit/s) comme il est 'déterminisme', ce terme est une mot-clé pour de nombreux réseaux industriels : un réseau déterministe permet de dire avec une certitude quasi totale qu'un événement s'est déjà produit dans une fenêtre de temps spécifique donc il doit répondre le plus souvent à des contraintes temporelles strictes, mais aussi garantir une continuité de service.

Plus de 70 % des pannes de réseau se produisent dans le support réseau et le matériel. C'est-à-dire que la majorité des pannes de réseau surviennent au niveau des câbles, connecteurs et commutateurs. C'est pourquoi la présence d'un réseau redondant est essentielle. Il doit être conçu de façon à permettre une récupération rapide en cas de panne. De tels réseaux s'appuient sur plusieurs chemins entre la source et la destination d'un message. Si l'un des chemins est défaillant, le message peut instantanément être envoyé par le biais d'une autre liaison.

Le fait de disposer de plusieurs chemins vers une destination s'appelle la redondance et ça peut provoquer des boucles qui peuvent être néfastes pour le fonctionnement du réseau.

Comme solution, un protocole appelé Spanning Tree Protocol (STP) a été créé et développé pour garder les réseaux de couche 2 sans boucle et pour empêcher les tempêtes de diffusion.

STP fonctionne essentiellement en bloquant les liens redondants entre les commutateurs ou les segments. Ils existent des liens redondants entre les commutateurs ou les segments pour fournir un lien de sauvegarde en cas de défaillance d'un lien. Outre la redondance, ces liaisons peuvent être utilisées pour fournir une bande passante supplémentaire entre ces commutateurs ou segments. Il n'est pas nécessaire de mettre à niveau la liaison vers une connexion plus coûteuse pour avoir davantage de bande passante. Au lieu d'avoir un seul lien pour transférer les données, le trafic peut être équilibré en charge entre deux liens ou plus.

Étant donné que STP bloque toutes les liaisons redondantes, la capacité d'équilibrage de charge est perdue, et les liaisons redondantes ne peuvent pas fournir une bande passante supplémentaire entre les commutateurs. Que fait-on pour surmonter ces limitations de STP ? . EtherChannel est utilisé pour regrouper jusqu'à 8 liens en un seul lien logique. Une fois les liens regroupés, STP ne voit qu'un seul lien logique et n'est pas en mesure de bloquer quoi que ce soit.

Dans le présent mémoire, nous focalisons notre étude à donner une solution aux problèmes des boucles dans les liaisons physiques tout en équilibrant le trafic. À cet effet, la thèse est divisée en trois chapitres :

Le premier chapitre porte sur les concepts de base des réseaux informatiques, pour mieux assimiler le fonctionnement des réseaux. Donc, toutes les notions nécessaires seront présentées, tels que les composants réseau, la classification des réseaux, les réseaux locaux virtuels ainsi le modèle OSI et TCP/IP.

Le deuxième chapitre est consacré à définir les différents notions et concepts de base des protocoles de gestion des liens en commençant par le protocole STP et ensuite le protocole Etherchannel.

Enfin, le troisième chapitre représente les résultats de configuration du protocole Etherchanel et ceci en utilisant un logiciel de conception et de simulation Cisco Packet Tracer. Ces résultats sont alors présentés et discutés.

Ce mémoire se termine par une conclusion générale des travaux présentés.

CHAPITRE I: GÉNÉRALITÉS SUR LES RÉSEAUX INFORMATIQUES

I.1 Introduction

L'informatique a envahi tous les aspects de notre vie quotidienne (communication, éducation, industrie…). Avec l'explosion d'internet, le réseau informatique est devenu un outil incontournable dans tous les domaines dans un monde où la concurrence est féroce et où la planète n'est plus qu'un petit village où l'information circule instantanément.

L'objectif de ce chapitre est de présenter quelques concepts de bases sur les réseaux informatiques, pour nous aider à mieux assimiler le fonctionnement des réseaux. Donc, toutes les notions nécessaires seront présentées, tels que les composants réseau, la classification des réseaux, le modèle OSI et TCP/IP ainsi les réseaux locaux virtuels.

I.2 Définition d'un réseau

Un réseau (network) est un ensemble des moyens matériels et logiciels mis en œuvre pour assurer les communications entre ordinateurs, stations de travail et terminaux informatiques. Les réseaux informatiques permettent aux utilisateurs de communiquer entre eux et de transférer des informations. Ces transmissions de données peuvent concernées l'échange de messages entre utilisateurs, l'accès à distance aux bases de données ou encore le partage de fichiers [1].

I.3 Composants réseau

I.3.1 Présentation des composants réseau

Le chemin emprunté par un message depuis une source jusqu'à une destination peut être aussi simple que la connexion entre deux ordinateurs via un seul câble ou aussi complexe qu'une collection de réseaux parcourant le globe terrestre. Cette infrastructure réseau fournit le canal stable et fiable à travers lequel nos communications peuvent s'établir.

L'infrastructure réseau comprend trois catégories de composants réseau :

- Appareils
- Supports
- Services

Les périphériques et les supports représentent les éléments physiques ou le matériel du réseau. Le matériel correspond souvent aux composants visibles de la plate-forme réseau, par exemple un ordinateur portable, un ordinateur de bureau, un commutateur, un routeur, un point d'accès sans fil ou le câblage qui sert à relier les périphériques.

Les services incluent de nombreuses applications de réseau courantes utilisées quotidiennement, comme les services d'hébergement de messagerie et les services d'hébergement web. Les processus fournissent les fonctionnalités qui dirigent et déplacent les messages à travers le réseau. Ils sont essentiels au bon fonctionnement des réseaux[2].

I.3.2 Périphériques finaux

Les périphériques réseau auxquels les personnes sont les plus habituées sont appelés périphériques finaux comme les ordinateurs de bureau, ordinateurs portables, imprimante, téléphone IP, tablette sans fil, système de téléprésence.

Un périphérique final est la source ou la destination d'un message transmis sur le réseau. Pour qu'il soit possible de distinguer les périphériques finaux, chaque périphérique final présent sur un réseau est identifié à l'aide d'une adresse. Lorsqu'un périphérique final initie une communication, il utilise l'adresse du périphérique final de destination afin de spécifier l'emplacement où le message doit être envoyé[3].

I.3.3 Périphériques intermédiaires

Les périphériques intermédiaires connectent les périphériques finaux individuels au réseau et peuvent connecter plusieurs réseaux individuels afin de former un interréseau. Ils fournissent la connectivité et s'assurent que les données sont transmises sur le réseau.

Les périphériques intermédiaires utilisent l'adresse du périphérique final de destination, ainsi que les informations concernant les interconnexions réseau, pour déterminer le chemin que doivent emprunter les messages à travers le réseau. Les plus courants sont [3] :

- **Répéteur :** dispositif permettant d´étendre la distance de câblage d'un réseau local. Il amplifie et répète les signaux qui lui parviennent. Il n'est pas un composant intelligent.
- **Pont :** Un pont (bridge) est un dispositif permettant de relier des réseaux distincts.

- **Routeur :** Un routeur (router) est un dispositif permettant de relier des réseaux locaux de telle façon à permettre la circulation de données d'un réseau à un autre de façon optimale.
- **Passerelle :** Une passerelle (Gateway) est un dispositif permettant d'interconnecter des architectures de réseaux différentes. Elle assure la traduction d'un protocole vers un autre par exemple : la fonction passerelle d'un système téléphonique sur IP est de traduire le protocole SIP en protocole ISDN et forme ainsi l'interface entre la Voix sur IP et la téléphonie classique.
- **Concentrateur :** Un concentrateur (hub) est un dispositif permettant de connecter divers éléments de réseau.
- **Commutateur :** Un commutateur (Switch) est un dispositif permettant de relier divers éléments tout en segmentant le réseau. Nous pouvons le considérer comme un hub intelligent.
- **Adaptateur :** les adaptateurs (adapter) sont destinés à être insérés dans un poste de travail ou un serveur afin de les connecter à un système de câblage.

I.3.4 Supports réseau

La communication à travers un réseau s'effectue sur un support (média). Ce support fournit le canal via lequel le message se déplace de la source à la destination.

Les réseaux modernes utilisent principalement trois types de supports pour interconnecter des périphériques et fournir le chemin par lequel des données peuvent être transmises. Ces supports sont les suivants [3] :

- **Fils métalliques réunis en câbles** : les données sont codées en impulsions électriques.
- **Fibres de verre ou plastiques (câble de fibre optique)** : les données sont codées sous forme d'impulsions lumineuses.
- **Transmission sans fil** : les données sont codées en utilisant les longueurs d'onde du spectre électromagnétique.

Les différents types de supports réseau possèdent divers avantages et fonctionnalités. Tous les supports réseau ne possèdent pas les mêmes caractéristiques et ils ne conviennent pas non plus à toutes les applications.

I.3.5 Représentations du réseau

Les schémas de réseau utilisent souvent des symboles, tels que ceux qui sont présentés à la figure I-1, pour représenter les périphériques et les connexions qui composent un réseau.

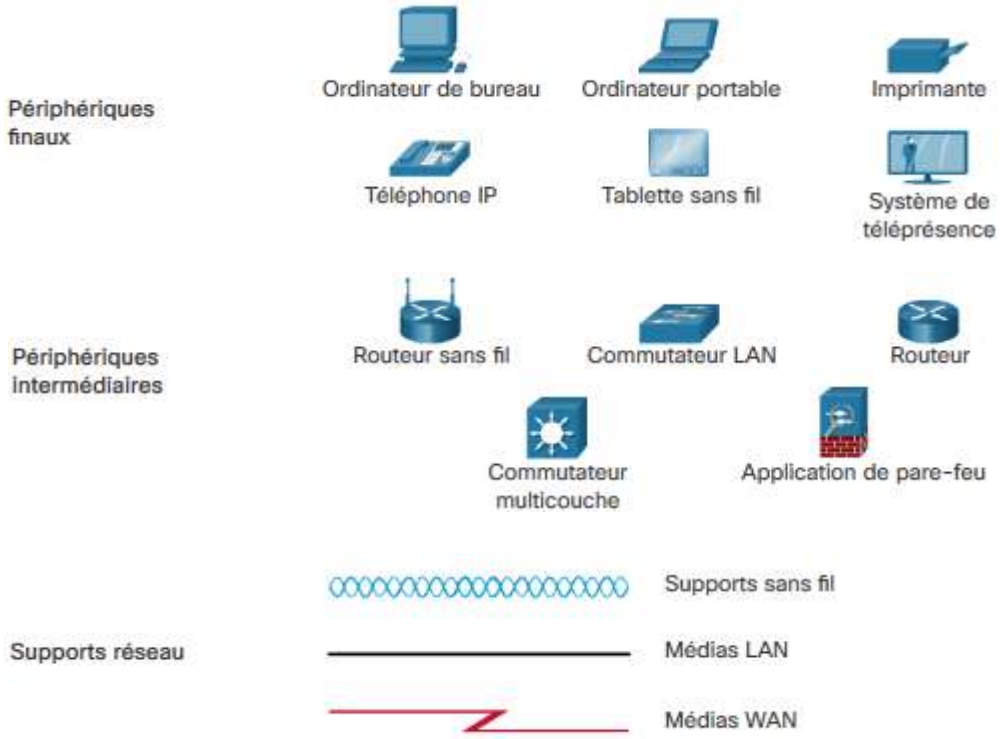


Figure I-1 : Symboles utilisées dans les schémas de réseau.

Un schéma constitue un moyen facile pour illustrer la façon dont les périphériques d'un grand réseau sont connectés. On appelle ce type de schéma de réseau « diagramme de topologie ».

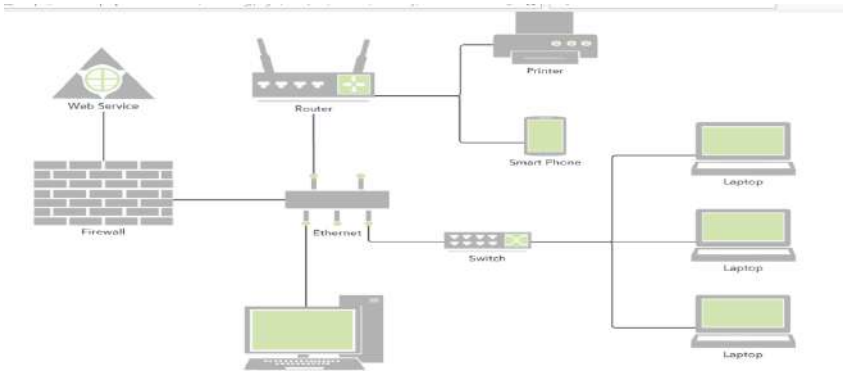


Figure I-2 : Diagramme d'un réseau.

En plus de ces représentations, une terminologie spécialisée est utilisée pour étudier la manière dont ces périphériques et supports se connectent entre eux. Les termes importants dont il faut se souvenir sont les suivants [3] :

- **Carte réseau :** une carte réseau, ou adaptateur de réseau local, fournit la connexion physique au réseau à partir de l'ordinateur ou d'un autre périphérique final. Les supports qui relient l'ordinateur au périphérique réseau se branchent directement à la carte réseau.
- **Port physique :** connecteur ou prise sur un périphérique réseau par lequel/laquelle le support est connecté à un périphérique final ou à autre périphérique réseau.
- **Interface :** ports spécifiques sur un périphérique réseau qui se connectent à des réseaux individuels. Puisque les routeurs sont utilisés pour interconnecter des réseaux, les ports sur un routeur sont appelés des interfaces réseau.

REMARQUE : Les termes « port » et « interface » sont souvent utilisés l'un pour l'autre

I.4 Classification des réseaux

On distingue différentes manières de classifier les réseaux selon leur étendue (LAN, MAN, WAN), leur relation fonctionnelle entre les composants ainsi que leur topologie (physique ou logique).

I.4.1 Par étendu

I.4.1.1 *PAN*

C'est un petit réseau composé des équipements d'une personne comme micro-ordinateur, imprimante, smart phone, télévision, etc [4].

I.4.1.2 *LAN*

Un réseau local est un réseau informatique à une échelle géographique relativement restreinte, il est utilisé pour relier entre les utilisateurs et les périphériques finaux d'une habitation particulière, d'une entreprise, d'une salle informatique [4].

I.4.1.3 *MAN*

Les MANs interconnectent plusieurs LAN géographiquement proches (au maximum quelque dizaines de Km) à des débits importants. Ainsi un MAN permet à deux nœuds distants de communiquer comme s'ils faisaient partie d'un même réseau local. Un MAN est formé de commutateurs ou de routeurs interconnectés par des liens hauts débits (en général en fibre optique) [4].

I.4.1.4 *WAN*

Un WAN (réseau étendu) interconnecte plusieurs LANs à travers de grandes distances géographiques. Les débits disponibles sur un WAN résultent d'un arbitrage avec le cout des liaisons (qui augmente avec la distance) et peuvent être faible. Les WANs fonctionnent grâce à des routeurs qui permettent de choisir le trajet le plus approprié pour atteindre un nœud du réseau. Le plus connu des WAN est Internet [4].

I.4.2 Par relation fonctionnelle entre les composants

Selon la nature des relations entre les postes, on distingue généralement deux types de réseaux bien différents, ayant tout de même des similitudes. Ils sont : [5]

- **Réseau client/serveur :** c'est un réseau qui contient des ordinateurs clients et un ordinateur serveur qui leur fournit des services. Ces services sont des programmes s'exécutant dans le serveur et qui fournissent des données telles que l'heure, des fichiers, une connexion à internet, ou le partage de certaines ressources.
- **Réseau poste à poste (Peer to Peer) :** contrairement au réseau client/serveur, dans un réseau poste à poste, il n'y a pas de serveur dédié. Ainsi chaque ordinateur dans un tel réseau est parfois un serveur et parfois un client. Cela signifie que chacun des ordinateurs du réseau est libre de partager ses ressources.

I.4.3 Par topologie

Une topologie de réseau informatique correspond à l'architecture (physique ou logique) de celui-ci, définissant les liaisons entre les équipements du réseau et la hiérarchie éventuelle entre eux.

I.4.3.1 *Topologie physique*

Elle peut définir la façon dont les équipements sont interconnectés et la représentation spatiale du réseau [6].

- ***Topologie en bus*** : une topologie en bus est l'organisation la plus simple d'un réseau. En effet, dans une topologie en bus tous les ordinateurs sont reliés à une même ligne de transmission par l'intermédiaire de câble, généralement coaxial. Le mot « bus » désigne la ligne physique qui relie les machines du réseau.

  Cette topologie a pour avantage d'être facile à mettre en œuvre et de posséder un fonctionnement simple.



Figure I-3 : Topologie en bus.

- ***Topologie en étoile*** *:* tous les terminaux sont reliés à un composant matériel unique (*hub* (ou *concentrateur), Switch (commutateur) ou Routeur*),afin d'assurer la communication entre les différents ordinateurs.

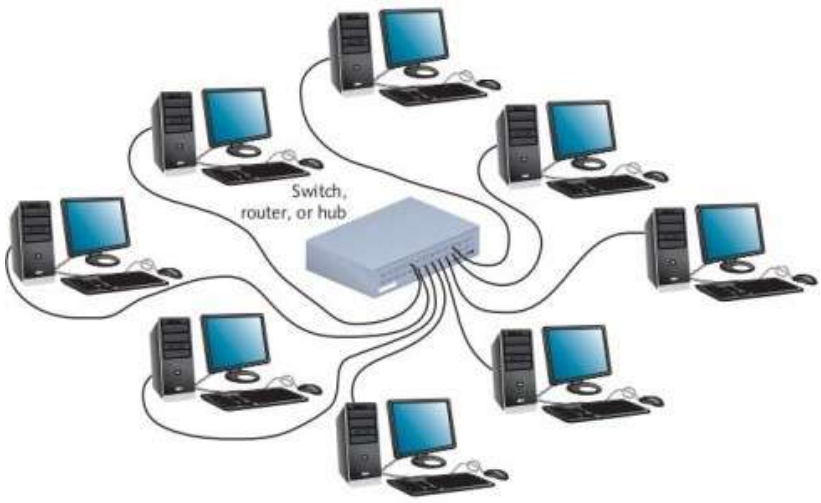


Figure I-4 : Topologie en étoile.

- ***Topologie en anneau*** *:* tous les terminaux sont reliés en anneau (boucle). Dans cette boucle, les ordinateurs communiquent chacun à leur tour.

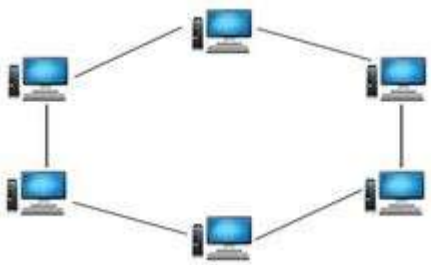


Figure I-5 : Topologie en anneau.

- ***Topologie maillée*** **:** chaque paire de terminaux sont reliées directement par un support unique. Cette topologie est rigide vis-à-vis l'extension et le nombre de liaisons croit rapidement avec le nombre de machines (n×(n-1)/2).

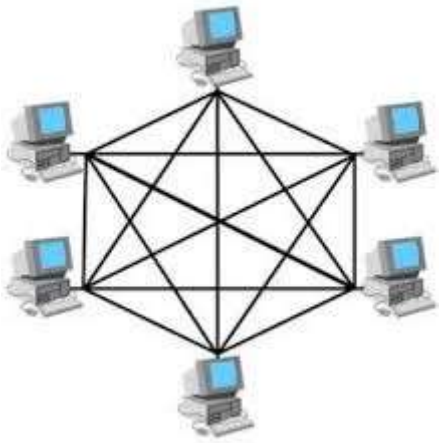


Figure I-6 : Topologie maillée.

- ***Topologie arborescente*** **:** connu aussi sous le nom de topologie hiérarchique, dans laquelle les équipements intermédiaires d'interconnexion sont organisés plusieurs niveaux. Le sommet, de haut niveau, est connectée à plusieurs nœuds de niveau inférieur, dans la hiérarchie. Ces nœuds peuvent être eux-mêmes connectés à plusieurs nœuds de niveau inférieur. Le tout dessine alors un arbre, ou une arborescence.



Figure I-7 : Topologie arborescente.

I.4.3.2 *Topologie logique*

Désigne la manière dont un réseau transfère les trames d'un nœud à l'autre. Cette configuration est composée de connexions virtuelles entre les nœuds d'un réseau. Ces chemins de signaux logiques sont définis par les protocoles de couche liaison de données. La topologie logique des liaisons point à point est relativement simple tandis que les supports partagés proposent des méthodes de contrôle d'accès différentes [6].

I.5 Réseaux locaux virtuels

I.5.1 Définition

Un réseau local virtuel (en anglais VLAN : Virtual Local Area Network ou Virtual LAN) est un réseau local regroupant un ensemble de machines de façon logique et non physique sans tenir compte de ses emplacements physiques. VLAN ont les mêmes attributs que les LAN physique [7].

I.5.2 Avantages des réseaux locaux virtuels

Le VLAN permet de définir un nouveau réseau au-dessus du réseau physique et à ce titre offre les avantages suivants [8] :

- Plus de souplesse pour l'administration et les modifications du réseau car toute l'architecture peut être modifiée par 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.
- La réduction des messages de diffusion (notamment les requêtes ARP) limités à l'intérieur d'un VLAN. Ainsi les diffusions d'un serveur être limitées aux clients de ce serveur.

- La création de groupes de travail indépendants de l'infrastructure physique, possibilité de déplacer la station sans changer de réseau virtuel.
- L'augmentation de la sécurité par le contrôle des échanges inter-VLAN en utilisant des routeurs (filtrage possible du trafic échangé entre les VLANs).

I.5.3 Types des réseaux locaux virtuels

I.5.3.1 *VLAN par défaut*

Au démarrage initial du commutateur, tous les ports deviennent membre du VLAN par défaut, ce qui les rend tous partie du même domaine de diffusion. Cela permet à tout dispositif de réseau connecté à un des ports de commutation de communiquer avec d'autres dispositifs sur d'autres ports de commutateur. Sur commutateurs Cisco le VLAN par défaut est VLAN1. Le VLAN 1 possède toutes les caractéristiques des VLANs, sauf qu'on ne peut pas le renommer ou le supprimer.

I.5.3.2 *VLAN de données*

Un VLAN de données peut aussi être considéré comme utilisateur VLAN. Celui-ci est configuré pour ne transporter que le trafic généré par les utilisateurs. L'importance de séparer les données de l'utilisateur à partir de tout autre type de VLAN est la gestion et le contrôle de l'interrupteur approprie.

I.5.3.3 *VLAN natif*

Un réseau local virtuel natif est affecté à un accès de jonction 802.1Q. Un port d'agrégation 802.1Q prend en charge le trafic provenant de plusieurs VLAN ainsi que le trafic qui ne viennent pas d'un VLAN. Le port d'agrégation 802.1Q place le trafic non balisé (trafic qui ne provient pas d'un VLAN) sur le VLAN natif. En résumé, le VLAN natif observe et identifie le trafic provenant de chaque extrémité d'un lien de tronc.

I.5.3.4 *VLAN de gestion*

Le VLAN de gestion est un VLAN spécifique attribué aux commutateurs pour qu'ils soient accessibles via une adresse IP.

I.5.3.5 *VLAN voix*

Un VLAN voix est configuré pour transporter le trafic voix.

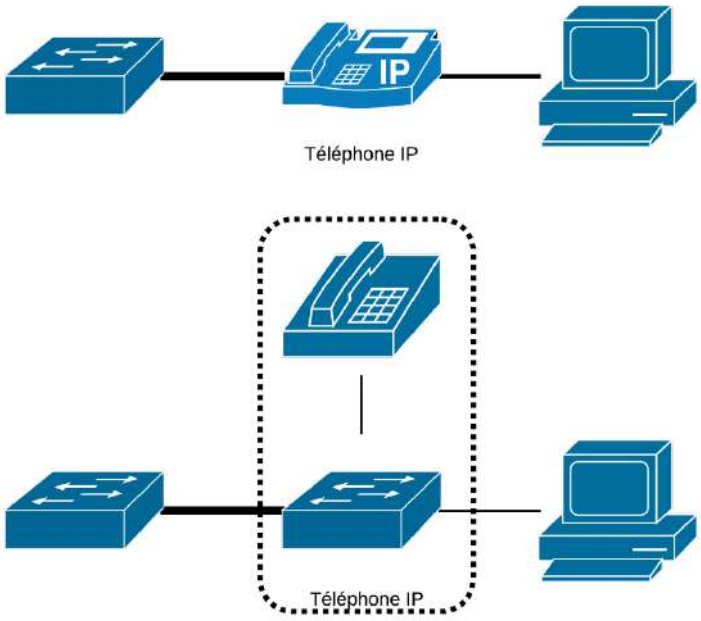


Figure I-8 : VLAN Voice Cisco.

I.6 Modèle de référence

I.6.1 Modèle de référence OSI

Pour assurer une communication fiable entre équipements informatiques plusieurs problèmes doivent être traités, notamment :

- Comment passer une information numérique entre des équipements ? sous quelle forme ? par quels médias ?
- Comment assurer une transmission fiable (sans erreurs) ?
- Comment étendre un réseau et connecter des équipements hétérogènes ?
- Comment faire communiquer des applications informatiques ?

Au début des années 70, chaque constructeur a développé sa propre architecture de réseau informatique avec son propre technologie propriétaire. Ceci peut créer des problèmes variés, notamment l'impossibilité d'implémenter des réseaux par des équipements de constructeurs différents.

Le traitement de ce problème consiste à imposer des normes à respecter par tous les concepteurs et constructeurs des réseaux. Ces normes concernent la détermination des :

- Différentes parties de l'architecture des réseaux.

- Les règles à respecter lors de l'implémentation de chaque partie.

I.6.1.1 *Modèle en couches OSI*

Proposé par ISO en 1977, le modèle OSI est basé sur une représentation en sept (07) couches (figure I-9). Chaque couche décrit une solution à un problème de communication spécifique [9].

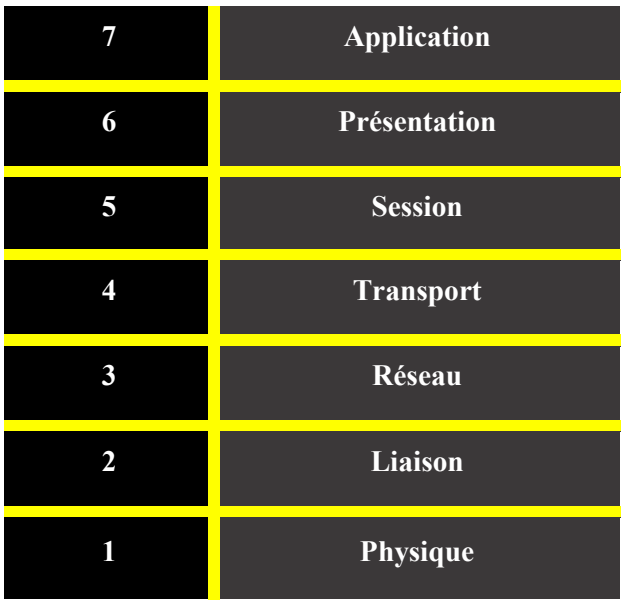


Figure I-9 : Modèle OSI.

- ***Niveau 1 : Couche Physique***

Assure le transfert des bits sur une liaison physique. Il fournit les moyens mécaniques, électriques, fonctionnels et procéduraux nécessaires pour la mise en œuvre des liaisons physiques entre équipements des réseaux. Les standards de cette couche spécifient :

- Les types des médias physiques et leurs caractéristiques.

- Les types des signaux et ondes porteurs de l'information et leurs caractéristiques.

- Les types des liaisons, procédures de gestion de ces liaisons, et leurs caractéristiques.

- ***Niveau 2 : Couche Liaison***

Fournit les moyens fonctionnels et procédures nécessaires pour l'établissement et la gestion des liaisons directes entre deux équipements. Elle permet surtout de contrôler

l'échange des informations binaires, entre deux nœuds adjacents, contre les erreurs de transmission.

- ***Niveau 3 : Couche Réseau***

Fournit les moyens (équipements et services) nécessaires pour l'interconnexion des réseaux (dans un seul réseau) et pour l'acheminement efficace des messages (qui s'appelle dans ce niveau paquets) vers le bon destinataire (éventuellement via un ou plusieurs relais ou équipements intermédiaires). Les standards de cette couche spécifient :

- Les types et les structures des adresses et des paquets.

- Les mécanismes de contrôle de congestion de réseaux.

- Les procédures d'échanges des paquets et de gestion des chemins.

- ***Niveau 4 : Couche Transport***

Cette couche permet d'assurer une communication directe, sans erreurs et sans saturation entre des applications communicantes en offrant des voix logiques à travers des connexions physiques sur le réseau. Elle assure aussi la segmentation des données en paquets et le réassemblage des paquets de l'autre côté.

- ***Niveau 5 : Couche Session***

Cette couche offre les moyens logiciels nécessaires pour l'organisation et la gestion de dialogue entre les applications en gérant des sessions d'échange.

Pour permettre une gestion efficace des sessions, cette couche fournit les moyens nécessaires pour assurer une reprise des sessions en cas de problèmes de coupure de connexion. Cela, en posant des points de resynchronisation et de reprise (pour redémarrer en cas de problème sur un point précis).

- ***Niveau 6 : Couche présentation***

Cette couche s'occupe des questions de la syntaxe et la sémantique (présentation) des informations transportées afin :

- Qu'elles soient compréhensibles par les applications communicantes.

- Que la communication soit optimisée, en compressant les informations transportées.

- De garantir une certaine sécurité, en encryptant les informations transportées (et en les décryptant à leurs réception).

- ***Niveau 7 : Couche application***

Cette couche est considérée comme point de contact entre les processus d'application (qui utilisent les services de communication) et le réseau. Elle fournit les services utilisables directement par les applications comme :

- Le transfert des informations et des fichiers.

- Partages des ressources et la gestion de leurs intégrités et cohérences.

- Le courrier électronique, le travail à distance.

I.6.2 Le modèle de référence TCP/IP

Le modèle TCP/IP (Transmission Control Protocol/Internet Protocol) est également un modèle de référence en couches, mais c'est un modèle à quatre couches. Il est généralement appelé TCP/IP parce que les protocoles de base sont TCP et IP, mais ce ne sont pas les seuls protocoles utilisés dans ce modèle [10].

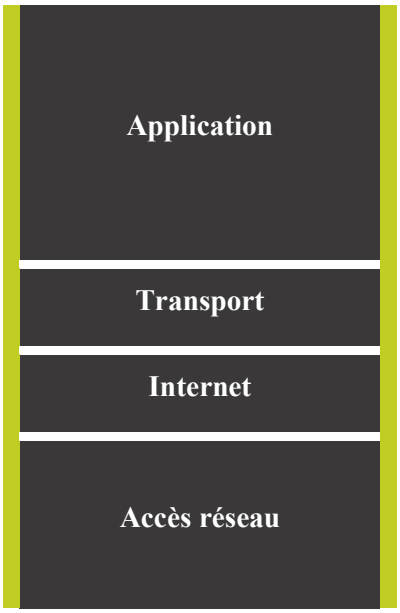


Figure I-10: Modèle TCP/IP.

I.6.3 Comparaison des modèles OSI et TCP/IP

Le modèle TCP/IP et le modèle OSI ont beaucoup de points communs. Tous les deux sont basés sur le concept d'empilement de protocoles indépendants. De plus les différentes couches ont des systèmes de fonctionnement similaires [11].

La figure I-11 illustre la différence entre le modèle TCP/IP et le modèle OSI.

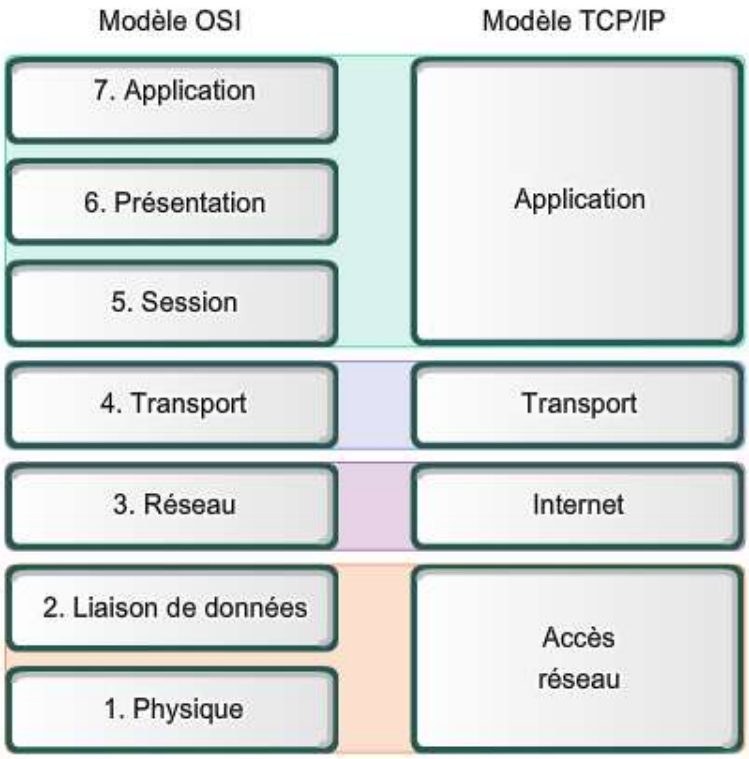


Figure I-11 : Comparaison entre le modèle TCP/IP et le modèle OSI.

I.7 Adresses de communication

I.7.1 Adresses IP

L'utilisation d'adresses IP (Internet Protocol) est le principal moyen permettant aux périphériques de se localiser et d'établir la communication de bout en bout sur Internet. Chaque périphérique final d'un réseau doit être configuré avec une adresse IP [12].

I.7.1.1 *Adresse IPv4*

La structure d'une adresse IPv4 est appelée « notation décimale à point » et est composée de quatre nombres décimaux compris entre 0 et 255. Les adresses IPv4 sont affectées à des périphériques individuels connectés à un réseau [13].

Avec une adresse IPv4, un masque de sous-réseau est également nécessaire. Un masque de sous-réseau IPv4 est une valeur 32 bits qui sépare la partie réseau de l'adresse de la partie hôte. Associé à l'adresse IPv4, le masque de sous-réseau détermine à quel sous-réseau spécifique le périphérique appartient.

L'exemple de la figure I-12 montre l'adresse IPv4 (192.168.1.10), le masque de sous-réseau (255.255.255.0) et la passerelle par défaut (192.168.1.1) attribués à un hôte. L'adresse de passerelle par défaut est l'adresse IP du routeur que l'hôte utilisera pour accéder aux réseaux distants, y compris à Internet.

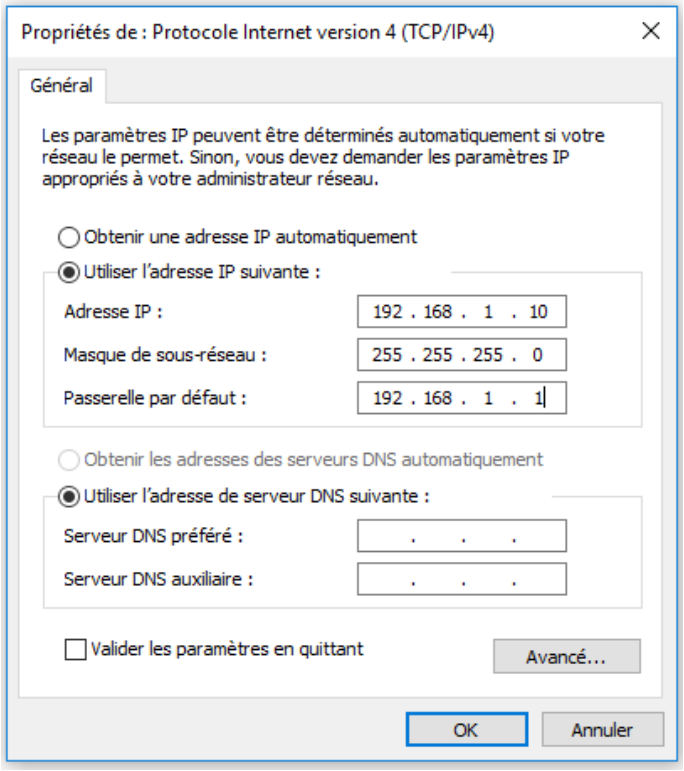


Figure I-12 : Propriété de protocole IPv4.

Les adresses IP peuvent être attribuées aux ports physiques et aux interfaces virtuelles des périphériques. Une interface virtuelle signifie qu'il n'y a aucun matériel physique sur le périphérique qui lui est associé.

I.7.1.2 *Adresse IPv6*

La croissance exponentielle du nombre d'utilisateurs accédant à Internet et des dispositifs liés au web ces dernières années a eu logiquement pour conséquence une

consommation exponentielle d'adresses IP. Un problème sérieux quand on sait que plus de la moitié de celles-ci a déjà été allouée à ce jour (bon nombre d'entre elles n'étant d'ailleurs pas utilisées). Au début des années 90, l'IETF a commencé à se soucier des problèmes liés à l'IPv4 et à chercher une alternative. Cela a conduit au développement de la version 6 du protocole IP (IPv6). L'IPv6 supprime les limites de l'IPv4 et améliore le protocole de façon efficace, grâce à des fonctionnalités qui correspondent mieux aux exigences actuelles et aux futures des réseaux.

Voici les améliorations apportées par l'IPv6 :

- ***Espace d'adressage plus important*** : Les adresses IPv6 sont basées sur un adressage hiérarchique 128 bits (au lieu de 32 bits pour l'IPv4).
- ***Traitement plus efficace des paquets*** : L'en-tête IPv6 a été simplifié et comporte moins de champs.
- ***Traduction d'adresses réseau inutile*** : grâce au grand nombre d'adresses publiques IPv6, la technologie NAT n'est plus nécessaire entre une adresse privée et publique. Cela évite certains des problèmes rencontrés par les applications nécessitant une connectivité de bout en bout.

L'espace d'adressage IPv4 de 32 bits fournit environ 4 294 967 296 adresses uniques. L'espace d'adressage IPv6 fournit 340 un décillions d'adresses (soit environs 340 E+36), ce qui correspond à peu près au nombre de grains de sable sur Terre [14].

I.7.2 Adresse MAC

L'adressage MAC fournit une méthode d'identification des périphériques au niveau inférieur du modèle OSI. Bien qu'Ethernet utilise désormais des cartes réseau et des commutateurs en mode duplex intégral, il reste possible qu'un périphérique reçoive une trame Ethernet alors qu'elle ne lui est pas destinée [15].

La valeur de l'adresse MAC est un résultat direct des règles mises en application par l'IEEE auprès des revendeurs pour garantir l'attribution d'adresses uniques à chaque périphérique Ethernet, et ce, à l'échelle mondiale. Les règles établies par l'IEEE exigent de chaque revendeur de périphérique Ethernet qu'il s'enregistre auprès de l'IEEE. L'IEEE attribue au constructeur un code de 3 octets (24 bits) appelé OUI.

L'IEEE demande aux constructeurs de respecter deux règles simples :

- Toutes les adresses MAC attribuées à une carte réseau ou à un autre périphérique Ethernet doivent utiliser, comme 3 premiers octets, l'identifiant OUI attribué au revendeur correspondant.
- Toutes les adresses MAC ayant le même identifiant OUI doivent utiliser une valeur unique dans les 3 derniers octets.

I.8 Conclusion

Dans ce chapitre nous avons présenté des notions fondamentales sur les réseaux, nous avons commencé par une définition de réseaux, puis nous avons vu les différents types de réseaux en fonction de leur étendu, leur relation entre les composants, leur topologie. Nous avons abordé aussi une vision générale sur les réseaux virtuels. Et nous avons terminé par une petite présentation des modèles de références (OSI et TCP/IP), ses couches, leur rôle, les types de données de chaque couche.

CHAPITRE II: PROTOCOLES DE GESTION DE LIENS

II.1 Introduction

La redondance est très important lors de la conception hiérarchique, car elle permet d'éviter l'interruption des services réseau offerts aux utilisateurs. Pour que la redondance fonctionne de manière systématique, l'utilisation de protocole STP et du protocole EtherChannel est très nécessaire.

Ce chapitre expose les principes fondamentaux et les différents notions et concepts de base des protocoles STP au niveau de la couche 2 (L2) ainsi que ceux du protocole de couche physique (L1) Etherchannel qui permet d'agréger les liaisons sur le plan logique.

II.2 Le protocole spanning tree

II.2.1 Introduction au protocole spanning tree

La redondance du réseau est essentielle pour garantir la fiabilité de celui-ci. La multiplication des liens physiques entre les périphériques offre des chemins d'accès redondants. Le réseau peut ainsi continuer à fonctionner, même lorsqu'un port ou un lien donné est défaillant. Les liens redondants permettent également de partager la charge du trafic et d'accroître la capacité. Les chemins multiples doivent être gérés de manière à ce qu'aucune boucle de couche 2 ne soit créée. Les meilleurs chemins sont déterminés, puis un chemin alternatif est défini en cas de défaillance du chemin principal. Le protocole STP est utilisé pour gérer la redondance au niveau de la couche 2 [16].

II.2.2 Problèmes majors de la redondance des liens

- **Instabilité de la table d'adressage MAC :** Les trames de diffusion sont envoyées à tous les ports de commutation, excepté au port d'entrée initial. Ceci garantit que tous les périphériques d'un domaine de diffusion reçoivent bien les trames. S'il existe plusieurs chemins possibles pour le réacheminement des trames, une boucle sans fin risque de se former. Dans un tel cas, la table d'adresses MAC d'un commutateur peut réagir en changeant constamment pour s'adapter à la mise à jour des trames de diffusion, entraînant une instabilité de la base de données MAC.
- **Tempêtes de diffusion :** Une tempête de diffusion se produit lorsque toute la bande passante disponible est consommée en raison du nombre trop élevé de

trames de diffusion prises dans une boucle de couche 2. Il ne reste alors plus de bande passante pour le trafic légitime et le réseau devient indisponible pour la communication de données. Il s'agit d'un déni de service efficace.

- **Trames de monodiffusion en double :** Les boucles ne concernent pas uniquement les trames de diffusion : lorsque des trames de monodiffusion (unicast) sont envoyées sur un réseau comportant des boucles, des trames en double peuvent parvenir à la destination finale [17].

II.2.3 Définition

Le protocole STP est un protocole réseau de niveau 2 permettant de déterminer une topologie réseau sans boucle (appelée algorithme de l'arbre recouvrant) dans les LANs avec ponts. Il est défini dans la norme IEEE 802.1D et est basé sur un algorithme décrit par Radia Perlman en 1985.

Tous les protocoles STP utilisent un algorithme qui calcule le meilleur chemin sans boucle à travers le réseau et qui sélectionne un pont d'un réseau connecté de manière redondante comme la racine d'un arbre associé à la topologie courante. Le STP assigne des rôles à chaque port selon la fonction du port dans la topologie courante [18].

II.2.4 Fonctionnement du protocole STP

Le STP utilise des BPDUs « Bridge Protocol Data Unit » pour la communication entre les switchs. Les BPDUs sont des trames qui sont échangées régulièrement, à peu près environ toutes les 2 secondes, et permettent aux switchs de garder une trace des changements sur le réseau afin d'activer ou de désactiver les ports des équipements [19].

L'algorithme du STP procède en trois étapes :

a. Élection du commutateur racine :

Une topologie sans boucle ressemble à un arbre et à la base de chaque arbre, on trouve ses racines, qu'on peut appeler « root ».

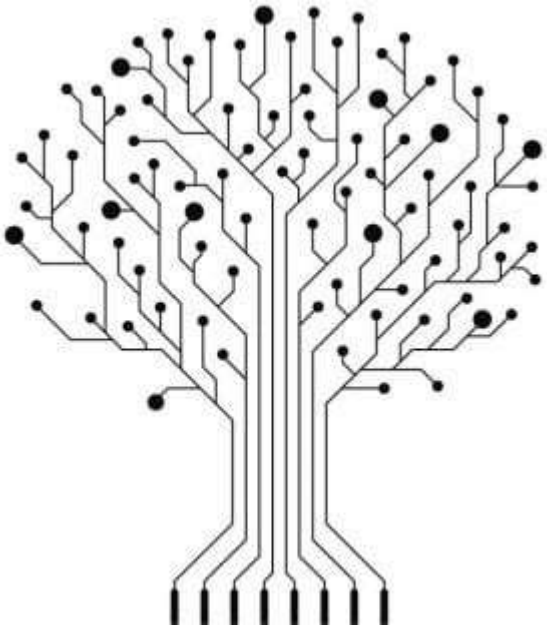


Figure II-1 : Topologie en arbre étendu.

Dans un réseau commuté, le root bridge, qui signifie commutateur racine, est élu. Chaque switch possède une adresse MAC et un numéro de priorité qu'on peut paramétrer. Ces deux nombres forment l'identifiant du pont, plus connu sous le nom de BID identifiant du pont. Le commutateur avec la priorité la plus basse devient le pont racine, et en cas d'égalité, c'est l'adresse MAC la plus basse qui l'emporte.

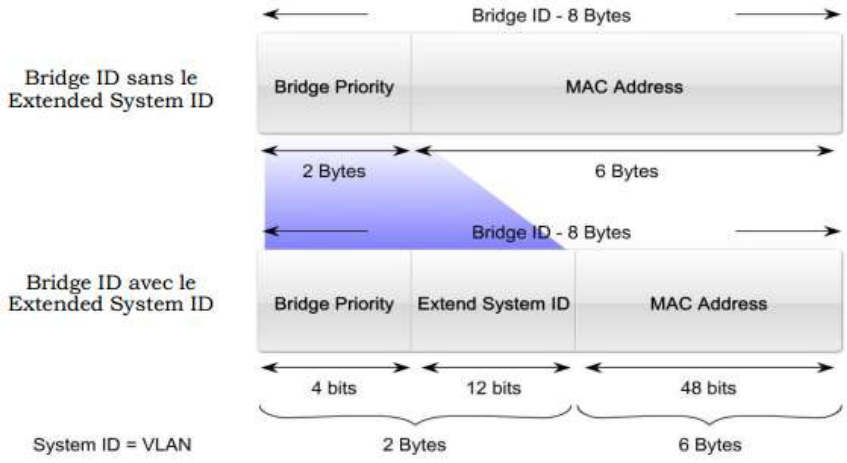


Figure II-2 : Champs BID.

b. Sélection des ports racines :

Cette élection porte sur la distance la plus courte vers le commutateur racine. il se base sur le « cout » de chaque lien traversé. Et la valeur du cout dépend de la bande passante du lien, comme le montre le tableau II-1. Le « port racine » qui est aussi connu sous le nom de root port, sera celui qui mène le plus directement au commutateur racine. Il ne peut y avoir qu'un seul root port par commutateur. En cas d'égalité, c'est-à-dire que deux ports ont le même coût vers le Bridge ID, alors le port ayant le port ID le plus faible qui sera élu.

Vitesse	Coût STP
4 Mbps	250
10 Mbps	100
16 Mbps	62
100 Mbps	19
1 Gbps	4
10 Gbps	2
100 Gbps	1

Tableau II-1 : Couts des liens.

c. Sélection des ports désignés :

Pour chaque segment réseau qui relie des commutateurs, un « port désigné » est sélectionné par le STP. Il s'agit du port relié au segment, qui mène le plus directement à la racine. Ensuite en cas d'égalité sur un segment, et bien la sélection, se fera aussi sur la priorité et la MAC-adresse la plus basse.

d. Blocage des autres ports pour ne pas créer de boucles :

Les ports qui ne sont ni racine, ni désignés sont bloqués. Un port bloqué peut recevoir des paquets BPDU mais ne peut pas en émettre.

Si la topologie change, par exemple un commutateur tombe en panne, l'algorithme du spanning-tree est de nouveau relancé et un nouvel arbre est mis en place.

II.2.5 Mode des ports sur les commutateurs

Lorsqu'il y a une convergence réseau (convergence spanning-tree) donc il y a un changement de topologie, les ports ne vont pas passer directement de l'état blocking vers l'état forwarding il y a des états transitoires. Les ports des commutateurs où STP actif sont dans l'un des états suivants [13] :

- ***Blocking*** **:** Il prend 20 secondes, le port rejette les trames entrantes et accepte les BPDUs mais ne les transmet pas, le port ne complète pas sa table d'adresses MAC.
- ***Listening*** : Il prend 15 secondes, le port jette les trames entrantes et accepte les BPDUs et les retransmets. Le port ne complète pas sa table d'adresses MAC
- ***Learning*** : il prend 15 secondes, le port accepte les trames entrantes mais ne les retransmet pas. Il accepte les BPDUs et les retransmets. Le port incorpore les nouvelles adresses MAC dans sa table.
- ***Forwarding*** : Le port accepte et retransmets les trames entrantes. il accepte les BPDUs et les retransmets. Le port incorpore les nouvelles adresses MAC dans sa table.

REMARQUE. — Lors d'un changement d'état un port restera en « Blocking » pendant 20 secondes afin d'éviter un recalcule de la topologie STP si ce n'est pas nécessaire (Un câble débranché et directement rebranché par exemple).

II.2.6 Rôles des ports :

Pour le protocole STP il y a trois rôles :

- ***Root*** : Il s'agit du port le plus proche (en termes de cout du chemin) du root bridge.
- ***Designated*** : Le port qui transmet les trames sur un segment.
- ***Non designated*** : Le port qui bloque les trames sur un segment.

Pour le protocole RSTP, les deux premiers rôles root et designated sont les mêmes que de STP, au lieu de non designated, il y a deux nouveaux rôles qui sont :

- ***Alternate*** : un port distinct du root port vers le root bridge. Il s'agit du meilleur chemin « alternatif » vers le port bridge, et passe (en cas de changement de défaillance du port root) directement à l'état forwarding.

- ***Backup*** : lors d'une connexion redondante d'un segment vers un autre bridge (deux connexions vers le même domaine de collision) un autre port vers un segment connecté au pont. L'un des ports (selon la priorité) aura comme rôle celui de Backup.

II.2.7 Exemple de STP :

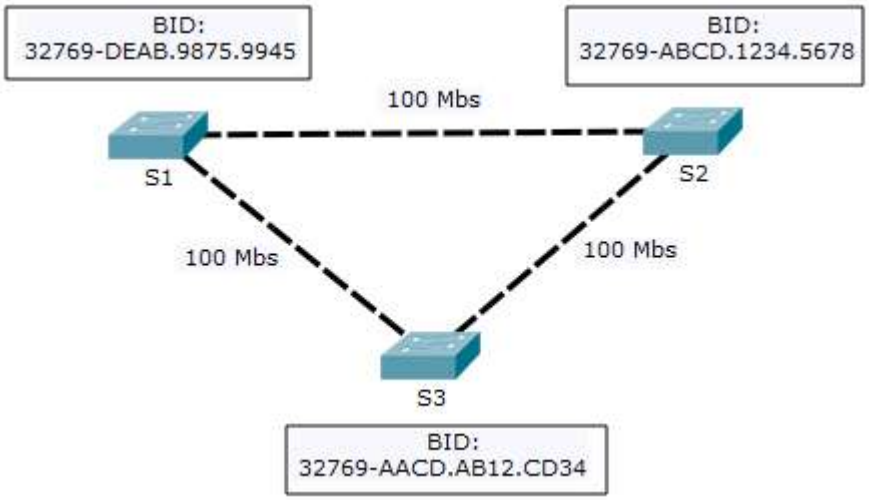


Figure II-3 : Topologie redondante.

L'algorithme du spanning-tree procède en trois étapes :

a. Élection du commutateur racine (root bridge) :

Au moment où le branchement est effectué, il y aura un échange de paquets PBDU parce que le protocole STP est activé par défaut au niveau des switchs CISCO, donc le switch qui a le bridge ID le plus inférieur c'est lui qui va être le root bridge. Donc d'après les BID de l'exemple de la figure II-3, nous remarquons que tous les switchs ont la même priorité 32769 c'est celui qui a l'adresse MAC la plus faible qui va être le root Bridge. Par conséquent le switch S3 va être le root bridge et leurs ports ont le rôle designated, et donc ce commutateur sera le point central de l'arbre STP.

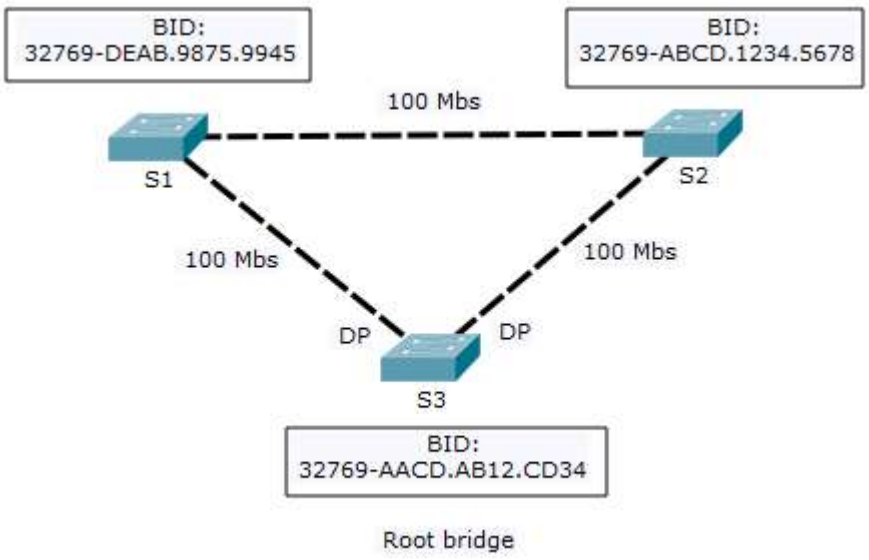


Figure II-4 : Élection du commutateur racine.

b. Sélection des ports racines (root port) :

Les switchs non root bridge sont le switch S1 et le switch S2, on prend le switch S1 et nous allons choisir le meilleur chemin qui mène vers le root bridge, on a deux chemins possible le premier qui est direct et le deuxième chemin en passant par le switch S2, là le choix va se faire par rapport le cout qui est calculé par rapport la bande passante, le cout est 19 pour les trois segments donc dans cet exemple les ports racines sont ceux liés directement au root bridge comme illustre la figure II-5.

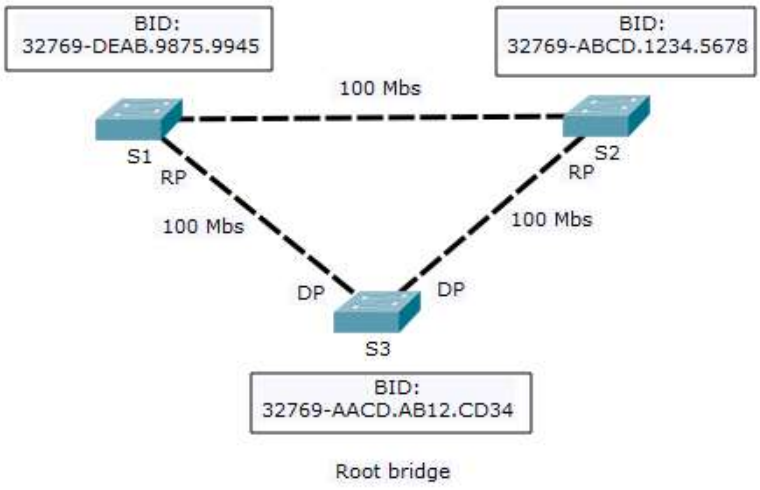


Figure II-5 : Sélection des ports racines.

c. Sélectionner des ports désignés et blocage des autres ports :

Le but est de casser la boucle entre le switch S1 et le switch S2, donc ça va jouer entre les deux autres ports des switchs S1 et S2, donc là nous parlons de la notion de port désigné qui fait passer la donnée et le port non désigné qui bloque la donnée. Donc le choix va se faire premièrement par rapport le chemin du port racine le moins couteux qui mène vers le root bridge et comme les chemins des deux ports racines vers le root bridge sont de même cout on passe au deuxième choix qui se base sur la priorité la plus petite, donc nous allons favoriser le switch S2 ça veut dire nous allons bloquer le port qui est du côté du switch S1 donc le port va être dans le rôle non désigné qui est équivalent à l'état blocking.

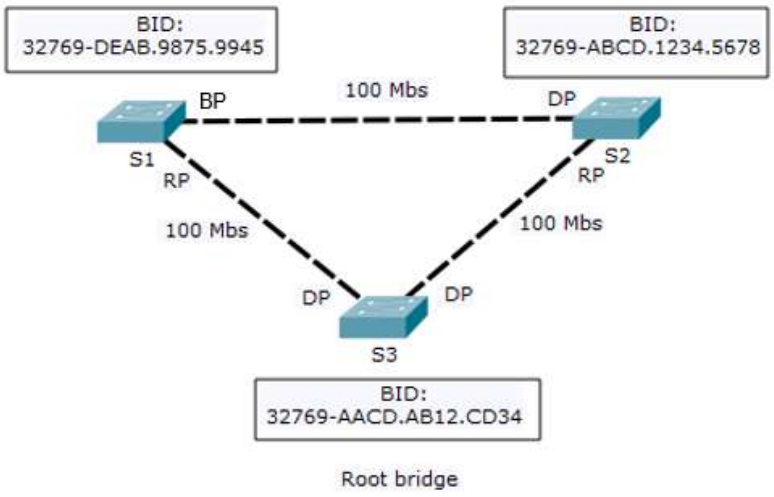


Figure II-6 : Sélection des ports désignés et blocage des autres ports.

II.2.8 Variantes STP

STP s'adapte aux besoins de chaque réseau, il prend donc en charge les variantes suivantes, dont certains appartiennent à Cisco et d'autres sont des normes IEEE [20].

II.2.8.1 *Normes IEEE :*

- RSTP : Introduit la première fois en 1982 comme une évolution de STP, fournit la convergence STP plus rapide après un changement de topologie. RSTP implémente les extensions de STP appartenant à Cisco dans la norme publique. Depuis 2004, l'IEEE intègre RSTP à 802.1D, en identifiant la spécification comme IEEE 802.1D-2004.

- MSTP : Ce protocole/algorithme permet aux trames qui appartiennent à différents VLANs de suivre différents chemins dans le réseau. Le protocole est compatible avec le STP et le RSTP, donc un réseau peut avoir des commutateurs qui communiquent au moyen de ces différents protocoles.

II.2.8.2 ***Propriété Cisco :***

- PVST : Gère une instance de STP pour chaque VLAN configuré sur le réseau. Cela permet à STP sur chaque VLAN d'être configuré indépendamment, offrant de meilleures performances et adaptées aux conditions spécifiques. PVST utilise le protocole ISL permettant à une liaison de jonction d'être trouvé dans l'état de transmission pour certains VLAN et dans l'état de blocage pour d'autres. Pour PVST, Cisco développe plusieurs extensions propriétaires du STP IEEE 802.1D d'origine, comme Back bone Fast, Up link Fast et Port Fast.
- PVST + : Cisco développe PVST + pour prendre en charge les jonctions IEEE 802.1Q. PVST + fournit les mêmes fonctionnalités que PVST, y compris les extensions STP propriétaires Cisco. PVST + n'est pas pris en charge sur les appareils non Cisco et inclut une amélioration de PortFast appelée BPDU Guard.
- PVRST + : Basé sur Norme IEEE 802.1w et a une convergence plus rapide que STP (standard 802.1D). PVRST+ comprend des extensions propriétaires de Cisco.

II.3 Le protocole EtherChannel

II.3.1 Introduction

Il est possible d'augmenter le débit entre deux machines. Pour cela nous pouvons penser à créer un lien double, le souci, c'est qu'en faisant ça, on va créer une boucle de redondance. En effet, si STP est activé alors l'un des liens va être bloqué pour éviter toute redondance. On ne pourra donc pas augmenter le débit entre les périphériques. Une solution très appréciée pour ce problème, c'est l'utilisation de la technologie EtherChannel.

II.3.2 Définition

EtherChannel est une technologie d'agrégation de liens utilisée principalement sur les commutateurs de Cisco. Elle permet d'assembler plusieurs liens physiques Ethernet identiques en un seul lien logique. Toute en évitant que STP bloque une ou plusieurs liaisons [21].

Un lien EtherChannel groupe de 2 à 8 liens actifs de 100 Mbit/s, 1 Gbit/s et 10 Gbit/s, plus éventuellement de 1 à 8 liens inactifs en réserve qui deviennent actifs quand des liens actifs sont coupés. Le but est d'augmenter la vitesse et la tolérance aux pannes entre les commutateurs, les routeurs et les serveurs et de partager la charge entre les liaisons physiques.

II.3.3 Avantages d'EtherChannel

La technologie EtherChannel a initialement été développée par Cisco comme une technique de réseau local entre deux commutateurs permettant de regrouper plusieurs ports Fast Ethernet ou Gigabit Ethernet en un seul canal logique. Quand un EtherChannel est configuré, l'interface virtuelle résultante est appelée un canal de port. Les interfaces physiques sont regroupées dans une interface de canal de port [22].

La technologie EtherChannel présente de nombreux avantages :

- La plupart des tâches de configuration peuvent être réalisées sur l'interface EtherChannel plutôt que sur chaque port, ce qui assure la cohérence de la configuration sur toutes les liaisons.
- Un EtherChannel repose sur les ports de commutation existants. Il n'est pas nécessaire de mettre à niveau la liaison vers une connexion plus rapide et plus coûteuse pour avoir davantage de bande passante.

- L'équilibrage de la charge se fait entre les liaisons appartenant au même EtherChannel. En fonction de la plate-forme matérielle, une ou plusieurs méthodes d'équilibrage de charge peuvent être implémentées. Ces méthodes incluent l'équilibrage de la charge entre les adresses MAC source et de destination ou entre les adresses IP source et de destination, sur les liaisons physiques.
- EtherChannel crée une agrégation considérée comme une seule liaison logique. Quand plusieurs groupes EtherChannel existent entre deux commutateurs, STP peut bloquer l'un des groupes pour éviter les boucles de commutation. Quand STP bloque l'une des liaisons redondantes, cela bloque la totalité de l'EtherChannel et c'est tous les ports appartenant à cette liaison EtherChannel qui sont bloqués. Quand il existe uniquement une liaison EtherChannel, toutes les liaisons physiques d'EtherChannel sont actives, car STP la considère comme une seule liaison (logique).
- EtherChannel offre de la redondance car la liaison globale est considérée comme une seule connexion logique. En outre, la perte d'une liaison physique dans le canal ne génère pas de modification de la topologie ; un recalcule de l'arbre recouvrant n'est donc pas nécessaire. En supposant qu'il existe au moins une liaison physique, l'EtherChannel fonctionne normalement, même si son débit global diminue à cause de la perte d'une liaison dansl'EtherChannel.

II.3.4 Fonctionnement d'EtherChannel

EtherChannel, est une technologie développée par Cisco, peut regrouper jusqu'à huit liaisons à vitesse égale entre deux commutateurs (Figure II-7).

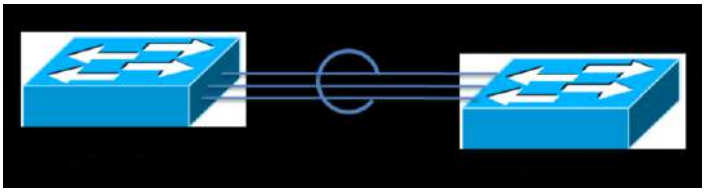


Figure II-7 : Agrégation des liens.

STP considère le faisceau de liens comme une interface unique. Par conséquent, si au moins l'une des liaisons est up, la convergence STP n'a pas besoin de se produire.

Cela permet une meilleure utilisation de la bande passante disponible tout en réduisant le nombre de convergences STP. Sans utiliser EtherChannel ou modifier la configuration STP, STP bloquerait tous les liens redondants sauf un [23].

II.3.5 Les composants de l'EtherChannel

- ***Channel :***Channel détermine le canal logique qui sera créé après avoir configuré l'EtherChannel entre deux équipements en vue d'y transmettre les données.
- ***Groupe :***Groupe suivi d'une valeur numérique détermine l'identifiant du groupe dans lequel feront partie les liens physiques qui seront agrégés.
- ***Mode :***Tel que le mot l'indique, il détermine le mode opératoire sur quoi se base cette technologie pour opérer [24].

II.3.6 Restrictions de mise en œuvre d'EtherChannel :

Il y a quelques remarques à prendre en compte lors de la mise en œuvre d'EtherChannel [25] :

- Les types d'interface, tels que Fast Ethernet et Gigabit Ethernet, ne peuvent être configuré sur le même EtherChannel.
- Chaque EtherChannel peut comporter jusqu'à huit ports Ethernet configurés de manière compatible.
- Le commutateur avec Cisco IOS supporte actuellement jusqu'à six canaux EtherChannels.
- Certains serveurs prennent également en charge EtherChannel lorsqu'ils sont connectés aux commutateurs et ceci afin d'augmenter la bande passante ; cependant, le serveur a besoin d'au moins deux canaux EtherChannel pour assurer la redondance car il peut envoyer du trafic vers un seul commutateur via EtherChannel.
- La configuration de l'EtherChannel doit être cohérente sur les deux commutateurs. La configuration du trunking (VLAN natif, VLAN autorisés, etc.) doit être la même.
- Tous les ports du canal EtherChannel doivent être des ports de couche 2, ou tous les ports du canal EtherChannel doivent être des ports de couche 3.

- EtherChannel fournit une bande passante full-duplex jusqu'à 800 Mb / s (Fast EtherChannel) ou 8 Gb / s (Gigabit EtherChannel).
- EtherChannel peut comporter jusqu'à 16 ports Ethernet compatible-configurés.

II.3.7 Protocoles EtherChannel

On peut configurer EtherChannel comme statique ou inconditionnel ; cependant, on peut également utiliser deux protocoles pour configurer le processus de négociation : protocole d'agrégation de ports (propriétaire PAgP-Cisco) et protocole de contrôle d'agrégation de liens (LACP-IEEE 802.3ad).

Ces deux protocoles garantissent que les deux côtés de la liaison ont des configurations compatibles : même vitesse, même configuration duplex et même informations VLAN. Les modes pour chacun diffèrent légèrement [26].

II.3.7.1 *Protocole d'agrégation des ports PAgP*

II.3.7.1.1 Définition

Le protocole PAgP est un protocole propriétaire de Cisco qui facilite la création automatique de liaisons EtherChannel. Quand une liaison EtherChannel est configurée grâce à PAgP, des paquets PAgP sont envoyés entre les ports compatibles EtherChannel pour négocier la formation d'un canal. Quand PAgP identifie des liaisons Ethernet associées, il groupe les liaisons dans un EtherChannel. L'EtherChannel est ensuite ajouté à l'arbre et est considéré comme port unique [27].

S'il est activé, PAgP gère également l'EtherChannel. Les paquets PAgP sont envoyés toutes les 30 secondes. PAgP vérifie la cohérence de la configuration et gère les ajouts de liaison et les défaillances entre deux commutateurs. Il garantit que tous les ports ont le même type de configuration quand un EtherChannel est créé.

REMARQUE. — Dans un EtherChannel, tous les ports doivent obligatoirement avoir une vitesse, un paramètre de bidirectionnalité et des informations VLAN identiques.

Toute modification d'un port après la création du canal modifie également tous les autres ports du canal. PAgP permet de créer la liaison EtherChannel en détectant la configuration de chaque côté et en assurant la compatibilité des liaisons, afin que la liaison EtherChannel puisse être activée si besoin.

II.3.7.1.2 Mode de PAgP

PAgP utilise les modes suivants :

- *On* : Ce mode force l'interface à établir un canal sans PAgP. Les interfaces configurées en mode On (Activé) n'échangent pas de paquets PAgP.
- *Desirable* : Ce mode PAgP place une interface dans un état de négociation actif, dans lequel l'interface entame des négociations avec d'autres interfaces en envoyant des paquets PAgP.
- *Auto* : Ce mode PAgP place une interface dans un état de négociation passif, dans lequel l'interface répond aux paquets PAgP qu'elle reçoit mais n'entame pas de négociation PAgP.

Par exemple S1 et S2 de la figureII-8 doivent être configurés avec l'une des combinaisons de réglages du tableau II-2.

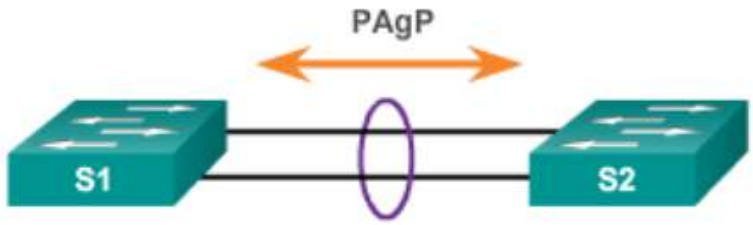


Figure II-8 : Protocole EtherChannel PAgP.

S1	S2	Canal établi ?
On	On	Oui
Auto / Désirable	Désirable	Oui
On / Auto / Désirable	Non configuré	Non
On	Désirable	Non
Auto / On	Auto	Non

Tableau II-2 : Réglage de modes PAgP.

Et les modes doivent être compatibles de chaque côté de telle sorte que :

- Si un côté est configuré pour être en mode Auto, il est placé dans un état passif et attend que l'autre côté entame la négociation EtherChannel.

- Si l'autre côté est également placé en mode Auto, la négociation ne commence jamais et l'EtherChannel ne se forme pas.
- Si tous les modes sont désactivés ou si aucun mode n'est configuré, l'EtherChannel est désactivé.

II.3.7.2 *Protocole de contrôle de l'agrégation des liens LACP*

II.3.7.2.1 Définition

LACP fait partie d'une spécification IEEE (802.3ad) qui permet de regrouper plusieurs ports physiques pour former un seul canal logique. LACP permet à un commutateur de négocier un regroupement automatique en envoyant des paquets LACP à l'homologue. Il assure une fonction semblable à celle de PAgP avec Cisco EtherChannel. LACP étant une norme IEEE, il peut être utilisé pour faciliter l'emploie d'EtherChannel dans des environnements multi fournisseurs. Sur les périphériques Cisco, les deux protocoles sont pris en charge. LACP offre les mêmes avantages en matière de négociation que PAgP. LACP permet de créer la liaison EtherChannel en détectant les configurations de chacun des côtés et en assurant leur compatibilité, afin que la liaison EtherChannel puisse être activée au besoin [16].

II.3.7.2.2 Mode de LACP

LACP utilise les modes suivants :

- *On :* Ce mode force l'interface à établir un canal sans LACP. Les interfaces configurées en mode On (Activé) n'échangent pas de paquets LACP.
- *active :* Ce mode LACP place un port dans un état de négociation actif. Dans cet état, le port entame des négociations avec d'autres ports en envoyant des paquets LACP.
- *passive :* ce mode LACP place un port dans un état de négociation passif. Dans cet état, le port répond aux paquets LACP qu'il reçoit, mais n'entame pas de négociation par paquet LACP.

Tout comme avec PAgP, les modes doivent être compatibles de chaque côté pour que la liaison EtherChannel se forme. Le mode On (Activé) est répété, car il crée la configuration EtherChannel de manière inconditionnelle, sans négociation dynamique PAgP ou LACP.

Par exemple S1 et S2 de la figure II-9 doivent être configurés avec l'une des combinaisons de réglages du tableau II-3.

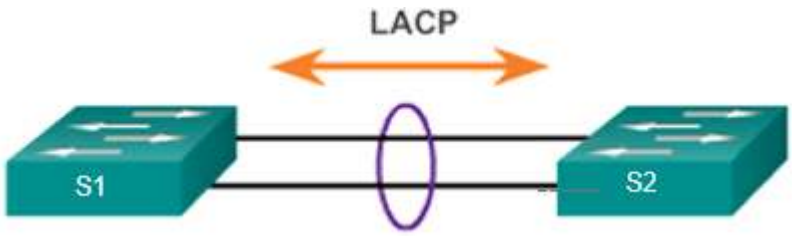


Figure II-9 : Topologie EtherChannel LACP.

S1	S2	Canal établi
On	On	Oui
Active / passive	Active	Oui
On / Active / passive	Non configuré	Non
On	Active	Non
Passive / On	Passive	Non

Tableau II-3: Réglages de mode LACP.

II.3.8 Dépannage de la fonctionnalité EtherChannel

Toutes les interfaces d'un EtherChannel doivent avoir la même configuration en termes de vitesse et utiliser le même mode bidirectionnel, les mêmes VLAN natifs et autorisés sur les trunks, et le même VLAN d'accès sur les ports d'accès [26] :

- Attribuez tous les ports du EtherChannel au même VLAN, ou configurez-les en tant que trunks. Des ports avec des VLAN natifs différents ne peuvent pas former un EtherChannel.
- Lorsque vous configurez un EtherChannel à partir de ports trunk, vérifiez que le mode trunking est le même sur tous les trunks. Des modes trunk incohérents sur des ports EtherChannel peuvent empêcher le fonctionnement d'EtherChannel et entraîner la désactivation des ports (état de désactivation des erreurs).
- Un EtherChannel prend en charge la même plage autorisée de VLAN sur tous les ports. Si la plage autorisée de VLAN n'est pas identique, les ports ne forment pas un EtherChannel**.**
- Des options de négociation dynamique pour PAgP et LACP doivent être configurées pour être compatibles aux deux extrémités de l'EtherChannel.

II.4 Conclusion

Dans ce chapitre, nous avons présenté en premier lieu les problèmes associés à un réseau redondant de couche 2. Comme solution, nous avons proposé l'utilisation du protocole STP de couche 2 qui garantit qu'il n'existe qu'un seul chemin logique entre toutes les destinations d'un réseau, en bloquant volontairement les chemins d'accès redondants pouvant générer une boucle.

Le protocole STP utilise les BPDUs pour élire le commutateur root et le port root pour le réseau commuté, aussi bien que le port root et le port désigné pour chaque segment commuté. Les différentes variantes STP ont été aussi abordées.

Nous avons également donné la solution au problème de redondance des liens multipliés entre deux commutateurs qui consiste à implémenter une configuration EtherChannel comme statique ou inconditionnel en utilisant deux protocoles pour configurer le processus de négociation : protocole d'agrégation de ports (propriétaire PAgP-Cisco) et protocole de contrôle d'agrégation de liens (LACP-IEEE 802.3ad).

CHAPITRE III: CONFIGURATION ET SIMULATION

III.1 Introduction

Après avoir détaillé les protocoles de gestion de liens STP et EtherChannel dédiées aux problèmes de redondance de liens entre les commutateurs dans le chapitre précédent, nous avons consacré ce chapitre aux configurations et simulation de l'EtherChannel.

Ce chapitre a pour but de vérifier le comportement de protocole de l'EtherChannel par rapport au protocole STP lorsque nous regroupons des liens redondants entre les commutateurs à l'aide de protocole EtherChannel. Nous commençons par une description globale du logiciel de conception Cisco Packet Tracer. Ensuite, nous configurons l'EtherChannel à l'aide du simulateur Cisco Packet Tracer.

III.2 Présentation du simulateur « Cisco Packet Tarcer »

III.2.1 Définition

Packet Tracer est un environnement d'apprentissage basé sur la simulation, destiné pour concevoir, configurer et dépanner des réseaux informatiques. Packet Tracer est un environnement intégré de simulation, de visualisation, de collaboration et d'évaluation. Comme toute simulation, Packet Tracer s'appuie sur un modèle simplifié de périphériques et de protocoles réseau [27].

III.2.2 Présentation de l'interface

Lorsque nous ouvrons Packet Tracer, l'interface par défaut est affichée :

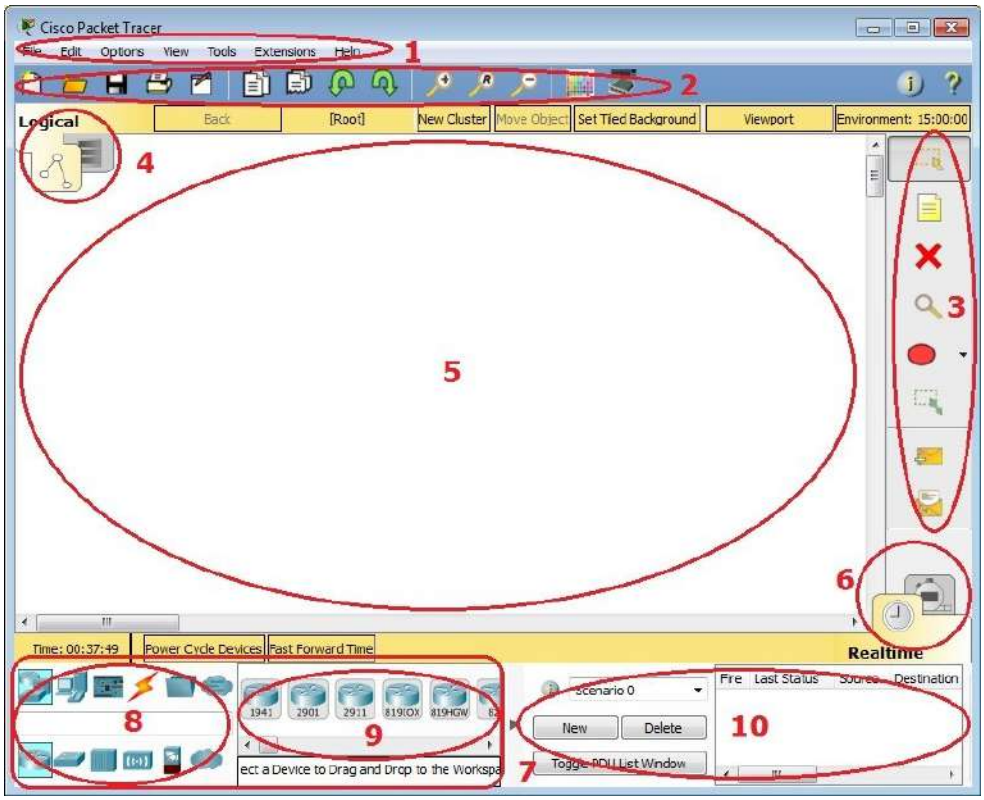


Figure III-1 : Interface de Packet Tracer.

Cette interface initiale contient dix composants :

1. ***Menu Bar***

Cette barre fournit les menus Fichier, Modifier, Options, Affichage, Outils, Extensions et Aide ou nous trouverons également des commandes de base telles qu'Ouvrir, Enregistrer, Enregistrer sous Pkz, Imprimer et Paramètres et préférences dans ces menus. Nous pouvons également accéder à l'assistant d'activité à partir du menu Extensions.

2. ***Main Tool Bar***

Cette barre fournit des icônes de raccourci vers les commandes de menu Fichier et Modifier. Cette barre contient également des opérations telles que Copier, Coller, Annuler, Rétablir, Zoom, la palette de dessin et la boîte de dialogue périphériques personnalisés. Sur la droite, nous trouverons également : Informations sur le réseau, que nous pouvons utiliser pour entrer une description du réseau actuel (ou tout texte que nous souhaitons inclure).

3. *Common Tools Bar*

Cette barre donne accès à ces outils d'espace de travail couramment utilisés : sélectionner, déplacer la disposition, placer une note, supprimer, inspecter, redimensionner la forme, ajouter une PDU simple et ajouter une PDU complexe.

4. *Logical/Physical Workspace and Navigation Bar*

Nous pouvons basculer entre l'espace de travail physique et l'espace de travail logique avec les onglets de cette barre. Dans Logical Workspace, cette barre permet également de revenir à un niveau précédent dans un cluster, de créer un nouveau cluster, de déplacer l'objet, de définir l'arrière-plan en mosaïque et de la fenêtre d'affichage. Dans l'espace de travail physique, cette barre permet de naviguer dans des emplacements physiques, de créer une nouvelle ville, de créer un nouveau bâtiment, de créer un nouveau placard, de déplacer un objet, d'appliquer une grille à l'arrière-plan, de définir l'arrière-plan et d'accéder au placard de travail.

5. *Workspace*

Cette zone est l'endroit où nous pouvons créer notre réseau, regarder des simulations et afficher de nombreux types d'informations et de statistiques.

6. *Realtime/Simulation Bar*

Nous pouvons basculer entre le mode temps réel et le mode simulation avec les onglets de cette barre. Cette barre fournit également des boutons pour les appareils Power Cycle et Fast Forward Time ainsi que les boutons Play Control et le bouton bascule Event List en mode Simulation. En outre, il contient une horloge qui affiche l'heure relative en mode temps réel et en mode simulation.

7. *Network Component Box*

C’est l'endroit où nous pouvons choisir les périphériques et les connexions à placer dans l'espace de travail. Il contient la boîte de sélection du type d'appareil et la boîte de sélection spécifique à l'appareil. Il y a un champ consultable qui permet d'entrer un nom d'appareil pour rechercher rapidement cet appareil spécifique. Le nom du périphérique s'affiche lorsqu’on passe la souris sur l'icône du périphérique dans la zone spécifique au périphérique.

8. *Device-Type Selection Box*

C'est là où nous sélectionnons les types de périphériques et de connexions disponibles dans Packet Tracer. La boîte de sélection spécifique à l'appareil change en fonction du type d'appareil que nous choisirons.

9. *Device-Specific Selection Box*

Cette case nous permettra de choisir les appareils que nous souhaiterons mettre dans le réseau et les connexions à établir. Dans cette boîte, nous trouverons des appareils qui étaient peut-être déjà obsolètes. Nous avons la possibilité de masquer les équipements hérités dans la fenêtre Préférences sous Options.

10. *User Created Packet Window*

Cette fenêtre gère les paquets qu'on met dans le réseau lors des scénarios de simulation. Nous pouvons masquer complètement la fenêtre de paquet créé par l'utilisateur (UCPW) en cliquant sur le bouton développer / réduire. Nous pouvons également redimensionner librement UCPW en plaçant le curseur près du bord gauche de la fenêtre, puis en faisant glisser le curseur vers la gauche ou la droite.

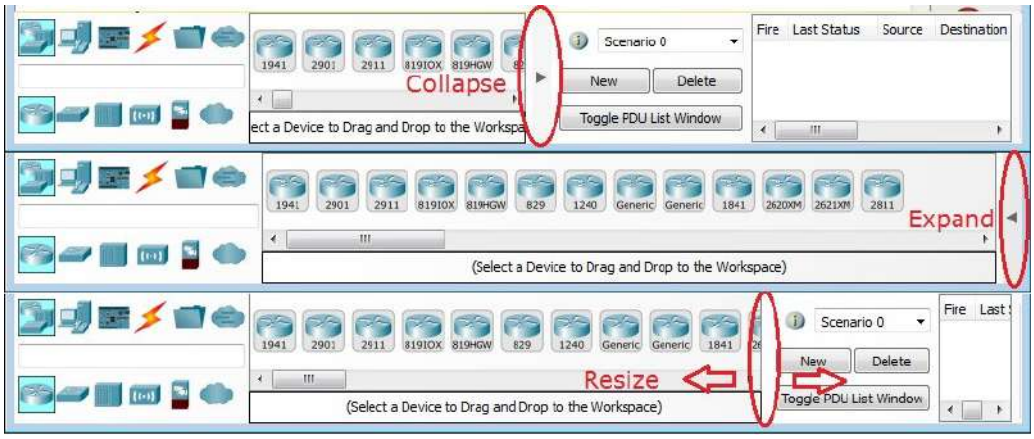


Figure III-2 : La fenêtre de paquet créé par l'utilisateur (UCPW).

III.2.3 Modes de fonctionnement

Mode temps réel

Le réseau s'exécute dans un modèle en temps réel, dans les limites des modèles de protocole utilisés. Le réseau répond immédiatement aux actions comme il le ferait dans un appareil réel. Par exemple, dès que nous établirons une connexion Ethernet, les voyants de liaison pour cette connexion apparaissent, montrant l'état de la connexion. Chaque fois que nous tapons une commande dans la CLI (telle que ping ou show), le résultat ou la réponse est généré en temps réel et nous le verrons comme tel. Toute l'activité du réseau, en particulier le flux de PDU à travers le réseau, se produit dans le modèle Packet Tracer en temps réel.

Mode Simulation

Nous pouvons "figer" le temps : Nous avons un contrôle direct sur le temps lié au flux des PDU. Nous pouvons voir le réseau fonctionner étape par étape ou événement par événement, aussi rapidement ou lentement que nous le souhaitons. Nous pouvons configurer des scénarios, tels que l'envoi d'un paquet ping d'un appareil à un autre. Lorsque nous capturons la simulation, nous verrons des représentations graphiques des paquets voyageant d'un appareil à un autre. Nous pouvons suspendre la simulation, ou avancer ou reculer dans le temps, en étudiant de nombreux types d'informations sur des PDU et des périphériques spécifiques à des moments spécifiques. D'autres aspects du réseau fonctionnant en temps réel est observable en mode simulation par exemple, si nous désactivons un port, son voyant de liaison répondra immédiatement en devenant rouge.

III.2.4 Connexions / Liens

Packet Tracer prend en charge une large gamme de connexions réseau. Chaque type de câble ne peut être connecté qu'à certains types d'interface.

- **Console**



Des connexions de console peuvent être établies entre les PC et les routeurs ou commutateurs. Certaines conditions doivent être remplies pour que la session console du PC fonctionne : la vitesse des deux côtés de la connexion doit être la même, les bits de données doivent être 7 pour les deux ou 8 pour les deux, la parité doit être la même, l'arrêt les bits doivent être 1 ou 2 (mais ils ne doivent pas nécessairement être les mêmes), et le contrôle de flux peut être n'importe quoi pour chaque côté.

❖ **Copper Straight-through**



Ce type de câble est le support Ethernet standard pour la connexion entre des périphériques fonctionnant sur différentes couches OSI (tels que concentrateur vers routeur, commutateur vers PC et routeur vers concentrateur). Il peut être connecté aux types de ports suivants : 10 Mbps cuivre (Ethernet), 100 Mbps cuivre (Fast Ethernet) et 1000 Mbps cuivre (Gigabit Ethernet).

❖ **Copper Cross-over**



Ce type de câble est le support Ethernet pour la connexion entre les périphériques qui fonctionnent sur la même couche OSI (tels que concentrateur à concentrateur, PC à PC, PC à imprimante). Il peut être connecté aux types de ports suivants : 10 Mbps cuivre (Ethernet), 100 Mbps cuivre (Fast Ethernet) et 1000 Mbps cuivre (Gigabit Ethernet).

❖ **Fiber**



Le média fibre est utilisé pour établir des connexions entre les ports fibre (100 Mbps ou 1000 Mbps).

❖ **Phone**



Les connexions de ligne téléphonique ne peuvent être établies qu'entre des appareils dotés de ports modem. L'application standard pour les connexions par modem est un périphérique final (tel qu'un PC) qui se connecte à un cloud réseau.

❖ **Coaxial**



Un support coaxial est utilisé pour établir des connexions entre des ports coaxiaux tels qu'un modem câble connecté à un Packet Tracer Cloud.

❖ **Serial DCE and DTE**



Les connexions séries, souvent utilisées pour les liaisons WAN, doivent être connectées entre les ports série. Notez que nous devons activer la synchronisation du côté DCE pour afficher le protocole de ligne. La synchronisation DTE est facultative. Vous pouvez dire à quelle extrémité de la connexion se trouve le côté DCE par la petite icône "horloge" à côté du port. Si vous choisissez le type de connexion Serial DCE, puis connectez deux appareils, le premier appareil sera du côté DCE et le deuxième appareil sera automatiquement réglé du côté DTE. L'inverse est vrai si nous choisissons le type de connexion Serial DTE.

❖ **Octal**



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

❖ **IoE Custom Cable**



Un câble pour connecter des objets, des composants, des microcontrôleurs (MCU-PT) et des ordinateurs à carte unique (SBC-PT). Le câble regroupe les fils de masse, d'alimentation et de données.

❖ **USB**



Câble USB utilisé pour connecter des objets, des composants, des microcontrôleurs (MCU-PT) et des ordinateurs à carte unique (SBC-PT) en tant que connexion de données.

III.2.5 Statut du lien

Lorsque nous connectons deux appareils, nous verrons généralement des voyants de liaison aux deux extrémités de la connexion. Certaines connexions n'ont pas de voyants de liaison.

- ***Vert clair*** **:**Le lien physique est en place. Cependant, cela n'indique pas l'état du protocole de ligne sur la liaison.
- ***Vert clignotant*** **:** Il y a une activité de lien.
- ***Rouge*** : Le lien physique est en panne. Il ne détecte aucun signal.
- ***Ambre*** : Le port est dans un état de blocage en raison de STP. Cela n'apparaît que sur les commutateurs.
- ***Noir*** : Il est utilisé uniquement par les connexions de console. La couleur noire indique que le câble de la console est connecté au bon port.

III.3 Système d'exploitation réseau Cisco IOS

Tout comme un PC, un commutateur ou un routeur, nécessite un système d'exploitation pour prendre en charge le matériel. L'IOS Cisco est le système d'exploitation réseau qui se trouve sur la plupart des équipements Cisco.

L'utilisateur accède à l'interpréteur de commandes à l'aide d'une interface en ligne de commande (CLI) ou d'une interface utilisateur graphique. Cependant, les interfaces utilisateur graphiques ne disposent pas toujours de toutes les fonctionnalités disponibles dans la CLI. Elles peuvent également tomber en panne ou simplement ne pas fonctionner correctement. C'est pourquoi l'accès aux périphériques réseau se fait habituellement via une CLI. La CLI demande moins de ressources et offre une grande stabilité par rapport à une interface utilisateur graphique.

Lorsque l'utilisateur utilise une interface en ligne de commande, il accède directement au système dans un environnement textuel, en entrant des commandes au clavier dans une invite de commandes.

III.3.1 Méthodes d'accès à la CLI

Il existe plusieurs moyens d'accéder à l'environnement CLI et de configurer le périphérique. Voici les méthodes les plus répandues :

- **Console** : il s'agit d'un port de gestion permettant un accès hors réseau à un périphérique Cisco.
- **SSH** : moyen d'établir à distance une connexion CLI sécurisée via une interface virtuelle sur un réseau.
- **Telnet** : moyen non sécurisé d'établir une session CLI à distance via une interface virtuelle sur un réseau.

III.3.2 Programmes d'émulation de terminal

Il existe d'excellents programmes d'émulation de terminal permettant de se connecter à un périphérique réseau via une connexion série sur un port de console ou via une connexion SSH ou Telnet. Voici quelques exemples :

- PuTTY
- Tera Term
- Secure CRT
- Terminal OS X

III.3.3 Principaux modes de commande

Par mesure de sécurité, le logiciel Cisco IOS sépare l'accès à la gestion en deux modes de commande :

- **Mode d'exécution utilisateur** : Permets d'accéder à un nombre limité de commandes. Il se reconnaît à l'invite qui se termine par le symbole >.
- **Mode d'exécution privilégié** : Permets d'accéder à toutes les commandes de configuration de l'appareil. Le mode d'exécution privilégié se reconnaît à l'invite qui se termine par le symbole #.

Différentes commandes sont utilisées pour entrer et sortir des invites de commandes. Pour passer du mode utilisateur au mode privilégié, on utilise la commande **enable**. On utilise

la commande **disable** du mode d'exécution privilégié pour retourner au mode d'exécution utilisateur.

REMARQUE. — le mode d'exécution privilégié est parfois appelé *mode actif*.

Pour passer en mode de configuration globale et le quitter, on utilise la commande de mode d'exécution privilégié **configure terminal**. Pour repasser en mode d'exécution privilégié, on tape la commande de mode de config. globale **exit**.

Il existe de nombreux sous-modes de configuration différents. Par exemple, pour passer en sous-mode de configuration de ligne, on utilise la commande **line** suivie du type et du numéro de la ligne de gestion à laquelle on souhaite accéder. Pour quitter un sous-mode de configuration et retourner au mode de configuration globale, on utilise la commande **exit**.

Pour passer de n'importe quel sous-mode de configuration du mode de configuration globale au mode situé un niveau plus haut dans la hiérarchie des modes, on saisit la commande **exit**.

Pour passer de n'importe quel sous-mode de configuration au mode d'exécution privilégié, on utilise la commande **end** ou on utilise la combinaison de touches **Ctrl+Z**.

III.3.4 Touches d'accès rapides et raccourcis

Dans l'interface CLI de Cisco IOS, des touches d'accès rapide et des raccourcis facilitent la configuration, la surveillance et le dépannage.

Il est possible de raccourcir les commandes et les mots-clés jusqu'au nombre minimal de caractères qui identifient une sélection unique. Par exemple, on peut raccourcir la commande **configure** en entrant **conf** parce que **configure** est la seule commande qui commence par **conf**. Par contre, la version raccourcie **con** ne fonctionne pas parce que plusieurs commandes débutent par **con**. On peut aussi raccourcir les mots clés.

1. **La touche Tabulation :** permet de compléter automatiquement une commande ou un mot-clé. Ce qui est très utile.
2. **CTRL-A :** amène le curseur au début de la ligne.
3. **CTRL-E** : amène le curseur à la fin de la ligne.
4. **CTRL-C** : annule la commande en cours de taper et quitte le mode de configuration.
5. **CTRL-Z** : met fin au mode de configuration.

III.4 Configuration du protocole EtherChannel :

Nous allons configurer l'EtheChannel avec les trois modes que nous avons vu dans la partie théorique PAgP, LACP et le mode ON. Pour cela nous allons prendre l'architecture de la figure III-3 dans laquelle nous disposons de trois switchs Cisco 2960-24TT reliés entre eux à l'aide de deux câbles Ethernet croisés (deux à deux), chaque commutateur connecté à un ordinateur PC par le biais d'un câble Ethernet droit.

Les connexions physiques sont comme suit :

- Switch S1 FastEthernet 0/1 connecté sur le Switch S2 FastEthernet 0/1.
- Switch S1 FastEthernet 0/2 connecté sur le Switch S2 FastEthernet 0/2.
- Switch S1 FastEthernet 0/3connecté sur le Switch S3FastEthernet 0/3.
- Switch S1 FastEthernet 0/4connecté sur le Switch S3FastEthernet 0/4.
- Switch S2FastEthernet 0/3connecté sur le Switch S3FastEthernet 0/1.
- Switch S2FastEthernet 0/4connecté sur le Switch S2 FastEthernet 0/2.
- Switch S1 FastEthernet 0/6connecté sur le PC-A FastEthernet 0.
- Switch S2FastEthernet 0/18connecté sur le PC-B FastEthernet 0.
- Switch S3FastEthernet 0/18connecté sur le PC-C FastEthernet 0.

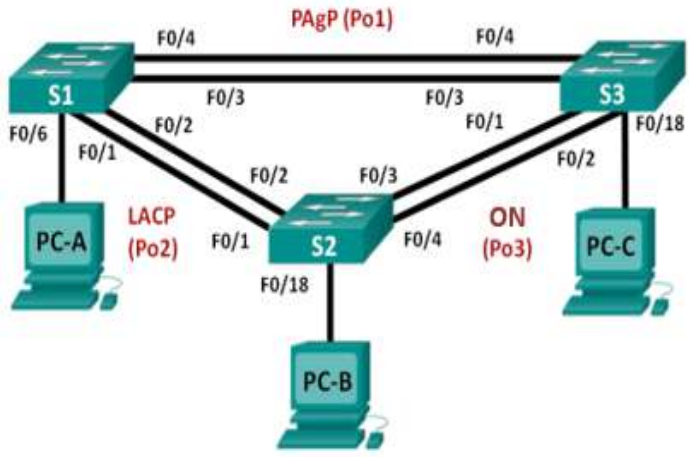


Figure III-3 : Topologie.

Nous attribuons les adresses IP de la table d'adressage (Tableau III-1) aux périphériques :

Périphérique	Interface	Adresse IP	Masque de sous-réseau
S1	VLAN 99	192.168.99.11	255.255.255.0
S2	VLAN 99	192.168.99.12	255.255.255.0
S3	VLAN 99	192.168.99.13	255.255.255.0
PC-A	NIC	192.168.10.1	255.255.255.0
PC-B	NIC	192.168.10.2	255.255.255.0
PC-C	NIC	192.168.10.3	255.255.255.0

Tableau III-1 : Table d'adressages.

Pour bien atteindre nos objectifs nous avons opté pour le plan suivant :

Partie 1 : configuration des paramètres de base du commutateur

Partie 2 : Configurer PAgP

Partie 3 : Configurer LACP

Partie 4 : Configurer ON

III.4.1 Partie 1 : Configuration des paramètres de base du commutateur

Dans la Partie 1, nous allons configurer la topologie du réseau et les paramètres de base, tels que les adresses IP de l'interface, le routage statique, l'accès des périphériques et les mots de passe.

Étape 1 : Câblage de réseau conformément à la topologie

Nous fixons les périphériques conformément au schéma de topologie, ainsi que les câbles.

Pour afficher les connexions disponibles, nous cliquons sur l'icône en forme d'éclair orange situé sur le coin inférieur gauche de la fenêtre.

Nous choisissons le câble adéquat pour relier les ports : entre les commutateurs nous utilisons deux connexions par câbles croisés en cuivre, et entre les commutateurs et les

ordinateurs nous utilisons une connexion par câble droit en cuivre. Lorsque nous branchons le câble adéquat, les voyants de liaison de ce dernier s'allument.

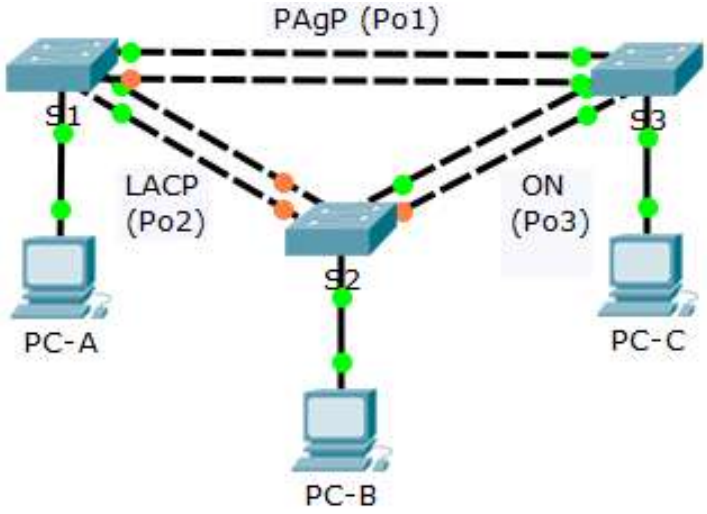


Figure III-4 : Câblage du réseau.

Étape 2 : Initialisation et redémarrage des commutateurs

```
Switch>en
Switch#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Switch#reload
Proceed with reload? [confirm]

Switch#delete vlan.dat
Delete filename [vlan.dat]?
Delete flash:/vlan.dat? [confirm]
```

Figure III-5 : Initialisation et redémarrage des commutateurs.

Étape 3 : Configuration des paramètres de base pour chaque commutateur

Nous désactivons la recherche DNS :

```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#no ip domain-lookup
```

Figure III-6 : Désactivation de la recherche DNS**.**

Nous configurons le nom du périphérique conformément à la topologie :

```
Switch(config)#hostname S1
S1(config)#
```

Figure III-7 : Configuration de nom du périphérique.

Nous désactivons tous les ports de commutation excepté les ports connectés à des PC :

Il est recommandé de commencer par désactiver ces interfaces, de sorte qu'aucune configuration incomplète n'entraîne d'activité sur la liaison.

```
S1(config)#int range fa0/1-5 , fa0/7-24 , g0/1-2
S1(config-if-range)#shutdown
```

Figure III-8 : Désactivons de tous les ports exceptés celles connectés à des PC.

Nous configurons le VLAN 99 :

```
S1(config)#vlan 99
S1(config-vlan)#name Management
S1(config-vlan)#exit
```

Figure III-9 : Configuration de VLAN 99.

Nous configurons le VLAN 10 :

```
S1(config)#vlan 10
S1(config-vlan)#name Staff
S1(config-vlan)#exit
```

Figure III-10 : Configuration de VLAN 10.

Nous configurons les ports de commutation avec des hôtes connectés en tant que ports d'accès au VLAN 10 :

```
S1(config)#int f0/6
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 10
S1(config-if)#exit
```

Figure III-11 : Configuration de port f0/6 en tant que ports d'accès au VLAN 10.

Nous attribuons les adresses IP conformément à la table d'adressage :

```
S1(config)#int vlan 99
S1(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up

S1(config-if)#ip address 192.168.99.11 255.255.255.0
S1(config-if)#no shut
```

Figure III-12 : Configuration des adresses IP.

Nous copions la configuration en cours en tant que configuration de démarrage :

```
S1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Figure III-13 : Enregistrement de la configuration.

REMARQUE. — Nous répétons les étapes 2 et 3 pour les autres commutateurs S2 et S3.

Étape 4 : Configuration des ordinateurs

Nous attribuons les adresses IP aux PC conformément à la table d'adressage.

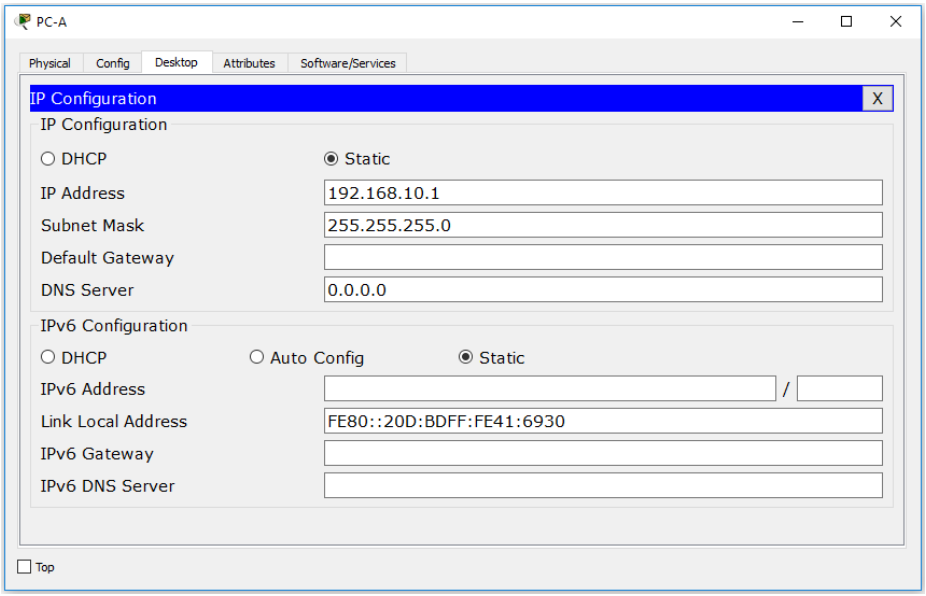


Figure III-14 : Configuration d'adresse IP.

REMARQUE. — Nous faisons la même chose pour PC-B et PC-C.

III.4.2 Partie 2 : Configuration de PAgP

Dans la Partie 2, nous allons configurer un lien entre S1 et S3 à l'aide de PAgP.

Étape 1 : Configurons PAgP sur S1 et S3

Pour un lien entre S1 et S3, nous allons configurer les ports sur S1 avec le mode PAgP désirable (PAgP souhaitable) et les ports sur S3 avec le mode PAgP auto. Nous allons activer les ports après avoir configuré les modes PAgP.

La commande c'est d'entrer en mode de configuration au niveau des deux interfaces F0/3 et F0/4 que nous voulons regrouper donc nous tapons la commande channel-group

```
S1(config)#int range f0/3-4
S1(config-if-range)#channel-group 1 mode desirable
S1(config-if-range)#
Creating a port-channel interface Port-channel 1

S1(config-if-range)#no shut
```

Figure III-15 : Configuration des ports sur S1 avec le mode PAgP desirable.

Sur le deuxième commutateur, nous ajoutons les ports F0/3 et F0/4 au Port Channel 1 à l'aide de la commande channel-group 1 mode auto :

```
S3(config)#int range f0/3-4
S3(config-if-range)#channel-group 1 mode auto
S3(config-if-range)#
Creating a port-channel interface Port-channel 1

S3(config-if-range)#no shut
```

Figure III-16 : Configuration des ports sur S3 avec le mode PAgP auto.

Nous pouvons voir le lien entre S1 et S3 a changé la couleur de l'ambre au vert comme elle montre la figureIII-17.

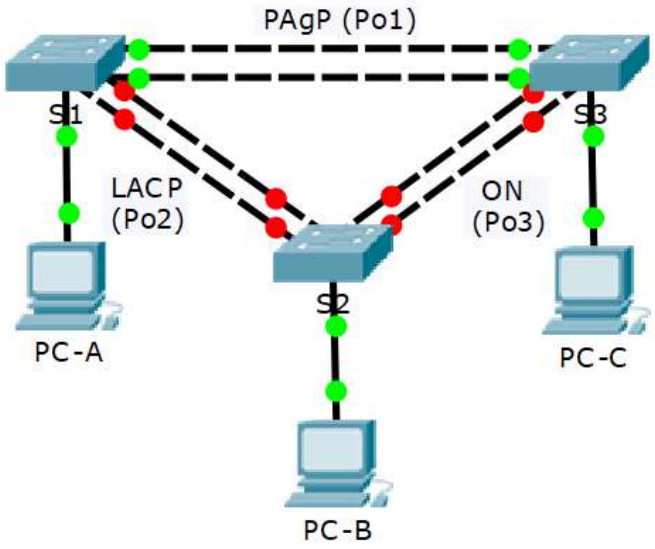


Figure III-17 : Topologie du réseau après avoir configuré PAgP sur S1 et S3.

Les deux ports Fa0/3 et Fa0/4 deviennent une seule interface qui est le canal de port Po1

Étape 2 : Examinons la configuration sur les ports.

Actuellement, les interfaces F0/3, F0/4 et Po1 (Port-channel 1) sur S1 et S3 sont en mode Access operational (Accès opérationnel) avec le mode Administrative (Administratif) configuré sur Dynamic auto (Dynamique automatique). Nous vérifions la configuration en utilisant la commandes **show running-config** Les résultats de l'exemple de configuration pour F0/3sur S1 sont les suivants :

```
S1#show running-config
Building configuration...
interface FastEthernet0/3
 channel-group 1 mode desirable
!
interface FastEthernet0/4
 channel-group 1 mode desirable
```

Figure III-18 : Vérification de la configuration sur les ports.

Étape 3 : S'assurer que les ports ont été agrégés.

Nous pouvons vérifier que les interfaces f0/3 et f0/4 sur chaque commutateur appartiennent au Po1 dans le mode PAgP souhaité pour S1 et dans le mode PAgP

automatique pour S3, et qui sont configurés en tant que jonctions affectées au VLAN 99 natif. Pour vérifier que les ports ont été correctement ajoutés au Po1, nous utilisons la commande **show etherchannel summary** sur les commutateurs S1 et S3 comme indiqué dans les figures III-19 et III-20.

```
S1#show etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-------------------------

1      Po1(SD)           PAgP   Fa0/3(P) Fa0/4(P)
```

Figure III-19 : Vérification du port-channel 1 en S1

```
S3#show etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-------------------------

1      Po1(SD)           PAgP   Fa0/3(P) Fa0/4(P)
```

Figure III-20 : Vérification du port-channel 1 sur S3

Le drapeau '**P**' indique que les ports sont regroupés dans un canal de port.

Le drapeau '**S**' indique que le canal est une couche 2.

Le drapeau '**U**' signifie que le canal est en place et en cours d'utilisation.

Étape 4 : Configuration des ports trunk.

Une fois les ports agrégés, les commandes appliquées sur l'interface du canal de port affectent tous les liens qui ont été regroupés. Nous devons configurer manuellement les ports Po1 sur S1 et S3 en tant que ports trunk et attribuer-les au VLAN 99 natif.

```
S1(config)#int port-channel 1
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 99

S3(config)#int port-channel 1
S3(config-if)#switchport mode trunk
S3(config-if)#switchport trunk native vlan 99
```

Figure III-21 : Configuration des ports trunks.

Étape 5 : Vérification que les ports sont configurés en tant que ports trunk :

Nous exécutons la commande ***show interfaces trunk*** sur S1 et S3 pour savoir quel port trunk est répertorié et Quel est le VLAN natif

```
S1#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Po1         on           802.1q         trunking      99

Port        Vlans allowed on trunk
Po1         1-1005

Port        Vlans allowed and active in management domain
Po1         1,10,99

Port        Vlans in spanning tree forwarding state and not pruned
Po1         1,10,99


S3#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Po1         on           802.1q         trunking      99

Port        Vlans allowed on trunk
Po1         1-1005

Port        Vlans allowed and active in management domain
Po1         1,10,99

Port        Vlans in spanning tree forwarding state and not pruned
Po1         1,10,99
```

Figure III-22 : Vérification du port-trunk et VLAN natif.

III.4.3 Partie 3 : Configuration de LACP

Dans la Partie 3, nous allons configurer le lien entre S1 et S2 à l'aide de LACP. En outre, il sera configuré en tant que trunk avant un regroupement en tant qu'EtherChannel.

Étape 1 : Configurons LACP entre S1 et S2

```
S1(config)#int range f0/1-2
S1(config-if-range)#switchport mode trunk
S1(config-if-range)#switchport trunk native vlan 99
S1(config-if-range)#channel-group 2 mode active
S1(config-if-range)#
Creating a port-channel interface Port-channel 2

S1(config-if-range)#no shut

S2(config)#int range f0/1-2
S2(config-if-range)#switchport mode trunk
S2(config-if-range)#switchport trunk native vlan 99
S2(config-if-range)#channel-group 2 mode passive
S2(config-if-range)#
Creating a port-channel interface Port-channel 2

S2(config-if-range)#no shut
```

Figure III-23 : Configuration de LACP entre S1 et S2.

Nous allons obtenir la topologie suivante :

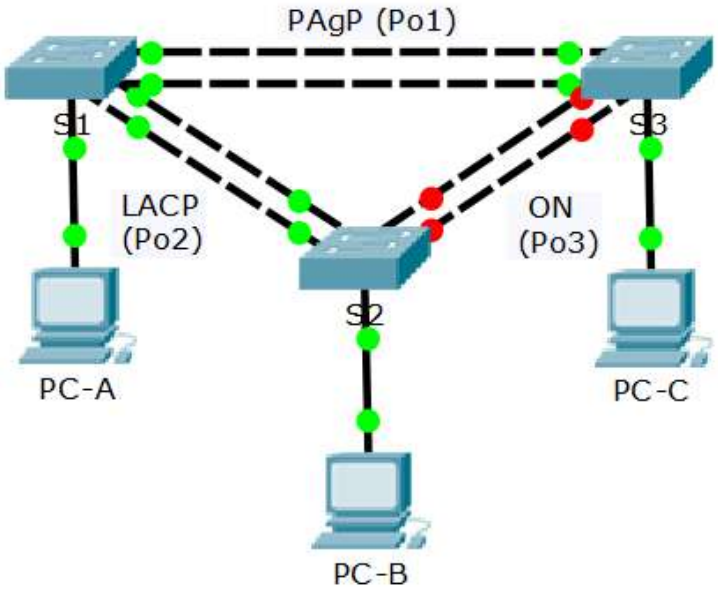


Figure III-24 : Topologie su réseau après avoir configuré LACP entre S1 et S2.

Étape 2 : S'assurer que les ports ont été agrégés.

Nous vérifions le protocole utilisé par Po2 pour l'agrégation de liens et quels sont les ports agrégés pour former Po2.

```
S1#show etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 2
Number of aggregators:           2

Group  Port-channel  Protocol    Ports
------+-------------+-----------+---------------------------

1      Po1(SU)           PAgP   Fa0/3(P) Fa0/4(P)
2      Po2(SU)           LACP   Fa0/1(P) Fa0/2(P)
```

Figure III-25 : Vérification de protocole EtherChannel utilisé par Po2 sur S1.

Nous voyons bien que nous avons un deuxième portchannel que vient de se créer donc le premier c'était avec le mode PAgP et le deuxième est le portchannel 2 avec le mode LACP

```
S2#show etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+---------------------------

2      Po2(SU)           LACP   Fa0/1(P) Fa0/2(P)
```

Figure III-26 : Vérification de protocole EtherChannel utilisé par Po2 sur S2.

III.4.4 Partie 4 : Configurer On

Étape 1 : Configurer ON entre S2 et S3

Il suffit d'ajouter les ports que nous voulons regrouper au Port Channel 3 en appliquant la commande la commande **channel-group 3 mode on**

```
S2(config)#int range f0/3-4
S2(config-if-range)#switchport mode trunk
S2(config-if-range)#switchport trunk native vlan 99
S2(config-if-range)#channel-group 3 mode on
S2(config-if-range)#
Creating a port-channel interface Port-channel 3
S2(config-if-range)#no shut

S3(config)#int range f0/1-2
S3(config-if-range)#switchport mode trunk
S3(config-if-range)#switchport trunk native vlan 99
S3(config-if-range)#channel-group 3 mode on
Creating a port-channel interface Port-channel 3
S3(config-if-range)#no shut
```

Figure III-27 : Configuration de mode ON entre S2 et S3.

Étape 2 : S'assurer que les ports ont été agrégés

Nous utilisons la commande **show etherchannel summary** afin de vérifier qu'EtherChannel fonctionne sur les deux commutateurs. Cette commande affiche le type d'EtherChannel, les ports utilisés ainsi que les états des ports.

```
S2#show etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 2
Number of aggregators:           2

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------

2      Po2(SU)           LACP   Fa0/1(P) Fa0/2(P)
3      Po3(SD)           -      Fa0/3(D) Fa0/4(D)
```

Figure III-28 : Vérification de protocole EtherChannel utilisé par Po3 sur S2.

```
S3#show etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 2
Number of aggregators:           2

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------

1      Po1(SU)           PAgP   Fa0/3(P) Fa0/4(P)
3      Po3(SU)           -      Fa0/1(P) Fa0/2(P)
```

Figure III-29: Vérification de protocole EtherChannel utilisé par Po3 sur S3.

Le signe (–) indique qu'il n'y a pas de protocole de négociation « mode ON »

Étape 4 : Vérification de la connectivité de bout en bout

Nous vérifions que les périphériques peuvent s'envoyer mutuellement des requêtes ping avec le même VLAN.

Ping et est un outil qui est indispensable pour tester la connectivité du réseau TCP/IP. La commande ping est un utilitaire de gestion de réseau qui permet de vérifier l'accessibilité d'un périphérique sur un réseau IP. Cet utilitaire mesure également la durée de transmission pour les messages envoyés depuis l'hôte source vers un ordinateur de destination. L'utilitaire ping est disponible sous Windows, les systèmes d'exploitation de type Unix et l'IOS de Cisco.

La commande ping par défaut envoie quatre requêtes à 32 octets chacune, la figure III-30 montre que le nombre de requêtes reçus est le même que le nombre de requêtes envoyés (4 envoyées, 4 reçues), Les périphériques sont donc connectés les uns aux autres.

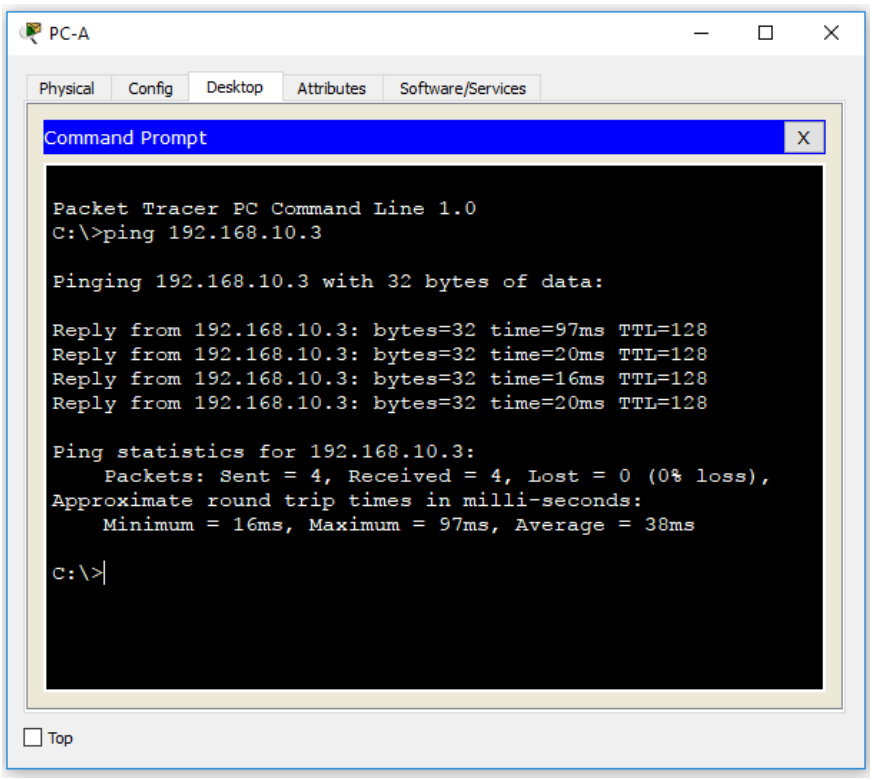


Figure III-30 : Test de connectivité entre PC-A et PC-C.

III.4.5 Test et vérification

Nous allons voir le comportement de protocole de l'EtherChannel par rapport au protocole spaning-tree, si nous faisons ***show spanning-tree*** nous remarquons bien que le STP il va plus voir les interfaces physiques mais plutôt les interfaces logiques qu'ont été créés :

il y a le port 1 que nous avons créé en mode PAgP et le port 2 que nous avons créé en mode LACP et le port 3 que nous avons créé en mode ON.

Nous pouvons diviser le ***show spanning-tree*** en trois parties différentes ; la première partie « Root ID » concerne le switch qui est le root bridge au niveau de notre topologie, la deuxième partie « Bridge ID » concerne le switch lui-même et la troisième partie « Interfaces » c'est les ports qui participent dans le protocole STP

Nous remarquons aussi que les switchs ont la même priorité qui égale 32867 c'est 32768 la priorité par défaut définie sur tous les commutateurs plus le vlan ID qui vaut 99 donc si nous comparons les adresses MAC des switchs nous concluons que le switch S3 ayant la plus petite adresse MAC qui est 0001.C9A0.3583 donc il est élu « root bridge »

En effet il y a trois indices qui disent que le switch S3 est le « root bridge », les informations visibles dans la figure III-32 les confirment :

- Le premier indice c'est que l'adresse MAC de la première partie est la même que celle de la deuxième partie.
- Le deuxième indice c'est la petite phrase qui dit « This bridge is the root ».
- Le troisième indice c'est que tous les ports du commutateur S3 jouent le rôle « designated » et ils sont dans l'état « forwarding ».

```
S3#show spanning-tree vlan 99
VLAN0099
  Spanning tree enabled protocol ieee
  Root ID     Priority    32867
              Address     0001.C9A0.3583
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32867  (priority 32768 sys-id-ext 99)
              Address     0001.C9A0.3583
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Po3              Desg FWD 9         128.28   Shr
Po1              Desg FWD 9         128.27   Shr
```

Figure III-31: Résumé de STP en S3.

D'après les figuresIII-33 et III-34 le port Po2 du côté du switch S2 est bloqué et mis dans le rôle « Alternating » équivalent à l'état « blocking » car les couts des ports vers le pont racine sont identiques et l'adresse MAC de S1 est 0009.7C94.C171 inférieur à celle de S2 qui vaut 0060.70BE.6A07.

Nous pouvons voir même avec les couleurs orange dans la figure III-32.

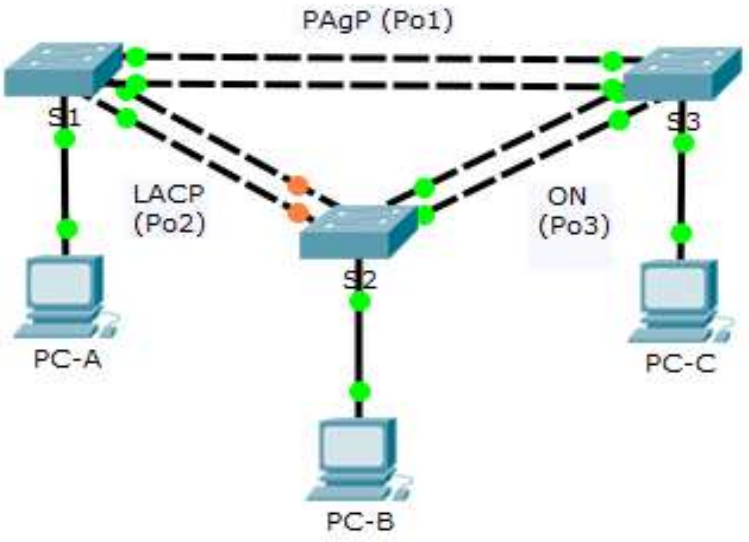


Figure III-32 : Topologie du réseau après avoir configuré l'EtherChannel

```
S1#show spanning-tree vlan 99
VLAN0099
  Spanning tree enabled protocol ieee
  Root ID     Priority    32867
              Address     0001.C9A0.3583
              Cost        9
              Port        27(Port-channel 1)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32867  (priority 32768 sys-id-ext 99)
              Address     0009.7C94.C171
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Po2              Desg FWD 9         128.28   Shr
Po1              Root FWD 9         128.27   Shr
```

Figure III-33 : Résumé de STP en S1.

```
S2#show spanning vlan 99
VLAN0099
  Spanning tree enabled protocol ieee
  Root ID     Priority    32867
              Address     0001.C9A0.3583
              Cost        9
              Port        28(Port-channel 3)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32867  (priority 32768 sys-id-ext 99)
              Address     0060.70BE.6A07
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Po2              Altn BLK 9         128.27   Shr
Po3              Root FWD 9         128.28   Shr
```

Figure III-34 : Résumé de STP en S2.

III.5 Conclusion

Dans ce chapitre, nous avons configuré l'EtherChannel entre les commutateurs où nous avons agrégé les multiples liaisons en un seul lien logique en utilisant les protocoles de négociation PAgP, LACP et le mode ON inconditionnel avec la prise en considération des conditions d'agrégation (même vitesse, même mode bidirectionnel et même informations sur l'ensemble des interfaces des périphériques aux deux extrémités) et grâce au simulateur Cisco Packet Tracer, nous avons pu comprendre le mécanisme du protocole d'EtherChannel de manière pratique et nous avons vu comment les liens redondants sont regroupés en un seul lien virtuel et comment ils ressemblaient à une seule liaison avec le protocole STP.

CONCLUSION GÉNÉRALE

CONCLUSION GÉNÉRALE

Ce mémoire a pour but de étudier la technologie EtherChannel responsable de surmonter les limitations du STP qui empêche de fournir une bande passante supplémentaire et d'équilibrer la charge entre les commutateurs Ethernets industriels en bloquant les liens redondants.

Il a fallu dans un premier temps définir les notions ainsi que les concepts de base du réseau informatique pour bien comprendre le sujet, tels que les composants réseau, la classification des réseaux, les réseaux locaux virtuels ainsi le modèle OSI et TCP/IP.

En second lieu, on a abordé les protocoles de gestion des liens. Pour cela nous avons commencé par voir comment le protocole STP peut résoudre les problèmes associés à un réseau redondant de couche 2 en garantissant qu'il n'existe qu'un seul chemin logique entre toutes les destinations d'un réseau. Nous avons vu aussi les différentes variantes de STP : Normes IEEE (STP et RSTP) et Propriété Cisco (PVST, PVST+ et PVRST+). Dans le but d'utiliser tous les liens disponibles entre deux périphériques et afin de découvrir le besoin en bande passante, nous avons abordé le protocole le plus approprié, le protocole EtherChannel. Nous avons aussi vu les deux principaux protocoles pour faire de l'agrégation de liens: le protocole d'agrégation des ports (PAgP), propriétaire Cisco et le protocole de contrôle d'agrégation des liens (LACP), normalisé IEEE 802.3ad.

La troisième partie est consacrée aux différentes simulations et configurations que nous avons effectuées pour bien comprendre le fondement et les notions de base de ce sujet. La simulation nous a montré qu'avec le protocole EtherChannel, nous avons bénéficié de la redondance des liens Ethernets entre les commutateurs. En effet à travers ces simulations nous avons remarqué que le lien EtherChannel est considéré comme un simple lien sans boucle par le protocole STP.

Enfin ce mémoire nous a permet de comprendre le fonctionnement du protocole EtherChannel mais surtout d'effectuer la simulation de ce dernier par les logiciels Cisco Packet Tracer.

.

BIBLIOGRAPHIE

1 Liste des termes, expressions et définitions du vocabulaire de l'informatique. Journal officiel, octobre 1998.

2 R. CIREDDU. Cours sur la topologie des réseaux. Lycée La Martinière Monplaisir.

3 https://www.netacad.com CCNA1: switchs& Routers.

4 Guy Pujolle, Initiation aux réseaux : Cours et exercices, Eyrolles. 2000.

5 Petit. Bertrand. Architecture des réseaux : Cours et exercices corrigés. Ellipses, 2013.

6 R. CIREDDU. Cours sur la topologie des réseaux. Lycée La Martinière Monplaisir.

7 T. Lammle et Kevin Hales, CCNP support study guide: Exam640-506, Sybex Inc US, 2000.

8 ANGELESCU, S. 2010. *CCNA Certification All-in-one for Dummies*, John Wiley & Sons.

9 Guy Pujolle, Les Réseaux, Eyrolles, 2014.

10 Mike Busby, Introduction à TCP/IP, Osman Eyrolles Multimedia, 2000.

11 A.Tanenbaum, Réseaux. Architectures, protocoles, applications. - InterÉditions, 1997.

12 A. Tanenbaum, Réseaux, Pearson Education France, 2003.

13 José Dordoigne, Réseaux informatiques, notions fondamentales : Protocoles, Architectures, Réseaux sans fil, Virtualisation, Sécurité, IP, Volume 6, ENI, 2015

14 Djillali Seba, CISCO Interconnexion Des Réseaux à L'aide Routeurs Et Commutateurs, ENI, 2003

15 Génael VALET. *Les LANs virtuels*. Greta industriel de technologies avancées, 2007.

16 El Hassan EL AMRI – Campus des Réseaux Informatiques et Télécommunications.

17 https://summarynetworks.com/ccna/ccna3/course/module2/2.1.1.3/2.1.1.3.html

18 Radia Perlman, *Interconnections, Second Edition,* Addison-Wesley, 2000 (ISBN 0-201-63448-1)

19 https://formip.com/fiche-resume-du-chapitre-stp-portfast-et-bpdu-guard/

20 WOJDAK, W. 2003. Rapid Spanning Tree Protocol: A new solution from an old technology.*Reprinted from CompactPCI Systems*

21 https://fr.wikipedia.org/wiki/EtherChannel"EtherChannel" on @Wikipedia: https://fr.wikipedia.org/wiki/EtherChannel?

22 https://www.google.com/amp/s/coursreseaux.com/configurer-depanner-etherchannel/amp/

23 Thomas ANCEL, EtherChannel en AIX Infos Produits, Décembre 2002

24 https://www.google.com/amp/s/coursreseaux.com/configurer-depanner-etherchannel/amp/

25 https://coursreseaux.com/configurer-depanner-etherchannel/

26 http://www.cisco.com/c/en/us/support/docs/lan-switching/etherchannel/12023-4.html

27 Cisco Packet Tracer Help.