

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE
SCIENTIFIQUE UNIVERSITE MOULOU MAMMERI, TIZI-OUZOU



FACULTE DE GENIE ELECTRIQUE ET DE L'INFORMATIQUE
DEPARTEMENT D'ELECTRONIQUE

Mémoire de fin d'études

En vue de l'obtention

Du Diplôme de Master II en Electronique

Option : Réseaux et télécommunications

Thème :

Protocoles de Routage à l'Etat de Liaisons.

Proposé et dirigé par :

Mr. ZIANI.R

Présenté par :

Mr.IBEGHOUCHE Amar

Année universitaire 2011/2012

Remerciement

À travers ce Modeste travail, Je tiens à remercier vivement Mon promoteur Mr R.Ziani qui m'a honoré en acceptant de m'encadrer et pour ses précieux conseils et orientations, ainsi que la confiance qui a placé en moi tout au long de la préparation de ce projet.

Mes remerciements et gratitude s'adressent aussi aux messieurs le président et les membres de jury d'avoir accepté d'examiner mon travail.


J'exprime également mon gratitude à tous les enseignants de l'Université de Mouloud MAMMERRI qui ont contribué à Ma formation Master.




Dédicaces

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

Je dédie ce modeste travail :

 *A mes très chère mère et père pour toutes ses tendresses et pour ses nombreux sacrifices. Que Dieu les garde.*

 *A tout la Famille Spécialement mes frères, mes sœurs.*

 *A tous les professeurs et enseignants qui ont collaboré à ma formation depuis mon cycle d'étude.*

 *A tous mes amis : Hakim, Sofiane, Idris, Boubeker, Faradj , Rabah Samir, Djamel, Sadi et abass.*

 *A mes cousins et cousines .*

 *A tous ceux qui m'ont aidé de loin ou de près mes études.*

 *A toutes la promotion 2012 et en particulieres les etudiants d'option Réseaux et Télécommunications.*

A.IBEGHOUCHE

Sommaire

Introduction générale	1
------------------------------------	---

Chapitre I : Introduction aux réseaux Informatiques

I.1 Introduction	2
I.1.1 Définition d'un réseau informatique	2
I.1.2 Intérêts d'un réseau	3
I.2 Les différents types de réseaux	3
I.2.1 Les réseaux Client/serveur	3
I.2.2 Architecture poste à poste	4
I.3 Classification de réseau.....	5
I.3.1 Classification par leur taille	5
I.3.2 Classification par leur Topologie.....	7
I.3.3 Classification par leur mode de connexion	9
I.3.4 Classification par leur méthode d'Accès	9
I.4 Supports physiques d'interconnexions	10
I.4.1 Lignes spécialisées.....	10
I.4.2 Ligne de transmission	10
I.5 Techniques de transmission des réseaux.....	12
I.5.1 Transmission série et parallèle.....	12
I.5.2 Sens de transmission	12
I.5.3 Transmission synchrone et asynchrone	13
I.5.4 Transmission en bande de base et large bande	13
I.5.5 Transmission analogique et modulation	13
I.5.6 Transmission numérique	13
I.6 Techniques de commutations.....	14
I.6.1 La commutation de circuits.....	14
I.6.2 La commutation de messages	14
I.6.3 La commutation de paquets	15
I.6.4 La commutation de cellules	15
I.7 Architecture des réseaux	15
I.7.1 Modèle OSI.....	15
I.7.2 Modèle TCP/IP	17
I.7.3 Modèle ATM	18
I.8 Dispositifs de communications	19
I.8.1 Les ponts	19
I.8.2 Les Passerelles	20
I.8.3 Les Routeurs	20
I.8.4 Les Hubs	21
I.8.5 Switch	21
I.9 les protocoles de modèle OSI	21
I.9.1 Introduction.....	23
I.9.2 Adressage IP	24

Chapitre II : Protocoles de routage

II.1 Introduction aux protocoles de routage	25
II.1.1 Le routage IP	25
II.1.2 Méthodes de routage IP	26
II.2 Table de routage	26
II.3 Les critères des protocoles de routage	27
II.4 Types de routage.....	27
II.4.1 Le routage statique.....	27
II.4.1.1 Avantages et inconvénients du routage statique.....	27
II.4.2 Le routage à système autonome.....	28
II.4.3 Le routage dynamique	28
II.4.3.1 Avantages et inconvénients du routage dynamique	28
II.5 Fonctionnement des protocoles de routage dynamique.....	29
II.6 Les différents protocoles de routage dynamique.....	30
II.7 Les fonctions de base des protocoles de routage.....	32
II.7.1 La Détermination du chemin	32
II.7.2 La commutation.....	32
II.8 L'objectif des protocoles de routage dynamique	33
II.9 les protocoles de routage à vecteurs à distances et l'état de liaisons	33
II.9.1 fonctionnement des protocoles de routage à vecteur de distance	33
II.9.2 fonctionnement des protocoles à état de liaisons.....	33
II.10 Métriques et protocoles de routage.....	34
II.10.1 Paramètres de métrique	34
II.10.2 Champ de métrique dans la table de routage.....	35
II.11 Comparaison des protocoles de routage dynamique	35
II.12 Identification des classes des protocoles de routage dynamique.....	36
II.13 Convergence de protocoles de routage	36

Chapitre III : Protocoles de routage dynamique à l'état de liaisons

III.1 Introduction	37
III.2 Présentation des Protocoles de routage à état de liaisons.....	37
III.3 Les éléments utilisés pour le routage à état de liaisons.....	38
III.4 Fonctions du protocole de routage à état de liaisons	38
III.4.1 Présentation de l'algorithme SPF	39
III.4.2 Processus de découverte du réseau pour le routage à état de liaisons.....	41
III.4.3 Topologie logique de protocoles de routage à état de liaisons.....	42
III.5 Considérations relatives au routage à état de liaison.....	42
III.6 Mise en œuvre des protocoles de routage à état de liaisons.....	43
III.6.1 Élaboration d'une carte topologique	43
III.6.2 Convergence rapide.....	44
III.6.3 Mises à jour pilotées par événement	44
III.6.4 Conception hiérarchique	44
III.7 Éléments requis pour un protocole de routage à état de liaisons.....	44
III.7.1 Mémoire requise.....	44
III.7.2 Temps processeur requis	44
III.7.3 Bande passante requise	44
III.8 Comparaison des protocoles de routage à état de liaisons	44
III.9 Le protocole OSPF	45

III.9.1 Origines du protocole OSPF	45
III.9.2 Présentation du protocole OSPF	46
III.9.3 Fonctionnement du protocole OSPF	47
III.9.4 Encapsulation de message OSPF	48
III.9.5 Types de paquet OSPF	48
III.9.5.1 Protocole Hello	49
III.9.5.2 Identification d'un routeur	50
III.9.5.3 Détection des voisins.....	50
III.9.5.4 Intervalles des paquets Hello et Dead OSPF.....	51
III.9.6 Algorithme OSPF	51
III.9.7 Zone du protocole OSPF	52
III.9.8 Configuration basique de protocole OSPF.....	52
III.9.8.1 Configuration chaque routeur commande routeur ospf 1.....	53
III.9.8.2 La commande Network IP masque réseau area	53
III.9.8.3 Visualiser le Router ID.....	53
III.9.8.4 Configuration par l'interface loopback	54
III.9.8.4.1Avantage d'utiliser une adresse de loopback	54
III.9.8.5 Vérification de la configuration	54
III.9.8.6 La table de routage	55
III.9.9 Les métriques OSPF.....	55
III.9.10 Le Coût total.....	56
III.9.11 OSPF et les réseaux à accès multiple	56
III.9.12 Mises à jour d'état de liens OSPF	57
III.9.13 Distance administrative	58
III.9.14 Authentification	59

Chapitre IV : Configuration du protocole OSPF dans un réseau

IV.1 Introduction.....	60
IV.2.1 Présentation de Packet tracer	60
IV. 3 Configuration d'un routeur	64
IV.4 Présentation du réseau.....	64
IV.5 configuration du réseau.....	69
IV.5.1 configuration des routeurs.....	69
IV.5.2 configurations des interfaces Ethernet de PC0, PC1 et PC2.....	73
IV.5.3 configuration le routage OSPF sur les Routeurs.....	75
IV.5.4 adresse de bouclage des routeurs	78
IV.5.5 Configuration du coût OSPF	80
IV.6 Conclusion	82

Conclusion générale	83
----------------------------------	-----------

Bibliographie.....	84
---------------------------	-----------

Liste des figures

Figure I.1 : Exemple d'un réseau informatique.....	2
Figure I.2 : Le réseau Client/serveur.....	4
Figure I.3 : Le réseau poste à poste.....	4
Figure I.4 : Classification de réseaux.....	6
Figure I.5 : Topologie en étoile.....	7
Figure I.6 : Topologie en bus.....	7
Figure I.7 : Topologie en anneau.....	8
Figure I.8 : Topologie maillée.....	8
Figure I.9 : commutation par circuit.....	14
Figure I.10: commutation par message.....	14
Figure I.11: modèle de référence ISO.....	16
Figure I.12: principe d'encapsulation.....	16
Figure I.13 : Modèle TCP/IP.....	17
Figure I.14: Réseau ATM.....	19
Figure I.15: Deux réseaux reliés avec un pont.....	19
Figure I.16: deux réseaux reliés avec passerelle.....	20
Figure I.17: Routeur connecter à deux réseaux locaux.....	21
Figure I.18 : les cinq classes d'adresses IP.....	24
Figure II.1 : Présentation de protocoles de routage.....	25
Figure II.2 : Routeurs sous administrateur commune.....	28
Figure II.3 : Fonctionnement de routage dynamique.....	29
Figure II.4 : Classification des protocoles de routage dynamique.....	30
Figure II.5 : Table de routage aux routeurs voisins et cumul des vecteurs de distance.....	31
Figure II.6 : Fonctionnement des protocoles à état de liaisons.....	32
Figure II.7 : Présentation des classes des protocoles de routage dynamique.....	36
Figure III.1 : Les protocoles de routage à état de liaisons IP.....	37
Figure III.2 : présentation les éléments de routage à état de liaisons.....	38
Figure III.3 : fonctionnement de l'algorithme SPF.....	39
Figure III.4 : la base donnée topologique de chaque routeur avec SPF.....	41
Figure III.5 : modification topologique et mise à jour d'une table de routage.....	42
Figure III.6 surcharge de SPF et des tables bande passante lors du flux initial de LSA.....	43
Figure III.7 : histoire du protocole OSPF.....	46
Figure III.8 : schéma de présentation du protocole OSPF.....	46
Figure III.9 : Exemple de fonctionnement du protocole OSPF.....	47
Figure III.10 : Message du protocole OSPF.....	48
Figure III.11 : Les paquets hello OSPF.....	49
Figure III.12 : Exemple de la découverte des voisins.....	51
Figure III.13 : présentation de l'algorithme OSPF.....	52
Figure III.14 : Les zones OSPF.....	52
Figure III.15 : Visualisation le Router ID.....	54

Figure III.16 : Vérification de la configuration.....	55
Figure III.18 : Utilisation la commande show ip dans la table routage.....	55
Figure III.18 : Exemple de calcul le coût total OSPF.....	56
Figure III.19 : les réseaux multiples par OSPF.....	57
Figure III.20 : Authentification OSPF.....	59
Figure IV.1 : La fenêtre principale du packet tracer.....	60
Figure IV.2 : présentation des matériels.....	61
Figure IV.3 : présentation des connecteurs.....	61
Figure IV.4 : Le paramétrage physique d'un PC.....	62
Figure IV.5: Configuration l'interface d'un PC.....	63
Figure IV.6 : Accès aux différents outils.....	63
Figure IV.7 : Les simulations du packet tracer.....	64
Figure IV.8 Les commandes de configuration d'un routeur.....	65
Figure IV.9 : Diagramme de la topologie.....	67
Figure IV.10 : configuration du nom et le mot de passe du routeur.....	70
Figure IV.11 : Configuration les interfaces du routeur	72
Figure IV.12 : La fenêtre de configuration d'un PC.....	74
Figure IV.13 : la configuration du PC par l'exécution d'une requête ping.....	75

Liste des tableaux

Tableau I.1: Caractéristiques physiques des différents câbles.....	12
Tableau I.2: Comparaison entre TCP/IP et modèle OSI.....	18
Tableau I.3: l'espace d'adresse.....	25
Tableau II.1 Comparaison des protocoles de vecteur à distance et l'état de liaison.....	35
Tableau III.1 résultats des paramètres d'un routeur R1	39
Tableau III.2 résultats des paramètres d'un routeur R2.....	40
Tableau III.3 résultats des paramètres d'un routeur R3.....	40
Tableau III.4 résultats des paramètres d'un routeur R4.....	40
Tableau III.5 résultats des paramètres d'un routeur R5.....	40
Tableau III.6 : présentation les différentes valeurs de coût de chaque interface.....	56
Tableau III.7 : La distance administrative OSPF.....	58
Tableau IV.1: adresses de chaque périphérique.....	69

*Introduction
générale*

Introduction générale

Les réseaux informatiques ont été développés en réponse à des besoins informatiques, commerciaux et gouvernementaux et pour assurer la compatibilité entre les équipements de différentes sociétés. L'application de normes aux fonctions du réseau a donné lieu à un ensemble de directives afin de créer des matériels et des logiciels pour le réseau, ces logiciels sont composés de protocoles.

Un protocole est une description formelle de règles et de conventions à suivre dans un échange d'informations, que ce soit pour acheminer les données jusqu'au destinataire ou pour que le destinataire comprenne comment il doit utiliser les données qu'il a reçues.

Toutefois, les professionnels des réseaux savent que c'est le routeur qui est responsable du transfert de paquets d'un réseau à l'autre, de la source à la destination.

Un routeur relie plusieurs réseaux. Pour ce faire, il dispose de plusieurs interfaces, chacune possédant une adresse IP différente. Lorsqu'un routeur reçoit un paquet IP sur une interface, il détermine quelle interface utiliser pour transférer le paquet vers sa destination. L'interface utilisée par le routeur pour transférer le paquet peut être le réseau de la destination finale du paquet.

Notre travail est partagé en quatre chapitres :

Le premier chapitre est une introduction aux réseaux informatiques. Nous décrivons les techniques de transmission entre réseaux, les types d'architectures et les protocoles de transmission.

Le deuxième chapitre introduit la définition de routage IP, les types de routage et les protocoles de routage dynamique que ce soit à vecteur de distance ou à l'état de liaison.

Le troisième chapitre est consacré aux protocoles de routage à l'état de liaisons.

Le quatrième chapitre présente la configuration du protocole de routage dynamique OSPF à l'état de liaisons en utilisant le logiciel **PACKET TRACER**.

Nous terminerons notre travail par une conclusion générale.

Chapitre I

*Introduction aux réseaux
Informatiques*

I.1 Introduction

Les réseaux informatiques qui permettaient à leur origine de relier des terminaux passifs à de gros ordinateurs centraux autorisent à l'heure actuelle l'interconnexion de tous types d'ordinateurs, que ce soit de gros serveurs, des stations de travail, des ordinateurs personnels ou de simples terminaux graphiques. Les services qu'ils offrent font partie de la vie courante des entreprises et administrations (banques, gestion, commerce, bases de données, recherche,...) et des particuliers (messagerie, loisirs, services d'informations et Internet ...).

I.1.1 Définition d'un réseau informatique

On peut définir le réseau informatique de plusieurs manières :

- ❖ C'est un ensemble d'ordinateurs et de périphériques connectés les uns aux autres pour échanger des informations et partager des ressources.
- ❖ C'est un ensemble d'équipements matériels et logiciels permettant d'échanger des données sous forme numérique.
- ❖ C'est ensemble de terminaux passifs (clients) reliés à de gros ordinateurs serveurs centraux à des fins d'offrir des services.

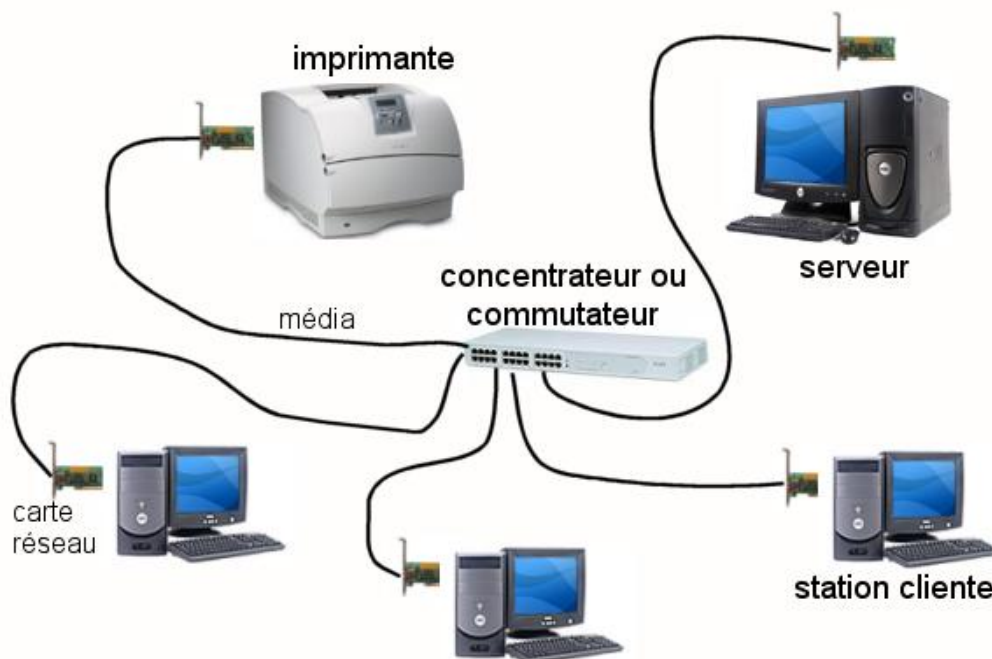


Figure I.1 : Exemple d'un réseau informatique.

I.1.2 Intérêt d'un réseau

Un ordinateur est une machine permettant de manipuler des données. L'homme a vite compris l'intérêt qu'il pouvait y avoir à relier ces ordinateurs entre eux afin de pouvoir échanger des informations. Voici un certain nombre de raisons pour lesquelles un réseau est utile, un réseau permet:

- ❖ Le partage de fichiers, d'applications.
- ❖ La communication entre personnes (grâce au courrier électronique, la discussion en direct, ...).
- ❖ La communication entre processus (entre des machines industrielles).
- ❖ La garantie de l'unicité de l'information (bases de données).
- ❖ Le jeu à plusieurs, ...
- ❖ Le transfert de la parole, de la vidéo et des données (réseaux à intégration de services ou multimédia).

Les réseaux permettent aussi de standardiser les applications, on parle généralement de groupware., comme par exemple la messagerie électronique et les agendas de groupe qui permettent de communiquer plus efficacement et plus rapidement.

Avantages de tels systèmes

- ❖ Diminution des coûts grâce aux partages des données et des périphériques.
- ❖ Standardisation des applications.
- ❖ Accès aux données en temps utile.
- ❖ Communication et organisation plus efficace.

I. 2 Les différents types de réseaux

On distingue généralement deux types de réseaux bien différents, ayant tout de même des similitudes.

I.2.1 Les réseaux Client/serveur

Un certain nombre de machines sont désignées comme serveur et centralisent les ressources communes du réseau qui seront exploitées par les autres machines du réseau qu'on appelle clients (Figure I.2).

De nombreuses applications fonctionnent selon un environnement client/serveur, cela signifie que des machines clientes (machines faisant partie du réseau) contactent un serveur, une machine généralement très puissante en terme de capacités d'entrée-sortie, qui leur fournit des services. Ces services sont des programmes fournissant des données telles que l'heure, des fichiers, une connexion,

Les services sont exploités par des programmes, appelés programmes clients, s'exécutant sur les machines clientes. On parle ainsi de client FTP, client de messagerie, ..., lorsque l'on

désigne un programme, tournant sur une machine cliente, capable de traiter des informations qu'il récupère auprès du serveur (dans le cas du client FTP il s'agit de fichiers, tandis que pour le client messagerie il s'agit de courrier électronique).

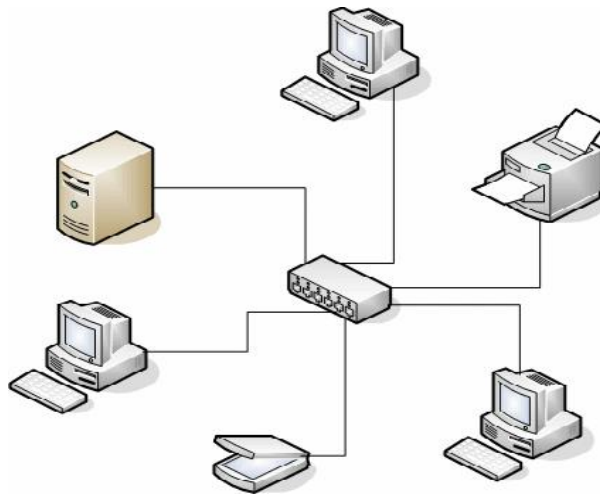


Figure I.2 : Le réseau Client/serveur.

a) Avantages de l'architecture client/serveur

Le modèle client/serveur est particulièrement recommandé pour des réseaux nécessitant un grand niveau de fiabilité. Ses principaux atouts sont :

- ❖ **des ressources centralisées**: étant donné que le serveur est au centre du réseau, il peut gérer des ressources communes à tous les utilisateurs, comme par exemple une base de données centralisée, afin d'éviter les problèmes de redondance et de contradiction.
- ❖ **Une meilleure sécurité**: car le nombre de points d'entrée permettant l'accès aux données est moins important.
- ❖ **Une administration au niveau serveur**: les clients ayant peu d'importance dans ce modèle, ils ont moins besoin d'être administrés.
- ❖ **Un réseau évolutif**: grâce à cette architecture, il est possible de supprimer ou rajouter des clients sans perturber le fonctionnement du réseau et sans modifications majeures.

b) Inconvénients du modèle client /serveur

L'architecture client/serveur a tout de même quelques lacunes parmi lesquelles :

- ❖ **Un coût élevé** : dû à la technicité du serveur.
- ❖ **Un maillon faible** : le serveur est le seul maillon faible du réseau client/serveur, étant donné que tout le réseau est construit autour de lui. Heureusement, le serveur a une grande tolérance aux pannes.

I.2.2 Architecture poste à poste

Dans une architecture poste à poste (dans sa dénomination anglaise *peer to peer*), il n'y a pas de serveur dédié, il n'y a donc pas de centralisation des ressources, les machines sont

autonomes et chaque utilisateur choisit les ressources qu'il veut mettre à disposition sur le réseau (Figure I.3).

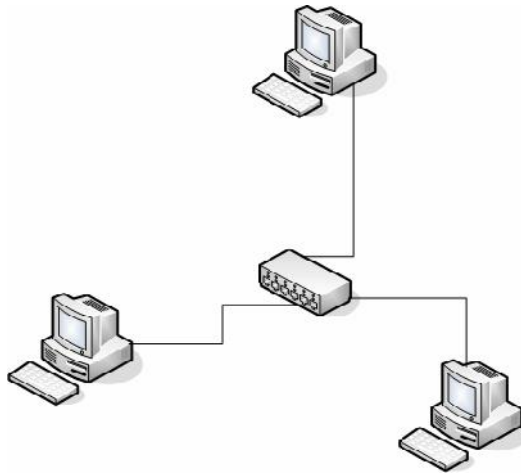


Figure I.3 : Le réseau poste à poste.

a) Inconvénients des réseaux poste à poste

Les réseaux poste à poste ont les inconvénients suivants:

- ❖ Ce système n'est pas du tout centralisé, ce qui le rend très difficile à administrer.
- ❖ La sécurité est très peu présente.
- ❖ Il n'est pas fiable.

Ainsi, les réseaux poste à poste ne sont valables que pour un petit nombre d'ordinateurs (généralement une dizaine), et pour des applications ne nécessitant pas une grande sécurité (il est donc déconseillé pour un réseau professionnel avec des données sensibles).

b) Avantages de l'architecture poste à poste

L'architecture poste à poste a tout de même quelques avantages parmi lesquels:

- ❖ Un coût réduit (les coûts engendrés par un tel réseau sont le matériel, les câbles et la maintenance)
- ❖ Une simplicité dans la réalisation.

I.3 Classification des réseaux

I.3.1 Classification par leur taille

On peut faire une classification des réseaux à l'aide de leur taille comme on peut le voir dans la figure I.4.

- ❖ **Les bus** : interconnectent plusieurs composants (mémoires, périphériques d'entrée-sortie, processeurs, ...). Ils sont considérés comme des réseaux dédiés à des tâches très spécifiques.
- ❖ **La structure d'interconnexion** : est basée sur la liaison des différents matériels : l'ordinateur, l'imprimante, le scanner, USB...etc., d'un même utilisateur.
- ❖ **Réseau local LAN** (Local Area Network) peut s'étendre de quelques mètres à quelques kilomètres et correspond au réseau d'une entreprise. Il peut se développer sur plusieurs bâtiments et permet de satisfaire tous les besoins internes de cette entreprise
- ❖ **Réseau métropolitain (MAN ; Metropolitan Area Network)** interconnecte plusieurs lieux situés dans une même ville, par exemple les différents sites d'une université ou d'une administration, chacun possédant son propre réseau local.
- ❖ **Réseau étendu (WAN ; Wide Area Network)** permet de communiquer à l'échelle d'un pays ou de la planète entière, les infrastructures physiques pouvant être terrestres ou spatiales à l'aide de satellites de télécommunications.

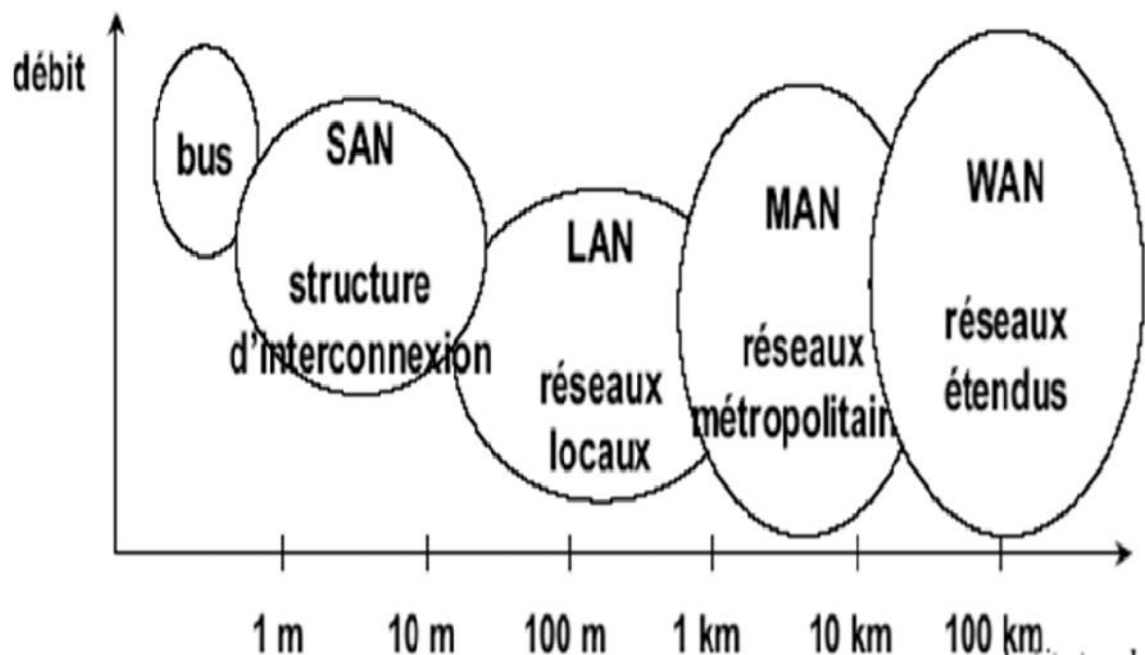


Figure I.4 : Classification des réseaux.

On parle aussi de réseaux :

- **Homogènes** : Tous les ordinateurs sont du même constructeurs : Apple - Talk.
- **Hétérogènes** : Les ordinateurs reliés au réseau sont de constructeurs divers. Exemple: Ethernet.

I.3.2 Classification par leur Topologie

La topologie des réseaux décrit la configuration selon laquelle leurs stations sont interconnectées via le support de transmission. On distingue principalement quatre types de topologies : le bus, l'étoile, l'anneau et la topologie maillée.

❖ Topologie en étoile

Dans une topologie en étoile, un contrôleur central raccorde directement toutes les stations du réseau. Toute communication entre deux stations quelconques passe par le nœud central, qui est chargé de les gérer et les contrôler.

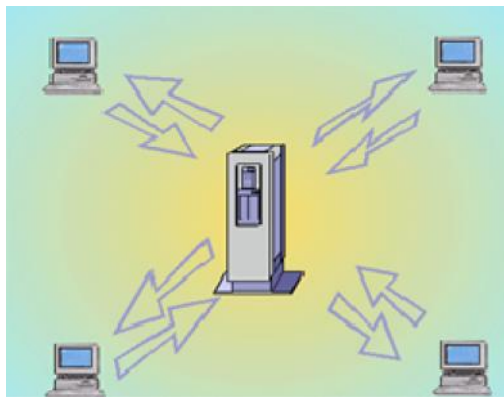


Figure I.5 : Topologie en étoile.

Le nœud central joue souvent le rôle d'un dispositif de commutation. Lorsqu'une station désire communiquer avec une autre station, le contrôleur établit un circuit entre elles ; les deux stations peuvent échanger les données entre elles exactement comme si elles étaient reliées par une liaison dédiée en point à point.

❖ Topologie en bus

Dans une configuration en bus, chaque station est directement attachée au canal de transmission commun. Suivant les types de support utilisé, le bus peut être unidirectionnel ou bidirectionnel.

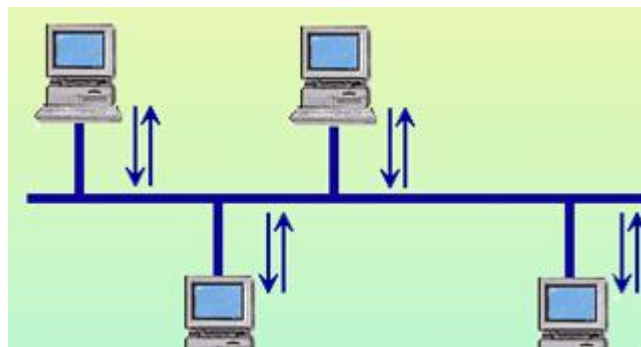


Figure I.6 : Topologie en bus.

Le bus bidirectionnel est utilisé principalement avec le câble coaxial, ce qui présente l'avantage de ne nécessiter que des terminateurs aux extrémités du câble. La fibre optique ne permet que des bus unidirectionnel.

❖ Topologie en anneau

Le câble forme ici une boucle, à laquelle vient s'attacher chacune des stations par l'intermédiaire d'un répéteur. Les différents répéteurs sont reliés deux à deux par des liens en point à point de manière à former la boucle. Les liens sont unidirectionnels et les répéteurs se contentent de recevoir bit à bit sur le lien d'entrée et de les retransmettre sur le lien de sortie. Les informations circulent toujours dans le même sens, une trame envoyée par une station est reçue par l'ensemble des stations et c'est l'adresse qu'elle contient qui permet de déterminer si une station donnée doit en tenir compte ou non.

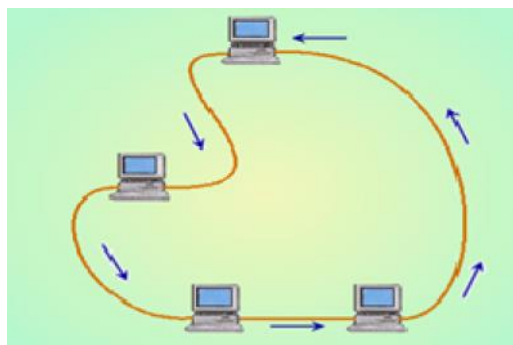


Figure I.7 : Topologie en anneau.

L'anneau est une structure active le rendant très sensible aux pannes. Le manque de fiabilité peut être pallié par un anneau doublé. Les deux anneaux peuvent transmettre dans le même sens ou en sens inverse. Dans les deux cas, lorsqu'une coupure survient pour l'un des anneaux, l'autre peut prendre le relais.

❖ Topologie maillée

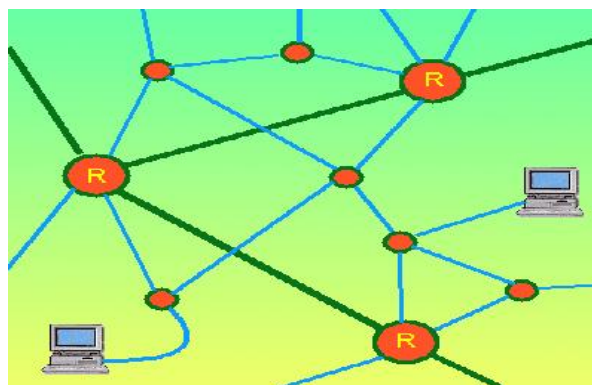


Figure I.8 : Topologie maillée.

Cette topologie se rencontre dans les grands réseaux de distribution. Des artères de grand débit (dorsales) et d'autres voies de moins grande circulation sont reliées à des éléments de routage et de commutation, dont la fonction est à la fois de déterminer la meilleure route et de décongestionner au plus vite les noeuds encombrés.

I.3.3 Classification par leur mode de connexion

a) Le mode avec connexion

Le mode avec connexion contient de négociation entre l'émetteur et le récepteur sur quelques paramètres définissant les limites admissibles pour le transfert des données, c'est la négociation de la qualité de service.

La transmission des données dans le mode avec connexion est sécurisée puisque l'émetteur et le récepteur se mettent d'accord, et par la suite le contrôle est effectué, au moins, au niveau des deux extrémités.

b) Le mode sans connexion

Le mode sans connexion ne contient pas de négociation entre l'émetteur et le récepteur. Pour mettre en place cette connexion, il faut penser à une logistique afin de s'assurer du transfert des données : c'est la structure en couches, telle que chaque couche rend service à celle qui est inférieure.

Le mode sans connexion réside en l'établissement du contrôle de communication par le gestionnaire de réseau qui doit prendre des précautions.

I.3.4 Classification par leur méthode d'Accès

a) La méthode d'accès CSMA/CD

CSMA/CD (Carrier Sens Method Access / Collision Detection) est un ensemble de règles qui déterminent la façon dont les périphériques du réseau répondent lorsque deux de ces périphériques tentent de transmettre simultanément des données sur le réseau. La transmission simultanée de données par plusieurs ordinateurs provoque une collision. Tous les ordinateurs du réseau, clients et serveurs, vérifient le câble sur lequel s'effectue le trafic réseau. Un ordinateur ne transmet des données que lorsqu'il détecte que le câble est libre. Une fois que l'ordinateur a transmis des données sur le câble, aucun autre ordinateur ne peut transmettre des données tant que les données d'origine n'ont pas atteint leur destination, libérant ainsi le câble.

Lorsqu'il détecte une collision, un périphérique attend pendant un délai aléatoire, puis tente de retransmettre le message. S'il détecte de nouveau une collision, il attendra deux fois plus longtemps avant de retransmettre le message.

b) La méthode d'accès par jeton

Un jeton est une séquence spéciale de bits qui transitent sur l'anneau. Un ordinateur ne peut pas transmettre des données tant qu'il n'est pas en possession du jeton ; tant que ce jeton est utilisé par un ordinateur, les autres ordinateurs ne peuvent pas transmettre de données.

Lorsque le premier ordinateur de l'anneau se retrouve en ligne, le réseau génère un jeton. Ce jeton transite sur l'anneau jusqu'à ce que l'un de ces ordinateurs prenne le contrôle du jeton. Cet ordinateur envoie alors une trame de données sur le réseau. Cette trame parcourt l'anneau jusqu'à ce qu'elle atteigne l'ordinateur dont l'adresse correspond à l'adresse de destination de la

trame. L'ordinateur destinataire copie la trame en mémoire et la marque pour indiquer que les informations ont été reçues.

La trame continue à parcourir l'anneau jusqu'à l'ordinateur expéditeur, sur lequel la transmission est réussie. L'ordinateur qui a transmis les données retire alors la trame de l'anneau, et envoie sur celui-ci un nouveau jeton.

I.4 Supports physiques d'interconnexions

I.4.1 Lignes spécialisées

Ce sont des lignes louées qui permettent la transmission de données à moyens et hauts débits (2,4 Kb/s à 140 Mb/s) en liaison point à point ou multipoints. Les 3 lignes les plus répandues sont les T1 (1.5 Mb/s), les T2 (6 Mb/s), et les T3 (45 Mb/s). Il existe aussi des lignes nettement plus rapides : ce sont les E1 (2 Mb/s), E2 (8 Mb/s), E3 (34 Mb/s), et E4 (140 Mb/s) qui sont inaccessibles pour les particuliers.

a) Les ondes hertziennes

Elles supportent de grandes distances et de grandes capacités pour une propagation en visibilité directe (entre 50 et 80 Km). Les débits sont très élevés mais les transmissions sont sensibles aux perturbations et les possibilités d'écoute sont nombreuses.

b) Le satellite

Les liaisons satellites sont très rapides, cependant elles sont dans un seul sens (réception), ainsi lorsque l'on veut aller sur un site on ne peut pas en donner l'ordre. La solution est simple, un modem sur une ligne téléphonique suffit pour envoyer ces informations. Le téléchargement de données s'effectue actuellement à un taux de transfert de 400Kb/s.

I.4.2 Ligne de transmission

a) Ligne bifilaire

C'est le moyen de transmission le plus simple. On peut l'utiliser pour des connexions n'excédant pas 50 m, pour relier un DTE à un DCE, un modem par exemple. Ce type de câble possède l'inconvénient d'être sensible d'une part à la diaphonie, à cause des capacités parasites, d'autre part aux perturbations électromagnétiques.

b) La paire torsadée

C'est un câble téléphonique constitué à l'origine de deux fils de cuivre isolés et enroulés l'un sur l'autre (d'où le nom). Actuellement on utilise plutôt des câbles constitués de 2 ou 4 paires torsadées. Elle est très répandue, d'une connexion facile et d'un faible coût mais elle possède une faible immunité aux bruits.

Il en existe deux types : blindées (STP : *Shielded Twisted Pair*), non blindées (UTP : *Unshielded Twisted Pair*).

c) Le câble coaxial

Il s'agit de 2 conducteurs concentriques isolés par une gaine diélectrique. Une gaine extérieure, parfois blindée, entoure l'ensemble. Cette construction assure au câble une bonne résistance aux signaux parasites.

Des débits de 10 Mb/s peuvent transiter par de tels câbles, dont la longueur n'excède pas quelques centaines de mètres. Il existe deux types de câbles coaxiaux, le câble épais (jaune) et le câble fin (noir).

d) La fibre optique

La fibre optique est utilisée pour véhiculer des signaux de données sous forme de signaux optiques modulés. Elle est constituée d'un cylindre de verre extrêmement fin (le cœur) entouré d'une couche concentrique de verre (le revêtement) et joue le rôle d'un guide d'ondes lumineuses pour les longueurs d'ondes dans la gamme infrarouges : 850 nm, 1300 nm, 1500 nm. L'indice de réfraction du revêtement étant plus faible que celui du cœur, les faisceaux lumineux sont réfléchis vers le cœur dès qu'il heurte le revêtement. Une onde optique guidée par des réflexions successives peut être représentée par des faisceaux de rayons que l'on appelle « modes ».

Les fibres optiques offrent des bandes passantes très importantes, de l'ordre du GHz. Leur atténuation est très faible, les signaux véhiculés n'étant pas sujets aux interférences électriques, et le taux d'erreur est très faible (de l'ordre de 10^{-9}). De plus le câble optique est plus léger et moins encombrant qu'un support à cuivre. Néanmoins, le prix d'une liaison en fibre optique reste élevé, en raison des coupleurs optoélectroniques d'une part, et de l'installation de la fibre proprement dite d'autre part. .

Il existe plusieurs types de fibre optique :

- ❖ la fibre multimode à saut d'indice (diamètres : 50- 125 μm) dont la bande passante est de 40 MHz sur 1 Km.
- ❖ La fibre multimode à gradient d'indice (mêmes diamètres) dont la bande passante atteint 500 MHz sur 1 km
- ❖ La fibre monomode (diamètres : 2-8 μm) qui est la plus fine. Elle ne transmet qu'un seul mode et elle présente le plus grand potentiel de bande passante, de l'ordre de 100 GHz /km.

Le tableau I.1 représente les différentes caractéristiques des principaux de chaque ligne de transmission.

	Paire torsadée	Câble coaxial	Fibre optique
Coût	Faible	Moyen	Assez élevé
Bande passante	Moyenne	Large	Très large
Longueur maximale	Moyenne	Elevée	Elevée
Immunité aux interférences	Basse (UTP) Moyenne (STP)	Moyenne à élevée	Très élevée
Facilité de connexion	Simple	Variable	Difficile
Facilité d'installation	Variable	Variable	Difficile
Fiabilité	Bonne	Bonne	Très bonne

Tableau I.1: Caractéristiques physiques des différents câbles.

I.5 Techniques de transmission des réseaux

I.5.1 Transmission série et parallèle

Le mode de transmission désigne le nombre d'unités élémentaires d'informations (bits) pouvant être simultanément transmise par le canal de communication.

- ❖ On désigne par liaison parallèle la transmission simultanée de N bits. Ces bits sont envoyés simultanément sur N voies différentes.
- ❖ Dans une liaison en série, les données sont envoyées bit par bit sur la voie de transmission. Toutefois, étant donné que la plupart des processeurs traitent les informations de façon parallèle, il s'agit de transformer des données arrivant de façon parallèle en données en série au niveau de l'émetteur, et inversement au niveau du récepteur.

I.5.2 Sens de transmission

- ❖ **Mode simplex** : La transmission ne peut se faire que de A vers B (ex : radio, télévision).
- ❖ **Mode semi-duplex** : La transmission peut se faire dans les deux sens, mais pas en même temps (ex : talkie-walkie).
- ❖ **Mode duplex intégral** : La transmission peut se faire dans les deux sens simultanément (ex : téléphone).

I.5.3 Transmission synchrone et asynchrone

- ❖ **Liaison asynchrone** : est laquelle chaque caractère est émis de façon irrégulière dans le temps (par exemple un utilisateur envoyant en temps réel des caractères saisis au clavier). Chaque caractère est précédée d'une information indiquant le début de la transmission du caractère (l'information de début d'émission est appelée bit START) et terminée par l'envoi d'une information de fin de transmission (appelée bit STOP, il peut éventuellement y avoir plusieurs bits STOP).
- ❖ **Liaison synchrone** : est laquelle émetteur et récepteur sont cadencés à la même horloge. De plus, des informations supplémentaires sont insérées afin de garantir l'absence d'erreurs lors de la transmission. Lors d'une transmission synchrone, les bits sont envoyés de façon successive sans séparation entre chaque caractère, il est donc nécessaire d'insérer des éléments de synchronisation, on parle alors de synchronisation au niveau caractère.

I.5.4 Transmission en bande de base et large bande

La transmission en bande de base consiste à transmettre directement des signaux numériques (les suites de bits) sur le support, cette transmission utilisée un simple codeur (codeur de bande de base, bien que l'on désire à tort " modem de bande de base ").

La transmission en large bande consiste à transposer le signal en fréquence via des modulateurs démodulateurs. Cela permet entre autre de multiplexer en fréquence les signaux. Quand il n'y a qu'un signal en large bande, le procédé est appelé " bande porteuse ".

I.5.5 Transmission analogique et modulation

La transmission analogique de données consiste à faire circuler des informations sur un support physique de transmission sous la forme d'une onde. La transmission des données se fait par l'intermédiaire d'une onde porteuse, une onde simple dont le seul but est de transporter les données par modification de l'une de ces caractéristiques (amplitude, fréquence ou phase), c'est la raison pour laquelle la transmission analogique est généralement appelée transmission par modulation d'onde porteuse.

I.5.6 Transmission numérique

La transmission numérique consiste à faire transiter les informations sur le support physique de communication sous forme de signaux numériques. Ainsi, des données analogiques devront préalablement être numérisées avant d'être transmises. Ce mode de transmission est peu sensible aux parasites, mais il nécessite une très grande bande passante.

I.6 Techniques de commutations

I.6.1 La commutation de circuits

Elle consiste à créer dans le réseau un circuit particulier entre l'émetteur et le récepteur avant que ceux-ci ne commencent à échanger des informations. Ce circuit sera propre aux deux entités communicant et il sera libéré lorsque l'un des deux coupera sa communication (Figure I.9).

Par contre, si pendant un certain temps les deux entités ne s'échangent rien le circuit leur reste quand même attribué. C'est pourquoi, un même circuit (ou portion de circuit) pourra être attribué à plusieurs communications en même temps.

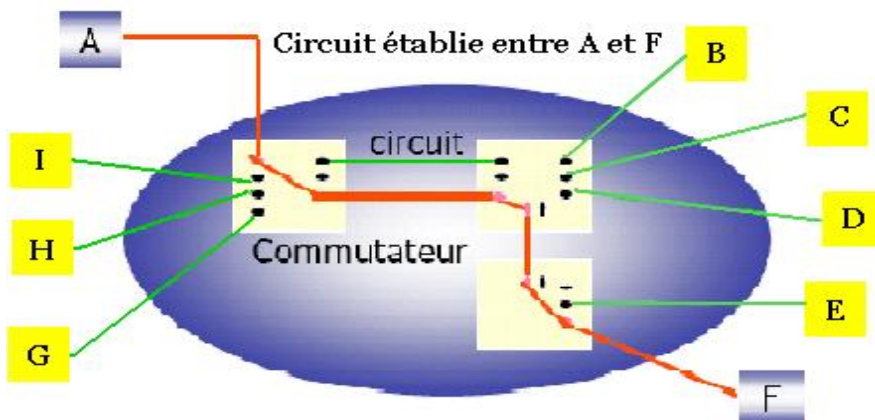


Figure I.9 : commutation de circuit.

I.6.2 La commutation de messages

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

Cette technique nécessite de prévoir de grandes zones tampon dans chaque nœud du réseau, mais comme ces zones ne sont pas illimitées il faut aussi prévoir un contrôle de flux des messages pour éviter la saturation du réseau (Figure I.10).

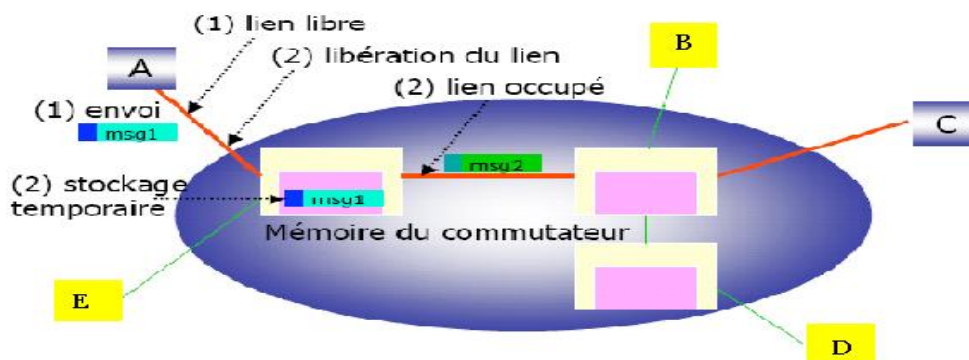


Figure I.10: commutation de message.

I.6.3 La commutation de paquets

Un message émis est découpé en paquets et par la suite chaque paquet est envoyé à travers le réseau comme dans le cas des messages. Les paquets sont envoyés indépendamment les uns des autres et sur une même liaison on pourra trouver les uns derrière les autres des paquets appartenant à différents messages.

Chaque nœud redirige chaque paquet vers la bonne liaison grâce à une table de routage. La reprise sur erreur est donc ici plus simple que dans la commutation de messages, par contre le récepteur final doit être capable de reconstituer le message émis en réassemblant les paquets.

I.6.4 La commutation de cellules

Une cellule est un paquet particulier dont la taille est toujours fixée à 53 octets (5 octets d'en-tête et 48 octets de données). C'est la technique de base des réseaux hauts débits ATM (Asynchronous Transfert Mode) qui opèrent en mode connecté où avant toute émission de cellules, un chemin virtuel par lequel passeront toutes les cellules est établi.

Cette technique mixe donc la commutation de circuits et la commutation de paquets de taille fixe permettant ainsi de simplifier le travail des commutateurs pour atteindre des débits plus élevés.

I.7 Architecture des réseaux

I.7.1 Modèle OSI

OSI signifie Open System Interconnections. Ce modèle a été mis en place par l'ISO (International Standard Organisation) afin de mettre en place un standard de communications entre les ordinateurs d'un réseau.

En effet, aux origines des réseaux chaque constructeur avait un système propre (on parle de système propriétaire). Ainsi de nombreux réseaux incompatibles coexistaient. Le modèle OSI est un modèle qui comporte 7 couches :

- ❖ **Couche physique:** S'occupe de la connexion physique d'une machine avec le réseau.
- ❖ **Couche liaison :** S'occupe de l'acheminement de trames de données entre deux équipements voisins.
- ❖ **Couche réseau :** Définit l'unité de données de base transférée sur le réseau entre deux sites extrêmes et inclut les concepts d'adressage et de routage.
- ❖ **Couche transport :** Assure un contrôle de bout en bout en permettant à un processus destinataire de communiquer directement avec le processus source.
- ❖ **Couche session :** Définit la manière dont les protocoles peuvent être organisées pour fournir toutes les fonctionnalités dont les programmes d'applications se servent.
- ❖ **Couche présentation :** Est destinée à supporter les fonctions dont beaucoup de programme ont besoin comme la compression de texte ou la conversion d'image graphique.

- ❖ **Couche application** : Comprend les programmes qui utilisent le réseau, la messagerie électronique ou le transfert des fichiers.

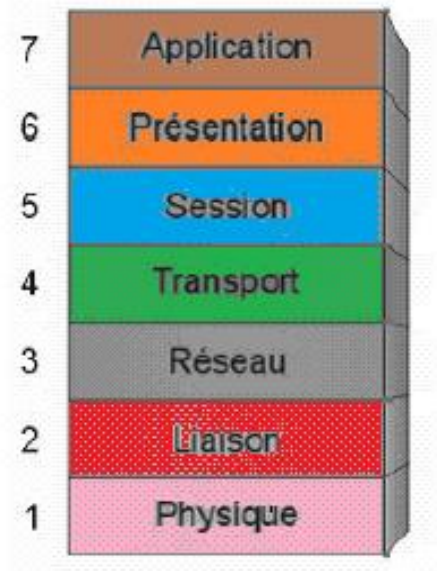


Figure I.11: modèle de référence ISO.

Encapsulation des données

Lors d'une transmission, les données traversent chacune des couches au niveau de la machine émettrice. A chaque couche, une information est ajoutée au paquet de données, il s'agit d'un en-tête, ensemble d'informations qui garantissent la transmission. Au niveau de la machine réceptrice, lors du passage dans chaque couche, l'en-tête est lu, puis supprimé. Ainsi, à la réception, le message est dans son état original.

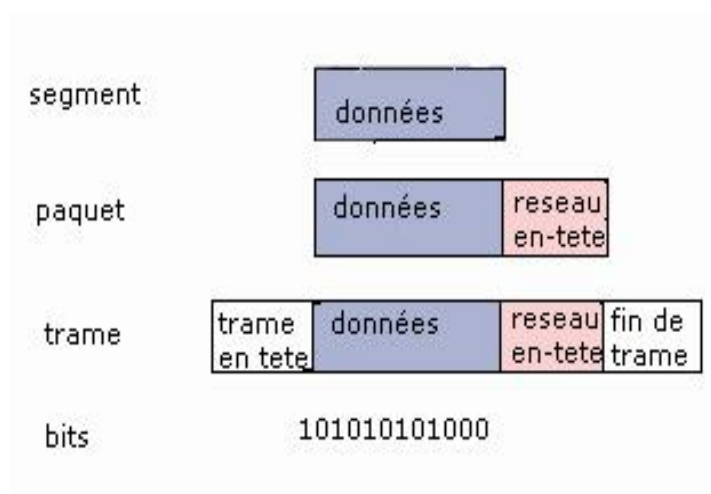


Figure I.12: principe d'encapsulation.

I.7.2 Modèle TCP/IP

TCP/IP représente l'ensemble des règles de communication sur Internet et se base sur la notion adressage IP, c'est-à-dire le fait de fournir une adresse IP à chaque machine du réseau afin de pouvoir acheminer des paquets de données.

TCP/IP est une suite de protocoles. TCP/IP signifie «Transmission Control Protocol/Internet Protocol».

TCP (*Transmission Control Protocol*). Ce protocole a en charge le découpage du message en datagrammes, le réassemblage à l'arrivée avec remise dans le bon ordre, ainsi que la réémission de ce qui a été perdu.

IP (*Internet Protocol*). Il assure le routage des datagrammes.

Les logiciels TCP/IP sont structurés en quatre couches de protocoles qui s'appuient sur une couche matérielle (Figure I.13).

- ❖ **La couche accès réseau** : est l'interface avec le réseau et est constituée d'un driver du système d'exploitation et d'une carte d'interface de l'ordinateur avec le réseau.
- ❖ **La couche réseau ou couche IP** : (*Internet Protocol*) gère la circulation des paquets à travers le réseau en assurant leur routage. Elle comprend aussi les protocoles ICMP (*Internet Control Message Protocol*) et IGMP (*Internet Group Management Protocol*).
- ❖ **La couche transport** : assure tout d'abord une communication de bout en bout en faisant abstraction des machines intermédiaires entre l'émetteur et le destinataire. Elle s'occupe de réguler le flux de données et assure un transport fiable (données transmises sans erreur et reçues dans l'ordre de leur émission) dans le cas de TCP (*Transmission Control Protocol*) ou non fiable dans le cas de UDP (*User Datagram Protocol*).
- ❖ **La couche application** : est celle des programmes utilisateurs comme telnet (connexion à un ordinateur distant), FTP (*File Transfert Protocol*), SMTP (*Simple Mail Transfert Protocol*), etc.

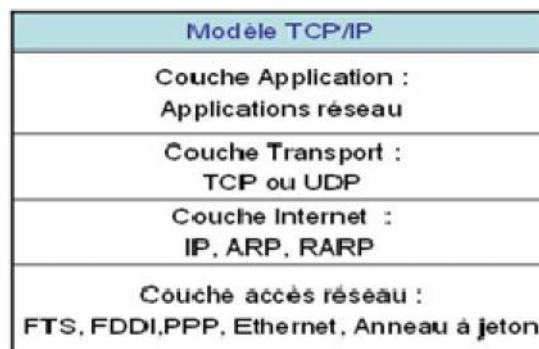


Figure I.13 : Modèle TCP/IP.

TCP/IP et le modèle OSI

Le modèle TCP/IP, inspiré du modèle OSI, reprend l'approche modulaire (utilisation de modules ou couches) mais en contient uniquement quatre couches comme suit :

Modèle TCP/IP	Modèle OSI
Couche Application	Couche Application
	Couche Présentation
	Couche Session
Couche Transport (TCP)	Couche Transport
Couche Internet (IP)	Couche Réseau
Couche Accès réseau	Couche Liaison données
	Couche Physique

Tableau I.2: Comparaison entre TCP/IP et modèle OSI.

Comme on peut le remarquer, les couches du modèle TCP/IP ont des tâches beaucoup plus diverses que les couches du modèle OSI, étant donné que certaines couches du modèle TCP/IP correspondent à plusieurs couches du modèle OSI.

I.7.3 Modèle ATM

La technologie ATM est très vaste et il recouvre l'ensemble de domaines de l'informatique, de la téléphonie et l'audiovisuel. Conçue à la base pour le transport simultané d'informations d'origines diverses, le réseau ATM permet de disposer de terminaux intégrés supportant l'ensemble des services de communication (Figure I.14).

Pour les réseaux privés d'entreprise, les utilisations actuelles recouvrent les nouvelles applications multimédias, la constitution d'un réseau fédérateur d'entreprise et l'interconnexion de sites en remplacement des multiplexeurs. Pour les réseaux d'opérateurs, la technologie ATM est utilisée pour constituer un réseau multiservice. Enfin elle sera utilisée dans des offres de vidéo à la demande.

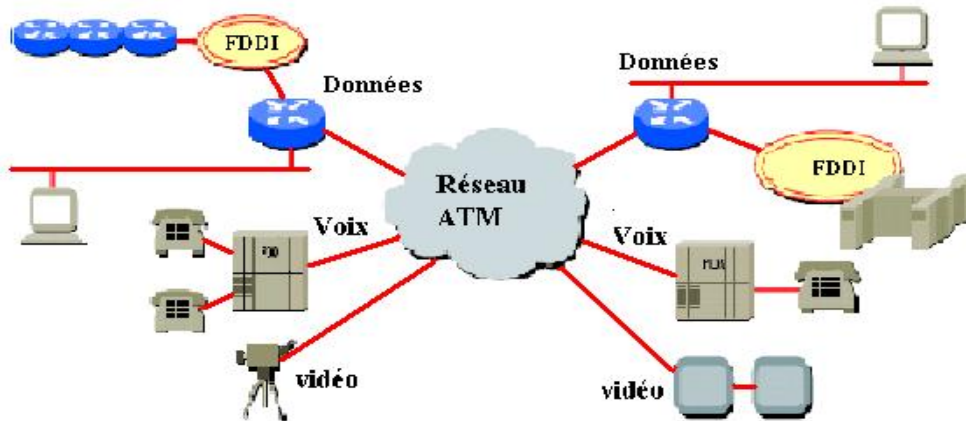


Figure I.14: Réseau ATM.

La technologie ATM possède trois caractéristiques majeures :

- ❖ C'est une technologie de commutation hybride entre la technique de commutation de circuit, utilisée dans le réseau téléphonique, et la technique de commutation de paquets utilisée dans les réseaux informatiques.
- ❖ C'est une technologie orientée de connexion puisque l'appel du correspondant est préalable au transfert des informations.
- ❖ Lors de cette phase d'appel, il y a une négociation de paramètres de trafic et de qualité de services qui se traduit par différentes possibilités d'acheminement de l'information, à la manière du courrier postal.

I.8 Dispositifs de communications

Les réseaux hétérogènes formant Internet sont reliés entre eux grâce à des dispositifs d'interconnexion (Passerelles, Routeurs, Ponts ...) qui assurent le transfert des données :

I.8.1 Les ponts

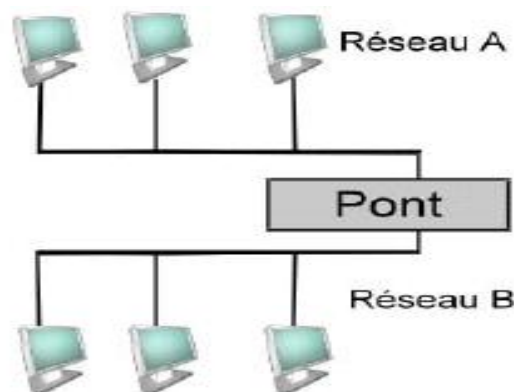


Figure I.15: Deux réseaux reliés avec un pont.

Ce sont des dispositifs matériels ou logiciels, permettant de relier des réseaux travaillant avec les mêmes protocoles. Le pont filtre les données et ne laisse passer que les données destinées aux ordinateurs situés de l'autre côté du pont (figure I.15).

Un pont possède deux connexions à deux réseaux distincts. Lorsqu'il reçoit un paquet de données sur l'une de ses interfaces, il analyse l'adresse physique (MAC) du destinataire et de l'émetteur. Si jamais le pont ne connaît pas l'émetteur, il stocke son adresse dans une table afin de savoir de quel côté du réseau se trouve l'émetteur.

Ainsi le pont est capable de savoir si l'émetteur et le destinataire sont situés du même côté ou bien de part et d'autre du pont. Dans le premier cas le pont ignore le message, dans le second le pont transmet la trame sur l'autre réseau.

I.8.2 Les Passerelles

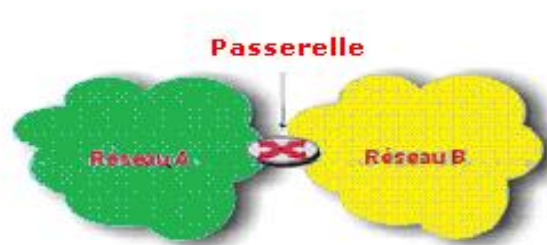


Figure I.16: deux réseaux reliés avec passerelle.

Ce sont des systèmes matériels et/ou logiciels permettant de faire des liaisons entre plusieurs réseaux de protocoles différents. L'information est codée et transportée différemment sur chacun des réseaux (Figure I.16).

Elles permettent aussi de manipuler les données afin de pouvoir assurer le passage d'un type de réseau à un autre. Les réseaux ne peuvent pas faire circuler la même quantité de données simultanément en terme de taille de paquet de données, mais la passerelle réalise cette transition en convertissant les protocoles de communication de l'un vers l'autre. Cette opération ralentie le transfert de données.

I.8.3 Les Routeurs

Ce sont des dispositifs matériels ou logiciels, permettant de choisir le chemin qu'un message doit emprunter. De plus, ils permettent de manipuler les données (qui circulent sous forme de datagrammes) afin de pouvoir assurer le passage d'un type de réseau à un autre (contrairement aux ponts). Ainsi, les réseaux ne peuvent pas faire circuler la même quantité simultanée d'information en terme de taille de paquets de données. Les routeurs ont donc la possibilité de fragmenter les paquets de données pour permettre leur circulation (figure I.17).

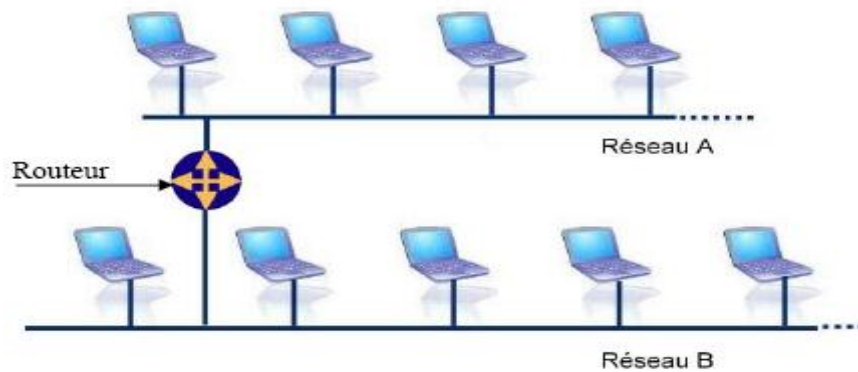


Figure I.17: Routeur connecté à deux réseaux locaux.

Ils fonctionnent grâce à des tables de routage et des protocoles de routage. Les routeurs intègrent souvent une fonction de passerelle leur permettant d'acheminer les paquets quelque soit l'architecture.

I.8.4 Les Hubs (concentrateurs)

Le Hub est également appelé concentrateur ou répéteur. C'est un boîtier électronique assurant la liaison des postes et des périphériques du réseau. Le répéteur se contente de transférer les ressources qui lui arrivent vers tous les autres éléments du réseau (dont le destinataire).

I.8.5 Le Switch

Le Switch est appelé Commutateur. C'est un Boîtier électronique assurant la liaison et l'optimisation des échanges entre les éléments du réseau. Contrairement au Hub, le switch est capable d'orienter les ressources vers leur unique destinataire sur le réseau. Le switch permet ainsi de libérer la bande passante en évitant le transfert de données inutiles sur le réseau.

I.9 Les protocoles de modèle OSI

I.9.1 Introduction

Un protocole est une méthode standard qui permet la communication entre deux machines c'est-à-dire un ensemble de règles et de procédures à respecter pour émettre et recevoir des données sur un réseau. Il en existe plusieurs selon ce que l'on attend de la communication. Certains protocoles seront par exemple spécialisés dans l'échange de fichiers (FTP), d'autres pourront servir à gérer simplement l'état de la transmission et des erreurs (protocole ICMP).

Dans le modèle OSI, on a l'ensemble de protocoles reliés entre eux par exemple :

a) Protocole TCP

Protocole sécurisé d'échange de données : créé dans le but d'établir une communication de haute fiabilité entre deux tâches exécutées sur deux ordinateurs autonomes et raccordés à un réseau (protocole orienté connexion).

b) Protocole UDP

Le protocole UDP (*User Data gram Protocol*) a été créé dans le but d'établir comme le TCP une communication entre deux ordinateurs mais il ne fournit pas de contrôle d'erreur (il n'est pas orienté connexion).

c) Protocole DNS

DNS (*Domain Name System*) est de permettre la mise en correspondance des adresses physiques dans le réseau et des adresses logiques. La structure logique est hiérarchique et utilise au plus haut niveau des domaines caractérisant principalement les pays, qui sont indiqués par deux lettres, comme *fr* pour la France, et des domaines fonctionnels comme :

• *com* : organisations commerciales ; • *gov* : gouvernement américain ...etc.

Il est difficile de se souvenir de 55.124.198.56 alors que *www.victim.com* sera assez aisé à mémoriser, C'est le but du protocole DNS : fournir une association (adresse IP, nom FQDN) et inversement.

Le service DNS est utilisé pour la « résolution de noms », Cette opération consiste à fournir aux clients DNS qui en font la demande une association adresse IP, un nom symbolique et vice-versa.

d) Protocole DHCP

Le protocole DHCP (*Dynamic Host Configuration Protocol*) attribue automatiquement des adresses IP aux équipements branchés au réseau. Lorsqu'un client essaie de se brancher au réseau, une demande de paramètres de configuration est envoyée au serveur DHCP. Une fois que le serveur a reçu le message, le protocole DHCP envoie une réponse au client, qui comprend les informations de configuration, puis enregistre en mémoire les adresses qui lui ont été attribuées. DHCP utilise le protocole *BOOTP* pour communiquer avec les clients. Les clients doivent renouveler leur adresse IP à 50 % de la période d'utilisation, puis de nouveau à 87,5 %, en envoyant un message *DHCPREQUEST*.

e) Protocole FTP

Le protocole FTP (*File Transfer Protocol*) est un protocole de transfert de fichier. La mise en place du protocole FTP date de 1971, date à laquelle un mécanisme de transfert de fichiers (décrit dans le RFC 141) entre les machines du MIT (*Massachusetts Institute of Technology*) avait été mis au point.

f) Protocole HTTP

Le protocole HTTP (*Hyper Text Transfer Protocol*) est le protocole le plus utilisé sur Internet depuis 19909 était uniquement destinée à transférer des données sur Internet (en particulier des pages Web en HTML) et permet de transférer des messages avec des en-têtes codage.

g) Protocole ARP

Le protocole ARP a un rôle phare parmi les protocoles de la couche Internet de la suite TCP/IP, car il permet de connaître l'adresse physique d'une carte réseau correspondant à une adresse IP, c'est pour cela qu'il s'appelle Protocole de résolution d'adresse. Chaque machine connectée au réseau possède un numéro d'identification sur 48 bits. Ce numéro est un numéro unique qui est fixé dès la fabrication de la carte réseau en usine.

h) Protocole ICMP

Occasionnellement, un routeur ou un hôte destinataire peut avoir à communiquer vers l'émetteur du datagramme, par exemple, pour signaler une erreur de traitement du datagramme. C'est dans cette perspective qu'a été mis en place le protocole Internet Control Message Protocol (ICMP). Il s'appuie sur le support de base fourni par IP comme s'il s'agissait d'un protocole d'une couche supérieure.

i) Protocole IP

C'est lui qui gère la fragmentation des données lorsque par exemple une section du réseau admet une taille différente des paquets, Mais le rôle le plus important de ce protocole est d'acheminer les données à travers un ensemble de réseaux interconnectés grâce à la gestion des adresses IP.

I.9.2 Adressage IP

Chaque ordinateur du réseau Internet dispose d'une adresse IP unique codée sur 32 bits. Plus précisément, chaque interface dispose d'une adresse IP particulière.

En effet, un même routeur interconnectant 2 réseaux différents possède une adresse IP pour chaque interface de réseau. Une adresse IP est toujours représentée dans une notation décimale pointée constituée de 4 nombres (1 par octet) compris entre 0 et 255 et séparés par un point.

Plus précisément, une adresse IP est constituée d'une paire (id. de réseau, id. de machine) et appartient à l'une des classes : A, B, C, D ou E selon la valeur de son premier octet.

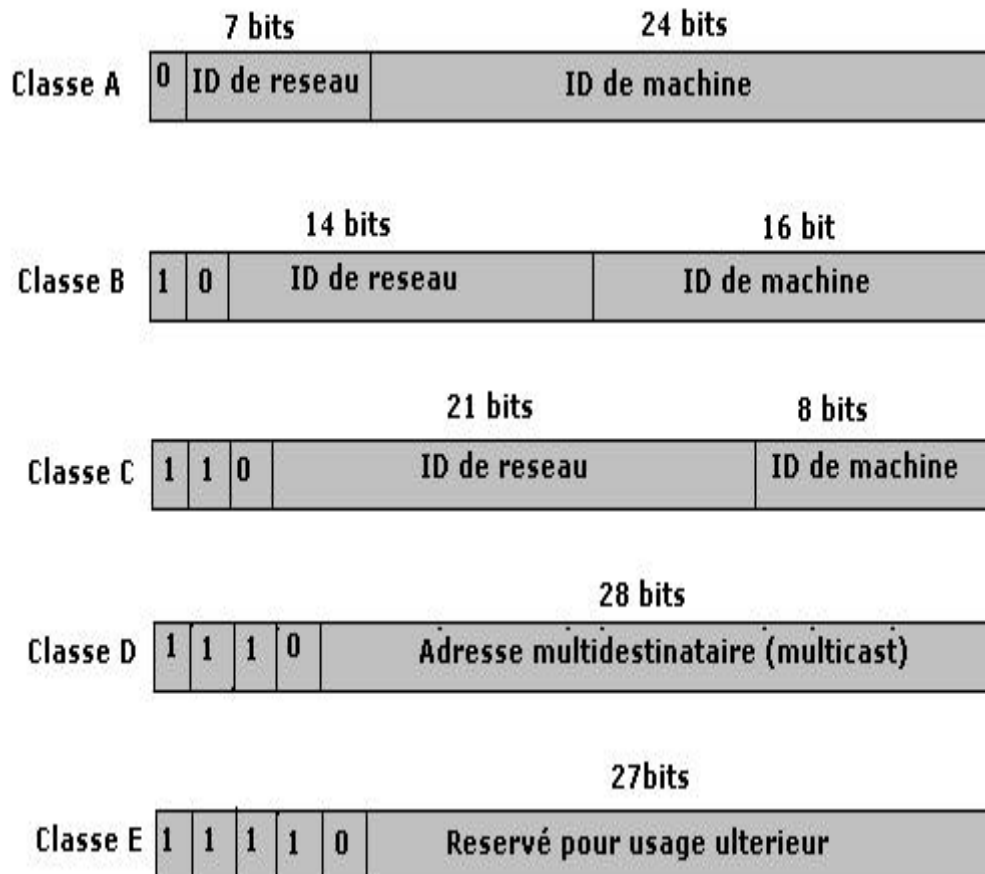


Figure I.18 : les cinq classes d'adresses IP.

Le tableau I.3 donne l'espace d'adresses possibles pour chaque classe :

Classe	Adresses
A	0. 0. 0. 0 à 127. 255. 255. 255
B	128. 0. 0. 0 à 191. 255. 255. 255
C	192. 0. 0. 0 à 223. 255. 255. 255
D	224. 0. 0. 0 à 239. 255. 255. 255
E	240. 0. 0. 0 à 247. 255. 255. 255

Tableau I.3: l'espace d'adresse.

Chapitre II

Protocoles de routage

II.1 Introduction aux protocoles de routage

Le protocole de routage permet à un routeur de partager avec d'autres routeurs des informations sur les réseaux qu'il connaît, ainsi que sur leur proximité avec d'autres routeurs. Les informations qu'un routeur reçoit d'un autre routeur, à l'aide d'un protocole de routage, servent à construire et à mettre à jour une table de routage.

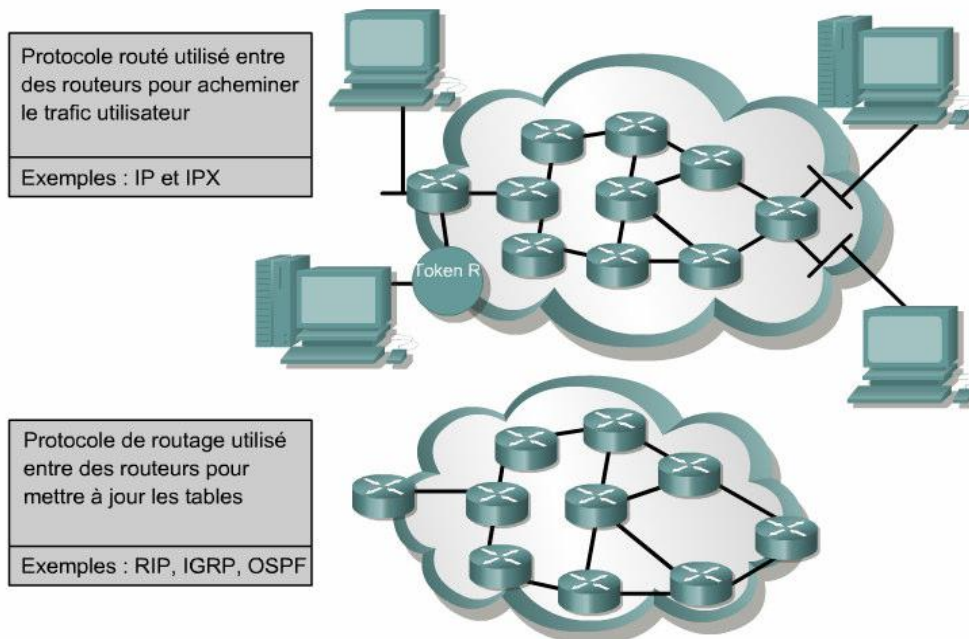


Figure II.1 : Présentation des protocoles de routage.

On a plusieurs protocoles de routage :

- ❖ Protocole d'informations de routage (RIP).
- ❖ Protocole IGRP (Interior Gateway Routing Protocol).
- ❖ Protocole EIGRP (Enhanced Interior Gateway Routing Protocol).
- ❖ Protocole OSPF (Open Shortest Path First).

II.1.1 Routage IP

Le routage est l'une des fonctionnalités principales de la couche IP et consiste à choisir la manière de transmettre un datagramme IP à travers les divers réseaux d'un internet. Ainsi un routeur réémettra des datagrammes venus d'une de ses interfaces vers une autre, alors qu'un ordinateur sera soit l'expéditeur initial, soit le destinataire final d'un datagramme. D'une manière générale on distingue le routage direct, qui correspond au transfert d'un datagramme entre deux ordinateurs du même réseau, et le routage indirect qui est mise en œuvre dans tous les autres cas, c'est-à-dire quand au moins un routeur sépare l'expéditeur initial et le destinataire final.

II.1.2 Méthodes de routage IP

a) Routage Direct

Le routage direct se produit quand la machine de destination se trouve sur le même réseau physique que la machine émettrice. Dans ce cas, un datagramme IP peut être émis directement, sans passer par un routeur, après avoir été en capsulé dans une trame correspondant au type du réseau local. C'est ce qu'on appelle la remise directe.

b) Routage Indirect

Si la machine de destination du datagramme ne se trouve pas sur le même réseau que la machine émettrice, il faut passer par un routeur. L'adresse de la première passerelle par laquelle il faut passer pour atteindre la destination est appelée la route indirecte.

En fait, la machine émettrice ne s'occupe pas de connaître le chemin complet jusqu'à la destination, elle doit juste connaître l'adresse de cette première passerelle.

Si la destination se trouve sur le même réseau physique mais sur un sous réseau différent, c'est le routage indirect qui sera utilisé. Ce qui implique qu'un routeur est nécessaire pour acheminer le trafic entre deux sous-réseaux.

Un routeur n'est pas nécessairement une machine séparée. Cela peut très bien être une station de travail ordinaire. Plusieurs cas de routage indirect peuvent se présenter :

b.1) Routage par table

Les machines communiquant avec TCP/IP possèdent une table de routage IP. Il s'agit d'un ensemble de correspondances entre une adresse de réseau IP et l'adresse de la première passerelle à emprunter. Quand une machine émet un datagramme, elle vérifie d'abord si l'adresse du réseau (pas de la machine) de destination est reprise dans cette table. Si c'est le cas, elle peut y lire l'adresse de la passerelle vers laquelle il faut envoyer le datagramme.

b.2) Routage par défaut

Si la table de routage IP ne contient aucune entrée faisant référence à la destination du datagramme, celui-ci est alors envoyé vers une passerelle dite passerelle par défaut (default Gateway), dont l'adresse est généralement stockée dans la table de routage.

II.2 Table de routage

La table de routage spécifique à chaque routeur qui permet de déterminer vers quelle voie de sortie envoyer un datagramme destiné à un réseau quelconque. Évidemment, à cause de la structure localement arborescente d'Internet la plupart des tables de routage ne sont pas très grandes. Par contre, les tables des routeurs interconnectant les grands réseaux peuvent atteindre des tailles très grandes ralentissant d'autant le trafic sur ces réseaux. D'un point de vue fonctionnel une table de routage contient des paires d'adresses du type (D, R) où D est l'adresse IP d'une machine ou d'un réseau de destination et R l'adresse IP du routeur suivant sur la route menant à cette destination.

II.3 Les critères des protocoles de routage

Les critères de routage s'appuient généralement sur les éléments suivants :

- ❖ **Longueur du trajet** : Définit un critère de décision à partir du nombre de liens qu'un paquet doit traverser pour se rendre du point d'origine au point de destination.
- ❖ **Fiabilité** : Définit un critère de décision fondé sur la fiabilité de chaque lien du réseau.
- ❖ **Délai de transmission** : Définit un critère de décision fondé sur le temps requis afin d'acheminer un paquet du point d'origine au point de destination.
- ❖ **Largeur de bande** : Définit un critère de décision fondé sur la capacité de transmission d'un lien.
- ❖ **Charge** : Définit un critère de décision fondé sur les ressources d'un routeur comme le nombre de paquets traités par seconde, ressource mémoire, etc.
- ❖ **Coût de la communication** : Définit un critère de décision fondé sur un coût appliqué à un lien.

II.4 Types de routage

II.4.1 Le routage statique

Une route donnée liée aux Routes statiques est dirigée par un administrateur. Cet itinéraire est similaire à une route statique car le chemin jusqu'à la destination est toujours le même et doit mettre à jour l'entrée liée à les routes statiques.

Les opérations de routage statique s'articulent par:

- ❖ L'administrateur réseau configure la route.
- ❖ Le routeur insère la route dans la table de routage.
- ❖ Les paquets sont acheminés à l'aide de la route statique.

II.4.1.1 Avantages et inconvénients du routage statique

a) Avantages du routage statique

- ❖ Plus facile à comprendre par l'administrateur.
- ❖ La configuration est simple.
- ❖ Effectue des traitements sur le processeur minimal.

b) Inconvénients du routage statique

- ❖ La configuration et la maintenance posées un problème de temps.
- ❖ Des risques d'erreurs sur la configuration, surtout dans les grands réseaux.
- ❖ L'intervention de l'administrateur est requise pour assurer la mise à jour des informations relatives aux routes.

II.4.2 Le Routage à système autonome

Un système autonome est un ensemble de réseaux gérés par un administrateur commun et partageant une stratégie de routage commune (figure II.2). Pour le monde extérieur, un système autonome est perçu comme une entité unique. Il peut être exécuté par un ou plusieurs opérateurs tout en présentant au monde extérieur une vue cohérente du routage.

L'InterNIC (Internet Network Information Center), un fournisseur de services ou encore un administrateur attribue un numéro d'identification à chaque système autonome. Ce numéro est un nombre à 16 bits. Les protocoles de routage, tels que l'IGRP de Cisco, nécessitent l'attribution d'un numéro de système autonome unique.

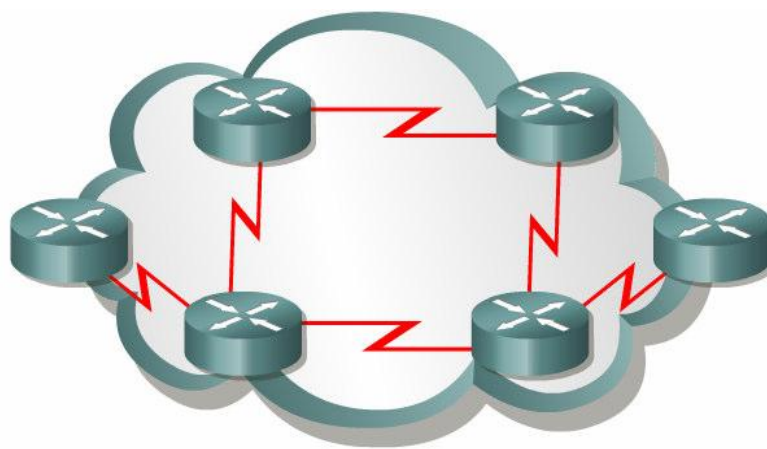


Figure II.2 : Routeurs sous administrateur commune.

II.4.3 Le Routage dynamique

Utilise une route qu'un protocole de routage modifie automatiquement en fonction de changements de topologie ou de trafic, Les informations permettent aux routeurs de découvrir de nouveaux réseaux et également de trouver d'autres chemins en cas d'échec d'un lien vers un réseau actif.

II.4.3.1 Avantages et inconvénients du routage dynamique

a) Avantages du routage dynamique

- ❖ la maintenance de la configuration est simplifiée pour l'administrateur lors de l'ajout et de la suppression de réseaux.
- ❖ plus évolutif, l'expansion du réseau ne présente généralement pas de problème.
- ❖ les protocoles réagissent automatiquement aux modifications topologiques.
- ❖ la configuration présente moins de risques d'erreurs.

b) Inconvénients du routage dynamique

- ❖ les ressources du routeur sont utilisées cycle de processeur, mémoire et bande passante du lien...etc.
- ❖ la configuration dispose plus de connaissances par l'administrateur, le dépannage et la contrôle.

II.5 Fonctionnement des protocoles de routage dynamique

Le schéma de la figure II.3 montre comment le protocole de routage dynamique construit et met à jour la table de routage.

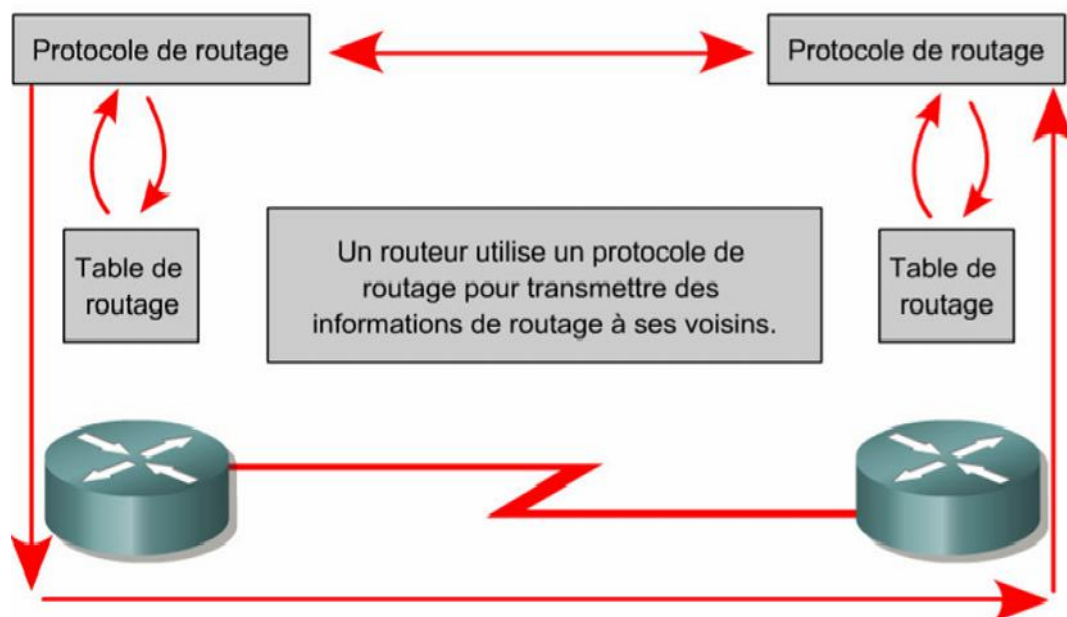


Figure II.3 : Fonctionnement du routage dynamique.

Le fonctionnement d'un protocole de routage dynamique peut être décrit de la manière suivante :

- ❖ Le routeur envoie et reçoit des messages de routage sur ses interfaces.
- ❖ Le routeur partage les messages et les informations de routage avec d'autres routeurs qui utilisent le même protocole de routage.
- ❖ Les routeurs échangent des informations de routage pour découvrir des réseaux distants.
- ❖ Lorsqu'un routeur détecte une modification de topologie, le protocole de routage peut l'annoncer aux autres routeurs.

On peut définir les composants d'un protocole de routage :

- ❖ **Structures de données** : pour fonctionner, certains protocoles de routage utilisent des tables et/ou des bases de données. Ces informations sont conservées dans la mémoire vive.

- ❖ **Algorithme** : un algorithme est une liste précise d'étapes permettant d'accomplir une tâche. Les protocoles de routage utilisent des algorithmes pour faciliter l'échange d'informations de routage et déterminer le meilleur chemin d'accès.
- ❖ **Messages de protocoles de routage** : les protocoles de routage utilisent différents types de messages pour découvrir les routeurs voisins, échanger des informations de routage et effectuer d'autres tâches afin d'obtenir et de gérer des informations précises sur le réseau.

II.6 Les différents protocoles de routage dynamique

Les protocoles de routage peuvent être classés dans différents groupes selon leurs caractéristiques. Les protocoles de routage les plus couramment utilisés sont les suivants :

- ❖ **RIP** : Protocole de routage interne à vecteur de distance.
- ❖ **IGRP** : Protocole de routage interne à vecteur de distance de Cisco.
- ❖ **OSPF** : Protocole de routage intérieur à état de liaisons.
- ❖ **EIGRP** : Protocole de routage intérieur à vecteur de distance avancé de Cisco.
- ❖ **BGP** : Protocole de routage extérieur à vecteur de distance.

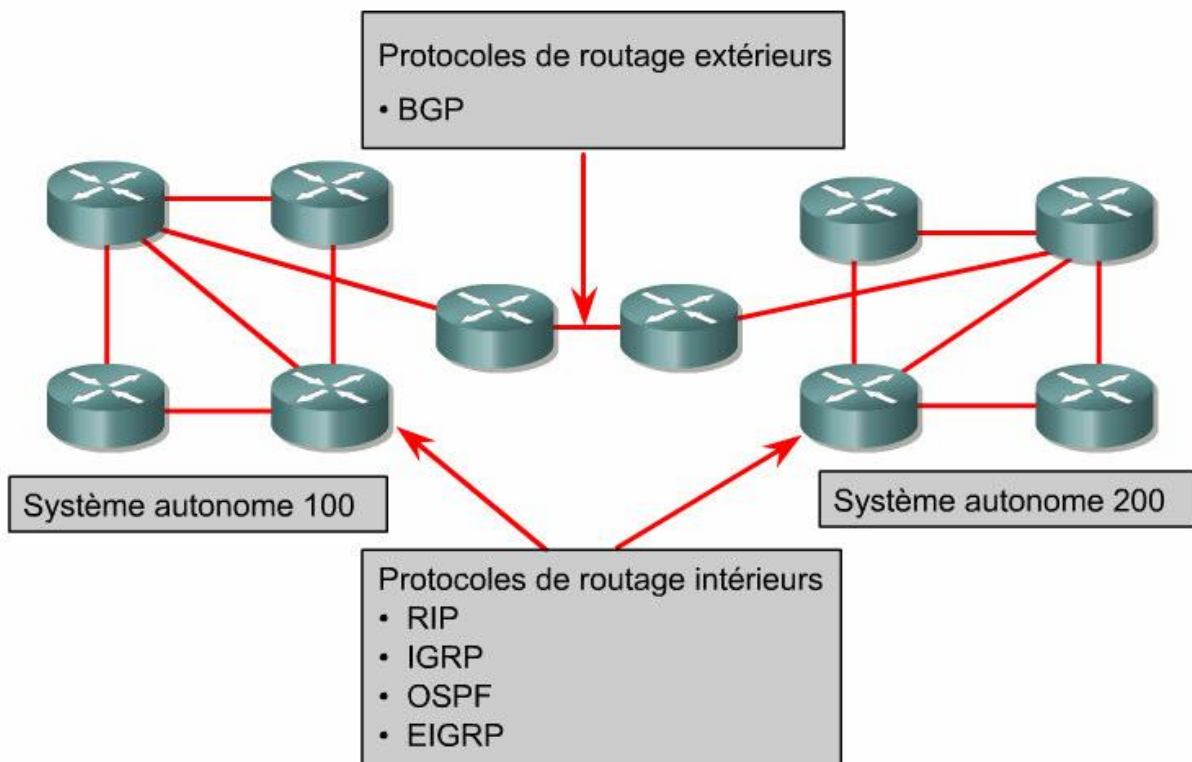


Figure II.4 : Classification des protocoles de routage dynamique.

Au niveau de la couche Internet de l'ensemble de protocoles de la pile TCP/IP, un routeur peut utiliser un protocole de routage IP pour réaliser le routage par la mise en œuvre d'un algorithme de routage particulier. Les protocoles suivants sont des exemples de protocoles de routage IP :

On peut définir les protocoles comme suit :

a) Protocole RIP : été initialement défini dans la RFC 1058. Ses principales caractéristiques sont les suivantes:

- ❖ Il s'agit d'un protocole de routage à vecteur de distance.
- ❖ Il utilise le nombre de sauts comme métrique pour la sélection du chemin.
- ❖ Si le nombre de sauts est supérieur à 15, le paquet est éliminé.
- ❖ Par défaut, les mises à jour du routage sont diffusées toutes les 30 secondes.

b) Protocole IGRP (Interior Gateway Routing Protocol) est un protocole propriétaire développée par Cisco. De par sa conception, le protocole IGRP est doté, entre autres, des caractéristiques suivantes:

- ❖ Il s'agit d'un protocole de routage à vecteur de distance.
- ❖ La bande passante, la charge, le délai et la fiabilité sont utilisés pour créer une métrique composite.
- ❖ Par défaut, les mises à jour du routage sont diffusées toutes les 90 secondes.

c) Protocole OSPF (Open Shortest Path First) est un protocole de routage à état de liens non propriétaire. Les caractéristiques clés de ce protocole sont les suivantes:

- ❖ Il s'agit d'un protocole de routage à état de liens.
- ❖ C'est un protocole de routage de norme ouverte décrit dans les requêtes pour commentaires RFC 2328.
- ❖ Il utilise l'algorithme SPF pour calculer le coût le plus bas vers une destination.
- ❖ Les mises à jour du routage sont diffusées à mesure des modifications de topologie.

d) Protocole EIGRP : est un protocole de routage à vecteur de distances améliorées et propriétaire développé par Cisco. Les caractéristiques clés de ce protocole sont les suivantes:

- ❖ Il s'agit d'un protocole de routage à vecteur de distance amélioré.
- ❖ Il utilise l'équilibrage de charge en coût différencié.
- ❖ Il utilise une combinaison de fonctions à vecteur de distance et à état de liens.
- ❖ Il utilise l'algorithme DUAL (Diffused Update Algorithm) pour calculer le chemin le plus court.
- ❖ Les mises à jour du routage sont diffusées en mode multicast en utilisant l'adresse 224.0.0.10 et sont déclenchées par des modifications topologiques.

e) Protocole BGP (Border Gateway Protocol) est un protocole de routage extérieur. Les caractéristiques clés de ce protocole sont les suivantes:

- ❖ Il s'agit d'un protocole de routage extérieur à vecteur de distance.
- ❖ Il est utilisé pour la connexion entre les FAI ou entre les FAI et les clients.
- ❖ Il est utilisé pour acheminer le trafic Internet entre des systèmes autonomes.

II.7 Les fonctions de base des protocoles de routage

En règle générale, un routeur détermine le chemin que doit emprunter un paquet entre deux liaisons à l'aide des deux fonctions de base suivantes:

- ❖ la détermination du chemin.
- ❖ la commutation.

II.7.1 La Détermination du chemin

La détermination du chemin se produit au niveau de la couche réseau. La fonction de détermination de chemin permet à un routeur d'évaluer les chemins vers une destination donnée et de définir le meilleur chemin pour traiter un paquet. Le routeur se sert de la table de routage pour déterminer le meilleur chemin et transmet ensuite le paquet en utilisant la fonction de commutation.

II.7.2 La commutation

La fonction de commutation est le processus interne qu'utilise un routeur pour accepter un paquet sur une interface et le transmettre à une deuxième interface sur le même routeur. La fonction de commutation a pour responsabilité principale d'encapsuler les paquets dans le type de trame approprié pour la prochaine liaison.

Le routeur utilise la portion réseau de l'adresse pour sélectionner le chemin qui permettra de transmettre le paquet au prochain routeur situé sur le chemin et une fois arrivé au routeur local, il utilise la partie hôte pour déterminer le port vers lequel envoyer le paquet.

II.8 L'objectif des protocoles de routage dynamique

Les protocoles de routage sont utilisés pour faciliter l'échange d'informations de routage entre des routeurs. Ils permettent aux routeurs de partager de manière dynamique des informations sur les réseaux distants et d'ajouter automatiquement ces informations à leurs propres tables de routage.

Les protocoles de routage déterminent le meilleur chemin vers chaque réseau, lequel est ensuite ajouté à la table de routage. L'un des principaux avantages de l'utilisation d'un protocole de routage dynamique est l'échange d'informations de routage entre des routeurs dès lors qu'une topologie est modifiée.

Les protocoles de routage dynamique requièrent une charge administrative moindre. Toutefois, l'utilisation de protocoles de routage dynamique implique qu'une partie des ressources d'un routeur est dédiée au fonctionnement du protocole.

II.9 Les protocoles de routage à vecteurs à distances et l'état de liaisons

II.9.1 Fonctionnement des protocoles de routage à vecteur de distance

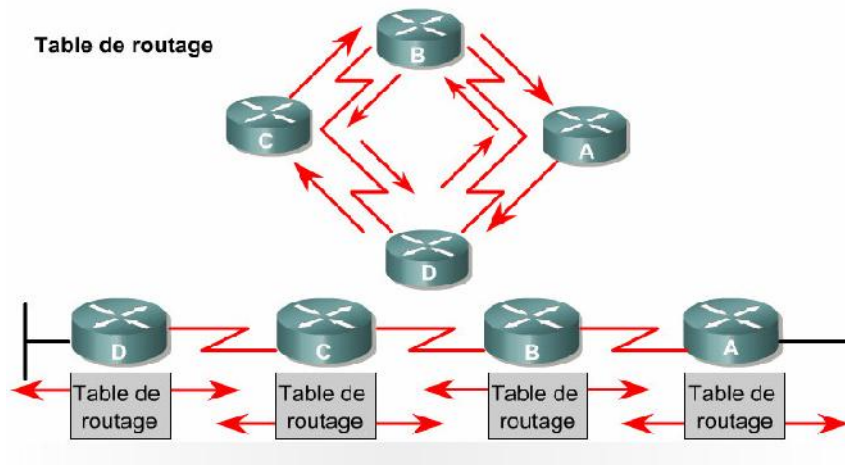


Figure II.5 : Table de routage aux routeurs voisins et cumul des vecteurs de distance.

Les algorithmes de routage à vecteur de distance transmettent régulièrement des copies de table de routage d'un routeur à l'autre (Figure II.5). Ces mises à jour régulières entre les routeurs permettent de communiquer les modifications topologiques. Les algorithmes de routage à vecteur de distance sont également appelés algorithmes Bellman-Ford.

Chaque routeur reçoit une table de routage des routeurs voisins auxquels il est directement connecté. Le routeur B reçoit des informations du routeur A. Le routeur B ajoute un nombre de vecteurs (par exemple, un nombre de sauts) qui allonge le vecteur de distance. Ensuite, le routeur B transmet la nouvelle table de routage à son voisin, le routeur C. La même procédure est répétée étape par étape dans toutes les directions entre les routeurs directement adjacents.

L'algorithme cumule les distances afin de tenir à jour la base de données contenant les informations sur la topologie du réseau. Cependant, les algorithmes de routage à vecteur de distance ne permettent pas à un routeur de connaître la topologie exacte d'un inter réseau, étant donné que chaque routeur voit uniquement ses voisins.

II.9.2 Fonctionnement des protocoles à état de liaisons

Les routeurs à état de liens utilisent une « carte » identique du réseau. Un routeur à état de liens utilise les informations d'état de liens pour créer une topologie et sélectionner le meilleur chemin vers tous les réseaux de destination de la topologie.

Avec certains protocoles de routage à vecteur de distance, les routeurs envoient des mises à jour régulières de leurs informations de routage à leurs voisins. Les protocoles de routage à état de liens n'utilisent pas de mises à jour régulières. Une fois que le réseau a convergé, une mise à jour d'état de liens est envoyée uniquement en cas de modification de la topologie.

Avec l'algorithme de Dijkstra ou algorithme SPF (shortest path first ou du plus court chemin d'abord). Ils gèrent une base de données complexe d'informations topologiques.

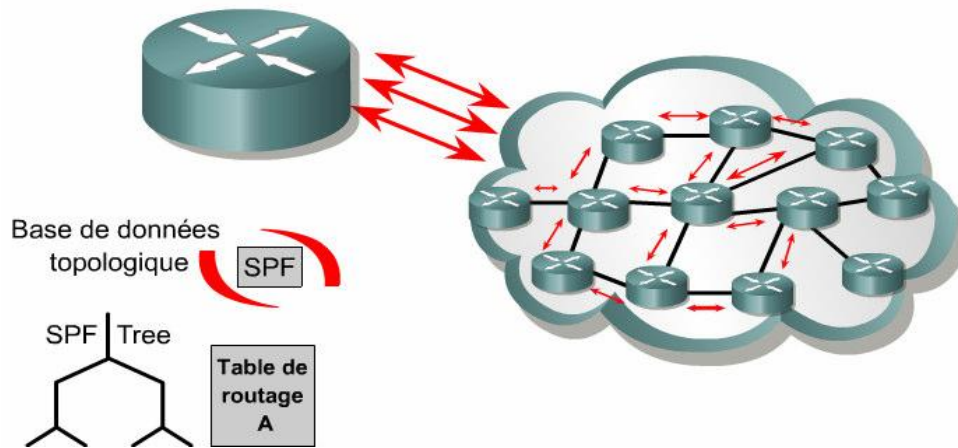


Figure II.6 : Fonctionnement des protocoles à état de liaisons.

Les protocoles à état de liaisons sont tout particulièrement adaptés dans les situations suivantes :

- ❖ réseau conçu de manière hiérarchique (il s'agit généralement de grands réseaux).
- ❖ administrateurs ayant une bonne connaissance du protocole de routage à état de liaisons implémenté.
- ❖ réseau pour lequel une convergence rapide est primordiale.

Les protocoles de routage à état de liaisons nécessitent davantage de mémoire et de capacités de calcul que les protocoles de routage à vecteur de distance. Les routeurs doivent disposer d'une mémoire suffisante pour stocker toutes les informations des différentes bases de données, l'arbre topologique et la table de routage.

II.10 Métriques et protocoles de routage

II.10.1 Paramètres de métrique

Les métriques utilisées par les protocoles de routage varient en fonction du protocole. La métrique utilisée par un protocole de routage n'est pas comparable à celle utilisée par un autre protocole. Deux protocoles de routage peuvent choisir des chemins différents avec une même destination par les métriques identifiées.

Le protocole RIP choisit le chemin impliquant le moins de sauts, tandis que le protocole OSPF choisit celui qui présente la bande passante la plus élevée.

Les métriques suivantes sont utilisées dans les protocoles de routage IP :

- ❖ **Fiabilité** : est la variation de la probabilité d'échec d'un lien, calculée à partir du nombre d'erreurs de l'interface ou des défaillances du lien.
- ❖ **Nombre de sauts** : métrique simple qui compte le nombre de routeurs.
- ❖ **Coût** : est la valeur déterminée par l'IOS ou par l'administrateur réseau et le Coût peut représenter une métrique, une combinaison de métriques ou une stratégie.

- ❖ **Bande passante** : est la sélection du chemin en préférant celui dont la bande passante est la plus élevée.
- ❖ **Charge** : est l'utilisation d'un lien spécifique en termes de trafic.
- ❖ **Délai** : est le temps nécessaire à un paquet pour parcourir un chemin.

II.10.2 Champ de métrique dans la table de routage

Métrique utilisée par chacun des protocoles de routage :

- ❖ **IGRP et EIGRP** : Délai, Charge, bande passante et la Fiabilité. Le meilleur chemin est la route présentant la plus petite valeur de métrique composite, calculée à partir de ces différents paramètres. Par défaut, seuls la bande passante et le délai sont utilisés.
- ❖ **OSPF** : leur coût est le meilleur chemin est la route associée au coût le plus faible.
- ❖ **RIP** : nombre de sauts. Le meilleur chemin est la route présentant le nombre de sauts le plus faible.

II .11 Comparaison des protocoles de routage dynamique

On peut comparer les protocoles de routages de vecteur à distance et à l'état de liaisons par la table suivante :

protocoles à vecteur distance	protocoles à état de liaison
Un routeur connaît ses voisins uniquement lors de la transmission de mise à jour de leur part.	Chaque routeur doit connaître ses voisins avant d'échanger des informations.
Les routeurs envoient des mises à jour régulières de leurs informations de routage à leurs voisins.	Les protocoles de routage à état de liens n'utilisent pas de mises à jour régulières, La mise à jour est envoyée uniquement en cas de modification de la topologie.
un routeur à vecteur de distance fait confiance à un autre routeur pour lui indiquer la distance réelle jusqu'au réseau de destination.	les routeurs à état de liens utilisent une carte pour déterminer leur chemin préféré vers une autre destination.
Temps de convergence est Lent à cause de la détection des boucles.	Temps de convergence est plus rapide.
Les protocoles à vecteur distance est un Protocole publique (RIP) ou propriétaire (IGRP).	Les protocoles à l'état de liaison est seulement publique (OSPF).

Tableau II.1 Comparaison des protocoles de vecteur à distance et l'état de liaison.

II. 12 Identification des classes des protocoles de routage dynamique

La plupart des algorithmes de routage peuvent être rangés dans l'une des catégories suivantes:

- ❖ vecteur de distance.
- ❖ état de liaisons.

Le routage à vecteur de distance détermine la direction (vecteur) et la distance jusqu'à une liaison quelconque de l'inter réseau.

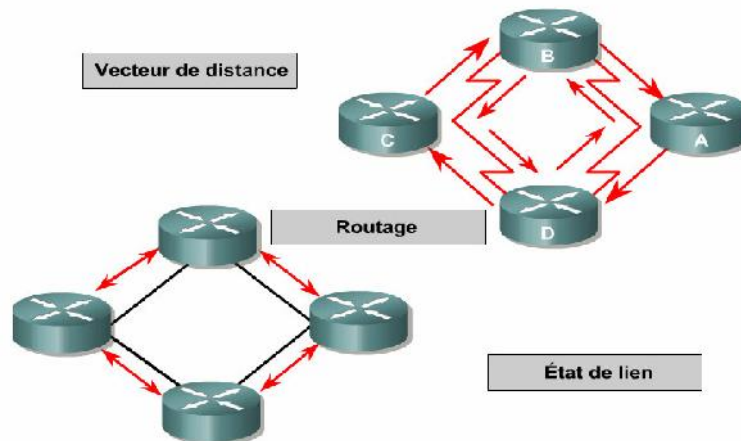


Figure II.7 : Présentation des classes des protocoles de routage dynamique.

L'approche à état de liaison, également appelée routage par le chemin le plus court, recrée la topologie exacte de l'intégralité du réseau (tient compte de la qualité des liaisons).

II.13 Convergence des protocoles de routage

Il y a convergence si les tables de routage de tous les routeurs sont cohérentes. Le réseau a convergé lorsque tous les routeurs disposent d'informations complètes et précises sur le réseau. Le temps de convergence est le temps nécessaire aux routeurs pour partager des informations, calculer les meilleurs chemins et mettre à jour leurs tables de routage. Un réseau n'est pas complètement opérationnel tant qu'il n'a pas convergé.

Les routeurs partagent des informations les uns avec les autres, mais doivent calculer chacun de leur côté l'impact des modifications de la topologie sur leurs propres routes donc La convergence est à la fois collaborative et indépendante.

Les propriétés de convergence incluent la vitesse de propagation des informations de routage et le calcul des chemins optimaux. Les protocoles de routage peuvent être classés en fonction de leur vitesse de convergence : une convergence rapide améliore un protocole de routage.

Chapitre III

*Protocoles de routage
Dynamique à l'état de liaisons*

Chapitre III protocoles de routage dynamique à l'état de liaisons

III.1 Introduction

Les protocoles de routage à état de liaisons suivent une approche différente. Ils ressemblent plutôt à une carte routière, car ils créent une carte topologique du réseau et chaque routeur utilise cette carte pour déterminer le chemin le plus court vers chaque réseau.

Les routeurs qui exécutent un protocole de routage à état de liaisons envoient des informations sur l'état de leurs liens vers d'autres routeurs du domaine de routage. L'état de ces liaisons concerne les réseaux qui leurs sont connectés directement et contiennent des informations sur le type de réseau et tous les routeurs de voisinage, d'où le nom de protocole de routage à état de liaisons.

L'objectif ultime est que chaque routeur reçoit les informations d'état de liaisons de tous les autres routeurs de la zone de routage. Avec ces informations, chaque routeur peut créer sa propre carte topologique du réseau et calculer de façon indépendante le chemin le plus court vers chacun des réseaux.

III.2 Présentation des Protocoles de routage à état de liaisons

Les protocoles de routage à état de liaisons sont également appelés *protocoles SPF (Shortest Path First)*, car ils sont conçus sur la base de l'algorithme SPF d'Edsger Dijkstra.

Les protocoles de routage à état de liaisons IP sont présentés dans la figure II.1 :

- protocole OSPF.
- protocole de routage IS-IS.

	Protocoles IGP		Protocoles EGP
	Protocoles de routage à vecteur de distance		Vecteur de chemin
	Protocoles de routage à état de liens		
Protocoles par classe	RIP	IGRP	EGP
Protocoles sans classe	RIPv2	EIGRP	BGPv4
Protocoles IPv6	RIPng	EIGRP pour IPv6	BGPv4 pour IPv6

Figure III.1 : Les protocoles de routage à état de liaisons IP.

Chapitre III protocoles de routage dynamique à l'état de liaisons

Les protocoles de routage à état de liaisons ont la réputation d'être beaucoup plus complexes que leurs équivalents à vecteur de distance. Les opérations OSPF de base peuvent être configurées à l'aide d'une commande **router ospf process-id** et d'une instruction **network**, comme pour les autres protocoles de routage de type RIP et EIGRP.

III.3 Les éléments utilisés pour le routage à état de liaisons

- ❖ **Mises à jour de routage à état de liaisons (LSA) :** Une mise à jour de routage à état de liaisons LSA (Link-State Advertisements) est un petit paquet d'informations de routage qui est transmis entre les routeurs.
- ❖ **Base de données topologique :** Une base de données topologique est un ensemble d'informations rassemblées à partir des mises à jour de routage à état de liaisons.
- ❖ **Algorithme SPF :** L'algorithme du plus court chemin d'abord (SPF) est un calcul effectué sur la base de données qui génère un arbre SPF.
- ❖ **Tables de routage :** Une liste des chemins et des interfaces connus.

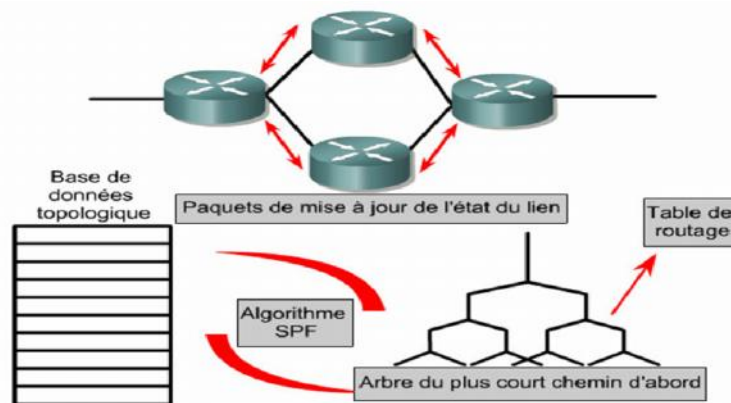


Figure III.2 : présentation des éléments de routage à état de liaisons.

Les routeurs envoient des LSA à leurs voisins. Les LSA sont utilisées pour créer une base de données topologique. L'algorithme SPF est fait pour calculer l'arbre du plus court chemin d'abord dans lequel la racine est le routeur lui-même et une table de routage est ensuite créée.

III.4 Fonctions du protocole de routage à état de liaisons

Les protocoles de routage à état de liens sont également appelés *protocoles SPF (Shortest Path First)* ou du plus court chemin d'abord, car ils sont conçus sur la base de l'algorithme de protocole SPF, ils gèrent une base de données complexe d'informations topologiques. L'algorithme à vecteur de distance comprend des informations non spécifiques sur les réseaux distants et ne fournit aucune information sur les routeurs distants. Un algorithme de routage à état de liaisons gère une base de connaissances complète sur les routeurs distants et leurs interconnexions.

III.4.1 Présentation de l'algorithme SPF

L'algorithme de Dijkstra est en général désigné sous le nom d'algorithme SPF (shortest path first - chemin le plus court). Cet algorithme cumule les coûts de chaque chemin, depuis leur source jusqu'à leur destination. Dans le schéma III.3, chaque chemin est étiqueté avec une valeur de coût arbitraire. Le coût du plus court chemin pour que R2 envoie un paquet au réseau local rattaché à R3 est de 29. Chaque routeur entre d'eux détermine son propre coût vers chaque destination de la topologie.

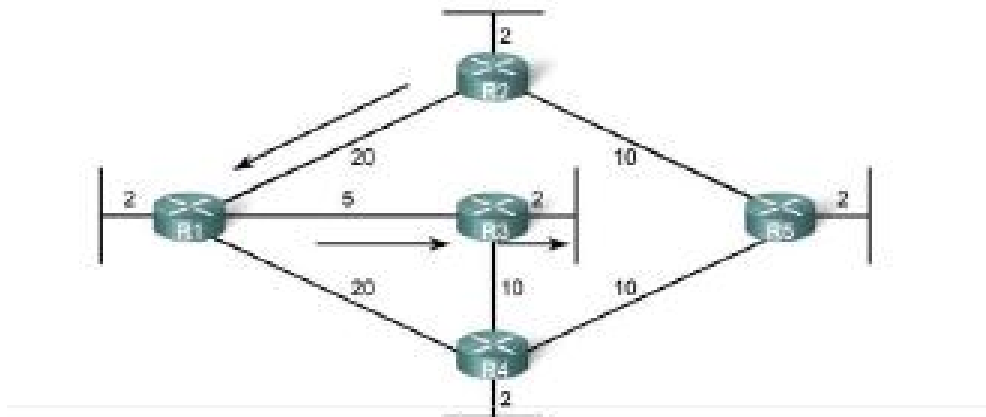


Figure III.3 : fonctionnement de l'algorithme SPF.

Dans le routeur R1, le chemin le plus court vers chaque réseau local, ainsi que son coût, s'affiche dans le tableau III.1. Le chemin le plus court n'est pas nécessairement celui qui comporte le moins de sauts. Par exemple, on regarde le chemin vers le réseau local R5. On peut penser que R1 enverrait directement vers R4 si non vers R3 et on obtient les résultats :

Destination	Chemin le plus court	Coût
Réseau local de R2	R1 à R2	22
Réseau local de R3	R1 à R3	7
Réseau local de R4	R1 à R3 à R4	19
Réseau local de R5	R1 R3 à R5	31

Tableau III.1 résultats des paramètres d'un routeur R1.

R2 jusqu'à R5.

On observe le chemin le plus court de chaque routeur pour atteindre chaque réseau local, comme indiqué dans les tables suivantes :

Chapitre III protocoles de routage dynamique à l'état de liaisons

Pour R2, on aura : **Tableau III.2 résultats des paramètres d'un routeur R2.**

Destination	Chemin plus court	Coût
Réseau local de R1	R2 à R1	22
Réseau local de R3	R1 à R3	7
Réseau local de R4	R2 à R5 à R4	24
Réseau local de R5	R2 à R5	12

Pour R3, on aura : **Tableau III.3 résultats des paramètres d'un routeur R3.**

Destination	Chemin plus court	Coût
Réseau local de R1	R3 à R1	7
Réseau local de R2	R3 à R1 à R2	29
Réseau local de R4	R3 à R4	12
Réseau local de R5	R3 à R4 à R5	24

Pour R4, on aura : **Tableau III.4 résultats des paramètres d'un routeur R4.**

Destination	Chemin plus court	Coût
Réseau local de R1	R4 à R3 à R1	19
Réseau local de R2	R4 à R5 à R2	24
Réseau local de R3	R4 à R3	12
Réseau local de R5	R4 à R5	12

Pour R5, on aura : **Tableau III.5 résultats des paramètres d'un routeur R5.**

Destination	Chemin plus court	Coût
Réseau local de R1	R5 à R4 à R1	34
Réseau local de R2	R5 à R2	12
Réseau local de R3	R5 à R4 à R3	24
Réseau local de R4	R5 à R4	12

III.4.2 Processus de découverte du réseau pour le routage à état de liaisons

Les mises à jour de routage à état de liens sont échangées entre routeurs en commençant par les réseaux directement connecté. Parallèlement à ses homologues, chaque routeur génère une base de données topologique comprenant toutes les mises à jour de routage à état de liens échangées.

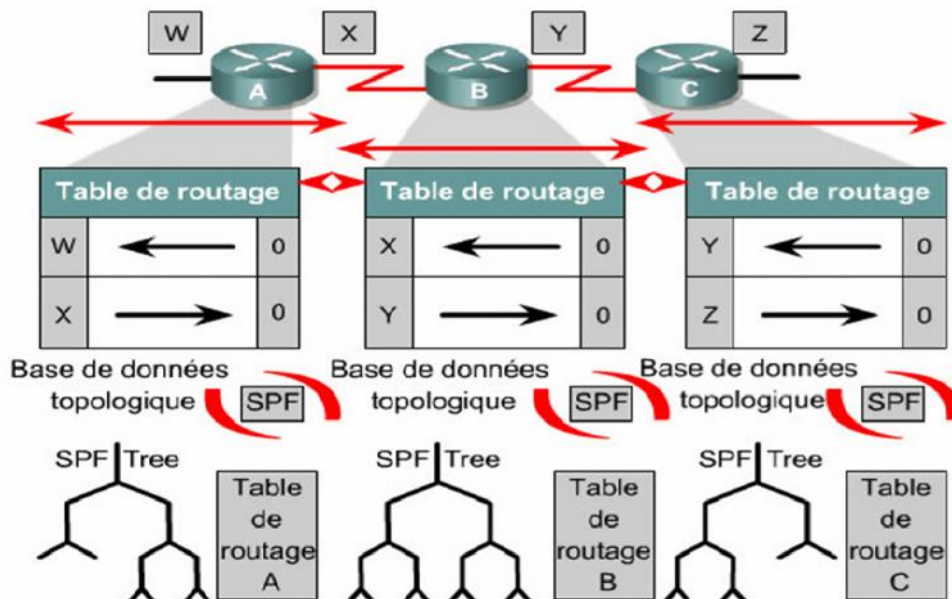


Figure III.4 : la base donnée topologique de chaque routeur avec SPF.

L'algorithme du plus court chemin d'abord (SPF) calcule l'accessibilité aux Réseaux.

Les routeurs de cette topologie vont effectuer le processus de routage à état de liens générique qui suit pour atteindre un état de convergence :

- ❖ Chaque routeur prend connaissance des réseaux qui lui sont connectés directement. Cette opération s'effectue en détectant qu'une interface se trouve dans l'état de microprocesseur.
- ❖ Chaque routeur est responsable de la détection de ses voisins sur les réseaux connectés directement. Comme avec le protocole EIGRP, les routeurs à état de liens effectuent cette détection en échangeant des paquets Hello avec d'autres routeurs à état de liens situés sur des réseaux connectés directement.
- ❖ Chaque routeur construit un paquet à état de liens LSP (Link-State Packet) contenant l'état de chacun des liens connectés directement. Il procède en enregistrant toutes les informations pertinentes sur chaque voisin, notamment l'ID du voisin, le type de lien et la bande passante.
- ❖ Chaque routeur diffuse le LSP à tous ses voisins, qui stockent l'ensemble des paquets LSP reçus dans une base de données. Les voisins diffusent ensuite le LSP à leurs voisins, jusqu'à ce que tous les routeurs de la zone aient reçu le LSP. Chaque routeur stocke une copie de chaque LSP reçu de ses voisins dans une base de données locale.
- ❖ Chaque routeur utilise la base de données pour élaborer une carte complète de la topologie et calcule le meilleur chemin vers chaque réseau de destination. Le routeur

Chapitre III protocoles de routage dynamique à l'état de liaisons

possède ainsi une carte complète s'apparentant à une carte routière de l'ensemble des destinations de la topologie et des routes pour les atteindre. L'algorithme SPF sert à construire la carte de la topologie et à déterminer le meilleur chemin vers chaque réseau.

III.4.3 Topologie logique de protocoles de routage à état de liaisons

Le routeur génère cette topologie logique sous la forme d'un arbre dont il est la racine et qui comporte tous les chemins possibles menant à chaque réseau de l'inter réseau utilisant le protocole à état de liaisons. Ensuite, il trie ces chemins sur la base du chemin le plus court. Le routeur répertorie dans sa table de routage les meilleurs chemins et les interfaces menant aux réseaux de destination. Il met également à jour d'autres bases de données contenant des éléments de topologie et les détails relatifs à leur état.

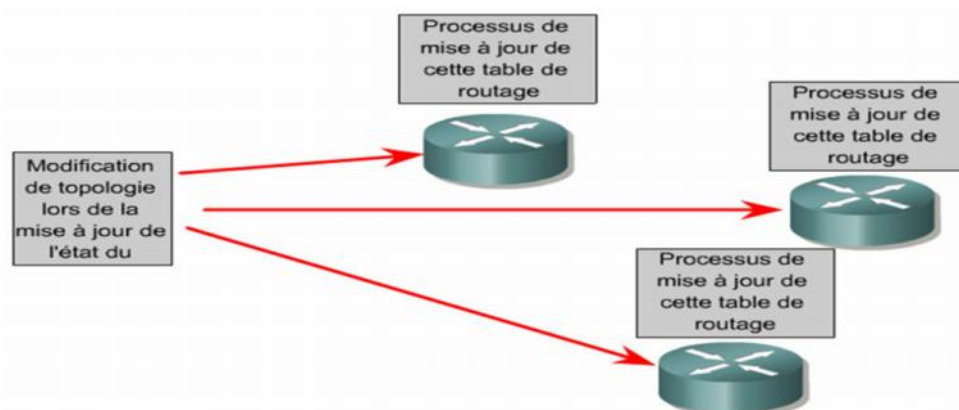


Figure III.5 : modification topologique et mise à jour d'une table de routage.

Le premier routeur informé de la modification de la topologie d'état de liaisons transmet l'information pour que tous les autres routeurs puissent l'utiliser pour des mises à jour. Ainsi, les informations de routage communes sont envoyées à tous les routeurs de l'inter réseau. Pour atteindre la convergence, chaque routeur effectue le suivi de ses routeurs voisins, Le routeur génère un paquet de mise à jour de routage (LSA) qui répertorie ces informations ainsi que les noms des nouveaux voisins, les modifications relatives aux coûts de liaison et les liaisons qui ne sont plus valides. Le paquet LSA est ensuite transmis à tous les autres routeurs.

Lorsque le routeur reçoit une LSA, la base de données est mise à jour avec les informations les plus récentes et il génère une carte de l'inter réseau à l'aide des données accumulées et détermine les routes vers tous les autres réseaux à l'aide de l'algorithme du plus court chemin d'abord. Chaque fois qu'un paquet de mise à jour de routage à état de liaisons entraîne une modification dans la base de données d'état de liaisons, l'algorithme du plus court chemin d'abord recalcule les meilleurs chemins et met à jour la table de routage.

III.5 Considérations relatives au routage à état de liaison

- ❖ Surcharge du système lors des calculs SPF.
- ❖ Mémoire requise à cause du nombre et de la taille des tables Consommation de bande passante lors du flux initial de LSA.
- ❖ Très peu de consommation de bande passante une fois que le système a convergé
- ❖ Convergence très rapide voire instantanée.

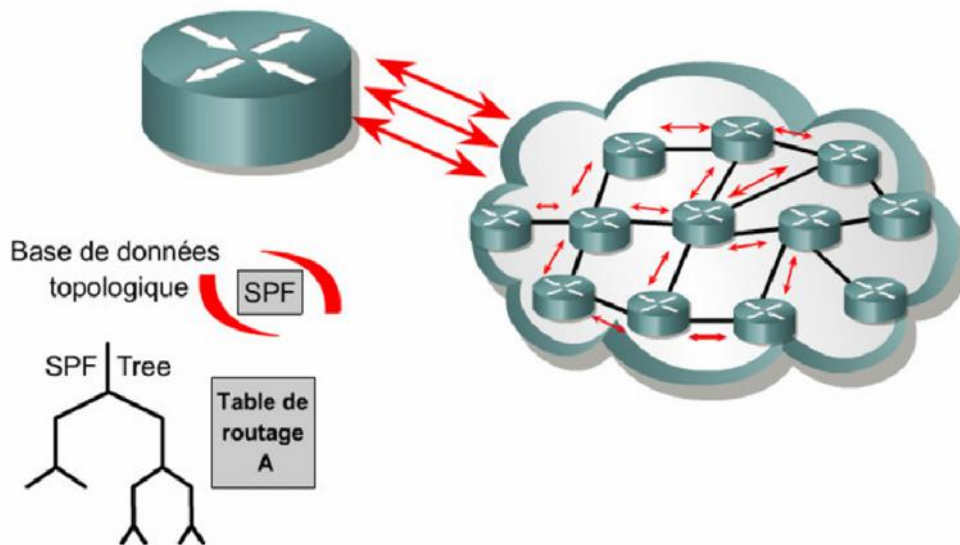


Figure II.6 : surcharge de SPF et des tables bande passante lors du flux initial de LSA.

Les protocoles de routage à état de liaisons nécessitent davantage de mémoire et de capacités de calcul que les protocoles de routage à vecteur de distance. Les routeurs doivent disposer d'une mémoire suffisante pour stocker toutes les informations des différentes bases de données, l'arbre topologique et la table de routage. Le flux initial des paquets de mise à jour de routage à état de liens consomme de la bande passante.

Durant le processus initial de découverte, tous les routeurs utilisant des protocoles de routage à état de liaisons transmettent les paquets de mise à jour aux autres routeurs. Cela a pour effet de submerger l'inter réseau et de réduire de façon temporaire la bande passante disponible pour le trafic routé des données utilisateur. Par la suite, les protocoles de routage à état de liaisons ne nécessitent généralement qu'un minimum de bande passante pour envoyer les paquets de mise à jour reflétant les modifications topologiques. L'envoi peut être sporadique ou déclenché par un événement.

III.6 Mise en œuvre des protocoles de routage à état de liaisons

III.6.1 Élaboration d'une carte topologique

Les protocoles de routage à état de liaisons créent une carte topologique, ou arborescence SPF de la topologie de réseau. Les protocoles de routage à vecteur de distance ne possèdent pas de carte topologique du réseau. Les routeurs qui mettent en œuvre le protocole de routage à vecteur de distance disposent uniquement d'une liste de réseaux indiquant le coût (distance) et les routeurs de tronçon suivant (direction) menant à ces réseaux. Les protocoles de routage à état de liaisons échangeant des états de liens, l'algorithme SPF peut construire une arborescence SPF du réseau. En utilisant l'arborescence SPF, chaque routeur peut déterminer le plus court chemin vers chaque réseau de façon indépendante.

III.6.2 Convergence rapide

À la réception d'un paquet à état de liens (LSP), les protocoles de routage à état de liaisons diffusent immédiatement le LSP sur toutes les interfaces, à l'exception de celle sur laquelle il a reçu le LSP. Un routeur qui utilise un protocole de routage à vecteur de distance doit traiter toutes les mises à jour de routage dans sa table de routage avant de les diffuser vers les autres interfaces, même lorsqu'il s'agit de mises à jour déclenchées. Les protocoles de routage à état de liaisons obtiennent des temps de convergence plus rapides. Il existe cependant une exception remarquable, le protocole EIGRP.

III.6.3 Mises à jour pilotées par événement

Après la diffusion initiale des LSP, les protocoles de routage à état de liaisons n'envoient un LSP que lorsqu'un changement de topologie intervient. Ce dernier ne contient que les informations relatives au lien concerné. Contrairement à certains protocoles de routage à vecteur de distance, les protocoles de routage à état de liaisons s'envoient pas des mises à jour périodiques.

III.6.4 Conception hiérarchique

Le protocole de routage à état de liaison comme OSPF utilise le concept de zones. Plusieurs zones créent un schéma hiérarchique des réseaux, ce qui permet un meilleur groupement (résumé) des routes et l'isolement des problèmes de routage dans une zone.

III.7 Éléments requis pour un protocole de routage à état de liaisons

III.7.1 Mémoire requise

Les protocoles de routage à état de liaisons nécessitent plus de mémoire, de temps processeur et parfois, davantage de bande passante que les protocoles de routage à vecteur de distance. La mémoire requise sert principalement à l'utilisation des bases de données à état de liens et à la création de l'arborescence SPF.

III.7.2 Temps processeur requis

Les protocoles à état de liaison peuvent également nécessiter davantage de temps processeur que leurs homologues à vecteur de distance. L'algorithme SPF a besoin de davantage de temps processeur que les algorithmes à vecteur de distance tels que Bellman-Ford, car les protocoles à état de liens construisent une carte topologique complète.

III.7.3 Bande passante requise

La diffusion des paquets à état de liaisons peut affecter la bande passante disponible sur le réseau de plusieurs façons. Il se peut que cela ne se produise que pendant le démarrage initial des routeurs, mais peut s'avérer problématique sur les réseaux instables.

III.8 Comparaison des protocoles de routage à état de liaisons

Aujourd'hui, deux protocoles de routage à état de liaisons sont utilisés pour le routage du trafic IP :

Chapitre III protocoles de routage dynamique à l'état de liaisons

- protocole OSPF.
- protocole de routage IS-IS.

OSPF

Le protocole OSPF a été conçu par le groupe de travail OSPF de l'IETF, Le développement du protocole OSPF a commencé en 1987 ; il en existe aujourd'hui deux versions :

- OSPFv2 : OSPF pour les réseaux IPv4.
- OSPFv3 : OSPF pour les réseaux IPv6.

IS-IS

IS-IS a été conçu par ISO (International Organization for Standardization - Organisme international de normalisation) et est décrit dans la norme ISO 10589. La première application pratique de ce protocole de routage fut développée chez DEC (Digital Equipment Corporation) et est également connue sous le nom de DECnet Phase V. Radia Perlman a été le principal concepteur du protocole de routage IS-IS.

Il était à l'origine conçu pour l'ensemble de protocoles OSI et non pour TCP/IP. Par la suite Integrated IS-IS ou Dual IS-IS a intégré la prise en charge des réseaux IP. Bien qu'IS-IS soit connu comme le protocole de routage de la plupart des FAI et opérateurs télécom, un nombre croissant de sociétés commencent à l'utiliser.

Les protocoles OSPF et IS-IS ont beaucoup de points communs, mais présentent également de nombreuses différences. OSPF et IS-IS ont chacun leurs partisans, qui discutent et débattent des avantages respectifs d'un protocole de routage sur l'autre. Les deux fournissent les fonctions de routage nécessaires.

III.9 Le protocole OSPF

III.9.1 Origines du protocole OSPF

Le développement initial du protocole OSPF a débuté en 1987, mené par le groupe de travail OSPF de l'IETF (Internet Engineering Task Force). À cette époque, Internet était un réseau dédié à l'enseignement et à la recherche fondé par le gouvernement des États-Unis.

En 1989, la spécification du protocole OSPFv1 fut publiée dans le document RFC 1131. Deux mises en œuvre y étaient décrites : l'une s'exécutait sur des routeurs, l'autre sur des stations de travail UNIX. Cette dernière devint par la suite un processus UNIX très répandu connu sous le nom de GATED. OSPFv1 était un protocole de routage expérimental qui ne fut jamais déployé.

En 1991, OSPFv2 fut présenté dans le document RFC 1247 par John Moy. Ce protocole offrait des améliorations techniques significatives par rapport à OSPFv1. Dans le même temps, ISO travaillait sur un protocole de routage à état de liaisons de leur cru, le protocole IS-IS (Intermediate System-to-Intermediate System). Sans surprise, IETF choisit de recommander le protocole OSPF comme IGP (Interior Gateway Protocol – Protocole de passerelle interne).

Chapitre III protocoles de routage dynamique à l'état de liaisons

En 1998, la spécification OSPFv2 fut mise à jour dans le document RFC 2328, qui est toujours le document RFC d'actualité pour OSPF.

En 1999, OSPFv3 pour IPv6 fut publié dans le document RFC 2740, rédigé par John Moy, Rob Coltun et Dennis Ferguson.



Figure III.7 : histoire du protocole OSPF.

III.9.2 Présentation du protocole OSPF

Le protocole OSPF (Open Shortest Path First) est un protocole de routage à état de liaisons qui a été développé pour remplacer le protocole de routage à vecteur de distance RIP. RIP était acceptable au début des réseaux et de l'Internet, mais le fait qu'il choisisse la meilleure route en prenant en compte uniquement le nombre de sauts est rapidement devenu inacceptable dans des réseaux plus grands nécessitant une solution de routage plus fiable. OSPF est un protocole de routage sans classe qui utilise le concept de zones pour son évolutivité. La métrique OSPF comme une valeur arbitraire nommée coût. Le système d'exploitation Internet (IOS) utilise la bande passante comme métrique de coût du protocole OSPF.

Les principaux avantages d'OSPF sur RIP sont une convergence rapide et une évolutivité vers la mise en œuvre de réseaux bien plus importants.

	Protocoles de routage à vecteur de distance		Protocoles de routage à état de liens		Protocole BGP
Par classe	RIP	IGRP			EGP
Sans classe	RIPv2	EIGRP	OSPFv2	IS-IS	BGPv4
IPv6	RIPng	EIGRP pour IPv6	OSPFv3	IS-IS pour IPv6	BGPv4 pour IPv6

Figure III.8 : schéma de présentation du protocole OSPF.

III.9.3 Fonctionnement du protocole OSPF

La figure III.9 permet d'expliquer le fonctionnement du protocole OSPF, on utilise cinq routeurs :

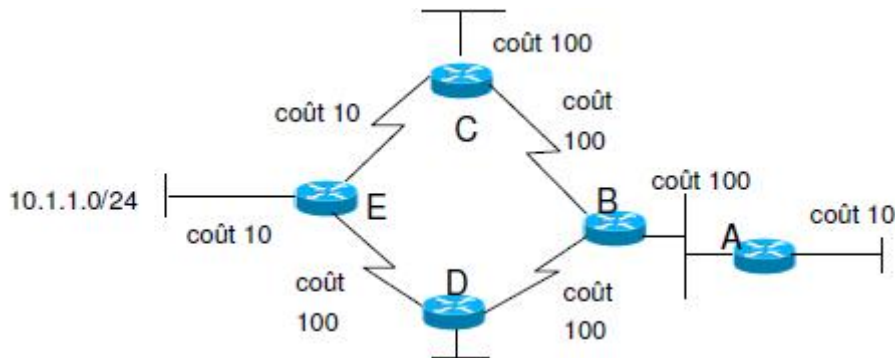


Figure III.9 : Exemple de fonctionnement du protocole OSPF.

- ❖ Dans les protocoles à état de liaison, B ne va pas donner à A le coût de la liaison mais la carte qu'il connaît du réseau avec les masques associés.
 - ❖ Ainsi, A va pouvoir calculer les meilleurs routes vers tous les sous-réseaux en se basant sur les informations topologiques transmises par B.
 - ❖ Comparativement aux protocoles à vecteur distance, les protocoles à états de liaisons doivent calculer les coûts vers toutes les sous-réseaux.
- Avec les vecteurs distances, B dit à A : sous-réseaux 10.1.1.0, métrique 3
 - Avec les états de liens : A va apprendre puis calculer :
 - A vers 10.1.1.0/24 : par C, coût 320
 - A vers 10.1.1.0/24 : par D, coût 310

Les résultats : A mettra dans sa table de routage la route vers 10.1.1.0/24 par D

L'algorithme utilisé pour trouver les meilleurs routes est l'algorithme : SPF (algorithme Dijkstra) du nom de son concepteur Les échanges d'informations ne se font pas dès le départ par un broadcast.

Initialisation du processus par une recherche des voisins et après qu'un routeur ait identifié un voisin, les routeurs s'échangent leurs informations topologiques et on a :

- Le déroulement complet d'OSPF est le suivant :
- ❖ Chaque routeur découvre son voisinage et conserve une liste de tous ses voisins.
 - ❖ utilise un protocole fiable pour échanger les informations topologiques avec ses voisins stocke les informations topologiques apprises dans leur base de données.
 - ❖ exécute l'algorithme SPF pour calculer les meilleures routes.
 - ❖ place ensuite la meilleure route vers chaque sous-réseau dans sa table de routage.
- Chaque routeur possède :
 - ❖ Une table de ses voisins.

Chapitre III protocoles de routage dynamique à l'état de liaisons

- ❖ Une base de données de la topologie du réseau.
- ❖ Une table de routage.

III.9.4 Encapsulation de message OSPF

La partie donnée d'un message OSPF est encapsulée dans un paquet. Cette zone de données peut inclure un des types de paquets OSPF.

Ici on place un pointeur sur les champs de la figure III.10 du message OSPF encapsulé pour voir le processus d'encapsulation.

L'en-tête de paquet OSPF est inclus dans chaque paquet OSPF, quel que soit son type. L'en-tête de paquet OSPF et les données spécifiques relatives à son type sont ensuite encapsulés dans le paquet IP. Dans l'en-tête de paquet IP, le champ protocole est défini à 89 pour indiquer OSPF, et l'adresse de destination a pour valeur une des deux adresses multidiffusion suivantes : 224.0.0.5 ou 224.0.0.6. Si le paquet OSPF est encapsulé dans une trame Ethernet, l'adresse MAC de destination est elle aussi une adresse multidiffusion : 01-00-5E-00-00-05 ou 01-00-5E-00-00-06.

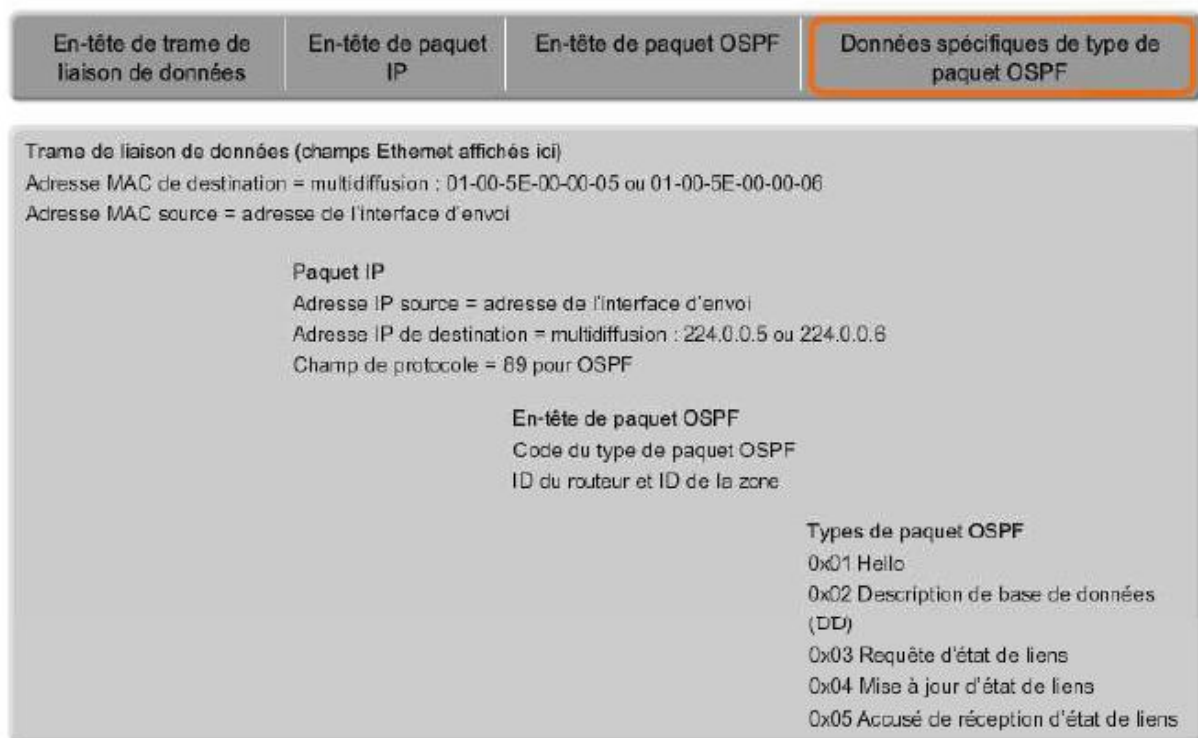


Figure III.10 : Message du protocole OSPF.

III.9.5 Types de paquet OSPF

Les paquets chacun d'eux a un objectif spécifique dans le processus de routage OSPF :

- ❖ **Hello** : les paquets Hello servent à établir puis à maintenir la contiguïté avec d'autres routeurs OSPF.

Chapitre III protocoles de routage dynamique à l'état de liaisons

- ❖ **DBD** : le paquet descripteur de base de données contient une liste abrégée de la base de données à état de liens du routeur expéditeur et est utilisé par les routeurs de destination pour contrôler la base de données à état de liens locale.
- ❖ **LSR** : les routeurs de destination peuvent alors demander plus d'informations sur n'importe quelle entrée du DBD, en envoyant un paquet LSR (Link-State Request).
- ❖ **LSU** : les paquets LSU (Link-State Update) sont utilisés pour répondre aux LSR, ainsi que pour annoncer de nouvelles informations.

III.9.5.1 Protocole Hello

Le schéma de la figure III.11, montre l'en-tête de paquet OSPF et le paquet Hello.

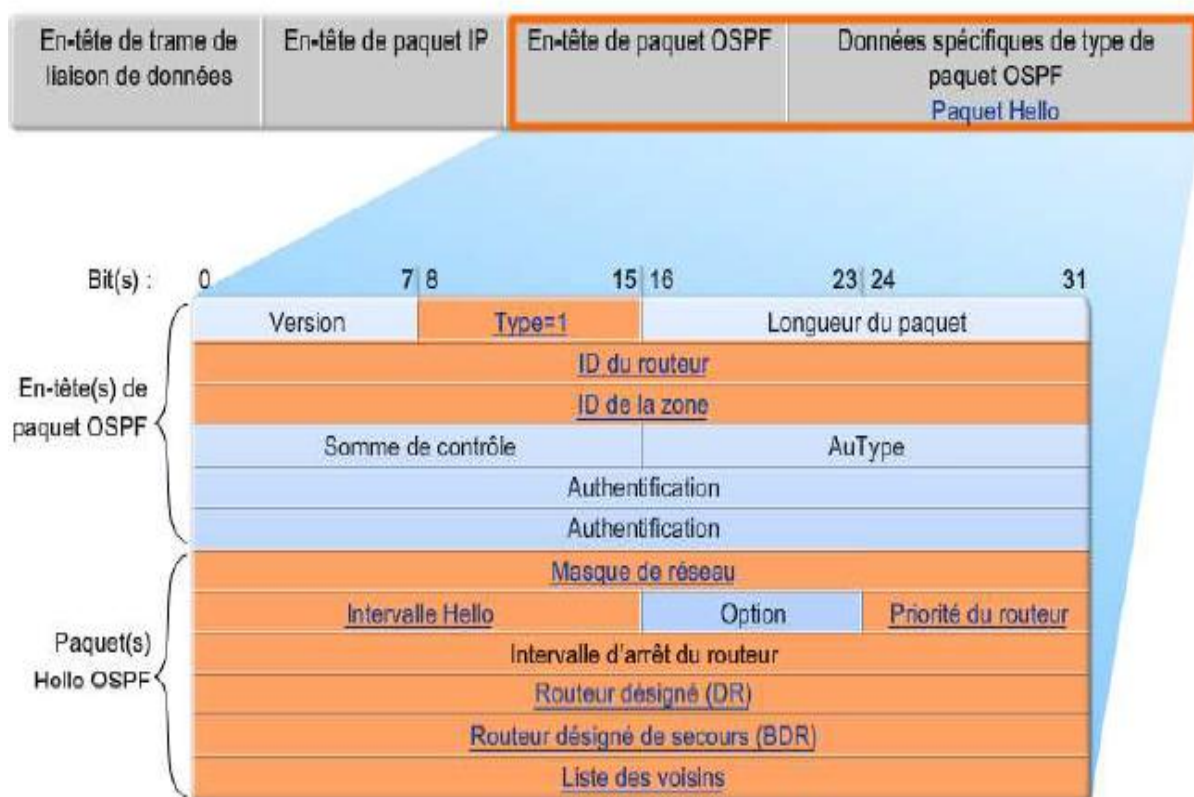


Figure III.11 : Les paquets hello OSPF.

Le premier type de paquet OSPF est le paquet Hello. Les paquets Hello sont utilisés pour :

- ❖ découvrir des voisins OSPF et établir des contiguïtés.
- ❖ annoncer les paramètres sur lesquels les deux routeurs doivent s'accorder pour devenir voisins.
- ❖ définir le routeur désigné (DR) et le routeur désigné de sauvegarde (BDR) sur les réseaux à accès multiple, de type Ethernet et Frame Relay.

Les champs importants indiqués dans la figure III.11 incluent :

- ❖ **Type** : type de paquet OSPF : Hello (1), DBD (2), LSR (3), LSU (4).
- ❖ **ID du routeur** : ID du routeur source.
- ❖ **ID de zone** : zone d'origine du paquet.
- ❖ **Masque de réseau** : masque de sous-réseau associé à l'interface émettrice.
- ❖ **Intervalle Hello** : nombre de secondes entre les intervalles Hello du routeur émetteur.
- ❖ **Priorité du routeur** : utilisé dans la sélection du routeur désigné ou du routeur désigné de sauvegarde.
- ❖ **Routeur désigné (DR)** : ID du routeur désigné, le cas échéant.
- ❖ **Routeur désigné de sauvegarde (BDR)** : ID du routeur désigné de sauvegarde, le cas échéant.
- ❖ **Liste des voisins** : indique l'ID de routeur OSPF du ou des routeurs voisins.

II.9.5.2 Identification d'un routeur

La base de données de la topologie du réseau contient la liste de tous les sous-réseaux, appelé lien, connu du routeur et de l'identité du routeur permettant de faire la liaison avec ce lien.

Il est facile d'identifier un sous-réseau et son masque associé, par contre identifier un routeur est plus compliqué.

La solution utilisée doit permettre d'identifier, de façon unique sur le réseau un routeur par un identifiant appelé ID.

La solution choisie est de se baser sur les adresses IP de ceux-ci :

- ❖ Si le routeur possède un adresse loopback, il prendra l'adresse la plus grande parmi ses adresses de loopback .
- ❖ Sinon, il choisira la plus grande adresse IP de ses interfaces opérationnelles.
- ❖ Chaque routeur choisit son OSPF ID à l'initialisation.

III.9.5.3 Détection des voisins

Pour pouvoir diffuser ses états de liens aux autres routeurs, un routeur OSPF doit d'abord déterminer s'il existe d'autres voisins OSPF sur un de ses liens. Dans la figure III.12, les routeurs OSPF envoient des paquets Hello sur toutes les interfaces OSPF pour déterminer s'il existe des voisins sur ces liens. Les informations contenues dans les paquets Hello OSPF comprennent l'ID routeur OSPF du routeur qui envoie le paquet Hello. La réception d'un paquet Hello OSPF confirme à un routeur qu'il existe un autre routeur OSPF sur le lien. OSPF établit ainsi des contiguïtés avec le voisin.

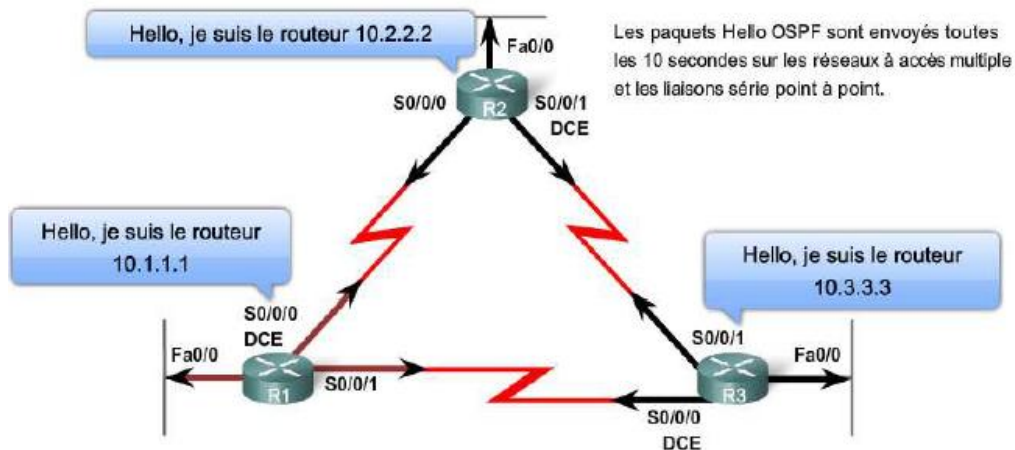


Figure III.12 : Exemple de la découverte des voisins.

III.9.5.4 Intervalles des paquets Hello et Dead OSPF

Pour que deux routeurs puissent former une contiguïté de voisinage OSPF, ils doivent d'abord s'entendre sur trois valeurs : l'intervalle Hello, l'intervalle Dead (arrêt) et le type de réseau. L'intervalle Hello OSPF indique la fréquence à laquelle un routeur OSPF envoie des paquets Hello. Par défaut, les paquets Hello OSPF sont envoyés toutes les 10 secondes sur des segments à accès multiple et point à point.

Dans la plupart des cas, les paquets Hello OSPF sont envoyés en multidiffusion à une adresse qui permet à un périphérique d'ignorer le paquet si son interface n'est pas activée pour accepter les paquets OSPF.

L'intervalle Dead est la période, exprimée en secondes, pendant laquelle le routeur attendra de recevoir un paquet Hello avant de déclarer le voisin « hors service » et pour les segments à accès multiple et point à point, cette période est de 40 secondes.

Si l'intervalle Dead expire avant que les routeurs ne reçoivent un paquet Hello, OSPF supprime le voisin de sa base de données à état de liens. Le routeur diffuse alors l'information d'état de liens concernant le voisin « hors service » vers toutes les interfaces OSPF.

III.9.6 Algorithme OSPF

Chaque routeur OSPF conserve une base de données d'état de liaisons contenant les LSA reçus de tous les autres routeurs. Une fois qu'un routeur a reçu tous les LSA et créé sa base de données à état de liens locale, OSPF utilise l'algorithme du plus court chemin de Dijkstra (SPF) pour créer une arborescence SPF. L'arborescence SPF est ensuite utilisée pour fournir à la table de routage IP les meilleurs chemins vers chaque réseau.

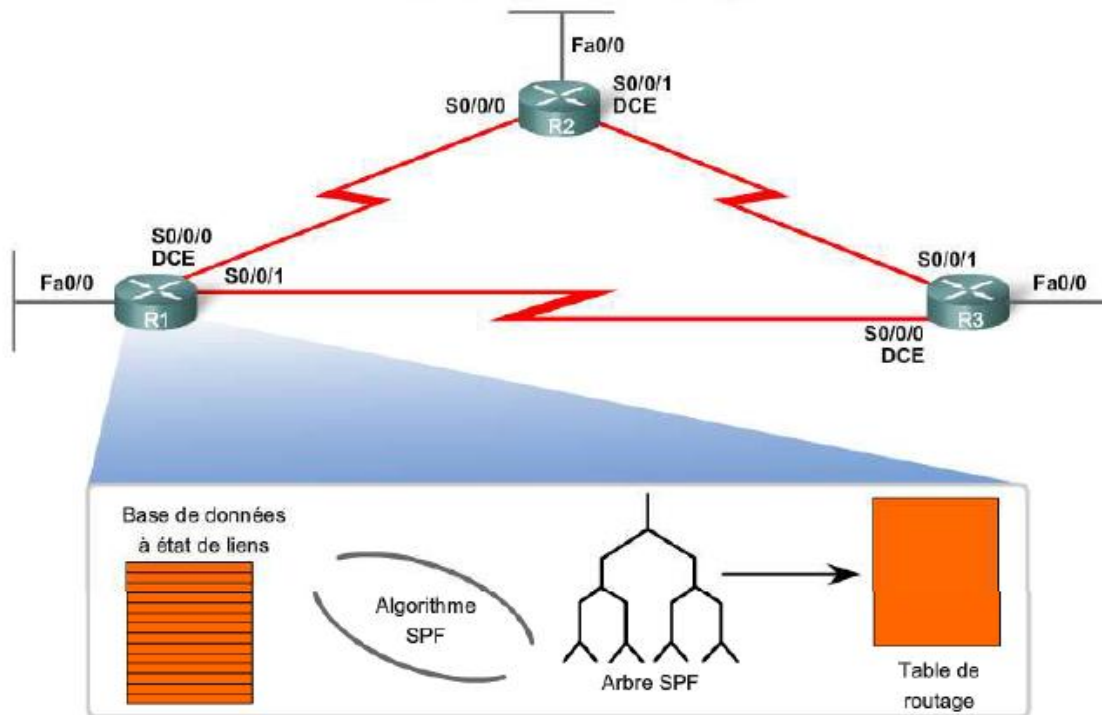


Figure III.13 : présentation de l'algorithme OSPF.

III.9.7 Zone du protocole OSPF

Les zones OSPF permettent d'isoler des parties du réseau afin de diminuer la taille de la topologie réseau à mémoriser sur chaque routeur.

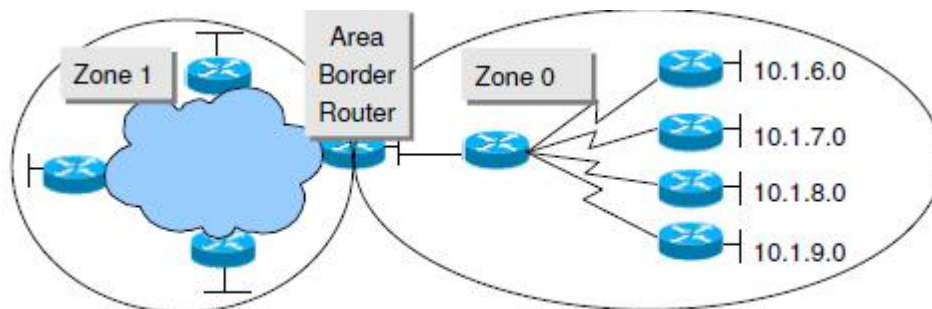


Figure III.14 : Les zones OSPF.

III.9.8 Configuration basique de protocole OSPF

- ❖ Activation du routage OSPF comme suit :
 - Router (config)#router **ospf process-id**.
- ❖ Process-id entre 1 et 65535 est :
 - Signification locale uniquement Permet d'avoir plusieurs processus OSPF.
 - Pour des usages et configurations inhabituelles.

III.9.8.1 Configuration d'un routeur avec commande `router ospf 1`

```
R1(config)#router ospf1
R1 (Config-router)#
```

III.9.8.2 La commande `Network IP masque réseau area`

On utilise la commande `network` dans chaque routeur par une adresse et de zone `area` par le script suivant :

```
Network adresse wildcard_mask area_id
```

- ❖ *adresse* : réseau devant être utilisé pour diffuser et écouter les messages OSPF.
- ❖ *area_id* : zone dans laquelle le réseau figure.

```
R1 (config) #router ospf 1
```

```
R1 (config-router) #network adresse IP masque réseau area 0
```

❖ Adresse de bouclage

Si la commande **router-id** OSPF n'est pas utilisée et que vous avez configuré des interfaces de bouclage, OSPF choisit l'adresse IP d'interface de bouclage la plus élevée. Une adresse de bouclage est une interface virtuelle et est automatiquement à l'état **up** lorsqu'elle est configurée.

```
Router(config)#interface loopback number
```

```
Router(config-if)#ip address adresse IP masque de sous-réseau
```

III.9.8.3 Visualiser le Router ID

L'ID de routeur OSPF permet d'identifier chaque routeur de façon unique dans le domaine de routage OSPF. Un ID de routeur est tout simplement une adresse IP. Les routeurs définissent leur ID de routeur en utilisant trois critères, selon la priorité ci-dessous :

- ❖ Utilisation de l'adresse IP configurée avec la commande **router-id** du protocole OSPF.
- ❖ Si **router-id** n'est pas configuré, le routeur choisit l'adresse IP la plus élevée parmi ses interfaces de bouclage IP.
- ❖ Si aucune interface de bouclage n'est configurée, le routeur choisit l'adresse IP active la plus élevée parmi ses interfaces physiques.

On utilise plusieurs commandes pour visualiser l'identification de routeur ID :

- ❖ `show ip protocols.`
- ❖ `show ip ospf.`
- ❖ `show ip ospf interface.`

Comme indiqué dans le schéma III.15, la commande **show ip protocols** offre un moyen rapide de vérifier des données de configuration OSPF cruciales, notamment l'ID de processus OSPF, l'ID de routeur, les réseaux que le routeur annonce, les voisins desquels le routeur

Chapitre III protocoles de routage dynamique à l'état de liaisons

reçoit des mises à jour et la distance administrative par défaut, à savoir 110 pour le protocole OSPF.

```
R1#show ip protocols
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 192.168.10.5
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
```

Figure III.15 : Visualisation le Router ID.

III.9.8.4 Configuration par l'interface loopback

Le Router ID est déterminé par soit l'adresse de loopback, soit par l'adresse IP d'une interface
Par exemple :

```
R1 ( Config)# interface loopback 0
```

```
R1 (config-if)# ip add 10.1.1.1 255.255.255.255
```

III.9.8.4.1Avantage d'utiliser une adresse de loopback

- ❖ Une interface de Loopback ne peut pas devenir défailante.
- ❖ Apporte une plus grande stabilité à OSPF.

III.9.8.5 Vérification de la configuration

Pour vérifier cette configuration on suivre les étapes suivantes :

- ❖ Visualiser les Neighbor adjacency table Router#show ip ospf neighbor.
- ❖ L'absence de voisin est indiquée par une absence de Router ID et un état FULL non affiché.
- ❖ Conséquence d'une absence de voisin c'est-à-dire aucune information link state ne sera échangée et que l'arbre SPF et les tables de routages ne seront pas justes.

```
R1#show ip ospf neighbor
Neighbor ID      Pri   State           Dead Time   Address        Interface
10.3.3.3         1    FULL/ -         00:00:30   192.168.10.6   Serial0/0/1
10.2.2.2         1    FULL/ -         00:00:33   192.168.10.2   Serial0/0/0
```

Figure III.16 : Vérification de la configuration.

III.9.8.6 La table de routage

La commande `show ip route` permet de visualiser les routes apprises par OSPF et la lettre O en début de ligne indique que la route a été apprise par OSPF.

```
R1#show ip route

Codes: <some code output omitted>
       D - EIGRP, EX - EIGRP external, C - OSPF, IA - OSPF inter area

Gateway of last resort is not set

192.168.10.0/30 is subnetted, 3 subnets
C      192.168.10.0 is directly connected, Serial0/0/0
C      192.168.10.4 is directly connected, Serial0/0/1
O      192.168.10.8 [110/128] via 192.168.10.2, 14:27:57, Serial0/0/0
172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
O      172.16.1.32/29 [110/65] via 192.168.10.6, 14:27:57, Serial0/0/1
C      172.16.1.16/28 is directly connected, FastEthernet0/0
10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
O      10.10.10.0/24 [110/65] via 192.168.10.2, 14:27:57, Serial0/0/0
C      10.1.1.1/32 is directly connected, Loopback0
```

Figure III.17 : Utilisation la commande show ip dans la table routage

III.9.9 Les métriques OSPF

OSPF calcule le coût d'un lien par la formule $100 \text{ Mb/s} / \text{bande passante}$ et le meilleur route sera la route avec le plus petit coût et la référence pour la bande passante est 100 Mb/s et on a le tableau III.6 ci-dessous les différentes valeurs de coût de chaque interface.

Type d'interface	Coût
Fast Ethernet et plus rapide	1
Ethernet	10
E1	48
T1	64
128 Kbits/s	781
64 Kbits/s	1562
56 Kbits/s	1785

Tableau III.6 : présentation les différentes valeurs de Coût de chaque interface.

III.9.10 Le coût total

Le coût total d'une route est la somme des coûts de chaque lien ce qui montre dans la figure III.18 :

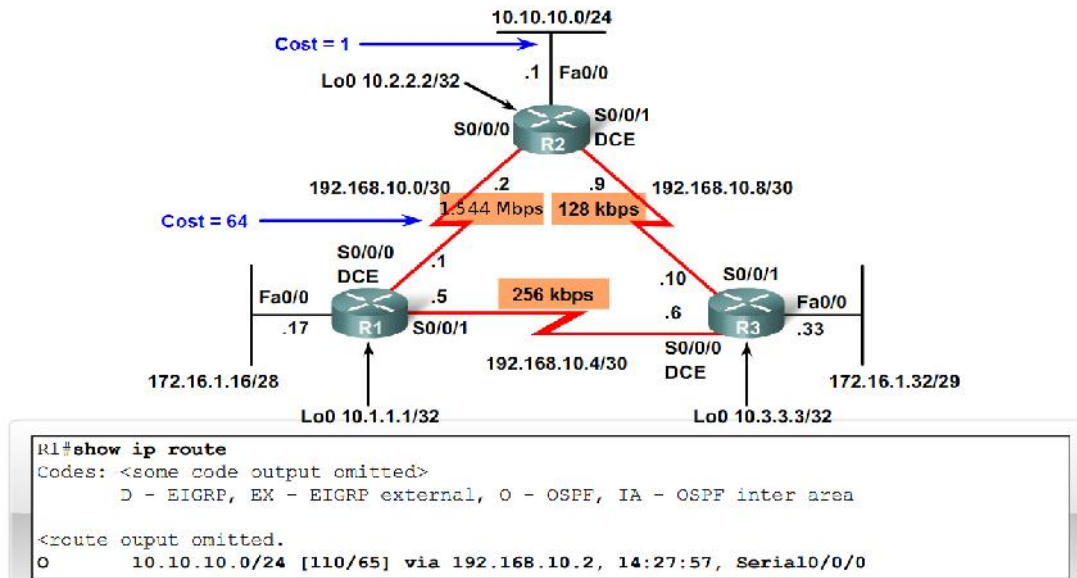


Figure III.18 : Exemple de calcul le Coût total OSPF.

III.9.11 OSPF et les réseaux à accès multiple

Un réseau à accès multiple est un réseau comportant plus de deux périphériques sur le même support partagé. Le réseau local Ethernet rattaché à R1 est étendu afin de montrer les différents périphériques qui peuvent être attachés au réseau 172.16.1.16/28. Les réseaux locaux Ethernet constituent un exemple de réseau à accès multiple de diffusion. Ce sont des réseaux de diffusion car tous les périphériques du réseau peuvent voir toutes les trames de diffusion.

Sur le réseau point à point, en revanche, le réseau ne comporte que deux périphériques, un à chaque extrémité. La liaison de réseau étendu entre R1 et R3 est un exemple de liaison point à point. La figure III.18, montre la liaison point à point entre R1 et R3.

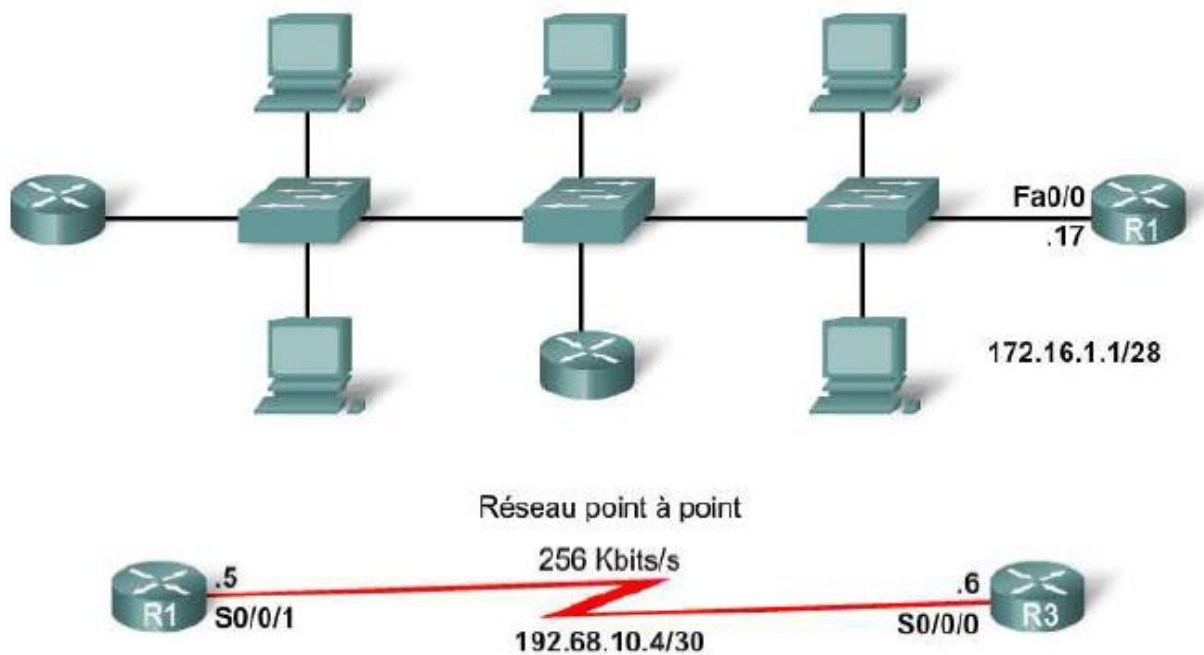


Figure III.19 : les réseaux multiples par OSPF.

Le protocole OSPF définit 4 types de réseau :

- Point à point.
- Accès multiple avec diffusion.
- Point à multipoint.
- Liaisons virtuelles.

III.9.12 Mises à jour d'état de liens OSPF

Les paquets LSU (Link-State Update) sont les paquets utilisés pour les mises à jour du routage OSPF. Le paquet LSU peut contenir 11 types différents de LSA.

III.9.13 Distance administrative

La distance administrative correspond à la fiabilité (ou préférence) de la route source. La distance administrative par défaut OSPF est de 110.

Source de la route	Distance administrative
Connecté	0
Statique	1
Résumé de routes EIGRP	5
BGP externe	20
EIGRP interne	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
EIGRP externe	170
BPG interne	200

Tableau III.7 : La distance administrative OSPF.

III.9.14 Authentification

Le protocole OSPF comme d'autres protocoles de routage peut être configuré pour l'authentification.

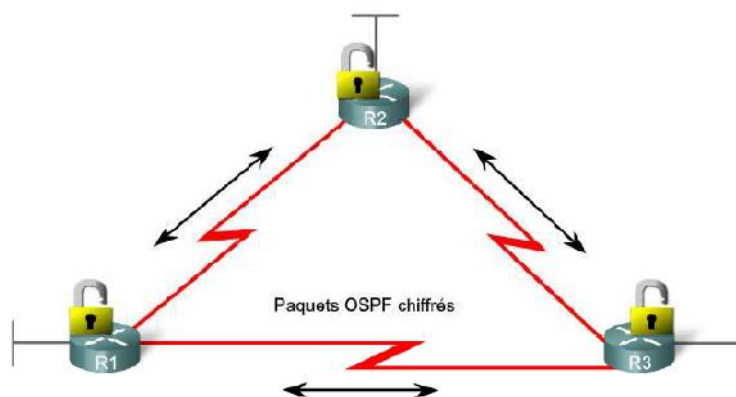


Figure III.20 : Authentification OSPF.

Chapitre III protocoles de routage dynamique à l'état de liaisons

Cela constitue une pratique saine. Les protocoles RIPv2, EIGRP, OSPF, IS-IS et BGP peuvent tous être configurés pour chiffrer et authentifier leurs informations de routage. Cette pratique garantit que les routeurs n'accepteront que les informations en provenance de routeurs ayant été configurés avec le même mot de passe ou les mêmes informations d'authentification.

Chapitre IV

*Configuration du protocole
OSPF dans un réseau*

IV .1 Introduction

Dans ce chapitre, on configure le routage dynamique du protocole OSPF à l'état de liaison par le simulateur ou le logiciel Packet Tracer.

Packet Tracer est un outil de simulation d'équipements Cisco, il permet de construire un réseau physique virtuel et de simuler le comportement des protocoles sur le réseau.

IV.2 Présentation de Packet Tracer

La fenêtre de la figure IV .1 présente les paramètres principaux de fonctionnement du simulateur Packet tracer.

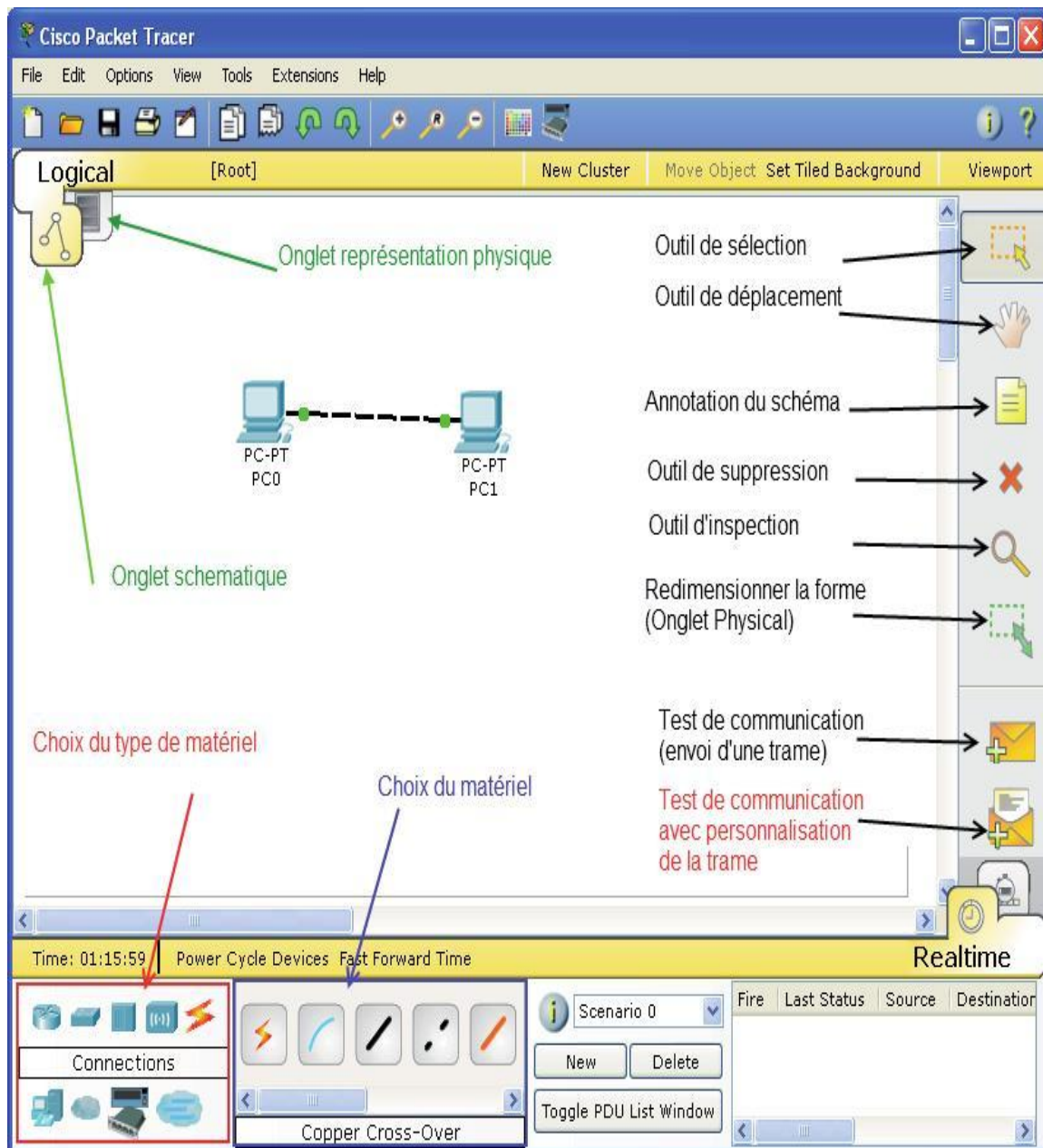


Figure IV.1 : La fenêtre principale du Packet Tracer.

Chapitre IV Configuration du protocole OSPF dans un réseau

Le Packet tracer dispose d'une barre de menu classique et d'une barre d'outils principaux comportant les fonctionnalités de base de gestion de fichier, d'impression, etc....

La barre d'outils à droite comportant les outils minimaux nécessaires, Ainsi que trois boites à outils :

- ❖ choix du type de matériel (ordinateur, routeurs, etc...).
- ❖ choix du matériel en fonction du type.
- ❖ des résultats de l'échange de données.

a) Les placements des matériels

La figure IV.2 représente plusieurs types de matériels qu'on peut utiliser. Selon le type, la liste du matériel change de manière dynamique. Cette liste est conséquente et basée souvent sur des références CISCO on clique sur le matériel souhaité puis on clique à nouveau dans l'espace de Travail pour placer le matériel. En suite on place de la sortie tout le matériel souhaité

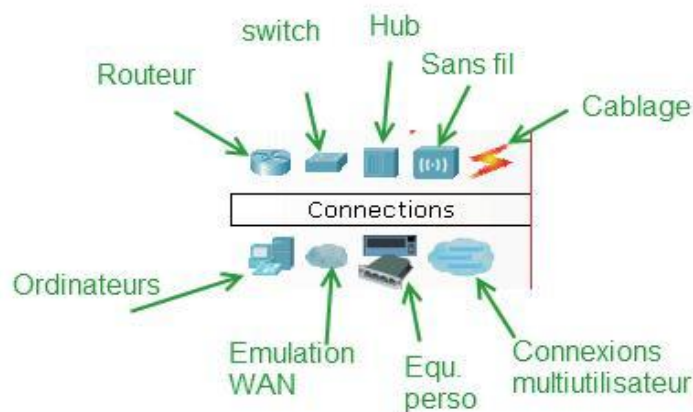


Figure IV.2 : présentation des matériels.

b) Les placement des connexions

La figure IV.3 représente plusieurs outils câblages et des connecteurs et ces différents outils permettent de relier tous les placements matériels.

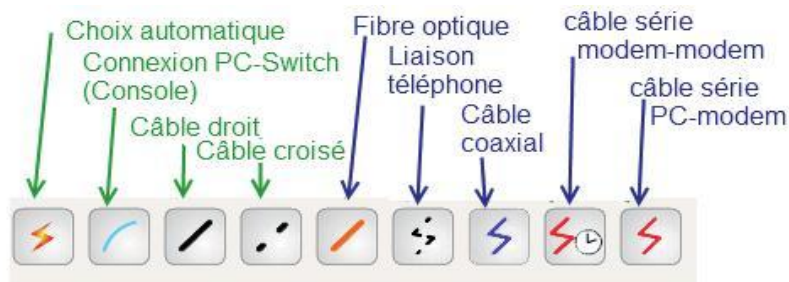


Figure IV.3 : présentation des connecteurs.

c) Le paramétrage physique (Physical)

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

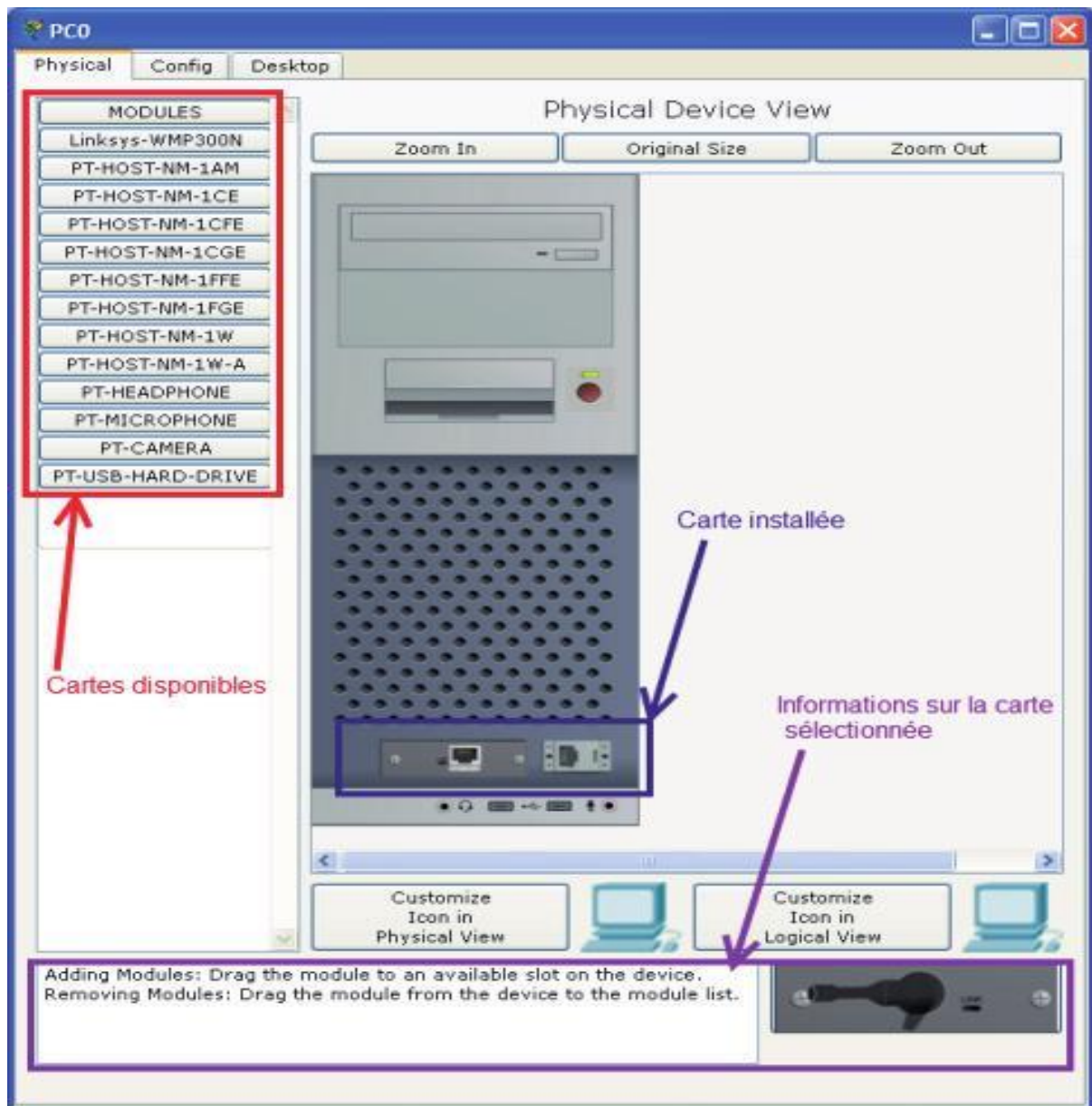


Figure IV.4 : Le paramétrage physique d'un PC.

d) Configuration

L'onglet **Config** permet de configurer l'équipement sélectionné et les boutons situés à gauche de la fenêtre déterminent le groupe de paramètres à configurer.

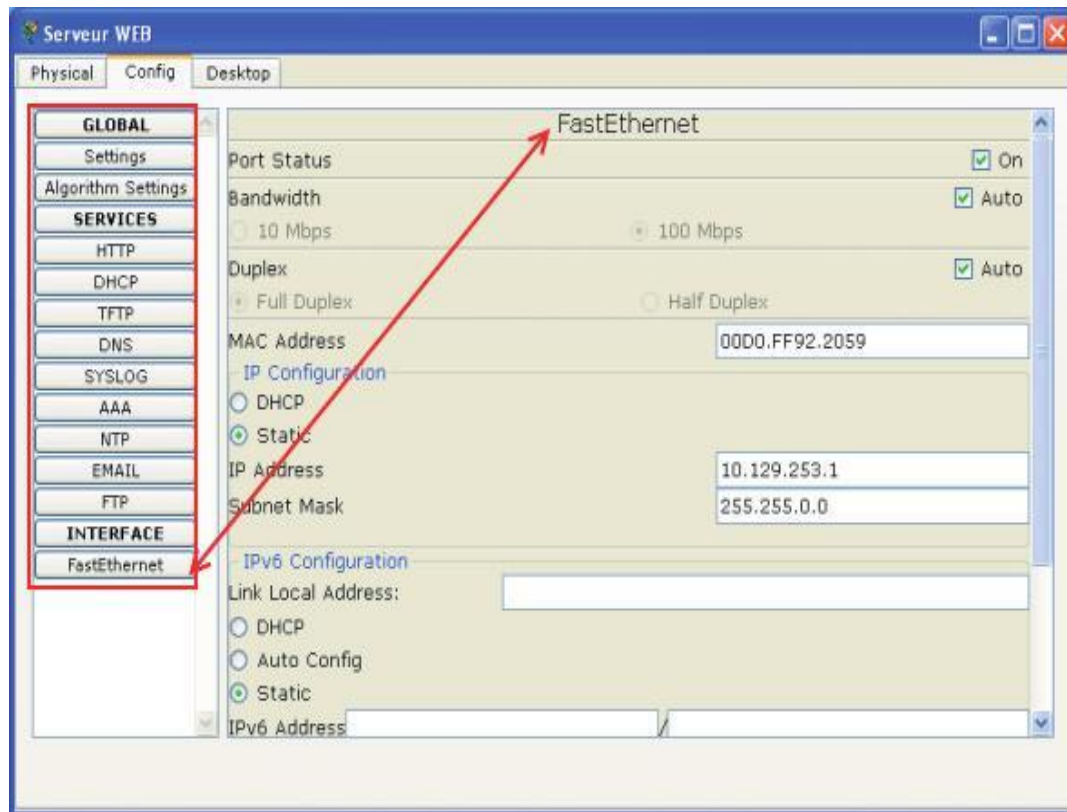


Figure IV.5: Configuration l'interface d'un PC

e) L'onglet Desktop

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

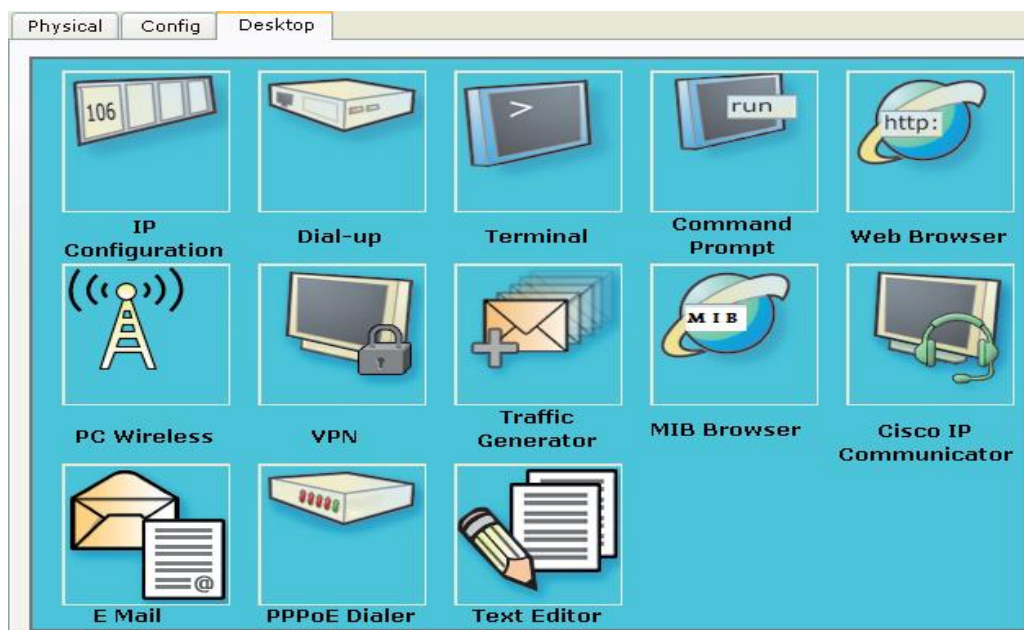


Figure IV.6 : Accès aux différents outils.

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

f) Simulation

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

- ❖ la simulation en temps réel (**REALTIME**): elle visionne immédiatement tous les séquences qui se produisent en temps réel.
- ❖ la simulation permet de visualiser les séquences au ralenti entre deux ou plusieurs équipements.

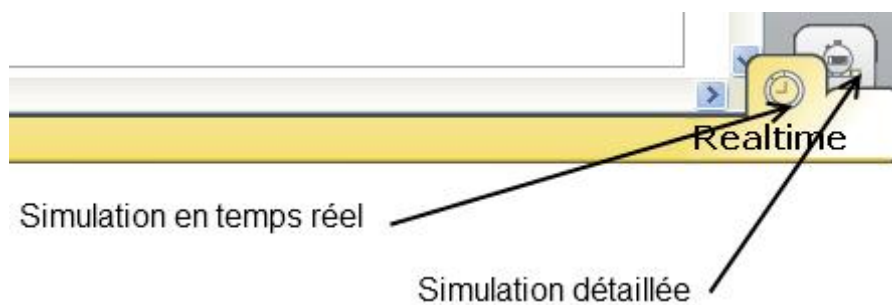


Figure IV.7 : Les simulations du packet tracer.

IV. 3 Configuration d'un routeur

Toutes les modifications de la configuration de l'interface de commande en ligne apportées sur un routeur sont effectuées en mode de configuration globale. D'autres modes spécifiques sont activés en fonction de la modification de configuration requise, mais ces modes sont tous des sous-ensembles du mode de configuration globale.

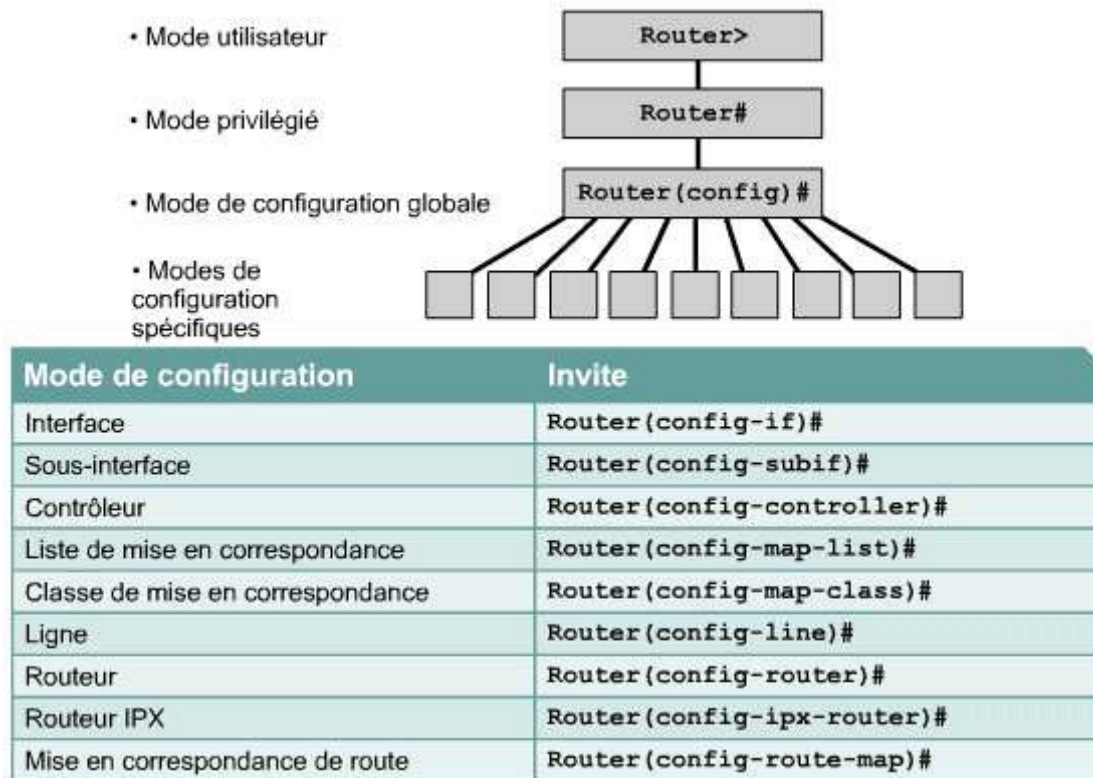


Figure IV.8 : Les commandes de configuration d'un routeur.

Les commandes de configuration globale sont utilisées sur un routeur pour appliquer des instructions de configuration qui affectent l'ensemble du système. La commande suivante place le routeur en mode de configuration globale et permet d'entrer des commandes à partir du terminal.

Le mode de configuration globale (global config) est le mode de configuration principal. Voici quelques-uns des modes auquel on peut accéder à partir du mode de configuration globale:

- ❖ Mode interface.
- ❖ Mode ligne.
- ❖ Mode routeur.
- ❖ Mode sous-interface.
- ❖ Mode contrôleur.

Les commandes de configuration

- ❖ **L'attribution d'un nom au routeur :**

La commande hostname
 Router (config)#**hostname** R

❖ **Choix d'un mot de passe pour la protection de la session du mode privilégié**

```
R (config) #enable password < mot >
```

❖ **Passage en mode de configuration d'interface**

```
R (config) #interface s0/0  
R (config-if) # ip address <ip adresse > <masque reseau>  
R (config-if) # no shutdown
```

❖ **La détermination de la vitesse d'horloge : la commande clock rate**

```
R (config-if) #clock rate 56000  
R (config-if) #no shutdown
```

❖ **La détermination de la Bande passante: la commande bandwidth**

```
R (config-if) #bandwidth 56  
R (config-if) #no shutdown
```

❖ **Sortie du mode de configuration d'interface**

```
R (config-if)#exit
```

❖ **Configuration des sessions telnet**

```
R (config) #line vty 0 4  
R (Config-line) #login  
R (config-line) #password< mot >  
R (config-line) #service password-encryption
```

❖ **configuration du port console**

```
R (config-line) #line con 0  
R (config-line) #login  
R (config-line) #password < mot >  
R (config-line) #ser password-encryption
```

IV.4 Présentation du réseau

La topologie dans la figure IV.9 permet de présenter le réseau. Il contient trois routeurs R1, R2, R3. Chaque routeur est connecté à réseau LAN Ethernet et représenté par un commutateur et un PC.

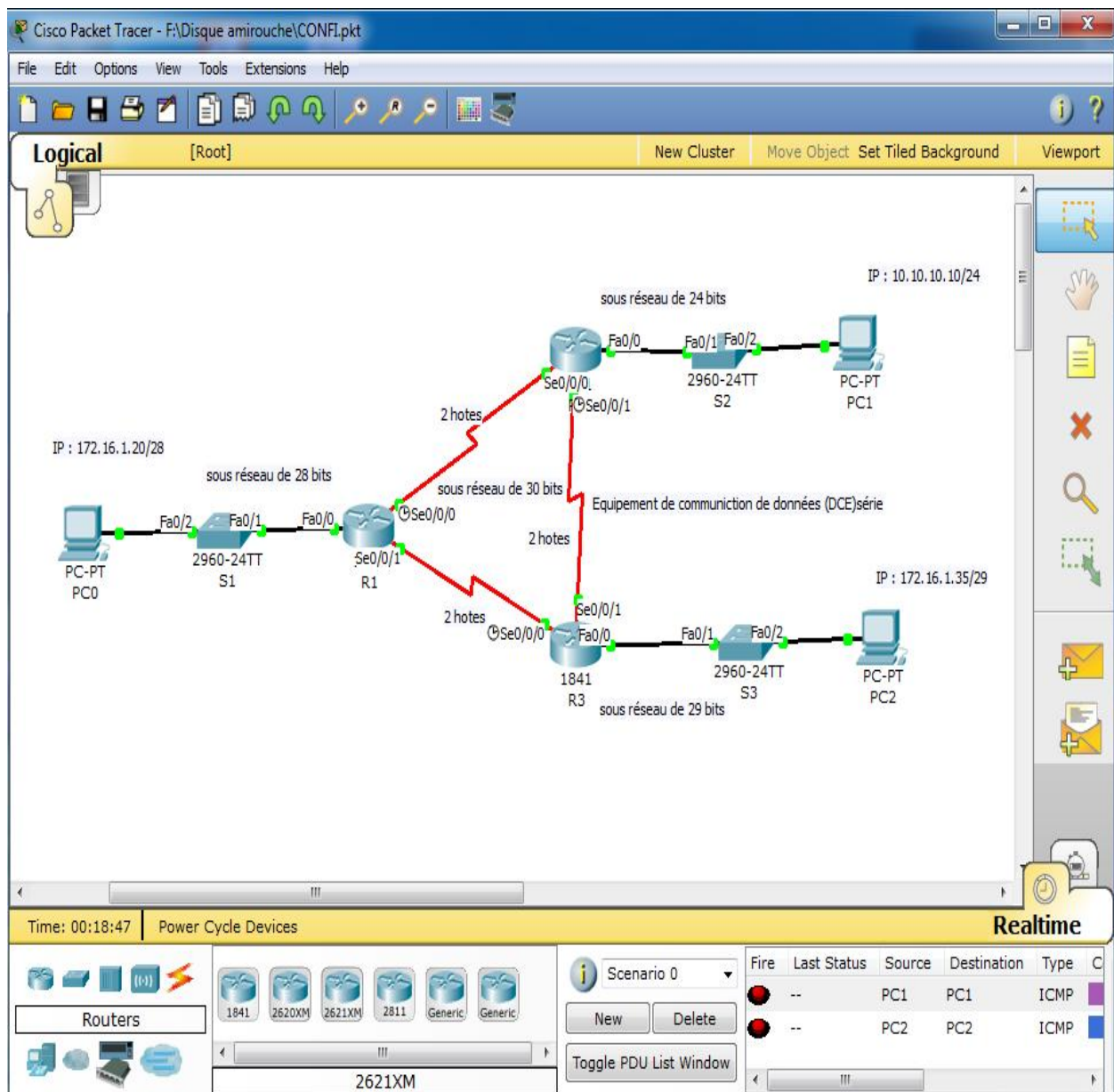


Figure IV.9 : Diagramme de la topologie.

Les routeurs utilisés sont de type Cisco 1841 et leurs interfaces sont :

- ❖ Deux interfaces FastEthernet : Fa 0/0 et 0/1.
- ❖ Deux interfaces série : Se 0/0/0 et 0/0/1.

a) Le câblage du réseau

a.1) câblage de la liaison série entre les trois routeurs

On utilise des câbles série entre les trois routeurs formant une boucle.

a.2) connections entre les trois routeurs et les commutateurs S

On utilise un câble Ethernet droit qui permet de relier l'interface FastEthernet des routeurs à l'interface FastEthernet des commutateurs.

a.3) connections entre les trois PCs aux commutateurs S

On utilise un câble Ethernet droit qui permet de relier la carte réseau de chaque PC à l'interface FastEthernet des commutateurs.

b) Adressages :

Grâce aux solutions OSPF on peut diviser les réseaux en sous-réseaux et en utilisant la technique VLSM (Variable-Length Subnet Masking), cette technique permet de donner les routes de chemin plus court par le protocole OSPF.

b.1) Définition de la technique VLSM

La technique VLSM permet d'utiliser plusieurs sous-masques dans le même espace d'adressage réseau. et peut être utilisée pour améliorer l'efficacité de l'adressage. Avec les protocoles de routage par classes (classful), un réseau doit utiliser le même masque de sous-réseau.

VLSM est simplement une fonction qui permet à un système autonome unique d'inclure des réseaux avec différents masques de sous-réseau et permet de créer des schémas d'adressage efficaces et évolutifs.

La technique VLSM permet de gérer les adresses IP. VLSM permet de définir un masque de sous-réseaux répondant aux besoins de la liaison ou du segment. Un masque de sous-réseau devrait en effet répondre aux besoins d'un LAN avec un masque de sous-réseau et à ceux d'une liaison WAN point à point avec un autre.

b.2) Partage des masques sous-réseaux par VLSM pour les interfaces

Les équipements série de routeurs R1, R2 et R3, on utilise les classes d'adressage C et les masques sous-réseaux 30 bits. Comme il ne faut que deux adresses, la portion hôte de l'adresse doit contenir au moins deux bits. Deux bits permettent de générer 2 adresses hôtes, la division donne donc ici l'adresse IP est 192.168.10.1/30 de série 0/0 de R1.

Le FastEthernet0/0 du routeur R1, son adresse IP est 172.16.1.17 et le masque sous-réseau de 28 bits (12 adresses hôtes) est 255.255.255.240.

Chapitre IV Configuration du protocole OSPF dans un réseau

Le FastEthernet0/0 du routeur R2, Son adresse IP est 10.10.10.1 et le masque sous réseau de 28 bits (12 adresses hôtes) est 255.255.255.240.

Le FastEthernet0/0 du routeur R3, Son adresse IP est 172.16.1.20 et le masque sous réseau de 29 bits (6 adresses hôtes) est 255.255.255.248.

Le PC0 et le PC2 ont même classe B et le masque sous réseau pour le PC0 est 28 bits (255.255.255.240) et le PC2 est 29 bits (255.255.255.248).

Le PC1, son classe d'adressage A et le masque sous réseau 24 bits (255.255.255.0).

Après les divisions des sous réseau par VLSM, on peut résumer par le tableau IV.1 ci-dessous :

périphérique	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
R1	Fa0/0	172.16.1.17	255.255.255.240	N/D
	S0/0/0	192.168.10.1	255.255.255.252	N/D
	S0/0/1	192.168.10.5	255.255.255.252	N/D
R2	Fa0/0	10.10.10.1	255.255.255.0	N/D
	S0/0/0	192.168.10.2	255.255.255.252	N/D
	S0/0/1	192.168.10.9	255.255.255.252	N/D
R3	Fa0/0	172.16.1.33	255.255.255.248	N/D
	S0/0/0	192.168.10.6	255.255.255.252	N/D
	S0/0/1	192.168.10.10	255.255.255.252	N/D
PC0	Carte réseau	172.16.1.20	255.255.255.240	172.16.1.17
PC1	Carte réseau	10.10.10.10	255.255.255.0	10.10.10.1
PC2	Carte réseau	172.16.1.35	255.255.255.248	172.16.1.33

Tableau IV.1 : adresses de chaque périphérique.

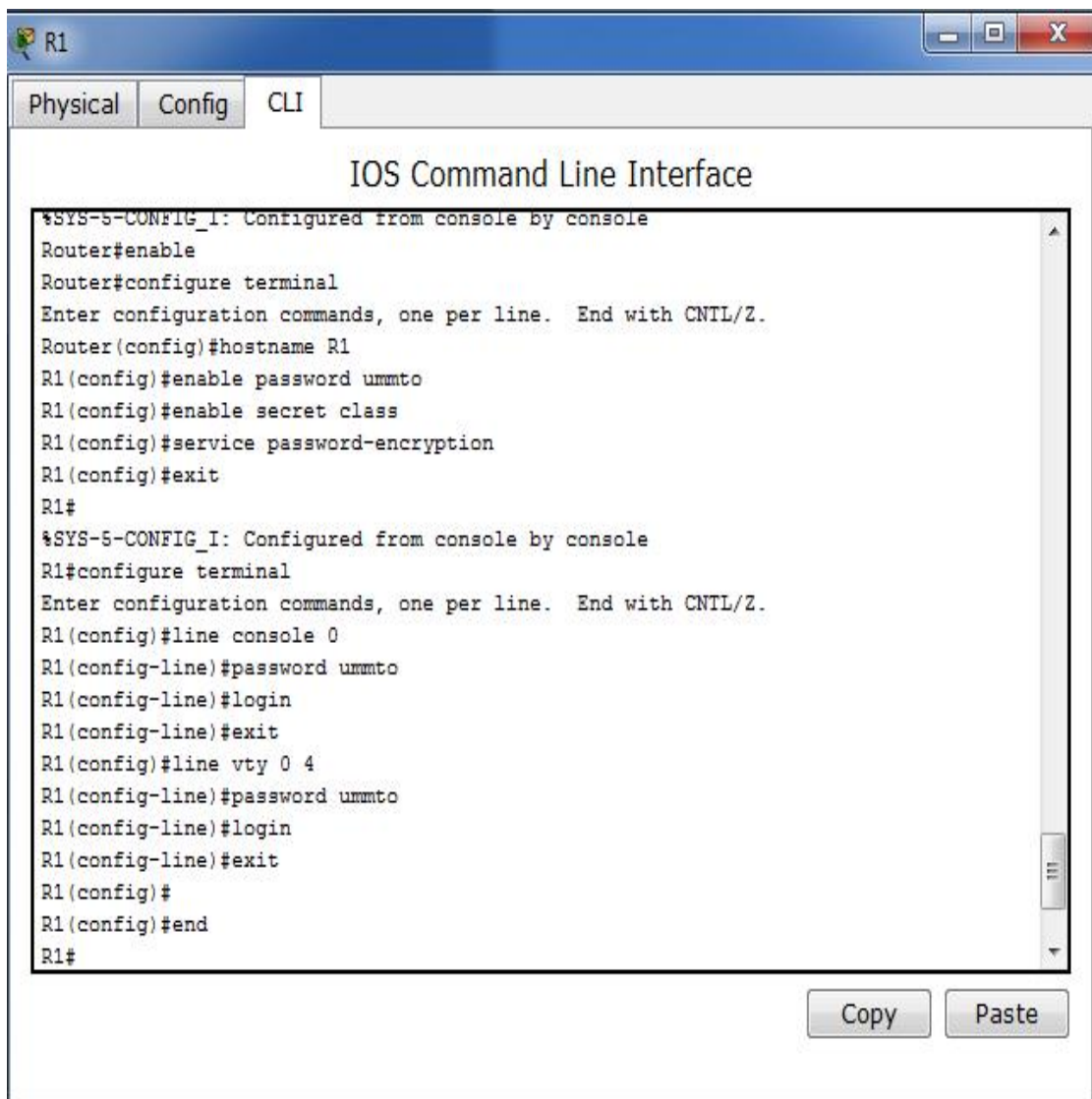
IV.5 configuration du réseau

IV.5.1 configuration des routeurs

Etape 1 :

On nomme chaque routeur et ensuite le mot de passe pour la sécurité et de la console le mot de passe vty

❖ Routeur R1 :



```
R1
Physical Config CLI
IOS Command Line Interface
%SYS-5-CONFIG_I: Configured from console by console
Router#enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R1
R1(config)#enable password ummto
R1(config)#enable secret class
R1(config)#service password-encryption
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#line console 0
R1(config-line)#password ummto
R1(config-line)#login
R1(config-line)#exit
R1(config)#line vty 0 4
R1(config-line)#password ummto
R1(config-line)#login
R1(config-line)#exit
R1(config)#
R1(config)#end
R1#
```

Copy Paste

Figure IV.10 : configuration du nom et le mot de passe du routeur.

❖ Routeur R2 : le programme de configuration de nom et le mot de passe.

```
Router#enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R2
R2(config)#enable password ummto
R2(config)#enable secret class
R2(config)#service password-encryption
R2(config)#exit
```

```
%SYS-5-CONFIG_I: Configured from console by console
R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#line console 0
R2(config-line)#password ummto
R2(config-line)#login
R2(config-line)#exit
R2(config)#line vty 0 4
R2(config-line)#password ummto
R2(config-line)#login
R2(config-line)#exit
R2(config)#
R2(config)#end
R2
```

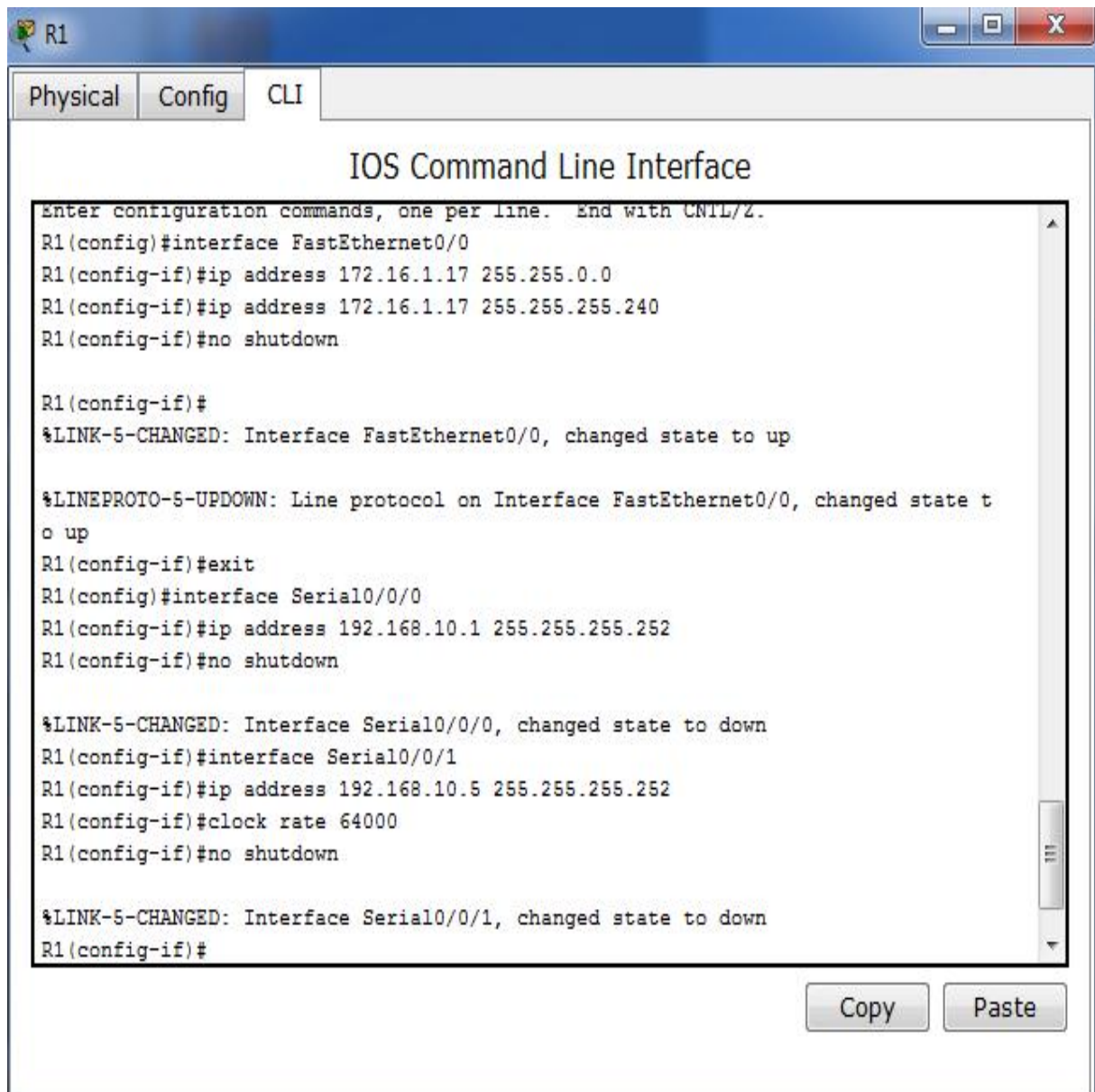
❖ **Routeur R3 : le programme de configuration de nom et le mot de passe.**

```
Router#enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R3
R3(config)#enable password ummto
R3(config)#enable secret class
R3(config)#service password-encryption
R3(config)#exit
R3#
%SYS-5-CONFIG_I: Configured from console by console
R3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#line console 0
R3(config-line)#password ummto
R3(config-line)#login
R3(config-line)#exit
R3(config)#line vty 0 4
R3(config-line)#login
R3(config-line)#exit
R3(config)#end
R3#
```

Etape 2 :

On configure les trois interfaces FastEthernet 0/0, Serial 0/0/0 et Serial 0/0/1 avec leurs adresses IP et les masques réseau, ensuite on active toutes les interfaces avec la commandes **no shutdown**

❖ Routeur R1 :



```
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#interface FastEthernet0/0
R1(config-if)#ip address 172.16.1.17 255.255.0.0
R1(config-if)#ip address 172.16.1.17 255.255.255.240
R1(config-if)#no shutdown

R1(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
R1(config-if)#exit
R1(config)#interface Serial10/0/0
R1(config-if)#ip address 192.168.10.1 255.255.255.252
R1(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial10/0/0, changed state to down
R1(config-if)#interface Serial10/0/1
R1(config-if)#ip address 192.168.10.5 255.255.255.252
R1(config-if)#clock rate 64000
R1(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial10/0/1, changed state to down
R1(config-if)#
```

Figure IV.11 : Configuration des interfaces du routeur.

❖ Routeur R2: programme de configuration des interfaces.

```
Router(config)#interface FastEthernet0/0
Router(config-if)#ip address 10.10.10.1 255.255.255.0
Router(config-if)#no shutdown
```

```
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
```

```
Router(config-if)#interface Serial0/0/0
Router(config-if)#ip address 192.168.10.2 255.255.255.252
Router(config-if)#no shutdown
```

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

```
Router(config-if)#interface Serial0/0/1
Router(config-if)#ip address 192.168.10.9 255.255.255.252
Router(config-if)#clock rate 64000
Router(config-if)#no shutdown
```

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
Router(config-if)#

❖ **Routeur R3 : programme de configuration des interfaces.**

```
R3(config)#interface FastEthernet0/0
R3(config-if)#ip address 172.16.1.33 255.255.0.0
R3(config-if)#ip address 172.16.1.33 255.255.255.248
R3(config-if)#no shutdown
```

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
o up

```
R3(config-if)#Interface Serial0/0/0
R3(config-if)#ip address 192.168.10.6 255.255.255.252
R3(config-if)#no shutdown
```

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

```
R3(config)#interface Serial0/0/1
R3(config-if)#ip address 192.168.10.10 255.255.255.252
R3(config-if)#clock rate 64000
R3(config-if)#no shutdown
R3(config-if)#
```

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up

IV.5. 2 configuration des interfaces Ethernet de PC 0, PC 1 et PC 2

Etape 1 :

On configure l'interface FastEthernet de chaque PC par son adresse IP et son masque réseau.

❖ Le PC 0 : configuration

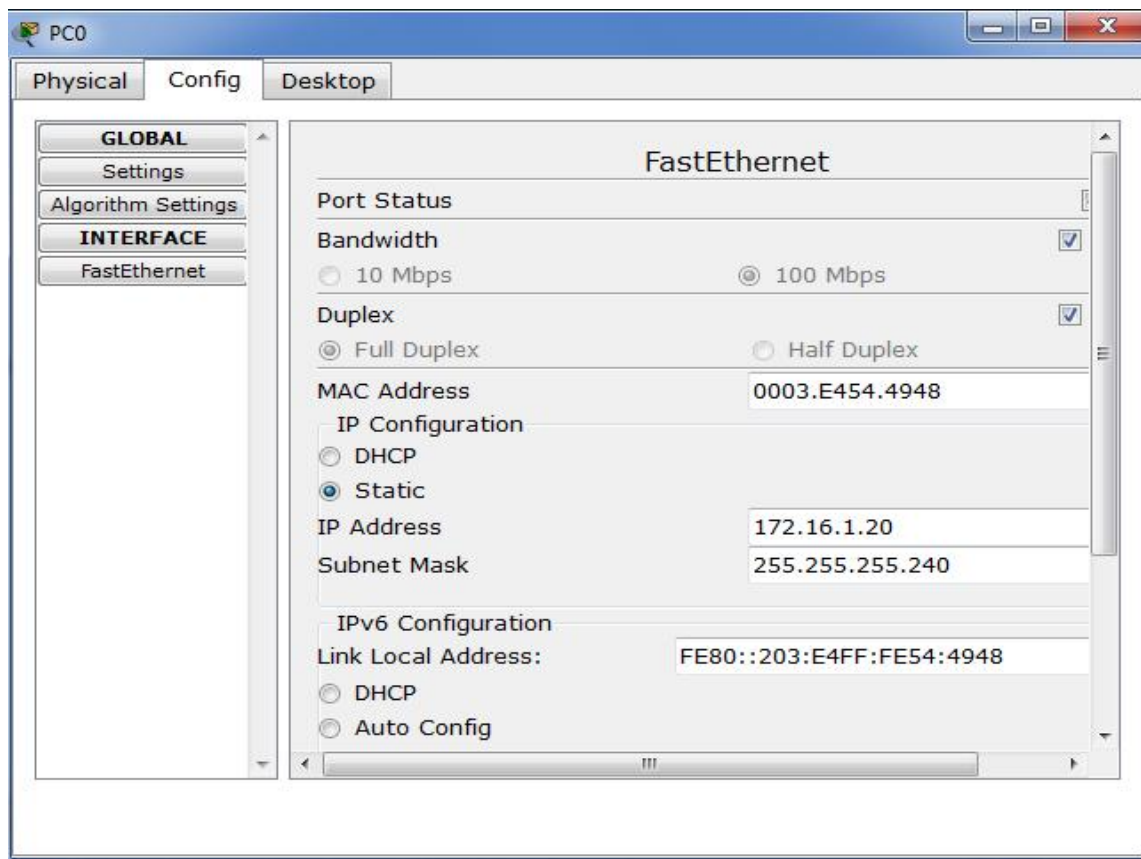


Figure IV.12 : La fenêtre de configuration d'un PC.

On applique la même configuration pour les deux autres PC 1 et PC 2 avec différentes adresses IP et masques réseaux

Étape 2 :

On applique aussi des configurations sur les trois PC avec les différentes passerelles par défaut on clique sur la commande settings.

Étape 3 :

On test la configuration de chaque ordinateur par l'exécution d'une requête ping sur la passerelle par défaut depuis l'ordinateur.

On ping adresse IP de PC 0 dans sur la passerelle PC 1 par **comand prompt**.

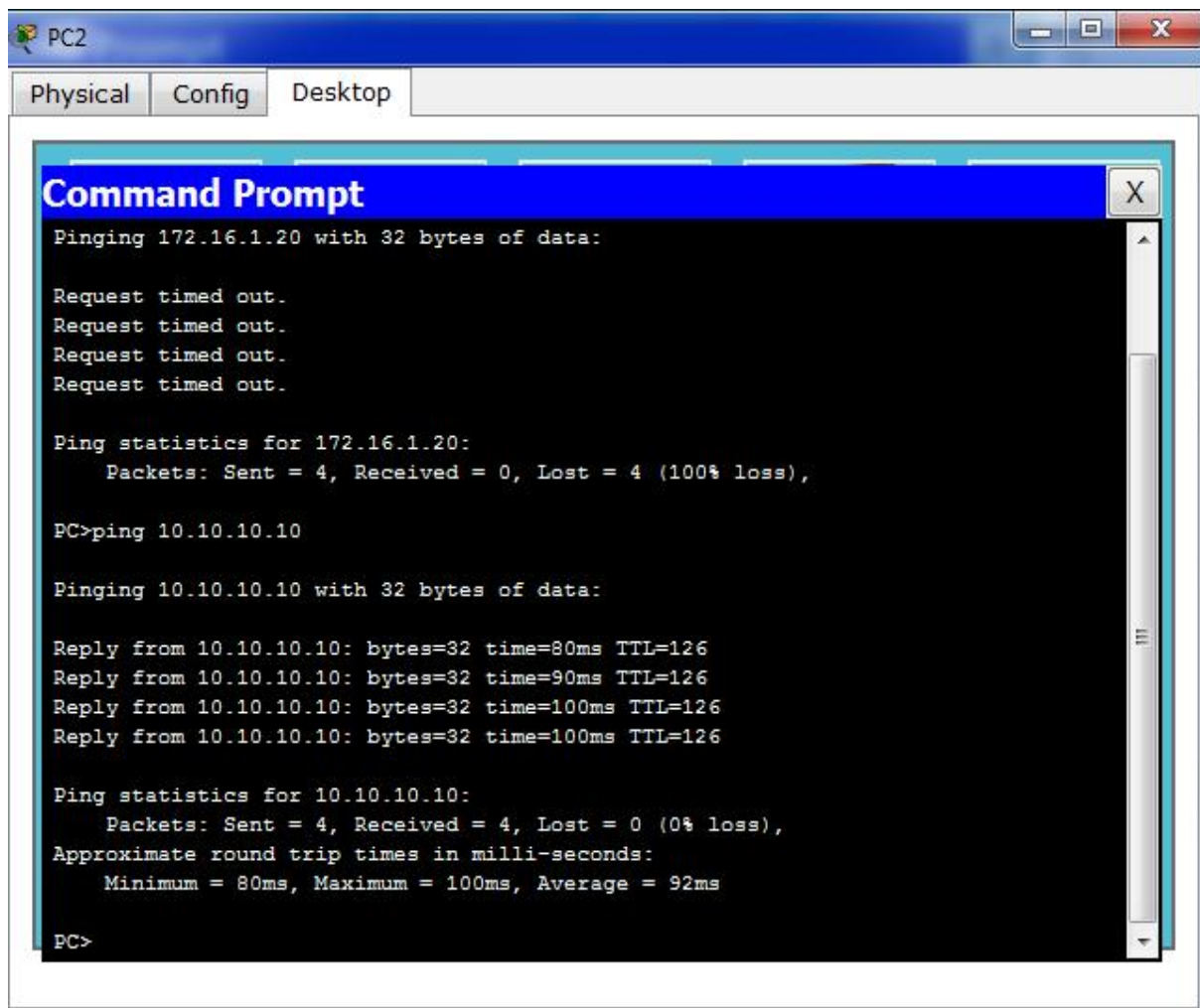


Figure IV.13 : la configuration du PC par l'exécution d'une requête ping.

On applique la même configuration sur les ordinateurs PC0 et PC2.

IV.5.3 Configuration du protocole OSPF sur les Routeurs

Etape 1 :

❖ Configuration du protocole OSPF sur le routeur R1

```
R1(config)#router ospf 1
R1(config-router)#
```

❖ Configuration du protocole OSPF sur le routeur R2

```
R2(config)#router ospf 1
R2(config-router)#
```

❖ Configuration du protocole OSPF sur le routeur R3

```
R3(config)#router ospf 1
R3(config-router)#
```

Étape 2 : configuration de l'instruction network pour le réseau local

Une fois dans le sous-mode de configuration Router OSPFest à tout les routeurs R1,R2 et R3, on configure le réseau local par la commande OSPF **network** utilise une combinaison adresse réseau et masque générique car le protocole OSPF nécessite obligatoirement le masque générique et on utilise 0 comme ID de zone pour le paramètre OSPF area-id. L'ID de zone OSPF aura la valeur 0 dans toutes les instructions **network** de cette topologie.

❖ Routeur R1 :

```
R1#enable
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#router ospf 1
R1(config-router)#network 172.16.1.17 0.0.0.15 area 0
R1(config-router)#network 192.168.10.1 0.0.0.3 area 0
R1(config-router)#network 192.168.10.5 0.0.0.3 area 0
R1(config-router)#
02:26:26: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.10.6 on Serial0/0/1 from LOADING
to FULL, Loading Done
```

❖ Routeur R2 :

```
R2#enable
R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#router ospf 1
R2(config-router)#network 10.10.10.1 0.0.0.255 area 0
R2(config-router)#network 192.168.10.2 0.0.0.3 area 0
R2(config-router)#network 192.168.10.9 0.0.0.3 area 0
R2(config-router)#
02:26:26: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.10.10 on Serial0/0/1 from LOADING
to FULL, Loading Done
```

❖ Routeur R3 :

```
R3#enable
R3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#router ospf 1
R3(config-router)#network 172.16.1.33 0.0.0.7 area 0
R3(config-router)#network 192.168.10.6 0.0.0.3 area 0
R3(config-router)#network 192.168.10.10 0.0.0.3 area 0
R3(config-router)#end
```

R3#

```
02:26:26: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.10.5 on Serial0/0/0 from LOADING to FULL, Loading Done
```

Étape 3 : examen des ID de routeur actuel dans la topologie

Étant donné qu'aucun ID de routeur et qu'aucune interface de bouclage n'a été configuré sur les trois routeurs, l'ID de chaque routeur est déterminé par l'adresse IP la plus élevée de toute interface active.

L'ID de routeur s'affiche également dans le résultat des commandes **show ip protocols**, **show ip ospf** et **show ip ospf interfaces**.

❖ Routeur R1 :

On utilise la commande **show ip protocols** et on obtient les résultats ci-dessous :
R1#show ip protocols

```
Routing Protocol is "ospf 1"  
  Outgoing update filter list for all interfaces is not set  
  Incoming update filter list for all interfaces is not set  
  Router ID 192.168.10.5  
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa  
  Maximum path: 4  
  Routing for Networks:  
    172.16.1.16 0.0.0.15 area 0  
    192.168.10.0 0.0.0.3 area 0  
    192.168.10.4 0.0.0.3 area 0  
  Routing Information Sources:  
    Gateway         Distance      Last Update  
    192.168.10.6          110         00:05:08  
  Distance: (default is 110)
```

R1#

❖ Routeur R2 :

R2#show ip protocols

```
Routing Protocol is "ospf 1"  
  Outgoing update filter list for all interfaces is not set  
  Incoming update filter list for all interfaces is not set  
  Router ID 192.168.10.9  
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa  
  Maximum path: 4  
  Routing for Networks:  
    10.10.10.0 0.0.0.255 area 0
```

```
192.168.10.0 0.0.0.3 area 0
192.168.10.8 0.0.0.3 area 0
Routing Information Sources:
  Gateway    Distance  Last Update
Distance: (default is 110)
```

R2#

❖ **Routeur R3 :**

R3#show ip protocols

```
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 192.168.10.6
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.16.1.32 0.0.0.7 area 0
    192.168.10.8 0.0.0.3 area 0
    192.168.10.4 0.0.0.3 area 0
  Routing Information Sources:
    Gateway    Distance  Last Update
    192.168.10.5    110    00:22:33
  Distance: (default is 110)
```

R3#

On déduit que :

Le routeur ID de routeur de R1 est **192.168.10.5**
Le routeur ID de routeur de R2 est **192.168.10.9**
Le routeur ID de routeur de R3 est **192.168.10.6**

IV.5.4 adresse de bouclage des routeurs

La commande **interface loopback 0** est une boucle pour modifier les ID des routeurs de la topologie réseau.

Étape 1 :

On utilise des adresses de bouclage pour modifier les ID des routeurs de la topologie

❖ **Routeur R1 :**

On utilise l'adresse IP : 10.1.1.1 et le masque réseau est: 255.255.255.255
Donc on aura le programme :

```
R1(config)#interface loopback 0
```

Chapitre IV Configuration du protocole OSPF dans un réseau

%LINK-5-CHANGED: Interface Loopback0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up

```
R1(config-if)#ip address 10.1.1.1 255.255.255.255
```

```
R1(config-if)#end
```

```
R1#
```

❖ **Routeur R2 :**

On utilise l'adresse IP : 10.2.2.2 et le masque réseau est: 255.255.255.255

Donc on aura le programme :

```
R2(config)#interface loopback 0
```

%LINK-5-CHANGED: Interface Loopback0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up

```
R2(config-if)#ip address 10.2.2.2 255.255.255.255
```

```
R2(config-if)#end
```

```
R2#
```

❖ **Routeur R3 :**

On utilise l'adresse IP : 10.3.3.3 et le masque réseau est: 255.255.255.255

Donc on aura le programme:

```
R3(config)#interface loopback 0
```

%LINK-5-CHANGED: Interface Loopback0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up

```
R3(config-if)#ip address 10.3.3.3 255.255.255.255
```

```
R3(config-if)#end
```

```
R3#
```

Étape 2:

On utilise de la commande `show ip ospf neighbors` pour vérifier que les ID de routeur ont été modifiés

❖ **Routeur R1**

```
R1#show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
192.168.10.6	0	FULL/ -	00:00:32	192.168.10.6	Serial0/0/1

```
R1#
```

❖ Routeur R2

```
R2#show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
192.168.10.9	0	FULL/-	00:00:34	192.168.10.9	Serial0/0/1

```
R2#
```

❖ Routeur R3

Neighbor ID	Pri	State	Dead Time	Address	Interface
192.168.10.5	0	FULL/-	00:00:36	192.168.10.5	Serial0/0/0

```
R3#
```

Dans cette configuration on remarque que les deux routeurs R1 et R3 sont des voisins ont changés les adresses IP de routeur ID entre l'interface Serial0/0/1 et l'interface Serial0/0/1.

IV.5.5 Configuration du coût OSPF

Étape 1 : utilisation de la commande show ip route sur le routeur R1 pour afficher le coût OSPF pour atteindre le réseau 10.10.10.0/24

❖ Pour R1 :

On Affiche la table de routage du routeur R1. Les routes OSPF sont signalées par un « O » dans la table de routage.

```
R1#show ip route
```

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

```
Gateway of last resort is not set
```

```
10.0.0.0/32 is subnetted, 1 subnets
C    10.1.1.1 is directly connected, Loopback0
172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C    172.16.1.16/28 is directly connected, FastEthernet0/0
O    172.16.1.32/29 [110/65] via 192.168.10.6, 01:52:44, Serial0/0/1
192.168.10.0/30 is subnetted, 1 subnets
C    192.168.10.4 is directly connected, Serial0/0/1
R1#
```

Même résultats pour les autres interfaces.

Étape 2 : utilisation de la commande show interfaces serial0/0/0 sur le routeur R1 pour afficher la bande passante de l'interface Serial0/0/0

```
R1#show interfaces serial0/0/0
Serial0/0/0 is up, line protocol is down (disabled)
Hardware is HD64570
```

```
Internet address is 192.168.10.1/30
MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
  reliability 255/255, txload 1/255, rxload 1/255
Encapsulation HDLC, loopback not set, keepalive set (10 sec)
Last input never, output never, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0 (size/max/drops); Total output drops: 0
<output omitted>
```

Même résultats pour les autres interfaces.

Étape 3 :

Vérification le coût de chaque liaison

```
R1#show ip ospf interface
FastEthernet0/0 is up, line protocol is up
  Internet address is 172.16.1.17/28, Area 0
  Process ID 1, Router ID 192.168.10.5, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 192.168.10.5, Interface address 172.16.1.17
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  Hello due in 00:00:07
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
Serial0/0/1 is up, line protocol is up
  Internet address is 192.168.10.5/30, Area 0
  Process ID 1, Router ID 192.168.10.5, Network Type POINT-TO-POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  Hello due in 00:00:05
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
  Adjacent with neighbor 192.168.10.9
  Suppress hello for 0 neighbor(s)
Serial0/0/1 is up, line protocol is up
  Internet address is 192.168.10.5/30, Area 0
  Process ID 1, Router ID 192.168.10.5, Network Type POINT-TO-POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
```

```
No designated router on this network
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  Hello due in 00:00:06
Index 3/3, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1 , Adjacent neighbor count is 1
  Adjacent with neighbor 192.168.10.10
Suppress hello for 0 neighbor(s)
R1#
```

IV.6 Conclusion

D'après les étapes de configurations on déduit que l'OSPF permet de :

- ❖ Sélectionner les routes en fonction du coût, qui est lié à la vitesse. Plus la vitesse est élevée, et plus le coût OSPF du lien est faible.
- ❖ Calculer le coût le plus bas vers une destination (Sélectionner le chemin plus court vers la destination).
- ❖ Garantir un routage de boucles et vitesse de convergence.
- ❖ prendre en charge le masque de sous-réseau de longueur variable.
- ❖ Prendre en considération la taille du réseau.
- ❖ Obtenir une table de routage avec les meilleures routes.
- ❖ Modifier les informations et après qu'un routeur ait identifié un voisin, les routeurs s'échangent leurs informations topologiques.

Conclusion générale

Conclusion générale

Dans cette contribution, nous avons étudié les réseaux informatiques en particulier le routage dynamique à l'état de liaison.

Ce travail m'a permis d'acquérir beaucoup de connaissances sur le fonctionnement des réseaux informatiques.

Le protocole de routage permet à un routeur de partager avec d'autres routeurs des informations sur les réseaux qu'il connaît, ainsi que sur leur proximité avec d'autres routeurs.

Nous avons expliqué le rôle de chaque protocole de routage dynamique et la comparaison entre protocoles à vecteur de distance et à l'état de liaison, Ensuite la mise en œuvre et les éléments requis d'un protocole de routage à l'état de liaison.

Enfin, nous avons utilisé le logiciel PACKET TRACER pour la configuration du protocole OSPF dans un réseau informatique. Les résultats de chaque étape de configuration sont satisfaisants pour l'étude de différentes métriques du protocole OSPF et notamment l'acheminement des données (le meilleur chemin le plus court) entre les routeurs. Le protocole OSPFV2 et OSPFV3 offrait des améliorations techniques significatives par rapport au protocole OSPFV1.

Nous espérons que ce travail sera utile pour les améliorateurs des réseaux informatiques.

Bibliographie

Bibliographie

Ouvrages :

- ❖ [Hav 05] j. Havez. " Routage Statique, Dynamique avec Ripv1, Ripv2 et OSPF". Ed .UTBM, 2005.
- ❖ [Hed 88]C. Hedrick. "Routing Information Protocol". Internet Request Comments RFC 1058, June 1988.
- ❖ [Moy 94] J. Moy. "OSPF Version 2". Internet Request For Comments RFC 1583, March 1994.
- ❖ [Puj 04] G. Pujolle. "Cours réseaux et télécom" .Ed. Eyrolles, 2004.
- ❖ [Rud 05] I. Rudenko. "Configuration IP des routeurs Cisco" .Ed. Eyrolles, 2005.
- ❖ [Sea 03] D.Seab. "Interconnexion des réseaux à l'aide des routeurs commutateurs". Ed. ENI, Novembre 2003.
- ❖ [Stev 99] G.Steve. " Synthèse de protocoles courants". Ed. Degouet Fabien ; 1999.

Thèses :

- ❖ [Gri, 11] N.Grim, "les protocoles de Routage dynamique à vecteur de distance", Mémoire de fin d'étude Master, Dpt Electronique, UMMTO 2011.
- ❖ [Ham 07] M.Hammar, "interaction entre le protocole MAC et les protocoles de couche hautes pour l'optimisation et la performance dans un réseau MANET", Mémoire de Magister, Dpt informatique, UMMTO, 2007.
- ❖ [Kab, 07] N.Kabeche, "Interconnexion du réseau TCP/IP à base des routeurs CISCO", Mémoire de fin d'étude Ingénieur, Dpt Electronique, UMMTO 2007.
- ❖ [Oul, 05] M.Ouled, "Etude des protocoles pour les réseaux Informatiques", Mémoire de fin d'étude Ingénieur, Dpt Electronique,(Institut de Télécommunication d'Oran) 2005.

Sites Web :

- ❖ <http://www.reseaux-telecoms.fr>
- ❖ <http://www.commentcamarche.com>.
- ❖ <http://www.guill.net>.
- ❖ <http://www.y> <http://bet.be>.
- ❖ <http://www.egs-howto.com>.
- ❖ <http://www.linux-france.org>.
- ❖ <http://www.supinfo.com> .
- ❖ <http://www.cisco.fr>.
- ❖ <http://www.commentcamarche.net/forum>
- ❖ <http://www.ipsec-howto.org/>
- ❖ <http://www.hsc.fr/>
- ❖ <http://www.ietf.org>

