REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE
UNIVERSITE MOULOUD MAMMERI
FACULTE DE GENIE ELECTRIQUE ET INFORMATIQUE
DEPARTEMENT D'ELECTRONIQUE

Memoire

De fin d'études

En vue de l'obtention du diplôme de Master en Electronique
Option Réseau et Télécommunication

Thème

Protocoles de routage dynamique à vecteur de distance

Dirigé par :
Mr Ziani.R

Réalisé par :
Mr. GRIM NACIM
Mr. IDIR KAMAL

Promotion 2010/2011

REMERCIEMENT

Tout d'abord gloire à notre dieu, qui nous a donné la force et le courage pour terminer nos études.

A travers ce modeste travail, nous tenons à remercier vivement notre promoteur Monsieur ZIANI pour son encadrement et ces conseils et pour intéressante documentation qu'il a mise à notre disposition, pour ses conseils précieux et pour toutes les commodités et aisances qu'il nous a apportées durant notre étude et réalisation de ce projet.

Les remerciements les plus vifs s'adressent aussi aux messieurs ; le président et les membres de jury d'avoir accepté d'examiner et d'évaluer notre travail.

Nous exprimons également notre gratitude à tous les professeurs et enseignants qui ont collaboré à notre formation depuis notre premier cycle d'étude jusqu'à la fin de notre cycle universitaire.

Sans omettre bien sur de remercier profondément tous ceux qui ont contribué de prés ou de loin à réalisation du présent travail.

Et enfin, que nos chers parents et familles, et bien avant tout, trouvent ici l'expression de nos remerciements les plus sincères et les plus profonds en reconnaissance de leurs sacrifices, aides, soutien et encouragement afin de nous assurer cette formation master2 dans les meilleures conditions.

Dédicaces

Je dédie ce modeste travail à :

- *Mes très chers parents qui m'ont toujours souhaité la réussite et qui m'ont beaucoup soutenu. Que Dieu les gardes.*
- *Mes grands parents.*
- *A mes chères sœurs : Shahrazed, Thinhinane .*
- *A tous mes amis : Ali, Amirouche, Djamel, Sofiane, Seddik et en particulière Hakim et Azzdine .*
- *A mes cousins et cousines.*
- *A mon binôme Kamal et toutes sa famille.*
- *A tous ceux qui m'ont aidé durant ma vie universitaire.*
- *A toutes la promotion 2011 et en particulière les étudiants d'option 'Réseaux et télécommunication'.*

N.GRIM

Dédicaces

Je dédie ce modeste travail à :

- *Mes très chers parents qui m'ont toujours souhaité la réussite et qui m'ont beaucoup soutenu. Que Dieu les gardes.*
- *A mes chers (es) frères et sœurs.*
- *A tous mes amis : Akli, Amirouche, Ali, Azzedine, Belaid, Djamel, Sedik et en particulière Hakim et kader.*
- *A mon binôme Nacim et toutes sa famille.*
- *A tous ceux qui m'ont aidé durant ma vie universitaire.*
- *A toutes la promotion 2011 et en particulière les étudiants d'option 'Réseaux et télécommunication'.*

k. IDIR

Sommaire

Chapitre II : protocoles de routage

Chapitre III Protocoles de routage dynamique à vecteur de distance

Chapitre IV Configuration du Protocole RIP sur un réseau

Conclusion générale

Bibliographie

Liste des figures

Liste des Tableaux

Introduction générale

Introduction générale

L'explosion de l'industrie informatique a profondément influencée le rapprochement du monde informatique et celui des télécommunications. La nécessité de pouvoir communiquer et de partager des informations ont contribué à l'émergence de l'idée de concevoir des réseaux.

Un réseau informatique est un ensemble de connexion entre plusieurs ordinateurs géographiquement dispersés sur une petite ou une plus grande surface. Pour réaliser ce réseau, il est nécessaire de ce procurer un environnement matériel (câble terrestres, des ondes radio, des ordinateurs, des commutateurs,…etc.) et un environnement logiciel composé de protocoles.

Un protocole réseau est un ensemble de règles et de procédures de communication. En effet, différentes piles de protocoles peuvent coexistées sur une même station selon les besoins de communication vers des environnements différents. Le plus souvent, les couches du modèle OSI sont constituées de pile de protocole. Ce modèle est la première étape vers une normalisation internationale des différents protocoles. Ce modèle est devisé en septe couches indépendantes. Une nouvelle architecture de référence a dû être développée pour permettre aux protocoles existants d'interagir entre eux. En fait, la possibilité d'interconnecter de nombreux réseaux de façon transparente était un des objectifs de la conception d'ARPANET. Plus tard, cette architecture est devenue le modèle TCP/IP, elle est la source du réseau internet.

Pour mettre en place des réseaux TCP/IP, il est nécessaire de disposer de routeur. Le but d'un routeur est de relier un réseau à un autre. Le routeur est donc responsable de la transmission de paquets à travers différents réseaux. La destination du paquet IP peut être un serveur Web se trouvant dans un autre pays ou un serveur de messagerie situé sur le réseau local. Les routeurs doivent transmettre ces paquets rapidement. L'efficacité des communications interréseaux dépend, en grande partie, de la capacité des routeurs à transférer des paquets de la manière la plus efficace possible.

Aujourd'hui, des routeurs sont ajoutés aux satellites dans l'espace. Ces routeurs sont capables d'acheminer le trafic IP entre les satellites dans l'espace, d'une manière similaire à l'envoi de paquets sur terre, ce qui permet de réduire les délais et d'accroître la flexibilité des réseaux.

Toutefois, le routeur ne sert pas seulement à transférer des paquets. Pour répondre aux demandes sur les réseaux actuels, les routeurs sont également utilisés pour :

- Ø Assurer une disponibilité 24 heures sur 24, 7 jours sur 7. Afin de garantir l'accessibilité des réseaux, les routeurs utilisent des chemins de remplacement si le chemin principal est défaillant.
- Ø Fournir des services intégrés de données, de vidéo et de voix sur les réseaux filaires et sans fil. Les routeurs utilisent la hiérarchisation de la qualité de service des paquets IP, pour veiller à ce que le trafic en temps réel, par exemple les données vocales et vidéo, ainsi que les données importantes, ne soit pas abandonné ni retardé.

Tous ces services reposent sur le routeur et sur sa responsabilité principale de transférer les paquets d'un réseau à l'autre. Les périphériques sur différents réseaux ne peuvent communiquer que si le routeur est capable d'acheminer des paquets entre les réseaux.

Nous avons partagé notre mémoire en quatre chapitres :

Le premier chapitre de ce mémoire introduit les notions de base des réseaux informatiques et la présentation du modèle OSI ainsi que le protocole TCP/IP qui est responsable de l'acheminement des données dans les supports de transmissions.

Le second chapitre présente la définition de routage IP et les protocoles de routage dynamique en donnant notamment des informations sur la classification des différents protocoles de routage, les mesures qu'ils utilisent pour déterminer le meilleur chemin et les avantages que présente l'utilisation d'un protocole de routage dynamique.

Le troisième chapitre décrit les caractéristiques, les opérations et les fonctionnalités propres aux protocoles de routage à vecteur de distance

Dans le quatrième chapitre, nous mettons en pratique l'interconnexion de trois réseau à l'aide d'un protocole de routage dynamique à vecteur de distance RIP, en utilisant le simulateur **Packet tracer version 5.1**.

CHAPITRE I

Généralités sur les réseaux

I.1 Introduction

Un réseau est un ensemble de nœuds (ordinateurs) reliés entre eux par des arcs (télécommunications). On dit souvent qu'un réseau connecte des machines, ce qui est une réalité, mais en fait il permet surtout la communication entre les tâches qui s'exécutent sur les machines.

Cet ensemble est constitué d'au moins un support de transmission pour l'acheminement des données, et de protocoles de communication selon une architecture en couches conforme ou non au modèle OSI (Open Systems Interconnection) ou Système ouvert. On parle parfois de système de communication pour désigner un réseau.

Afin de simplifier la définition des normes de communication, en les situant les unes par rapport aux autres, l'organisation internationale de normalisation (ISO) a lancé en 1977 un projet de définition d'un modèle de référence pour l'interconnexion de systèmes ouverts, appelé simplement **«modèle OSI »** ou **«modèle de référence OSI »**.La version finale du modèle OSI date de 1984.

Un système est dit **ouvert** lorsqu'il permet la communication entre équipements de types différents, pouvant provenir de constructeurs différents, pourvu que ces équipements respectent les règles de communication dans un environnement OSI. Les règles de communication sont publiques, accessibles à tous. Dans le cas contraire, le système est dit **priv**é, lorsqu'il ne permet la communication qu'entre des équipements d'un même type, ou d'un même constructeur, en utilisant des protocoles qui sont la propriété de quelqu'un.

Le réseau informatique est né du besoin de relier des terminaux distants à un site central, pour faire du télétraitement (utilisation à distance d'un ordinateur), puis des ordinateurs entre eux pour le besoin de partager des ressources.

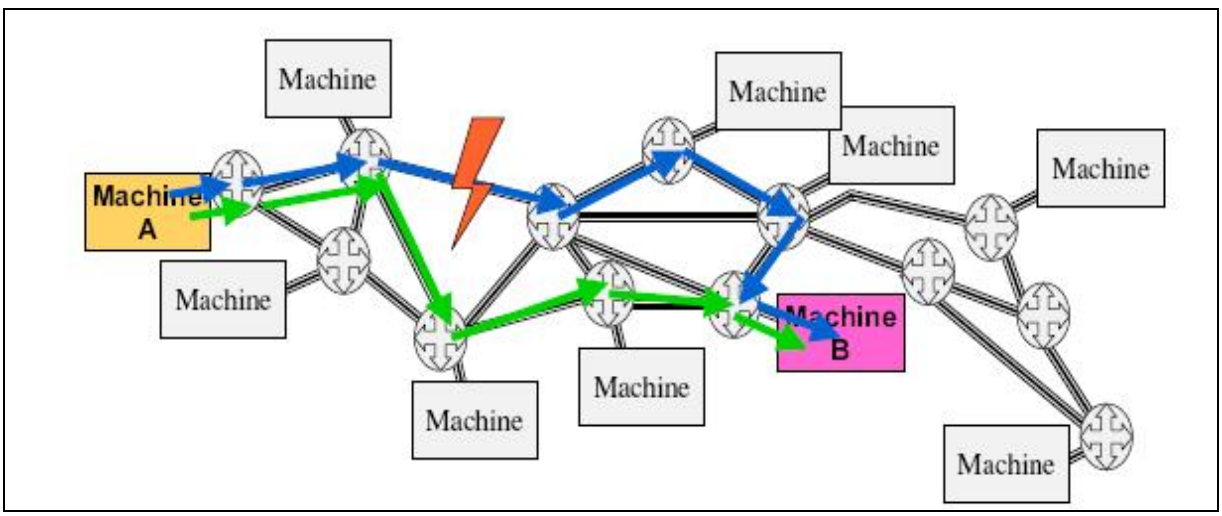


Figure I.1 : Structure générale d'un réseau.

I.2 Classification des réseaux

Les réseaux informatiques peuvent être classés en se basant sur plusieurs critères, par exemple la distance entre entités communicantes, la topologie et le type d'accès ….

I.2.1 Classification selon leur taille

On peut faire une première classification des réseaux à l'aide de leur taille comme on peut le voir dans la figure (Fig.1-2). On trouve des réseaux limités à des très courtes distances déterminées par des fils électriques spéciales à l'intérieur d'un même ordinateur, ces fils électriques sont appelés des bus. Cette approche peut être étendue pour atteindre un environnement local, on parle de RLE ou LAN. Si la distance est plus grande, nous parlons de RM ou MAN qui correspond à un réseau de ville. Enfin, si la distance est très grande nous parlons de RLE ou WAN qui sont des réseaux destinés à transporter les données à l'échelle d'un pays ou à l'échelle mondiale.

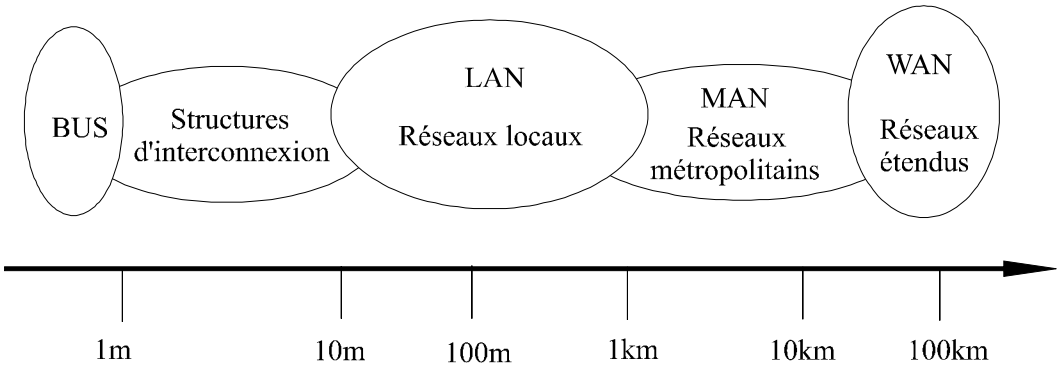


Figure I.2 : Classification des réseaux informatiques selon leur taille.

a. Les Bus

Les bus que l'on trouve dans un ordinateur pour relier ses différents composants (mémoires, périphériques d'entrée-sortie, processeurs, ...) peuvent être considérés comme des réseaux dédiés à des tâches très spécifiques. (Distance ≤ 1 mètre)

b. Les structures d'interconnexion

Permettent de relier plusieurs calculateurs à l'intérieur d'une même salle. On les retrouve dans les architectures multiprocesseurs.

c. Le réseau LAN (Local Area Network)

Représente une architecture localisée géographiquement (quelques mètres à quelques kilomètres). Leur but est la transmission de données à l'intérieur d'une entreprise. On dit aussi que ce sont des réseaux intra-entreprises

d. Réseau local industriel

Un réseau local industriel est un réseau local utilisé dans une usine ou tout système de production pour connecter diverses machines, afin d'assurer la commande, la supervision, la maintenance, en un mot, l'exploitation de l'installation. Réseau local d'entreprise

Alors que les réseaux locaux industriels sont utilisés par les processus déclenchés selon l'état des machines et par les événements survenant dans leur environnement, les réseaux locaux d'entreprise sont utilisés en final par des êtres humains. Les utilisateurs de réseaux locaux d'entreprise du point de vue technique, sont les stations de travail, les terminaux, les micro-ordinateurs et les serveurs qui leur sont connectés. Mais devant ces matériels, ce sont des êtres humains qui décident ou non d'utiliser leur outil de travail et le réseau en fonction de ce qu'ils ont à faire.

e. Les réseaux métropolitains MAN (Metropolitain Area Network)

Un réseau métropolitain 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.

f. Les réseaux étendus WAN (Wide Area Network)

Un réseau étendu permet de communiquer à l'échelle d'un pays, ou de la planète entière, les infrastructures physiques pouvant être terrestres (infrastructures au niveau sol), ou spatiales à l'aide de satellites de télécommunications c'est le cas de l'Internet.

On peut également différencier les réseaux par leur structure ou topologie physique (disposition des stations et manière dont elles sont reliées).

I.2.2 Classification selon la topologie

Un réseau informatique est constitué d'ordinateurs reliés entre eux grâce au matériel (câblage, cartes réseau, ainsi que d'autres équipements permettant d'assurer la bonne circulation des données). L'arrangement physique de ces éléments est appelé topologie physique

a. Topologie en bus

Le bus, est un segment central où circulent les informations, s'étend sur toute la longueur du réseau, et les machines viennent s'y accrocher. Lorsqu'une station émet des données, elles circulent sur toute la longueur du bus et la station destinatrice peut les récupérer. Une seule station peut émettre à la fois. En bout de bus, un « bouchon » permet de supprimer définitivement les informations pour qu'une autre station puisse émettre.

L'avantage du bus est qu'une station en panne ne perturbe pas le reste du réseau. Elle est, de plus, très facile à mettre en place. Par contre, en cas de rupture du bus, le réseau devient inutilisable. Notons également que le signal n'est jamais régénéré, ce qui limite la longueur des câbles.

Cette topologie est utilisée dans les réseaux Ethernet 10 Base 2 et 10 Base 5.

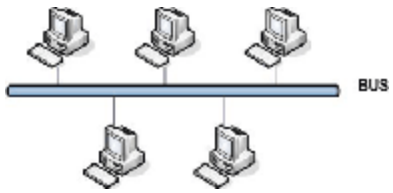


Figure I.3 : Topologie en bus.

b. Topologie en anneau (RING)

Développée par IBM, cette architecture est principalement utilisée par les réseaux Token Ring. Ce dernier la technique d'accès par « jeton ». Les informations circulent de stations en stations, en suivant l'anneau. Un jeton circule autour de l'anneau. La station qui a le jeton émet des données qui font le tour de l'anneau. Lorsque les données reviennent, la station qui les a envoyées les élimine du réseau et passe le jeton à son voisin, et ainsi de suite…

Cette topologie permet d'avoir un débit proche de 90% de la bande passante. De plus, le signal qui circule est régénéré par chaque station. Par contre, la panne d'une station rend l'ensemble du réseau inutilisable. L'interconnexion de plusieurs anneaux n'est pas facile à mettre en œuvre.

Cette topologie est utilisée par les réseaux Token Ring et FDDI.

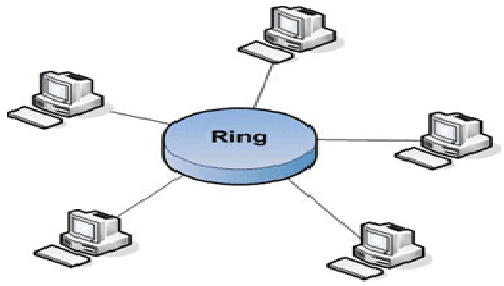


Figure I.4 : Topologie en anneau (Ring).

c. Topologie en étoile (Star)

C'est la topologie la plus courante. Toutes les stations sont reliées à un seul composant central (concentrateur). Quand une station émet vers le concentrateur, celui-ci envoie les données à toutes les autres machines (hub).

Ce type de réseau est facile à mettre en place et à surveiller. La panne d'une station ne met pas en cause l'ensemble du réseau. Par contre, il faut plus de câbles que pour les autres topologies, et si le concentrateur tombe en panne, tout le réseau est anéanti. De plus, le débit pratique est moins bon que pour les autres topologies.

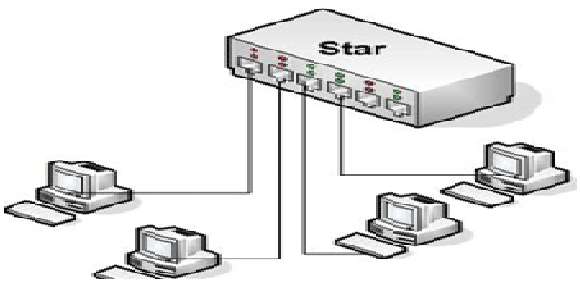


Figure I.5 : Topologie en étoile.

b. Structure Hybride

La structure hybride de réseau emploie un mélange de différentes structures de réseau, comme l'anneau, le Bus et également l'étoile.

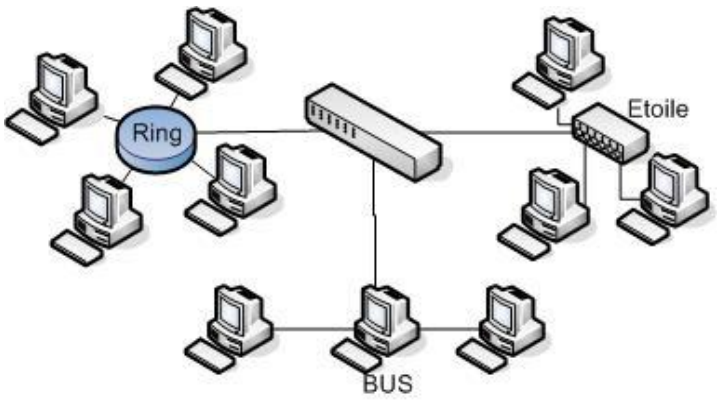


Figure I.6 : Topologie hybride.

I.2.3 Classification selon le mode de connexion

a. Les modes avec connexion

Le mode avec connexion consiste à faire appel à 3 phases distinctes:

- L'établissement de la connexion, le transfert de données et la libération de laconnexion.
- Dans le mode avec connexion, la transmission des données 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.
- En plus, l'émetteur et le récepteur négocient, sur quelques paramètres définissant les limites admissibles pour le transfert des données, c'est la négociation de la qualité de service.

En revanche, le mode avec connexion présente quelques inconvénients:

- la lourdeur de mise en œuvre : temps d'émission plus long,... ;
- la difficulté de mise en œuvre de plusieurs requêtes de même nature (exemple : diffusion de fichier) : applications multipoints.

Exemple de réseau en mode connecté est l'ATM (Asynchronous Transfer Mode).

b. Les modes sans connexion

Le mode sans connexion n'a pas besoin de présence, à la fois et en même temps, des entités communicantes distantes. Il n'y a 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.

La difficulté de mode sans connexion réside sur l'établissement du contrôle de communication par le gestionnaire de réseau qui doit prendre des précautions. En outre, dans une communication en mode non connecté, les données (ou unités de données) sont connues à l'avance, et joignes par des informations de contrôle ainsi que l'adresse complète des deux entités c'est-à-dire émetteur et récepteur.

I.2.4 Classification selon la Méthodes d'Accès

Dans un réseau local, chaque nœud est susceptible d'émettre sur le même câble de liaison. L'ensemble des règles d'accès, de durée d'utilisation et de surveillance constitue le protocole d'accès aux câbles ou aux média de communication. Les méthodes d'accès proprement dites sont aux nombres de deux : CSMA/CD, Token Ring (jeton).

a)- La méthode d'accès CSMA/CD

Dans la norme 802.3 et Ethernet la méthode choisie est CSMA (Carrier Sens Method Access). Son principe est celui de la politesse : on ne parle que quand personne ne parle.

Lorsque la station veut émettre, elle écoute. Si personne d'autre n'émet, elle émet. Si une autre station émet, elle attend. Ensuite soit elle réessaye plus tard (CSMA non persistant, la méthode n'est plus utilisée), soit elle écoute et lorsque c'est libre elle émet (CSMA persistant).

Cette méthode a un inconvénient : lorsque deux stations attendent, elles vont émettre en même temps. Les deux signaux vont se superposer et être incompréhensibles. On appelle cela une collision. Pour résoudre ce problème on va effectuer une détection des collisions (CD : Collision Detection). D'où le nom de CSMA/CD. Pour reconnaître une collision, l'émetteur écoute son écho, s'il correspond à ce qu'il émet c'est bon, si non c'est qu'il y a une collision. Il émet alors un « JAM » pour avertir tout le monde qu'il y a eu une collision. Ensuite les stations qui voulaient parler calculent un nombre aléatoire et se mettent en veille pendant un temps proportionnel à ce nombre. Et ainsi de suite jusqu'à ce qu'elles puissent parler.

b. La méthode d'accès par jeton

Dans le cas des réseaux à topologie en anneau ou en bus, une trame vide circule en permanence sur le câble qui relie l'ensemble des machines. Cette trame s'appelle le jeton.
Les différentes étapes de cette méthode sont :
Attendre la réception du jeton de transmission. Le jeton circule et passe de nœud en nœud d'une manière séquentielle. Seul le détenteur du jeton peut transmettre un message.

- Ø Si le jeton de transmission est reçu et qu'il n'y a aucun message à envoyer, acheminer le jeton au prochain nœud.
- Ø Si le jeton de transmission est reçu et qu'il y a un message à transmettre, alors:

a. seul le détenteur du jeton peut transmettre un message.
b. le message est prélevé au passage par le destinataire, qui renvoie à l'émetteur après lui avoir «signé un accusé de réception».
c. lorsque le message a fait le tour complet de l'anneau, il est prélevé par l'émetteur, qui vérifie sa bonne réception avant de le détruire et de libérer le jeton.
d. le jeton est passé au prochain nœud.

Avec l'anneau à jeton circulant, le jeton suit l'ordre physique des postes, tandis qu'avec le jeton circulant, il suit le numéro logique qui se trouve sur la carte d'interface de réseau de chaque poste. La méthode du jeton circulant est très fiable, car un seul poste peut émettre à un moment donné. La collision est donc impossible.

I.3 Les modes de commutation (switching)

La commutation est une fonction qui permet de réaliser une liaison temporaire entre l'équipement demandeur (émetteur), et l'équipement demandé (récepteur), à travers le réseau.

a. Commutation de circuits

Avant d'effectuer une communication entre deux entités, il est établi un circuit entre les deux à travers lequel, durant la communication, les informations transitent. Le circuit est libéré dès que les deux abonnés décident d'interrompre la communication, et mettent fin au transmission des données. Le problème qui se pose est de pouvoir réserver des ressources (mémoires, files d'attente,..) dans le cas ou plusieurs communications utilisent la même liaison c'est-à-dire le même circuit.

L'application par exemple de commutation de circuit est le service téléphonique. Le service offert est orienté connexion où on distingue trois étapes :

- l'établissement de la connexion ;
- le transfert de l'information ;
- la libération de la connexion.

b. Commutation de messages

Dans ce type de commutation, le message transitant sur la ligne, passe à travers des éléments intermédiaires avant d'arriver au destinateur. Ces éléments sont appelés les nœuds de commutation qui servent de contrôler et corriger les erreurs des messages avant qu'ils soient acquittés au nœud suivant. D'où, il faut penser au contrôle du flux des messages et l'introduction des politiques de sécurisation des données si, par exemple, une liaison tombe en panne. Donc l'inconvénient est le temps d'attente qui augmente énormément, par contre l'utilisation meilleure des ressources est un avantage.

c. Commutation par paquets (packet switching)

Le temps de réponse sera plus important dans le cas où les messages sont très longs. La solution est de découper le message en morceaux appelés paquets dont la longueur maximale est de l'ordre de 1000 ou 2000 bits.

Les paquets sont envoyés indépendamment les uns des autres, et les nœuds de commutations tiennent en compte de cette situation pour les aiguiller vers la bonne sortie en se servant, par exemple, d'une table de routage.

Plusieurs paquets provenant des messages différents peuvent arriver au même nœud, et pour les faire sortir on procède au multiplexage temporel. Cette technique de commutation est meilleure en temps de réponse et reprise sur erreur, mais le problème à résoudre est le réassemblage des paquets pour reformer le message original avant de le donner à la couche supérieure.

Remarque : Internet utilise une commutation de paquets.

d. Commutation des cellules

La commutation de cellules (ATM) est une commutation de paquets assez particulière, les paquets ont une longueur fixe maximale de 53 octets. Chaque cellule possède un certain nombre de champs d'informations y compris l'en-tête de cellule

I.4.Architecture des réseaux

Communiquer consiste à transmettre des informations, mais tant que les interlocuteurs ne lui ont pas attribué un sens, il ne s'agit que de données et pas d'information. Les interlocuteurs doivent donc non seulement parler un langage commun mais aussi maîtriser des règles minimales d'émission et de réception des données. C'est le rôle d'un protocole de s'assurer de tout cela.

L'architecture des réseaux est organisée en série de couches ou niveaux. Le nombre de couches, leurs noms et leurs fonctions varient selon les constructeurs. Trois grandes architectures se disputent le marché mondial :

- Architecture OSI.
- Architecture TCP / IP.
- Architecture ATM.

I.4.1 Modèle de référence OSI

OSI signifie (Open Systems Interconnection, ce qui se traduit par Interconnexion de systèmes ouverts). Ce modèle a été mis en place par l'ISO (International Standard Organization) afin de mettre en place un standard de communications entre les ordinateurs d'un réseau, c'est-à-dire les règles qui gèrent les communications entre des ordinateurs.

En effet, aux origines des réseaux chaque constructeur avait un système propre (on parle de système propriétaire).

Ainsi de nombreux réseaux incompatibles coexistaient. C'est la raison pour laquelle l'établissement d'une norme a été nécessaire. Le rôle du modèle OSI consiste à standardiser la communication entre les machines afin que différents constructeurs puissent mettre au point des produits (logiciels ou matériels) compatibles (pour peu qu'ils respectent scrupuleusement le modèle OSI).

Le modèle OSI définit 7 niveaux différents pour le transfert de données, ces niveaux sont également appelés couches.

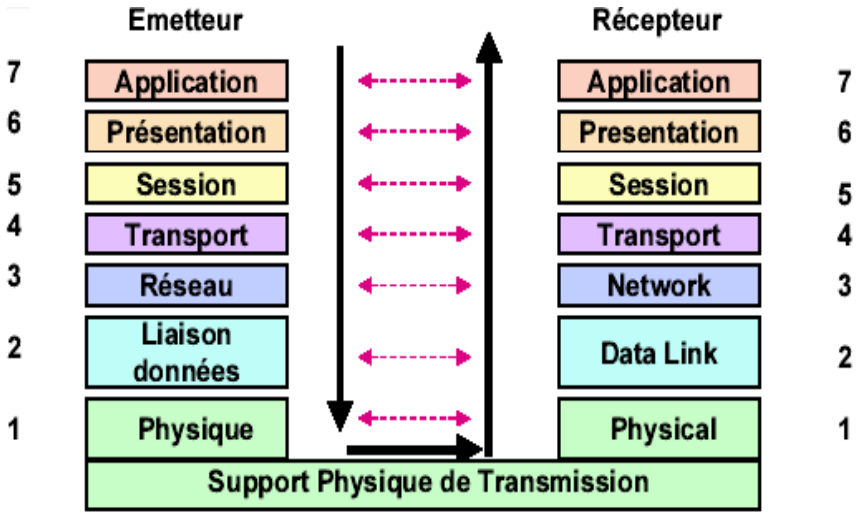


Tableau I.1 : Le Modèle OSI.

La communication passe par un ensemble de **couches** empilées:

- Ø chaque couche a un rôle précis (conversion, routage, découpage, vérification...)
- Ø chaque couche dialogue avec la couche juste au-dessus et celle juste au-dessous: Elle fournit des services à la couche au-dessus, et utilise les services de la couche en-dessous.
- Ø chaque couche encapsule les données venant de la couche du dessus en y ajoutant ses propres informations avant de le passer à la couche du dessous (et opération inverse dans l'autre sens).

I.4.1.1 la couche physique

Cette couche définit les caractéristiques techniques, électriques, fonctionnelles et procédure les nécessaires à l'activation et à la désactivation des connexions physiques destinées à la transmission de bits entres deux entités de la liaison de données.

I.4.1.2 la couche liaison

Cette couche définit les moyens fonctionnels et procéduraux nécessaires à l'activation et à l'établissement ainsi qu'au maintien et à la libération des connexions de liaisons de donnes entre les entités du réseau.

Cette couche détecte et corrige, quand cela est possible, les erreurs de la coche physique et signale à la couche réseau les erreurs irrécupérables.

I.4.1.3 La couche réseau

Cette couche assure toutes les fonctionnalités de services entre les entités du réseau, c'est à dire : l'adressage, le routage, le contrôle de flux, la détection et le correction d'erreurs non résolues par la couche liaison pour préparer le travail de la couche transport.

I.4.1.4 La couche transport

Cette douche définit un transfert de données entre les entités en les déchargeant des détails d'exécution (contrôle entre l'**OSI** et le support de transmission).

Son rôle est d'optimiser l'utilisation des services de réseau disponibles afin d'assurer à moindre coût les performances requise par la couche session.

I.4.1.5 La couche session

Cette couche fournit aux entités de la couche présentation les moyens d'organiser et de synchroniser les dialogues et les échanges de données.
Il s'agit de la gestion d'accès, de sécurité et d'identification des services.

I.4.1.6 La couche présentation

Cette couche se charge de la syntaxe des informations que se communiquent les éléments du réseau, c'est-à-dire que ces éléments utilisent bien un langage commun pour transférer des données.

I.4.1.7 La couche application

C'est la dernière couche du modèle OSI. Elle donne aux applications le moyen d'accéder aux couches inférieures. Cette couche a été normalisée en 1987 au sein d'une structure globale : la structure de la couche application, ou ALS (*Application Layer Structure*). Elle détermine comment différentes applications vont pouvoir coexister et utiliser des modules communs. De très nombreuses normes ont été définies sur cette base.

I.4.2 Le modèle TCP / IP

Le modèle OSI est trop lourd et trop complexe à implémenter. Les industriels ont donc choisi de n'implémenter que la partie du modèle OSI qui les intéresse, et chaque industriel a créé son propre système. Certains protocoles, plus populaires que d'autres, ont été adoptés comme standard (exemple, le protocole IP).

Il arrive très souvent que des logiciels (en couche 7) implémentent eux-mêmes certaines fonctions comme le chiffrement, la gestion des sessions ou la fiabilité au lieu de laisser les couches en dessous s'en occuper, parce que cela permet à ces logiciels d'être plus indépendants des protocoles et de fonctionner sur des couches réseaux ne proposant pas ces services.

C'est ainsi que l'on obtient un modèle à quatre couches :

- La couche **Interface réseau** spécifie la forme sous laquelle les données sont acheminées
- La couche **Internet** est chargée de fournir les paquets de données
- La couche **transport** assure l'acheminement des données
- La couche **application** regroupe les applications du réseau

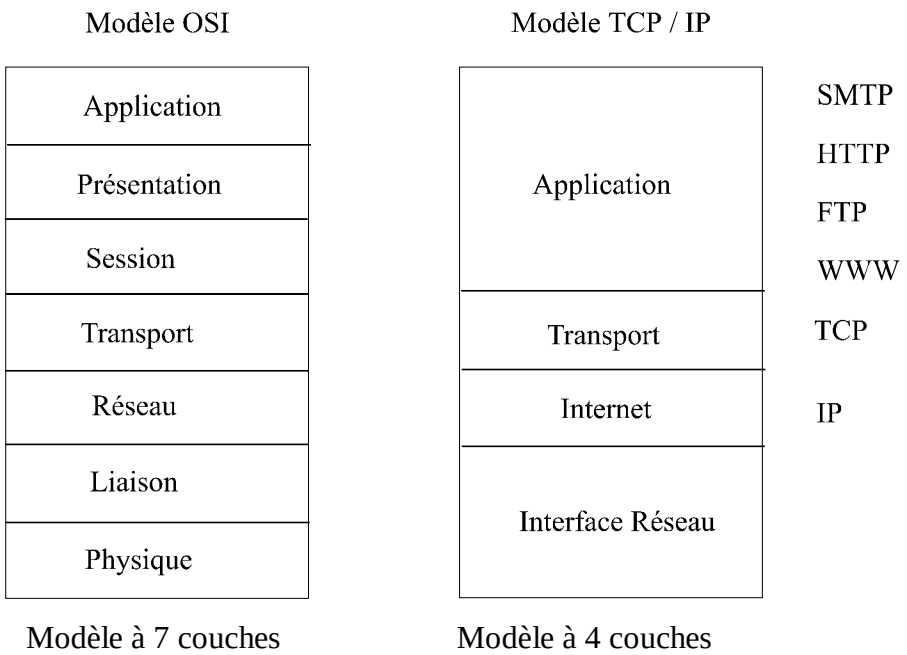


Tableau I.2 : modèle OSI et TCP / IP.

1.4.2.1 Les protocoles liés à chaque couche

Internet signifie **Inter-networks**, c'est à dire "entre réseaux". Internet est l'interconnexion des réseaux de la planète.

IP : signifie ***Internet Protocol*** (le protocole d'Internet). C'est le principal protocole utilisé sur Internet. Il permet aux ordinateurs reliés à ces réseaux de dialoguer entre eux.

TCP : (Transmission Control Protocol) : Ensemble de protocoles standard de l'industrie permettant la communication dans un environnement hétérogène.

UDP : (User Datagram Protocol.) Le protocole UDP est un protocole simple, sans connexion, Il présente l'avantage d'imposer peu de surcharge pour l'acheminement des données. Les blocs de communications utilisés dans le protocole UDP sont appelés des datagrammes. Ces datagrammes sont envoyés « au mieux » par ce protocole de couche transport.

RIP : (Routing Information Protocol) est un protocole à vecteur de distance qui utilise comme métrique le nombre de sauts. Défini initialement au sein de l'IETF dans la [Hedrick88], il a été redéfini dans les nouvelles versions : RIPv2 [Malkin98] ou RIPng [Malkin97].

OSPF : (Open Shortest Path First) : Protocole de routage intérieur d'état des liaisons .Il Utilise une variante d'algorithme de Dijkstra pour calculer la route optimale à partir de l'arbre de plus court chemin.

FTP : (File Transfer Protocole) : protocole de transfert de fichier entre les ordinateurs de manière interactive.

HTTP : (Hyper Text Transfer Protocol) : protocole utilisé pour transporter des pages webs sur le réseau. L'accès aux services Webs se fait en donnant une adresse de type http://nom de domaine/répertoire…

SMTP :(***Simple Mail Transfer Protocol) :*** protocole simple de transfert de courrier. Il sert aux applications de messagerie électronique.

Couche	Données	Matériel associé	Quelques protocoles
7 : Application		Serveur	HTTP, SMTP, FTP, TFTP, etc.
6 : Présentation			ASN.1, XDR, etc.
5 : Session			SIP, H323, etc
4 : Transport	segment		TCP, UDP, OSPF, RIP, etc.
3 : Réseau	paquet	Routeur	IP, NetBeui, IPx, X.25, etc.
2 : Liaison	trame	Commutateur (*switch*), pont (*bridge*)	Ethernet, Frame Relay, Token Ring, Wifi…
1 : Physique	bit	Concentrateur (*hub*), répéteur	CSMA/CD, CSMA/CA, 10base-T, ADSL, etc.

Tableau I.3 : Les protocoles liés à chaque couche.

1.4.2.2 Encapsulation des données

Les données des logiciels sont encapsulées (enveloppées) par la couche TCP. Le paquet TCP et lui-même encapsulé par la couche IP. Et le paquet IP peut également être encapsulé par PPP (pour être transmis par modem) ou Ethernet (pour être transmis sur réseau local).

Le paquet de données prend naissance dans la couche application : **c'est un message** Il est ensuite encapsulé sous forme de **segment** dans la couche transport. Dans la couche internet, il prend le nom de **datagramme.** Enfin, dans la couche accès réseau, il devient **une trame.**

Les données traversent les couches vers le bas quand elles sont envoyées, et elles remontent les couches à la réception (comme vu précédemment avec OSI).

Faisons un parallèle avec la poste. Quand on veut envoyer une lettre par la poste :

- on met la lettre dans une enveloppe,
- sur le recto on inscrit l'adresse du destinataire,
- au dos, on écrit l'adresse de l'expéditeur (la notre).

Ce sont des règles utilisées par tout le monde. C'est un **protocole**. Sur Internet, c'est à peu près la même chose qui se passe : chaque paquet de données est enveloppé par IP qui y ajoute différentes informations :

- l'adresse de l'expéditeur (notre adresse IP),
- l'adresse IP du destinataire,
- différentes données supplémentaires (qui permettent de bien contrôler l'acheminement du message).

I.4.3 Architecture ATM (Asynchronous Transfert Mode)

C'est également un modèle à quatre couches. La couche physique rassemble les fonctions liées à la transmission des données, tandis que la couche d'adaptation AAL (ATM Adaptation Layer) fait le lien avec les applications. La couche ATM est l'équivalent de la couche liaison dans le modèle OSI, elle s'occupe notamment des erreurs de transmission. Au niveau supérieur, le plan d'usager contient les protocoles applicatifs, le plan de commande rassemble les procédures liées au traitement d'appel et à la signalisation. Enfin le plan de gestion comporte toutes les fonctions de gestion à l'intérieur des différentes couches ainsi que les rapports de gestion entre couches.

Dans l'architecture ATM, les données sont transmises sous forme de cellules.

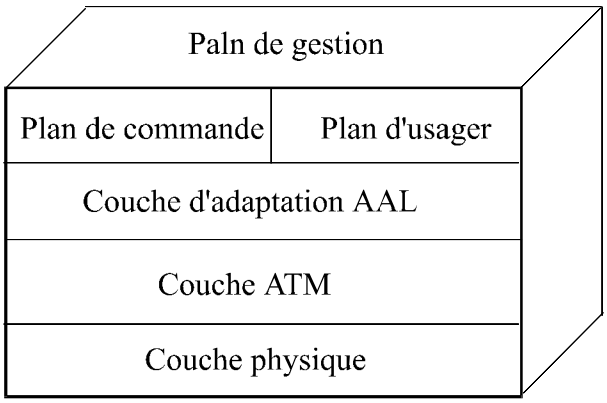


Tableau I.4 : Architecture ATM.

I.5 L'adresse IP

L'adresse IP est un nombre de 32 bits qui identifie, de manière unique, un nœud (ordinateur, imprimante, routeur, etc.) d'un réseau TCP/IP Les adresses IP sont généralement exprimées dans un format décimal pointé, fait de quatre nombres séparés par des points, par exemple 192.168.100.85. Le fonctionnement d'un réseau étendu composé de plusieurs réseaux TCP/IP n'exige pas que les routeurs chargés de faire passer les données entre les réseaux connaissent l'adresse exacte de l'hôte auquel est destiné un paquet. Tout ce que doivent connaître les routeurs, c'est le réseau auquel appartient cet hôte; ils utilisent les données de leurs tables de routage pour déterminer la façon d'envoyer le paquet au réseau contenant l'hôte cible. Une fois le paquet remis au réseau du récepteur, il sera ensuite livré au bon hôte. Ce processus repose sur la décomposition de l'adresse IP en deux parties: ID de réseau et ID d'hôte.

1.5.1 Les classe d'adresse IP

La partie réseau de l'espace d'adressage 32 bits est divisée en classes.

- Les adresses de classe A
- Les adresses de classe B
- Les adresses de classe C
- Les adresses de classe D
- Les adresses de classe E

a. Classe A

Le premier octet a une valeur strictement inférieure à 128 (valeur du bit de poids fort égal à 0). Ce premier octet désigne le numéro de réseau et les 3 autres correspondent à l'adresse de l'hôte.

Classe A			
Partie réseau	**Partie hôte**		
0xxxxxxx	**xxxxxxxx**	**xxxxxxxx**	**xxxxxxxx**
Octet 1	**Octet 2**	**Octet 3**	**Octet 4**

Tableau I.5 : Forma d'adressage (classe A).

b. Classe B

Le premier octet a une valeur comprise entre 128 et 192 (valeur des 2 bits de poids fort égale à 10). Les 2 premiers octets désignent le numéro de réseau et les 2 autres correspondent à l'adresse de l'hôte.

Classe B			
Partie réseau		**Partie hôte**	
10xxxxxx	**xxxxxxxx**	**xxxxxxxx**	**xxxxxxxx**
Octet 1	**Octet 2**	**Octet 3**	**Octet 4**

Tableau I.6 : Forma d'adressage (classe B).

c. Classe C

Le premier octet a une valeur comprise entre 192 et 223 (valeur des 3 bits de poids fort égale à 110). Les 3 premiers octets désignent le numéro de réseau et le dernier correspond à l'adresse de l'hôte.

Classe C			
Partie réseau			***Partie hôte***
110xxxxx	**xxxxxxxx**	**xxxxxxxx**	**xxxxxxxx**
Octet 1	**Octet 2**	**Octet 3**	**Octet 4**

Tableau I.7 : Forma d'adressage (classe C).

d. Classe D

Le premier octet a une valeur comprise entre 224 et 239 (valeur des 3 bits de poids fort égale à 111). Il s'agit d'une zone d'adresses dédiées aux services de multidiffusion vers des groupes d'hôtes (*host groups*).

Classe D			
Adresse multidiffusion			
111xxxxx	**xxxxxxxx**	**xxxxxxxx**	**xxxxxxxx**
Octet 1	**Octet 2**	**Octet 3**	**Octet 4**

Tableau I.8 : **Forma d'adressage (classe D).**

e. Classe E

Le premier octet a une valeur supérieure à 240. Il s'agit d'une zone d'adresses réservées aux expérimentations. Ces adresses ne doivent pas être utilisées pour adresser des hôtes ou des groupes d'hôtes.

A chaque classe correspond un nombre maximum de réseau pouvant appartenir à cette classe, et à chaque réseau d'une certaine classe, correspond un nombre maximum d'adresses, c'est à dire un nombre maximum de stations pouvant bénéficiées d'un adresse fixe à l'intérieur de ce réseau.

Le tableau suivant représente les propriétés des différentes classes :

Les classes des adresses IP					
	Classe A	**Classe B**	**Classe C**	**Classe D**	**Classe E**
Fonction	Multinationales	Grande entreprises	Petites entreprises	Multicasting	Recherche expérimentale
Réseau	Sur 1 octet	Sur 2 octets	Sur 3 octets		
Station	Sur 3 octets	Sur 2 octets	Sur 1 octet		
Structure de la partie réseau	1.0.0.0 à 126.0.0.0	128.1.0.0 à 191.254.0.0	192.0.1.0 à 223.254.254.0		
Valeur du 1er octet en binaire	00000001 à 01111110	10000000 à 10111111	11000000 à 11011111		
Nombre de machines par réseau	16 millions	65 536	256		

Tableau I.9 : la classe d'adressage.

I-6 Les adresses IP conventionnelles (Adresses réservées) :

Certaines adresses sont réservées pour une utilisation conventionnelle :

- 0.0.0.0 est utilisée par les machines pendant la procédure de démarrage de l'ordinateur (le BOOT).
- 127.0.0.0 est utilisée pour tester une adresse IP.
- 192.168.0.0 n'existe pas sur Internet, afin d'être réservée pour les réseaux locaux sous TCP/IP
- 255.255.255.255 est utilisée comme adresse de broadcast générale.

I.7 Les équipements réseau

I.7.1 Répéteurs

Un répéteur est un amplificateur qui a plusieurs connexions au réseau. Il permet de dépasser la longueur maximale de la norme d'un réseau en amplifiant et en régénérant le signal électrique. Sa principale utilisation est le passage d'un média à un autre (par exemple d'une connexion en cuivre vers une connexion en fibre optique) ou d'interconnecter deux câbles en fibre optique en régénérant le signal. Le répéteur opère sur la couche physique (couche 1 du modèle OSI).

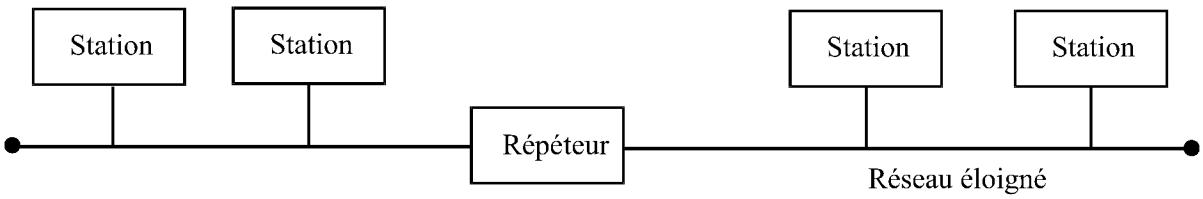


Figure I.7 : Répéteurs.

I.7.2 Concentrateurs, Hubs

Un **concentrateur** est un élément matériel permettant de concentrer le trafic réseau provenant de plusieurs hôtes. Il possède autant de ports qu'il peut connecter de machines entre elles, généralement 4, 8, 16 ou 32. Son but est de récupérer les données parvenant sur un port, les amplifier et les diffuser sur l'ensemble des ports. Il est parfois appelé répéteur multiports. Le concentrateur opère sur la couche liaison (couche 2 du modèle OSI).

Le concentrateur permet ainsi de connecter plusieurs machines entre elles, parfois disposées en étoile, ce qui lui vaut le nom de hub (signifiant moyeu de roue en anglais; la traduction française exacte est répartiteur), pour illustrer le fait qu'il s'agit du point de passage des communications des différentes machines. Les données sont envoyées sur tous les ports aux périphériques qui décodent la trame d'en-tête pour savoir si elles leurs sont destinées.

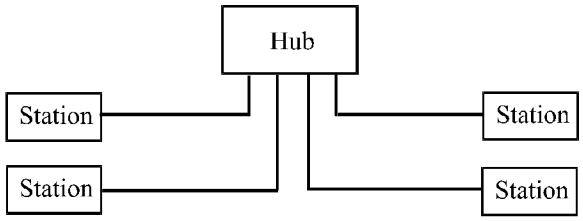


Figure I.8 : Hub.

La bande passante totale est limitée à la vitesse du hub. Un hub 100 base-T offre 100 Mbps de bande passante partagée entre tous les ordinateurs, quelque soit le nombre de ports. Le problème de ce type de concentrateur, c'est justement le renvoi des données vers tous les équipements.

Dès que le nombre d'ordinateurs connectés augmente, le taux de collision augmente en proportion, réduisant la vitesse effective du réseau. Ils sont remplacés par les **switchs** dans tous les réseaux actuels.

I.7.3 Le Switch

Analyse l'entête des données qu'il reçoit et ne les envoie que vers la station concernée. La bande passante est déterminée par le nombre de ports. i.e. Un Switch 100 Mbps, 8 ports, peut gérer jusqu'à 800 Mbps en half duplex, le double en full duplex. On peut dire qu'un switch est un Hub intelligent.

1.7.4 Ponts ou Bridges

Ils permettent la subdivision d'un réseau en sous réseaux pour optimiser les débits. On mesure la qualité d'un pont par son taux de filtrage et son taux de transfert. Un pont multiports est appelé commutateur ou Switch. C'est en quelque sorte une passerelle particulière, le pont opère sur la couche liaison (couche 2 du modèle OSI).

.

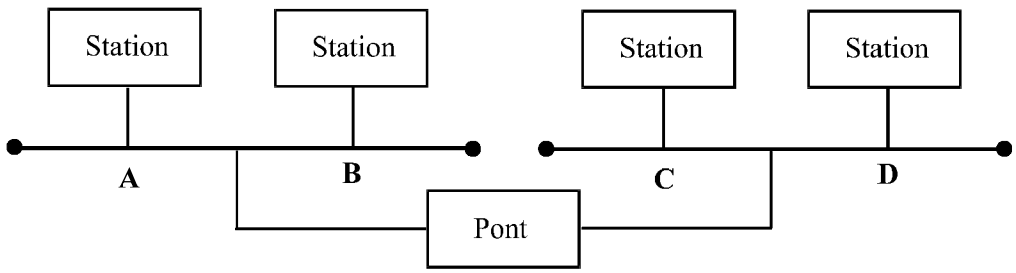


Figure I.9 : Le Pont.

Le trafic local entre les nœuds A et B ne traverse pas le pont et n'encombre pas le réseau.

I.7.5 Routeurs

Ils servent à diriger les informations dans la direction appropriée, notamment lors de communications entre stations de réseaux différents Pour y parvenir, les routeurs tiennent à jour des tables de routage, véritable cartographie des itinéraires à suivre en fonction de l'adresse visée. Il existe de nombreux protocoles dédiés à cette tâche. Le routeur opère sur la couche réseau (couche 3 du modèle OSI)

La commutation et le routage symbolisent deux manières opposées d'acheminer l'information. Les commutateurs utilisent des références de circuits ou chemins. Les routeurs utilisent des tables de routage. Par exemple, le réseau ATM utilise la commutation, le réseau INTERNET le routage et le réseau ETHERNET se place entre les deux, il utilise un routage fixe qui ressemble à une commutation.

I.7.6 Passerelles ou Gates

Ce sont des interfaces qui permettent de relier des réseaux de type différent. Elles sont nécessaires pour changer de protocoles (par exemple pour passer du modèle OSI au modèle TCP/IP). Elles peuvent être matérielles ou logicielles ou les deux.

CHAPITRE II

Protocoles de routage

II.1 Définition de routage IP

Pour pouvoir communiquer avec des entités éloignées, une entité doit faire passer ses données par d'autres qui se chargeront de les acheminer. Pour cela, il est primordial que toutes les entités du réseau se situent les unes par rapport aux autres, et soient capables de construire des routes entre elles : c'est le rôle du protocole de routage.

Le principe de base du routage est la commutation qui permet à un routeur d'accepter un paquet d'une interface et de le transmettre par le bais d'une autre interface. Le paquet pris en charge à une interface et retransmis via une autre interface représentant le meilleur chemin vers le réseau de destination.

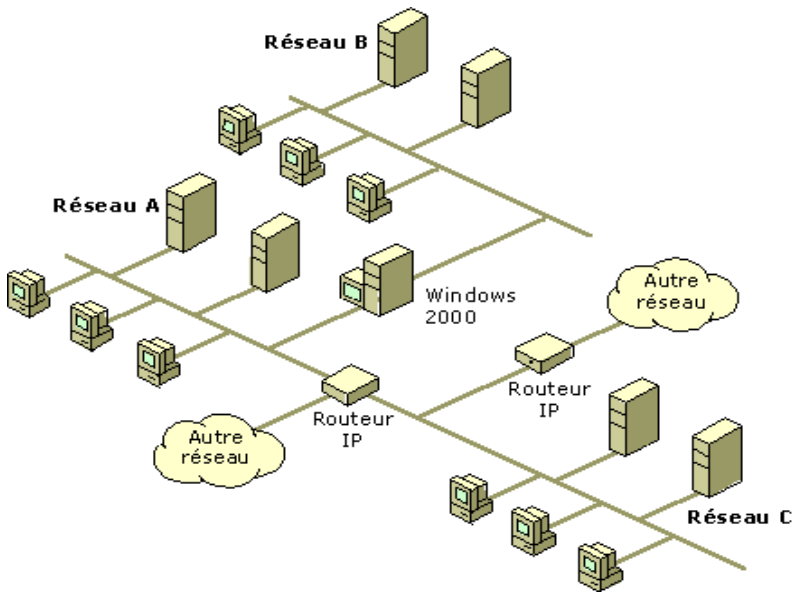


Figure II.1 : Routage IP.

II.2 Tables de routage

Une table de routage est un fichier de données stoker dans la mémoire vive non volatile (NVRAM) servant à stocker les informations sur la route à emprunter sur les réseaux directement connectés et les réseaux distants. La table de routage contient des associations réseau/tronçon suivant. Celles-ci informent un routeur qu'une destination donnée peut être atteinte de manière optimale en envoyant le paquet à un routeur donné, lequel représente le « tronçon suivant » sur le chemin menant à la destination finale. L'association de tronçon suivant peut également être constituée de l'interface de sortie vers la destination finale.

L'association réseau/interface de sortie peut également représenter l'adresse réseau de destination du paquet IP. Cette association se produit sur les réseaux directement connectés au routeur.

Un réseau distant n'est pas directement connecté au routeur. En d'autres termes, un réseau distant est un réseau qui peut être atteint uniquement en envoyant le paquet à un autre routeur. Les réseaux distants sont ajoutés à la table de routage grâce à un protocole de routage dynamique ou à la configuration de routes statiques. Les routes dynamiques, qui mènent à des réseaux distants, sont apprises automatiquement par le routeur et utilisent un protocole de routage dynamique. Les routes statiques mènent à des réseaux configurés manuellement par l'administrateur réseau.

II.3 Types de routage

On classe généralement les protocoles de routage, d'abord en fonction de leur manière de découvrir le réseau, et après dans leur façon d'établir leurs tables de routage.

II.3.1 Routage statique

L'information relative aux routes statique est gérée manuellement par un administrateur de réseau qui l'enregistre dans la configuration d'un routeur. L'administrateur doit mettre à jour l'entrée relative à la route statique chaque fois qu'une modification apportée à la topologie d'un interréseau nécessite une mise à jour.

Le routage statique est principalement utilisé pour les raisons suivantes :

- Faciliter la maintenance des tables de routage dans les réseaux de petite taille qui ne sont pas amenés à se développer de manière significative.
- Effectuer le routage depuis et vers des réseaux d'extrémité.
- Utiliser une seule route par défaut, servant à représenter un chemin vers tout réseau ne présentant aucune correspondance plus spécifique avec une autre route indiquée dans la table de routage.

a) Avantages du routage statique

- Traitement processeur minimal.
- Moins de surcharge par rapport au routage dynamique.

b) Inconvénients du routage statique

- La configuration et la maintenance prennent du temps.
- La configuration présente des risques d'erreurs, tout particulièrement dans les grands réseaux.
- L'intervention de l'administrateur est requise pour assurer la maintenance des informations changeantes relatives aux routes.
- N'évolue pas bien pour les réseaux en expansion ; la maintenance devient fastidieuse.
- Exige une connaissance complète de l'ensemble du réseau pour une implémentation correcte.

II.3.2 Système autonome

Un système autonome (SA), également appelé domaine de routage, est un ensemble de routeurs dont l'administration est commune. Le réseau interne d'une société et le réseau d'un fournisseur de services Internet en sont des exemples. Dans la mesure où Internet repose sur le concept de système autonome, deux types de protocoles de routage sont nécessaires : des protocoles de routage intérieurs et extérieurs. Ces protocoles sont les suivants :

a. Les protocoles IGP (Interior Gateway Protocols) : Protocoles de routage intra-domaines (intérieurs) ou protocoles de routage proactifs, ils sont utilisés à l'intérieur d'un domaine (découverte des routes à l'avance).

b. Les protocoles EGP (Exterior Gateway Protocol) : Protocoles de routage inter-domaines (extérieurs) ou protocoles de routage réactifs : ils sont utilisés pour la communication avec les autres domaines (découverte des routes à la demande).

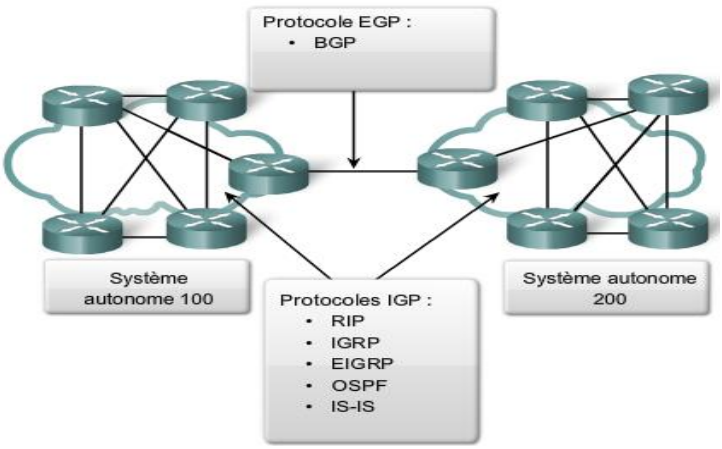


Figure II.2 : Protocoles de routage IGP/EGP.

II.3.3 Routage dynamique

Les informations relatives aux routes dynamiques sont gérées différemment. Une fois qu'un administrateur réseau a saisi les commandes de configuration pour lancer le routage dynamique, les informations relatives à la route sont mise à jour automatiquement par un processus de routage, et ce à chaque fois que l'interreseau envoie de nouvelles informations.

Les modifications apportées aux informations dynamiques sont échangées entre les routeurs dans le cadre de processus de mise à jour.

a. Avantages du routage dynamique

- Réduction pour l'administrateur des tâches de maintenance de la configuration lors de l'ajout et de la suppression de réseaux.
- Les protocoles réagissent automatiquement aux modifications topologiques.
- La configuration est moins sujette aux erreurs.
- Plus évolutif, l'expansion du réseau ne présente généralement pas de problème.

b. Inconvénients du routage dynamique

- Utilisation des ressources du routeur (cycle de processeur, mémoire et bande passante de liaison).
- Les administrateurs doivent avoir des connaissances plus approfondies pour la configuration, la vérification et le dépannage.

II.3.3.1 Protocoles de routage dynamique

Les protocoles de routage dynamique sont généralement utilisés dans des réseaux plus importants pour réduire la surcharge administrative et fonctionnelle liée à l'utilisation exclusive de routes statiques. Un réseau utilise généralement à la fois un protocole de routage dynamique et des routes statiques. Dans la plupart des réseaux, un seul protocole de routage dynamique est utilisé. Toutefois, différentes parties du réseau peuvent utiliser des protocoles de routage différents.

II.3.3.2 Évolution des protocoles de routage dynamique

Les protocoles de routage dynamique sont utilisés dans les réseaux depuis le début des années 80. La première version du protocole RIP a vu le jour en 1982, mais certains de ses algorithmes de base étaient déjà utilisés dans ARPANET depuis 1969.

De nouveaux protocoles de routage ont émergé à mesure que les réseaux ont évolué.

RIP (Routing Information Protocol) est l'un des tous premiers protocoles de routage. Il a évolué pour donner naissance à la version **RIPv2**. Toutefois, cette nouvelle version n'est toujours pas adaptée aux grands réseaux. Aussi, deux protocoles de routage avancés ont été développés pour répondre aux besoins des réseaux plus importants : **OSPF** (Open Shortest Path First) et **IS-IS** (Intermediate System-to-Intermediate System). Cisco a développé les protocoles **IGRP** (Interior Gateway Routing Protocol) et **EIGRP** (Enhanced IGRP), qui présentent également une bonne évolutivité dans les réseaux plus importants.

II.3.3.3 Rôle du protocole de routage dynamique

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. Cet échange permet aux routeurs de découvrir automatiquement de nouveaux réseaux et également de trouver d'autres chemins en cas d'échec d'une liaison vers un réseau actif.

Par rapport au routage statique, l'utilisation de protocoles de routage dynamique implique qu'une partie des ressources d'un routeur est dédiée au fonctionnement du protocole (y compris le temps processeur et la bande passante de la liaison de réseau).

II.3.3.4 Fonctionnement des protocoles de routage dynamique

Tous les protocoles de routage ont la même fonction qui consiste à découvrir des réseaux distants et à s'adapter rapidement en cas de modification de la topologie. La méthode adoptée à cette fin par un protocole de routage dépend de l'algorithme qu'il utilise et des caractéristiques de fonctionnement de ce protocole. Les opérations d'un protocole de routage dynamique dépendent du type de protocole de routage et du protocole de routage lui-même.

D'une manière générale, 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 topologique, le protocole de routage peut l'annoncer aux autres routeurs.

II.3.3.5 Classification des protocoles de routage dynamique

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

- **RIP :** Protocole de routage intérieur à vecteur de distance.
- **IGRP :** Protocole de routage intérieur à vecteur de distance développé par Cisco.
- **OSPF :** Protocole de routage intérieur d'état des liaisons.
- **IS-IS :** Protocole de routage intérieur d'état des liaisons.
- **EIGRP :** Protocole de routage intérieur à vecteur de distance avancé développé par Cisco.

II.4 Vecteur de distance et état de liaisons

Les protocoles IGP (Interior Gateway Protocols) peuvent appartenir à deux types :

- Protocoles de routage à vecteur de distance.
- Protocoles de routage d'état des liaisons.

II.4.1 Fonctionnement du protocole de routage à vecteur de distance

Vecteur de distance signifie que les routes sont exprimées en tant que vecteurs de distance et de direction. La distance est définie en termes de mesure, comme le nombre de sauts, et la direction est simplement le routeur de tronçon suivant ou l'interface de sortie. Les protocoles à vecteur de distance utilisent généralement l'algorithme Bellman-Ford pour déterminer le meilleur chemin.

Certains protocoles à vecteur de distance envoient régulièrement des tables de routage entières à tous les voisins connectés. Dans le cas des grands réseaux, ces mises à jour de routage peuvent être gigantesques et générer un trafic important sur les liaisons.

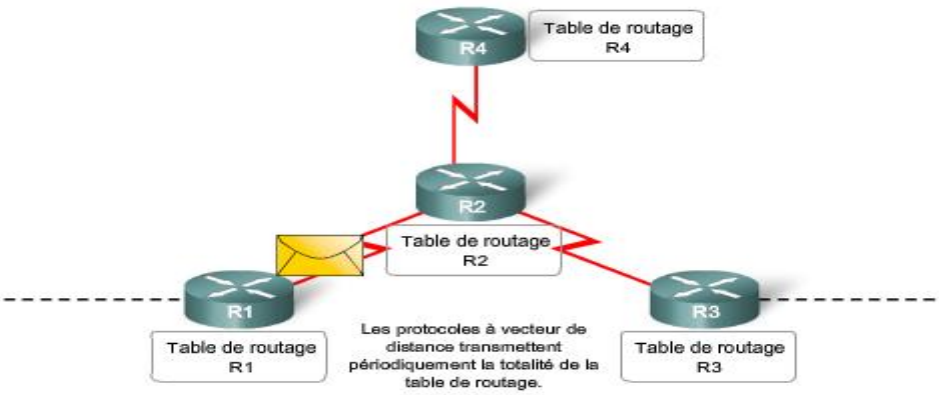


Figure II.3 : Fonctionnement du protocole à vecteur de distance.

Bien que l'algorithme Bellman-Ford parvienne à rassembler suffisamment d'informations pour gérer une base de données des réseaux accessibles, il ne permet pas à un routeur de connaître la topologie exacte d'un interréseau. Le routeur ne dispose que des informations de routage qu'il a reçues de ses voisins.

Les protocoles à vecteur de distance utilisent les routeurs comme poteaux indicateurs le long du chemin et ceci jusqu'à la destination finale. La seule information dont dispose un routeur à propos d'un réseau distant est la distance ou mesure d'éloignement de ce réseau et le chemin ou l'interface à utiliser pour y accéder.

Les protocoles à vecteur de distance sont particulièrement adaptés aux situations suivantes :

- Ø Le réseau est simple et linéaire et ne nécessite pas de conception hiérarchique particulière.
- Ø Les administrateurs ne sont pas suffisamment expérimentés pour configurer et dépanner les protocoles d'état des liaisons.
- Ø Des délais de convergence extrêmement longs sur un réseau ne posent pas problème.

II.4.2 Fonctionnement du protocole d'état des liaisons

Contrairement à un routeur configuré avec un protocole de routage à vecteur de distance, un routeur configuré avec un protocole de routage d'état des liaisons peut créer une vue complète ou topologie du réseau en récupérant des informations provenant de tous les autres routeurs. Pour reprendre l'analogie avec les poteaux indicateurs.

Les poteaux indicateurs le long du chemin entre la source et la destination ne sont pas nécessaires, car tous les routeurs d'état des liaisons utilisent une carte identique du réseau.

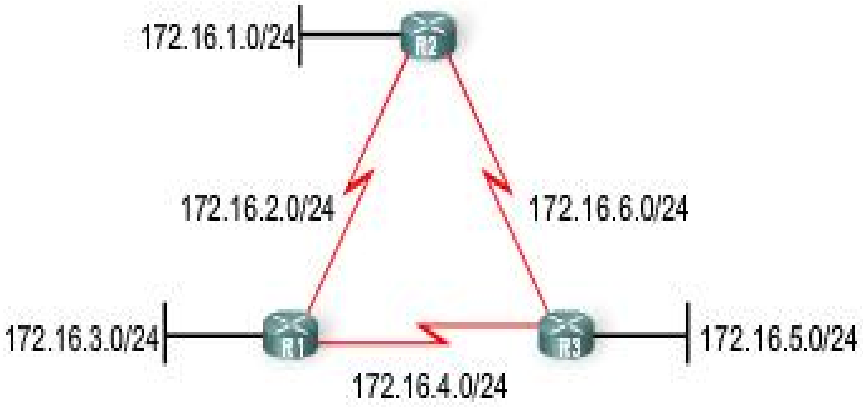
Un routeur d'état des liaisons utilise les informations d'état des liaisons pour créer une topologie et sélectionner le meilleur chemin vers tous les réseaux de destination de la topologie.

II.5 Protocoles de routage par classe

Les protocoles de routage par classe n'envoient pas d'informations sur les masques de sous-réseau dans les mises à jour de routage. Les premiers protocoles de routage comme RIP (Version 1) étaient des protocoles par classe. Les adresses réseau étaient alors allouées en fonction de classes (A, B ou C). Il n'était pas nécessaire que le protocole de routage inclue le masque de sous-réseau dans la mise à jour de routage, car le masque de réseau pouvait être déterminé en fonction du premier octet de l'adresse réseau.

Les protocoles de routage par classe peuvent encore être utilisés dans certains réseaux actuels, mais dans la mesure où ils n'incluent pas le masque de sous-réseau, ils ne peuvent pas être utilisés dans toutes les situations. Les protocoles de routage par classe ne peuvent pas être utilisés lorsqu'un réseau est découpé en sous-réseaux à l'aide de plusieurs masques de sous-réseau. En d'autres termes, les protocoles de routage par classe ne prennent pas en charge les masques de sous-réseau de longueur variable.

Les protocoles de routage par classe présentent d'autres limites comme leur incapacité à prendre en charge les réseaux discontinus. Les protocoles de routage par classe incluent RIPv1 et IGRP. (Voire la figure II.4 suivante).

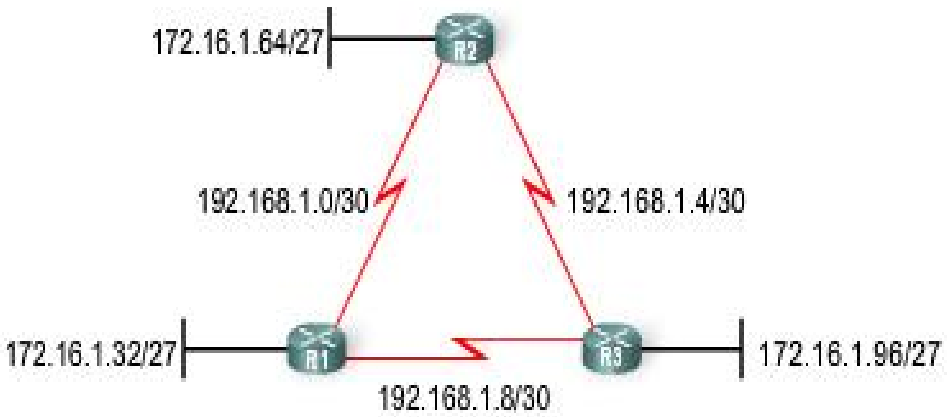


Par classe : le masque de sous-réseau est identique dans toute la topologie

Figure II.4 : routage par classe.

II.6 Protocoles de routage sans classe

Les protocoles de routage sans classe incluent le masque de sous-réseau avec l'adresse réseau dans les mises à jour de routage. Les réseaux actuels ne sont plus alloués en fonction de classes et le masque de sous-réseau ne peut pas être déterminé par la valeur du premier octet. Les protocoles de routage sans classe sont requis dans la plupart des réseaux actuels, car ils prennent en charge les masques de sous-réseau de longueur variable. Les protocoles de routage sans classe sont RIPv2, EIGRP, OSPF, IS-IS et BGP. (Voire la figure suivante).



Sans classe : le masque de sous-réseau peut varier dans la topologie

Figure II.5 : routage sans classe.

II.7 Convergence

On parle de convergence lorsque les tables de routage de tous les routeurs ont atteint un état de cohérence. 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. La plupart des réseaux nécessitent un bref temps de convergence.

La convergence est à la fois collaborative et indépendante. 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. Comme ils développent un accord avec la nouvelle topologie de manière indépendante, il est dit qu'ils convergent sur ce consensus.

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. Généralement, les protocoles RIP et IGRP mettent du temps à converger, alors que les protocoles EIGRP et OSPF sont plus rapides.

II.8 Mesures

Il peut arriver qu'un protocole réseau découvre plusieurs routes menant à la même destination. Pour sélectionner le meilleur chemin, il doit pouvoir évaluer et différencier les chemins disponibles. Une mesure est utilisée à cette fin. Une **mesure** est une valeur utilisée par les protocoles de routage pour affecter des coûts d'accès aux réseaux distants. La mesure est utilisée pour déterminer quel chemin est préférable en présence de plusieurs chemins vers le même réseau distant.

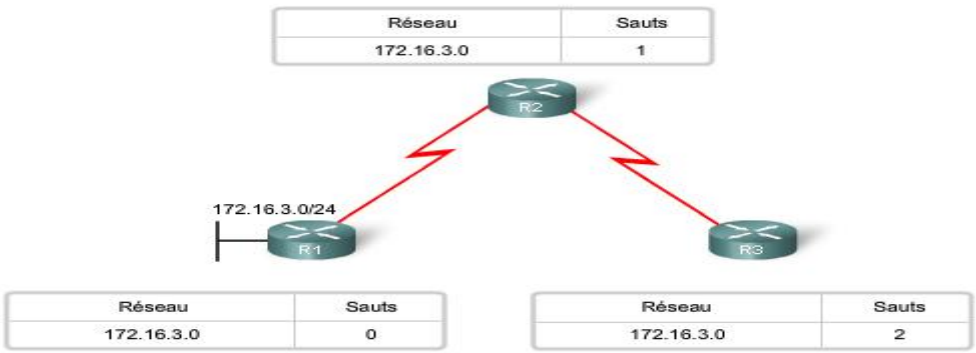


Figure II.6 : Mesures.

Chaque protocole de routage utilise sa propre mesure. Dans la figure présidente, le réseau 172.16.3.0 est à deux sauts ou deux routeurs de R3.

II.8.1 Mesures et protocoles de routage

a. Paramètres de mesure

Deux protocoles de routage différents peuvent choisir des chemins différents vers une même destination en raison des mesures qu'ils utilisent.

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

- **Nombre de sauts** : Mesure simple qui compte le nombre de routeurs qu'un paquet doit traverser.
- **Bande passante** : Influence la sélection du chemin en préférant celui dont la bande passante est la plus élevée.
- **Charge** : Prend en considération l'utilisation d'une liaison spécifique en termes de trafic.
- **Délai** : Prend en considération le temps nécessaire à un paquet pour parcourir un chemin.
- **Fiabilité** : Évalue la probabilité d'échec d'une liaison, calculée à partir du nombre d'erreurs de l'interface ou des échecs précédents de la liaison.
- **Coût** : Valeur déterminée par l'IOS ou par l'administrateur réseau pour indiquer une route préférée. Le coût peut représenter une mesure, une combinaison de mesures ou une stratégie.

b. Mesure utilisée par chacun des protocoles de routage dynamique

- **RIP** : Nombre de sauts - Le meilleur chemin est la route ayant le nombre de sauts le plus faible.
- **IGRP et EIGRP** : Bande passante, Délai, Fiabilité et Charge - Le meilleur chemin est la route ayant la valeur de mesure composite la plus faible, calculée à partir de ces paramètres multiples. Par défaut, seuls la bande passante et le délai sont utilisés.
- **IS-IS et OSPF** : Coût - Le meilleur chemin est la route associée au coût le plus faible.

.

Les protocoles de routage déterminent le meilleur chemin en fonction de la route ayant la mesure la plus faible.

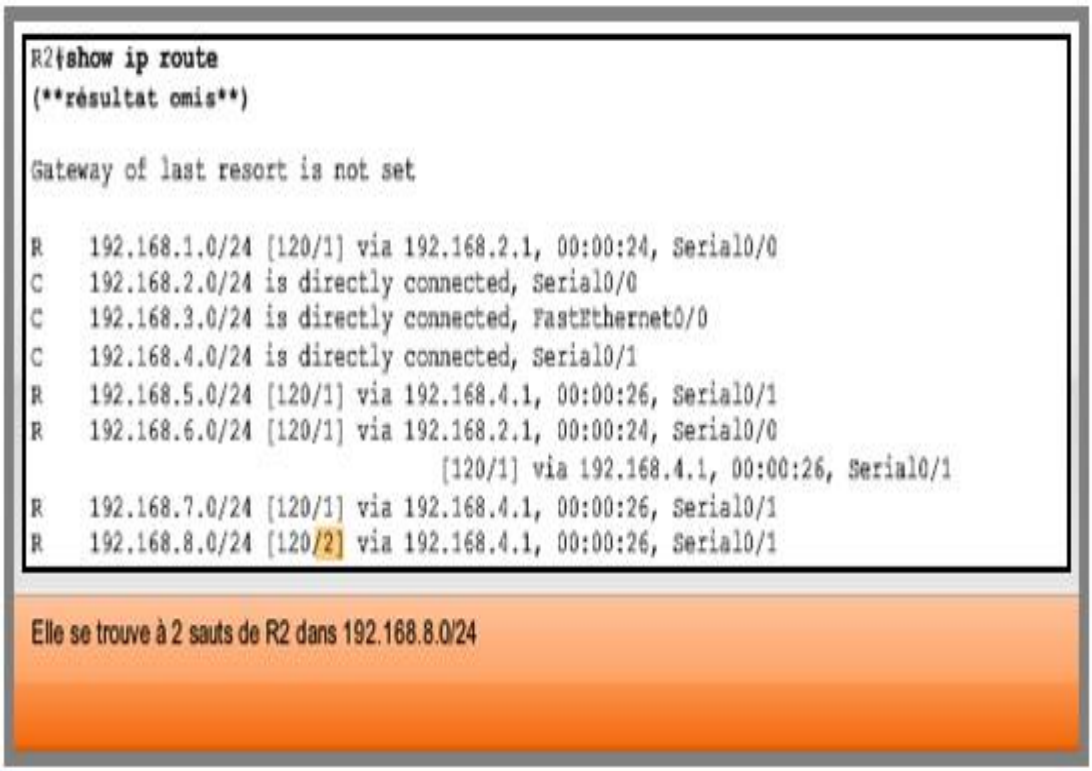


Tableau II.1: Paramètres de mesure de routage

Dans le tableau II.1 ; les routeurs utilisent le protocole de routage RIP. La mesure associée à une route particulière peut être affichée à l'aide de la commande **show ip route**. La valeur de la mesure est la seconde valeur entre crochets d'une entrée de la table de routage. Dans ce tableau, le routeur R2 présente une route vers le réseau 192.168.8.0/24 duquel il est séparé par 2 sauts.

R 192.168.8.0/24 [120/2] via 192.168.4.1, 00:00:26, Serial0/0/1.

c. Equilibrage de charge

Lorsque deux routes ou plus ont des valeurs de mesure identiques vers la même destination, Dans cette situation, le routeur ne choisit pas une seule route. Il équilibre la charge entre ces chemins à coût égal. La transmission des paquets se fait via des chemins à coût égal.

II.9 Distance administratives

La distance administrative (AD) définit la préférence d'une source de routage. Chaque source de routage est classée par ordre de priorité, du plus préférable au moins préférable, à l'aide d'une valeur de distance administrative. Les routeurs utilisent la distance administrative (AD) pour sélectionner le meilleur chemin lors de la découverte du même réseau de destination à partir d'au moins deux sources de routage différentes.

La distance administrative est une valeur entière comprise entre 0 et 255. Plus la valeur est faible, plus la source de la route est privilégiée. Une distance administrative de 0 est idéale. Seul un réseau directement connecté a une distance administrative égale à 0, laquelle ne peut pas être modifiée.

Une distance administrative de 255 signifie que le routeur ne se fiera pas à la source de cette route et qu'elle ne sera pas installée dans la table de routage.

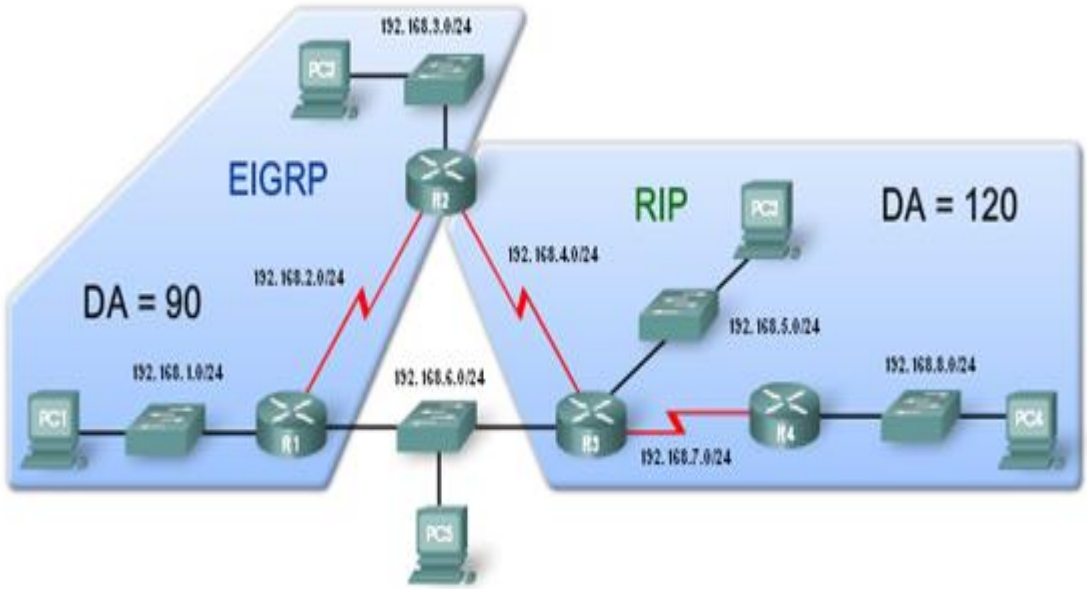


Figure II.7 : Comparaison des distances administratives.

La valeur de distance administrative vérifiée à l'aide de la commande **show ip route** et peut également être vérifiée à l'aide de la commande **show ip protocols**. Cette commande affiche toutes les informations pertinentes sur les protocoles de routage fonctionnant sur ce routeur.

Ce tableau représente Les différentes valeurs de distance administrative pour les différents protocoles de routage :

Origine de la route	Distance administrative
Connecté	**0**
Statique	**1**
Récapitulatif de routage du protocole EGRP	**5**
Protocole BGP externe	**20**
EIGRP interne	**90**
Protocole IGRP	**100**
Protocole OSPF	**110**
Protocole routage IS-IS	**115**
Protocole RIP	**120**
Protocole EIGRP externe	**170**
Protocole BGP interne	**200**

Tableau II.2 : Distance administratives par défaut.

CHAPITRE III

Protocoles de routage dynamique à vecteur de distance

III.1 Introduction

Ce chapitre relatif au routage dynamique traite des protocoles IGP (Interior Gateway Protocol). Comme décrit dans le chapitre 2, les protocoles IGP se répartissent en deux catégories : les protocoles à vecteur de distance et les protocoles d'état des liaisons. Ce chapitre décrit les caractéristiques, les opérations et les fonctionnalités propres aux protocoles de routage à vecteur de distance. Quel que soit le protocole de routage utilisé, tous présentent des avantages et des inconvénients. C'est pourquoi les conditions influençant le fonctionnement des protocoles à vecteur de distance, les pièges qu'ils présentent et les solutions appropriées sont décrites ci-dessous.

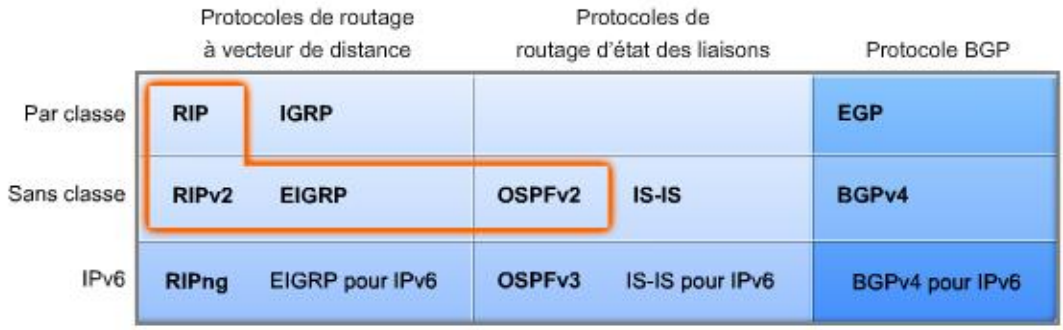


Tableau III.1 : Protocoles de routage dynamique.

III.2 Présentation des protocoles de routage à vecteur de distance

Les protocoles de routage dynamique à vecteur de distance comprennent : RIP, IGRP et EIGRP.

- **RIP :** Le protocole RIP (Routing Information Protocol) a été initialement défini dans le document RFC 1058. Ses principales caractéristiques sont les suivantes :
  - Il utilise le nombre de sauts comme mesure de sélection d'un chemin.
  - Si le nombre de sauts pour un réseau est supérieur à 15, le protocole RIP ne peut pas fournir de route à ce réseau.
  - Par défaut, les mises à jour de routage sont diffusées ou multidiffusées toutes les 30 secondes.

- **IGRP :** Le protocole IGRP (Interior Gateway Routing Protocol) est un protocole propriétaire développé par Cisco. Les principales caractéristiques conceptuelles du protocole IGRP sont les suivantes :
  - La bande passante, le délai, la charge et la fiabilité sont utilisés pour créer une mesure composite.
  - Par défaut, les mises à jour de routage sont diffusées toutes les 90 secondes.
  - Prédécesseur du protocole EIGRP, le protocole IGRP est désormais obsolète.

- **EIGRP**

Le protocole EIGRP (Enhanced IGRP) est un protocole de routage à vecteur de distance propriétaire développé par Cisco. Ses principales caractéristiques sont les suivantes :

- Il peut effectuer un équilibrage de charge à coût inégal.
- Il utilise l'algorithme DUAL (Diffused Update Algorithm) pour calculer le chemin le plus court.
- Contrairement aux protocoles RIP et IGRP, il n'y a pas de mises à jour régulières. Des mises à jour de routage sont envoyées uniquement en cas de modification de la topologie.

III.2.1 Fonctionnement des protocoles de routage à vecteur de distance

Un routeur utilisant un protocole de routage à vecteur de distance ne connaît pas le chemin complet vers un réseau de destination. Le routeur ne connaît que les éléments suivants :

- La direction ou l'interface dans laquelle les paquets doivent être transmis.
- La distance le séparant du réseau de destination.

Par exemple, dans la **figure III.1**, R1 sait que la distance le séparant du réseau 172.16.3.0/24 est égale à un saut et que la direction va de l'interface S0/0/0 vers R2.

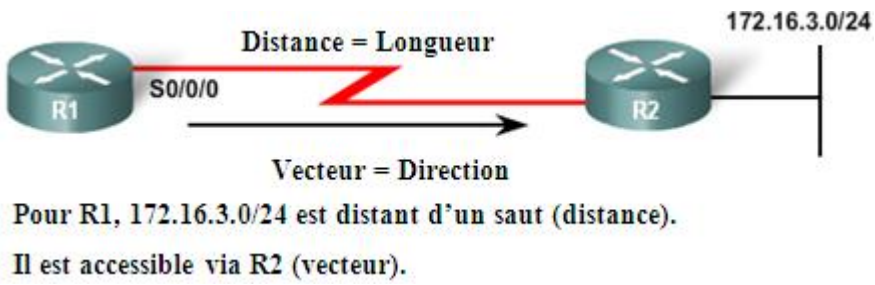


Figure III.1 : Signification du vecteur de distance.

Certains protocoles de routage à vecteur de distance appellent le routeur pour qu'il diffuse régulièrement la totalité de la table de routage à chacun de ses voisins. Cette méthode est inefficace car les mises à jour sollicitent non seulement de la bande passante, mais également les ressources processeur du routeur pour traiter ces mises à jour.

III.2.2 Algorithme des protocoles de routage à vecteur de distance

Au centre du protocole à vecteur de distance, l'algorithme est utilisé pour calculer les meilleurs chemins et pour envoyer ces informations aux voisins.

Un algorithme est une procédure permettant d'accomplir une certaine tâche, avec un état initial donné et un état de fin défini. Les protocoles de routage utilisent des algorithmes différents pour installer des routes dans la table de routage, envoyer des mises à jour aux voisins et déterminer le meilleur chemin.

L'algorithme utilisé pour les protocoles de routage définit les processus suivants :

- Mécanisme d'envoi et de réception des informations de routage
- Mécanisme de calcul des meilleurs chemins et d'installation de routes dans la table de routage
- Mécanisme de détection des modifications topologiques et de réaction à celles-ci

Dans la **figure III.2**, R1 et R2 sont configurés avec un protocole de routage (RIP). L'algorithme envoie et reçoit des mises à jour. R1 et R2 recueillent ensuite de nouvelles informations à partir de la mise à jour. Dans le cas présent, chaque routeur découvre un nouveau réseau.

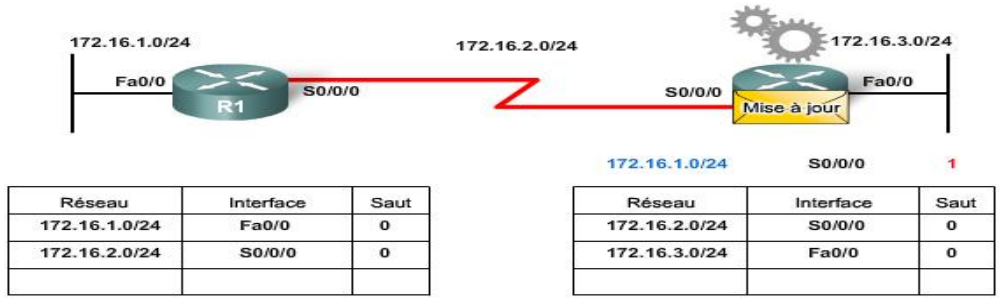
172.16.1.0/24 1

Réseau	Interface	Saut
172.16.1.0/24	Fa0/0	0
172.16.2.0/24	S0/0/0	0

Réseau	Interface	Saut
172.16.2.0/24	S0/0/0	0
172.16.3.0/24	Fa0/0	0

Figure III.2 : Envoie et réception des mises à jour.

L'algorithme de chaque routeur effectue ses calculs indépendamment et met à jour la table de routage en y incluant les nouvelles informations.



Réseau	Interface	Saut
172.16.1.0/24	Fa0/0	0
172.16.2.0/24	S0/0/0	0

Réseau	Interface	Saut
172.16.2.0/24	S0/0/0	0
172.16.3.0/24	Fa0/0	0

Figure III.3 : Calcul du meilleur chemin et de la route d'installation.

En cas de panne du réseau local sur R2, l'algorithme construit une mise à jour « déclenchée » et l'envoie à R1. R1 supprime ensuite le réseau de la table de routage.

Réseau	Interface	Saut
172.16.1.0/24	Fa0/0	0
172.16.2.0/24	S0/0/0	0
~~172.16.3.0/24~~	~~S0/0/0~~	~~1~~

Réseau	Interface	Saut
172.16.2.0/24	S0/0/0	0
~~172.16.3.0/24~~	~~Fa0/0~~	~~0~~
172.16.1.0/24	S0/0/0	1

Figure III.4 : Détection et réaction face aux modifications de la topologie.

III.2.3 Caractéristiques des protocoles de routage dynamique à vecteur de distance

Plusieurs caractéristiques permettent de différencier les protocoles de routage :

Ø **Temps de convergence** : Le temps de convergence définit la rapidité à laquelle les routeurs dans la topologie du réseau parviennent à partager les informations de routage et à disposer d'une base de connaissances cohérente. Plus la convergence est rapide, plus le protocole est recommandé. Des boucles de routage peuvent apparaître lorsque des tables de routage incohérentes ne sont pas mises à jour en raison d'une convergence plus lente dans un environnement réseau changeant.

Ø **Évolutivité** : L'évolutivité définit la taille maximale d'un réseau en fonction du protocole de routage qui est déployé. Plus le réseau est grand, plus le protocole de routage doit être évolutif.

Ø **Sans classe ou par classe** : Les protocoles de routage sans classe incluent le masque de sous-réseau dans les mises à jour. Cette fonctionnalité prend en charge l'utilisation de masques de sous-réseau de longueur variable et permet un meilleur résumé des routes. Les protocoles de routage par classe n'incluent pas le masque de sous-réseau et ne peuvent pas prendre en charge les masques de sous-réseau.

Ø **Utilisation des ressources** : Inclut les exigences d'un protocole de routage telles que l'espace mémoire, l'utilisation du processeur et l'utilisation de la bande passante de liaison. Pour des besoins en ressources plus élevés, un matériel plus puissant est nécessaire pour prendre en charge le fonctionnement du protocole de routage en plus des processus de transfert de paquets.

Ø **Implémentation et maintenance** : L'implémentation et la maintenance font référence aux connaissances qu'un administrateur réseau doit posséder pour implémenter et gérer le réseau en fonction du protocole de routage déployé.

a. Avantages des protocoles de routage à vecteur de distance

Ø **Implémentation et maintenance simples**. Le niveau de connaissances requis pour déployer et effectuer la maintenance ultérieure d'un réseau avec un protocole à vecteur de distance n'est pas élevé.

Ø **Faibles ressources requises**. Les protocoles à vecteur de distance n'ont généralement pas

besoin de grandes quantités de mémoire pour stocker les informations. Ils ne nécessitent pas non plus une UC puissante. Selon la taille du réseau et l'adressage IP implémentés, ils ne nécessitent généralement pas une bande passante importante pour envoyer les mises à jour de routage. Cependant, cela peut devenir un problème si un protocole à vecteur de distance est déployé dans un réseau important.

b. Inconvénients des protocoles de routage à vecteur de distance :

Ø **Convergence lente**. L'utilisation de mises à jour périodiques peut ralentir la convergence. Même si des techniques avancées sont utilisées, telles que les mises à jour déclenchées qui seront abordées ultérieurement, la convergence globale est toujours plus lente que celle constatée avec les protocoles de routage d'état des liaisons.

Ø **Évolutivité limitée**. La convergence lente peut limiter la taille du réseau car des réseaux
plus importants nécessitent davantage de temps pour propager les informations de routage.

Ø **Boucles de routage**. Des boucles de routage peuvent survenir lorsque des tables de routage incohérentes ne sont pas mises à jour en raison d'une convergence lente dans un réseau changeant.

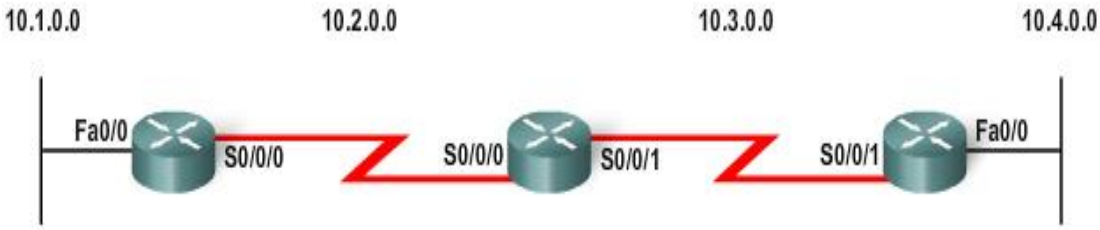
III .3 : Découverte du réseau

III.3.1 : Démarrage à froid

Lorsqu'un routeur démarre à froid ou est mis sous tension, il ne dispose d'aucune information sur la topologie du réseau. Il ne sait même pas que des périphériques sont connectés à l'autre extrémité de ses liaisons. Les seules informations dont dispose un routeur sont celles de son propre fichier de configuration qui est stocké dans la mémoire vive non volatile (NVRAM). Une fois amorcé avec succès, le routeur applique la configuration enregistrée, le routeur détecte initialement ses propres réseaux connectés directement si l'adressage IP a été correctement configuré.

III.3.2 : Détection de réseau initiale

Après un démarrage à froid et avant l'échange d'informations de routage, les routeurs détectent initialement leurs propres réseaux connectés directement et masques de sous-réseau. Ces informations sont ajoutées à leurs tables de routage. (Figure III.5).



Réseau	Interface	Saut
10.1.0.0	Fa0/0	0
10.2.0.0	S0/0/0	0

Réseau	Interface	Saut
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/1	0

Réseau	Interface	Saut
10.3.0.0	S0/0/1	0
10.4.0.0	Fa0/0	0

Figure III.5 : Découverte du réseau : démarrage à froid.

R1 :

- 10.1.0.0 disponible via l'interface FastEthernet 0/0
- 10.2.0.0 disponible via l'interface Serial 0/0/0

R2 :

- 10.2.0.0 disponible via l'interface Serial 0/0/0
- 10.3.0.0 disponible via l'interface Serial 0/0/1

R3 :

- 10.3.0.0 disponible via l'interface Serial 0/0/0
- 10.4.0.0 disponible via l'interface FastEthernet 0/0

III.3.3 : Echange initial d'informations de routage à vecteur de distance

Si un protocole de routage est configuré, les routeurs commencent à échanger des mises à jour de routage. Au départ, ces mises à jour n'incluent que des informations concernant leurs réseaux directement connectés. Dès qu'il reçoit une mise à jour, le routeur recherche les nouvelles informations. Toute route ne figurant pas actuellement dans la table de routage du routeur est ajoutée.

Réseau	Interface	Saut
10.1.0.0	Fa0/0	0
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/0	1

Réseau	Interface	Saut
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/1	0
10.1.0.0	S0/0/0	1
10.4.0.0	S0/0/1	1

Réseau	Interface	Saut
10.3.0.0	S0/0/0	0
10.4.0.0	Fa0/0	0
10.2.0.0	S0/0/1	1

Figure III.6 : Découverte du réseau : échange initial

R1, R2 et R3 démarrent l'échange initial. Les trois routeurs envoient leurs tables de routage à leurs voisins, qui à ce stade contiennent uniquement les réseaux connectés directement. Chaque routeur traite les mises à jour de la façon suivante :

R1 :

- Envoie une mise à jour sur le réseau 10.1.0.0 via l'interface Serial 0/0/0.
- Envoie une mise à jour sur le réseau 10.2.0.0 via l'interface FastEthernet 0/0.
- Reçoit une mise à jour de R2 sur le réseau 10.3.0.0 avec une mesure de 1.
- Stocke le réseau 10.3.0.0 dans la table de routage avec une mesure de 1.

R2 :

- Envoie une mise à jour sur le réseau 10.3.0.0 via l'interface Serial 0/0/0.
- Envoie une mise à jour sur le réseau 10.2.0.0 via l'interface Serial 0/0/1.
- Reçoit une mise à jour de R1 sur le réseau 10.1.0.0 avec une mesure de 1.
- Stocke le réseau 10.1.0.0 dans la table de routage avec une mesure de 1.
- Reçoit une mise à jour de R3 sur le réseau 10.4.0.0 avec une mesure de 1.
- Stocke le réseau 10.4.0.0 dans la table de routage avec une mesure de 1.

R3 :

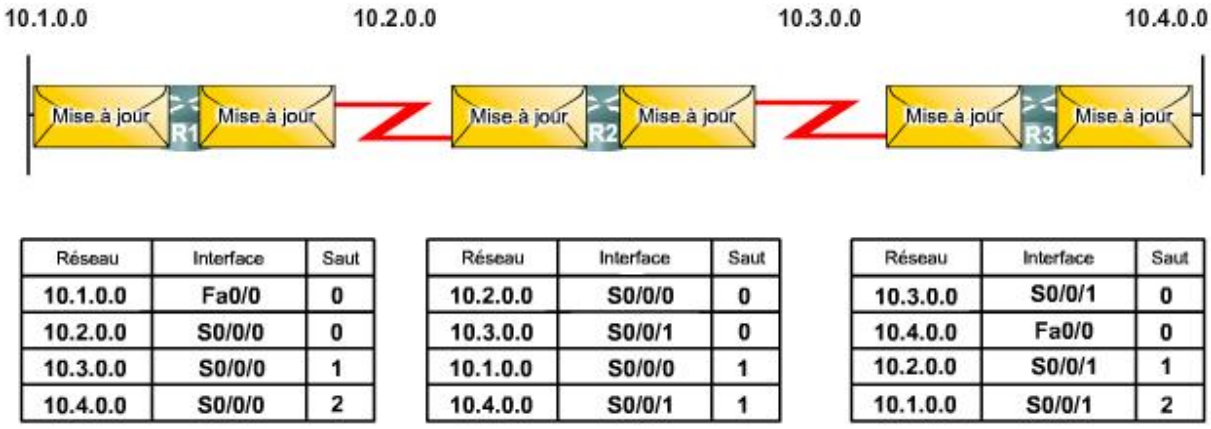
- Envoie une mise à jour sur le réseau 10.4.0.0 via l'interface Serial 0/0/0.
- Envoie une mise à jour sur le réseau 10.3.0.0 via l'interface FastEthernet 0/0.
- Reçoit une mise à jour de R2 sur le réseau 10.2.0.0 avec une mesure de 1.
- Stocke le réseau 10.2.0.0 dans la table de routage avec une mesure de 1.

Chaque routeur a connaissance des réseaux connectés de leurs voisins connectés directement. Toutefois, R1 ne connaît pas encore l'existence du réseau 10.4.0.0 et que R3 ne connaît pas encore l'existence du réseau 10.1.0.0. La connaissance du réseau ne sera pas complète et sa convergence ne pourra pas avoir lieu tant qu'un autre échange d'informations de routage n'aura pas été effectué.

III.3.4 : Echange d'informations de routage

Les routeurs connaissent leurs propres réseaux directement connectés et les réseaux connectés de leurs voisins immédiats. Pour se rapprocher de la convergence, les routeurs échangent des mises à jour régulières (figure III.7) et Chaque routeur vérifie une nouvelle fois les mises à jour à la recherche de nouvelles informations.

Dans la **figure III.7** suivante ; R1, R2 et R3 envoient la dernière table de routage à leurs voisins.



Réseau	Interface	Saut
10.1.0.0	Fa0/0	0
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/0	1
10.4.0.0	S0/0/0	2

Réseau	Interface	Saut
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/1	0
10.1.0.0	S0/0/0	1
10.4.0.0	S0/0/1	1

Réseau	Interface	Saut
10.3.0.0	S0/0/1	0
10.4.0.0	Fa0/0	0
10.2.0.0	S0/0/1	1
10.1.0.0	S0/0/1	2

Figure III.7 : Découverte du réseau : mise à jour.

Chaque routeur traite les mises à jour de la façon suivante :

R1 :

- Envoie une mise à jour sur le réseau 10.1.0.0 via l'interface Serial 0/0/0.
- Envoie une mise à jour sur les réseaux 10.2.0.0 et 10.3.0.0 via l'interface FastEthernet 0/0.
- Reçoit une mise à jour de R2 sur le réseau 10.4.0.0 avec une mesure de 2.

- Stocke le réseau 10.4.0.0 dans la table de routage avec une mesure de 2.
- La même mise à jour de R2 contient des informations sur le réseau 10.3.0.0 avec une mesure de 1. Aucune modification n'est intervenue ; par conséquent, les informations de routage restent les mêmes.

R2 :

- Envoie une mise à jour sur les réseaux 10.3.0.0 et 10.4.0.0 via l'interface Serial 0/0/0.
- Envoie une mise à jour sur les réseaux 10.1.0.0 et 10.2.0.0 via l'interface Serial 0/0/1.
- Reçoit une mise à jour de R1 sur le réseau 10.1.0.0. Aucune modification n'est intervenue ; par conséquent, les informations de routage restent les mêmes.
- Reçoit une mise à jour de R3 sur le réseau 10.4.0.0. Aucune modification n'est intervenue ; par conséquent, les informations de routage restent les mêmes.

R3 :

- Envoie une mise à jour sur le réseau 10.4.0.0 via l'interface Serial 0/0/0.
- Envoie une mise à jour sur les réseaux 10.2.0.0 et 10.3.0.0 via l'interface FastEthernet 0/0.
- Reçoit une mise à jour de R2 sur le réseau 10.1.0.0 avec une mesure de 2.
- Stocke le réseau 10.1.0.0 dans la table de routage avec une mesure de 2.
- La même mise à jour de R2 contient des informations sur le réseau 10.2.0.0 avec Une mesure de 1. Aucune modification n'est intervenue ; par conséquent, les informations de routage restent les mêmes.

III.3.5 : Convergence de protocole de routage à vecteur de distance

Le temps nécessaire à un réseau pour converger est directement proportionnel à la taille de ce réseau. Dans la **figure III.8**, un routeur de succursale dans la Région 4 (R2-R4) effectue un démarrage à froid. La figure suivante montre la propagation des nouvelles informations de routage à mesure que des mises à jour sont échangées entre les routeurs voisins. Cinq séries d'échanges de mises à jour régulières sont nécessaires pour que la plupart des routeurs de succursale des Régions 1, 2 et 3 découvrent les nouvelles routes annoncées

par R2-R4. Les protocoles de routage sont évalués en fonction de la vitesse à laquelle ils peuvent propager ces informations : on parle de vitesse de convergence.

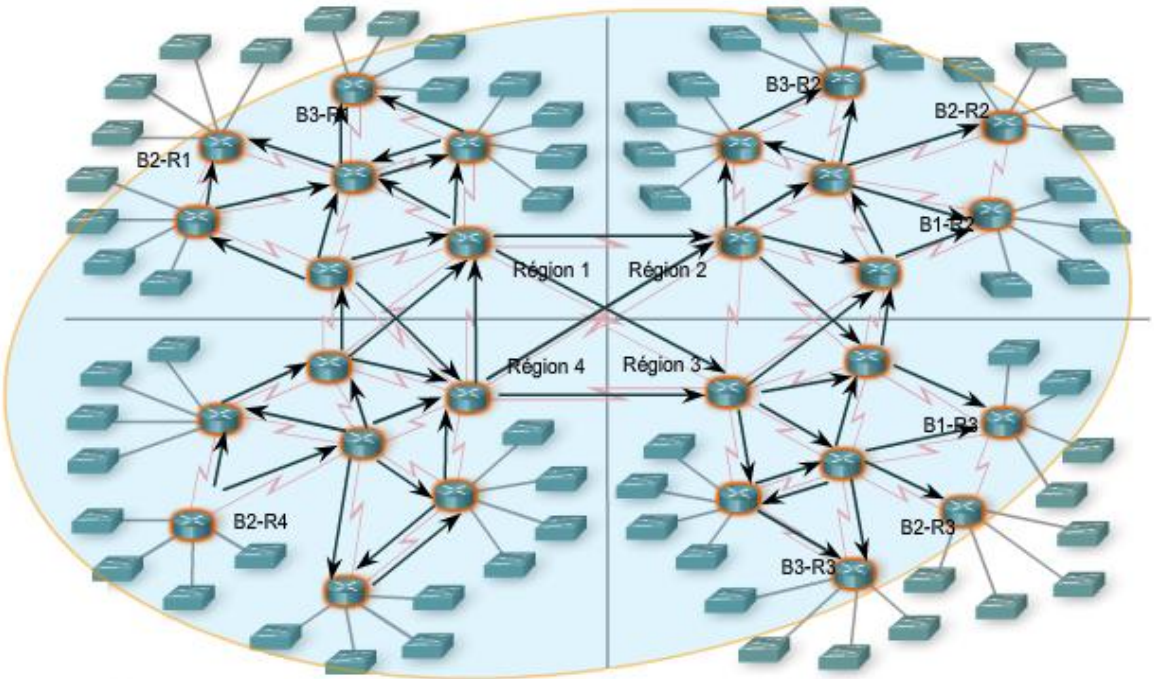


Figure III.8 : Durée de convergence.

La vitesse de convergence englobe les éléments suivants :

- La vitesse à laquelle le routeur propage une modification de la topologie lors d'une mise à jour de routage à ses voisins ;
- La vitesse de calcul des meilleurs chemins à l'aide des nouvelles informations de routage collectées.

Un réseau n'est pas complètement opérationnel tant qu'il n'a pas convergé. C'est pourquoi les administrateurs réseau préfèrent les protocoles de routage avec des temps de convergences courts.

III.4 Maintenance des tables de routage à vecteur de distance

III.4.1 : Mises à jour régulières : Protocoles RIPv1 et IGRP

a. Mise à jour de la table de routage

Plusieurs protocoles à vecteur de distance ont recours à des mises à jour régulières pour échanger des informations de routage avec leurs voisins et maintenir les informations de routage à jour dans la table de routage. RIP et IGRP sont des exemples de protocoles agissant de la sorte.

Dans la **figure III.9** suivante, les routeurs envoient régulièrement la table de routage à leurs voisins. Le terme de mise à jour régulière fait référence au fait qu'un routeur envoie la table de routage complète à ses voisins à un intervalle prédéfini. Pour les protocoles RIP, ces mises à jour sont envoyées toutes les 30 secondes sous forme de diffusion (255.255.255.255) que la topologie ait été ou non modifiée. L'intervalle de 30 secondes est un minuteur de mise à jour des routes qui permet également de connaître l'âge des informations de routage dans une table de routage.

L'âge des informations de routage d'une table de routage est actualisé à chaque réception d'une mise à jour. Les informations de la table de routage peuvent ainsi être mises à jour dès que la topologie est modifiée. Des modifications peuvent avoir lieu pour plusieurs raisons, notamment :

- Défaillance d'une liaison
- Introduction d'une nouvelle liaison
- Défaillance d'un routeur
- Modification des paramètres de liaison

Réseau	Interface	Saut
10.1.0.0	Fa0/0	0
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/0	1
10.4.0.0	S0/0/0	2

Réseau	Interface	Saut
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/1	0
10.1.0.0	S0/0/0	1
10.4.0.0	S0/0/1	1

Réseau	Interface	Saut
10.3.0.0	S0/0/1	0
10.4.0.0	Fa0/0	0
10.2.0.0	S0/0/1	1
10.1.0.0	S0/0/1	2

Figure III.9 : Mises à jour périodiques.

b. Minuteurs RIP

Outre le minuteur de mise à jour, l'IOS implémente trois minuteurs supplémentaires pour le protocole RIP :

Minuteur de temporisation (Invalid Timer) : Si aucune mise à jour n'a été reçue pour actualiser une route existante dans les 180 secondes (par défaut), la route est marquée comme non valide (valeur 16 attribuée à la mesure). La route est conservée dans la table de routage jusqu'à l'expiration du minuteur d'annulation.

Minuteur d'annulation (Flush Timer) : Par défaut, le minuteur d'annulation une valeur de 240 secondes, ce qui représente 60 secondes de plus que le minuteur de temporisation. Lorsque le délai du minuteur d'annulation expire, la route est supprimée de la table de routage.

Minuteur de mise hors service (Holddown Timer) : Ce minuteur stabilise les informations de routage et peut permettre d'éviter les boucles de routage au moment de la convergence de la topologie sur la base de nouvelles informations. Une fois marquée comme inaccessible, une route doit rester hors service suffisamment longtemps pour que tous les routeurs de la topologie découvrent le réseau inaccessible. Par défaut, le minuteur de mise hors service à une valeur de 180 secondes.

```
R1#show ip route
<output omitted>

Gateway of last resort is not set

     10.0.0.0/16 is subnetted, 4 subnets
C       10.2.0.0 is directly connected, Serial0/0/0
R       10.3.0.0 [120/1] via 10.2.0.2, 00:00:04, Serial0/0/0
C       10.1.0.0 is directly connected, FastEthernet0/0
R       10.4.0.0 [120/2] via 10.2.0.2, 00:00:04, Serial0/0/0
```

Tableau III.2 : Vérification des compteurs avec la commande show ip route.

Les valeurs du minuteur vérifier avec deux commandes : **show ip route** et **show ip protocols**. Dans la sortie de la commande show ip route, chaque route découverte par le biais du protocole **RIP** indique le temps écoulé depuis la dernière mise à jour (exprimé en secondes).

```
R1#show ip protocols
Routing Protocol is "rip"
  Sending updates every 30 seconds, next due in 13 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  <output omitted>
  Routing for Networks:
    10.0.0.0
  Routing Information Sources:
    Gateway         Distance      Last Update
    10.3.0.1             120      00:00:27
  Distance: (default is 120)
```

Tableau III.3 : Vérification des compteurs avec la commande show ip protocols.

Ces informations sont aussi répétées dans la sortie show ip protocols sous le titre **Last Update**. La commande show ip protocols indique à quel moment le routeur R1 est supposé envoyer sa prochaine série de mises à jour. Elle énumère également les valeurs par défaut des minuteurs de temporisation, de mise hors service et d'annulation.

III.4.2 Mise à jour limitées : Protocole EIGRP

À la différence des autres protocoles de routage à vecteur de distance, le protocole EIGRP n'envoie pas de mises à jour régulières. Au lieu de cela, le protocole EIGRP envoie des mises à jour limitées à propos d'une route en cas de modification d'un chemin ou de la mesure pour cette route. Lorsqu'une nouvelle route devient disponible ou qu'une route doit être supprimée, le protocole EIGRP envoie une mise à jour ne concernant que ce réseau et non la table entière. Ces informations sont envoyées uniquement aux routeurs qui en ont besoin.

Le protocole EIGRP utilise des mises à jour qui présentent les caractéristiques suivantes :

- Elles ne sont pas régulières car elles ne sont pas envoyées périodiquement.
- Des mises à jour partielles sont envoyées uniquement en cas de modification

- topologique influençant les informations de routage.
- Elles sont limitées, ce qui signifie que la propagation des mises à jour partielles est automatiquement limitée de sorte que seuls les routeurs ayant besoin de ces informations sont mis à jour.

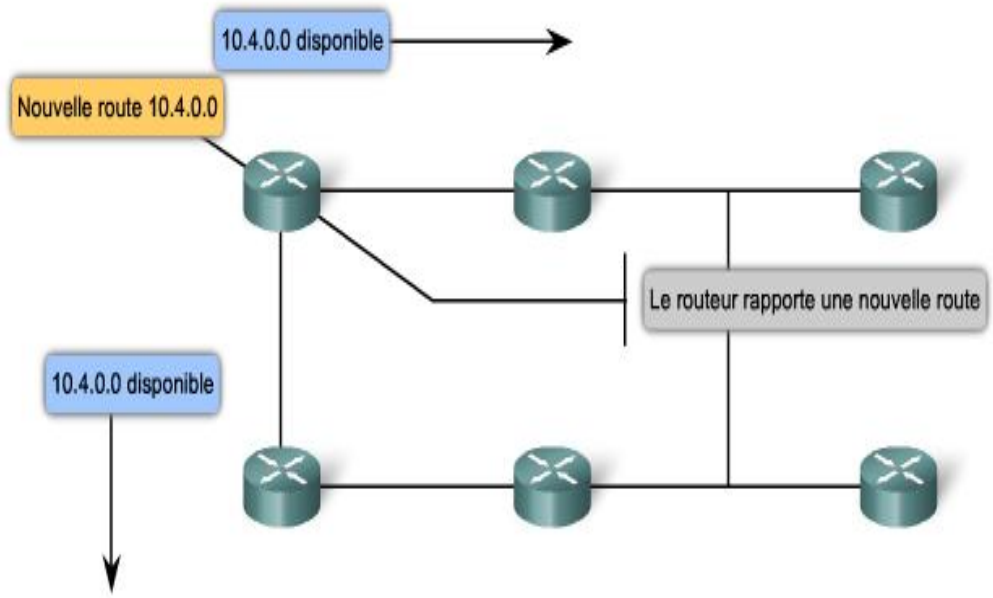


Figure III.10 : Mise à jour limitées : EIGRP.

III.4.3 Mises à jour déclenchées

Pour accélérer la convergence en cas de modification de la topologie, le protocole RIP utilise des mises à jour déclenchées. Une mise à jour déclenchée est une mise à jour de la table de routage qui est envoyée immédiatement en réponse à la modification d'un routage. Les mises à jour déclenchées n'attendent pas l'expiration des minuteurs. Le routeur qui détecte la modification envoie immédiatement un message de mise à jour aux routeurs adjacents. Les routeurs qui reçoivent cette information génèrent à leur tour des mises à jour déclenchées pour informer leurs voisins de la modification.

Des mises à jour déclenchées sont envoyées lorsque l'un des événements suivants se produit :

- Une interface change d'état (activée ou désactivée)
- Une route passe à l'état « inaccessible ».
- Une route est installée dans la table de routage

Pour pouvoir utiliser uniquement des mises à jour déclenchées, il faudrait avoir la certitude que la vague de mises à jour atteigne immédiatement chaque routeur approprié. Toutefois, deux problèmes sont associés aux mises à jour déclenchées :

- Les paquets contenant le message de mise à jour peut être abandonné ou endommagé par une liaison dans le réseau.
- Les mises à jour déclenchées ne se produisent pas instantanément. Il est possible qu'un routeur qui n'a pas encore reçu la mise à jour déclenchée émette une mise à jour régulière au mauvais moment, provoquant ainsi la réinsertion de la route incorrecte dans un voisin ayant déjà reçu la mise à jour déclenchée.

Une modification de la topologie du réseau est propagée à l'ensemble du réseau. Lorsque le réseau 10.4.0.0 n'est plus disponible et que le routeur C en prend connaissance, il envoie les informations à ses voisins. Cette information est ensuite propagée sur l'ensemble du réseau (voir la **figure III.11**).

Figure III.11 : Mise à jour déclenchées.

III.5 Boucle de routage dynamique à vecteur de distance

Une boucle de routage est une condition dans laquelle un paquet est transmis en continu entre une série de routeurs sans jamais atteindre le réseau de destination souhaité. Une boucle de routage peut se produire lorsque deux routeurs ou plus possèdent des informations de routage qui indiquent, à tort, qu'il existe un chemin valide vers une destination inaccessible.

La boucle peut être le résultat des problèmes suivants :

- Routes statiques configurées incorrectement.
- Redistribution de routes configurées incorrectement (la redistribution, c.-à-d. le processus de transmission des informations de routage d'un protocole de routage à un autre).
- Tables de routage incohérentes qui ne sont pas mises à jour en raison d'une convergence lente dans un réseau changeant.

- Routes de suppression configurées ou installées incorrectement.

Les protocoles de routage à vecteur de distance sont d'un fonctionnement simple. Cette simplicité se traduit par des inconvénients, comme les boucles de routage. Les boucles de routage sont moins susceptibles de se produire avec les protocoles de routage d'état des liaisons, mais elles peuvent néanmoins survenir dans certaines circonstances.

III.5.1 Les implications des boucles de routage à vecteur de distance

Une boucle de routage peut avoir des effets dévastateurs sur un réseau, notamment la réduction des performances réseau voire une panne du réseau.

Une boucle de routage peut créer les conditions suivantes :

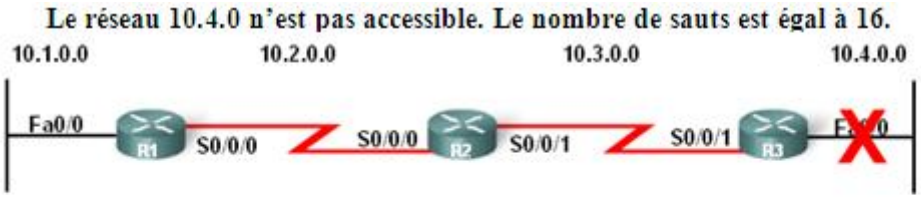
- La bande passante de la liaison est utilisée pour faire tourner le trafic en boucle entre les routeurs dans une boucle.
- Le processeur d'un routeur est fortement sollicité en raison des paquets tournant en boucle.
- Le processeur d'un routeur est surchargé en raison du réacheminement inutile de paquets, ce qui impacte négativement la convergence du réseau.
- Les mises à jour de routage peuvent se perdre ou ne pas être traitées en temps voulu. Ces conditions introduisent des boucles de routage supplémentaires qui aggravent davantage la situation.
- Les paquets peuvent se perdre dans des « trous noirs ».

Plusieurs mécanismes, principalement associés aux protocoles de routage à vecteur de distance, sont disponibles pour éliminer les boucles de routage. Ces mécanismes incluent les éléments suivants :

- Définition d'une mesure maximale pour éviter le comptage à l'infini.
- Minuteurs de mise hors service.
- Découpage d'horizon.
- Empoisonnement de routage ou antipoison.
- Mises à jour déclenchées.

III.5.2 Définition d'une valeur maximale

Pour arrêter l'incrémentation d'une mesure, l'« infini » est défini par l'attribution d'une valeur maximale à la mesure. Par exemple, le protocole RIP considère que 16 sauts représentent l'infini, ce qui correspond à une mesure inaccessible. Une fois que les routeurs ont compté jusqu'à l'infini, ils marquent la route comme étant inaccessible.



Réseau	Interface	Saut
10.1.0.0	Fa0/0	0
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/0	1
10.4.0.0	S0/0/0	16

Réseau	Interface	Saut
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/1	0
10.1.0.0	S0/0/0	1
10.4.0.0	S0/0/1	16

Réseau	Interface	Saut
10.3.0.0	S0/0/1	0
10.4.0.0	S0/0/1	16
10.2.0.0	S0/0/1	1
10.1.0.0	S0/0/1	2

Figure III.12 : Définition d'une valeur maximale.

III.5.3 Règle de découpage d'horizon

Le découpage d'horizon est une autre méthode qui permet d'empêcher les boucles de routage provoquées par la convergence lente d'un protocole de routage à vecteur de distance. Selon la règle de découpage d'horizon, un routeur ne doit pas annoncer de réseau par le biais de l'interface dont est issue la mise à jour.

L'application du découpage d'horizon à la route 10.4.0.0 de la figure III.12 précédente, génère les actions suivantes :

- R3 annonce le réseau 10.4.0.0 à R2.
- R2 reçoit l'information et met à jour sa table de routage.
- R2 annonce ensuite le réseau 10.4.0.0 à R1 via S0/0/0. R2 n'annonce pas 10.4.0.0 à R3 via S0/0/1 car la route provient de cette interface.
- R1 reçoit l'information et met à jour sa table de routage.

  En raison du découpage d'horizon, R1 n'annonce pas non plus les informations sur le réseau 10.4.0.0 à R2.

Des mises à jour de routage complètes sont échangées, à l'exception des routes qui transgressent la règle de découpage d'horizon. Le résultat ressemble à ceci :

- R2 annonce les réseaux 10.3.0.0 et 10.4.0.0 à R1.
- R2 annonce les réseaux 10.1.0.0 et 10.2.0.0 à R3.
- R1 annonce le réseau 10.1.0.0 à R2.
- R3 annonce le réseau 10.4.0.0 à R2.

III.6 Protocoles RIP et EIGRP

Pour les protocoles de routage à vecteur de distance, le choix se limite à RIP ou EIGRP. Le choix du protocole à utiliser dans une situation donnée varie en fonction d'un certain nombre de facteurs, dont les suivants :

- Taille du réseau
- Compatibilité entre les modèles de routeurs
- Connaissances administratives requises

III.6.1 Caractéristiques du protocole RIP

- Prise en charge du découpage d'horizon.
- Possibilité d'équilibrer la charge sur six chemins à coût égal au maximum. L'option par défaut est de quatre chemins à coût égal.

III.6.2 Caractéristiques du protocole EIGRP

- Mises à jour déclenchées (EIGRP n'a pas de mises à jour régulières).
- Utilisation d'une table topologique pour maintenir toutes les routes reçues des voisins (pas seulement les meilleurs chemins).
- Établissement de contiguïtés avec des routeurs voisins par le biais du protocole Hello EIGRP.
- Prise en charge des masques de sous-réseau de longueur variable et du résumé de routes manuel, permettant ainsi au protocole EIGRP de créer des grands réseaux structurés hiérarchiquement.

III.7 Protocole RIP Version 1

Le protocole RIP est le plus ancien des protocoles de routage à vecteur de distance. Bien qu'il ne soit pas aussi sophistiqué que des protocoles de routage plus avancés, sa simplicité et son utilisation généralisée à ce jour sont le garant de sa longévité. Le protocole RIP n'est pas en train de disparaître. Une version IPv6 du protocole RIP, appelée RIPng (nouvelle génération), est désormais disponible.

RIP est né d'un protocole antérieur développé par Xerox, appelé Gateway Information Protocol (GWINFO). Avec le développement de Xerox Network System (XNS), GWINFO a évolué en RIP. Il a par la suite gagné en popularité suite à son implémentation dans Berkeley Software Distribution (BSD) en tant que démon nommé routed (prononcé « route-d »). Plusieurs autres fournisseurs ont alors créé leurs propres implémentations du protocole RIP en y intégrant de légères différences. En 1988, reconnaissant le besoin de normaliser ce protocole, Charles Hedrick écrit le document RFC 1058 dans lequel il documente le protocole existant et propose quelques améliorations. Depuis, le protocole RIP a été amélioré avec RIPv2 en 1994 et RIPng en 1997.

La première version du protocole RIP est souvent appelée RIPv1 pour la distinguer de RIPv2. Toutefois, les deux versions sont très similaires en termes de fonctionnalités. Lorsque nous étudierons les fonctionnalités communes aux deux versions, nous parlerons du protocole RIP ; lorsque nous étudierons les fonctionnalités propres à chaque version, nous utiliserons RIPv1 et RIPv2.

La partie données d'un message RIP est encapsulée dans un segment UDP, avec les numéros de ports source et de destination définis sur 520. L'en-tête IP et les en-têtes de liaison de données ajoutent des adresses de destination de diffusion avant l'envoi du message à toutes les interfaces configurées RIP.

III.7.1 Message RIPv1 encapsulé

Ø En-tête de trame liaison de données

Adresse source MAC = Adresse de l'interface émettrice.

Adresse de destination MAC = diffusion : FF-FF-FF-FF-FF-FF.

Ø En-tête de paquet IP

Adresse IP source = Adresse de l'interface émettrice.

Adresse IP de destination = diffusion : 255.255.255.255

Champ de protocole = 17 pour UDP.

Ø En-tête de segment UDP

Port source =520.

Port de destination = 520.

Message RIP (512 octet ; jusqu'à 25 routes) :

Commande : demande (1) ; réponse (2).

Version = 1.

ID de famille d'adresse = 2 pour IP.

Route = adresse IP de réseau

Mesure = nombre de sauts.

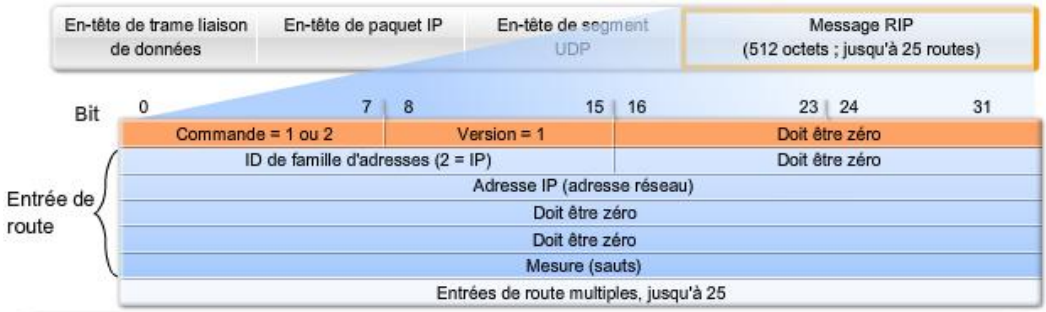
III.7.2 Caractéristique et format des messages du protocole RIPv1

a. Format des messages du protocole RIPv1 : En-tête RIPv1

Trois champs sont spécifiés dans la partie en-tête à quatre octets apparaissant en orange dans le tableau III.4 suivant**.** Le champ Commande identifie le type de message. Le champ Version est défini sur 1 pour Protocole RIP version 1. Le troisième champ est défini sur Must be zero. Les champs « Must be zero » fournissent de la place pour une extension future du protocole.

b. Format de message RIPv1 : Entrée de route

La partie entrée de route du message comprend trois champs avec le contenu suivant : Identificateur de famille d'adresses (de valeur 2 pour le protocole IP sauf si un routeur exige une table de routage complète, auquel cas ce champ doit avoir la valeur zéro), Adresse IP et Mesure. Cette partie du message relative à l'entrée de route représente une route de destination avec sa mesure associée. Une mise à jour RIP peut contenir jusqu'à 25 entrées de route. La taille maximale du datagramme est 512 octets, sans compter les en-têtes IP ou UDP.



Commande	1 pour une demande ou 2 pour une réponse.
Version	1 pour RIP v1 ou 2 pour RIP v2.
ID de famille d'adresses	2 pour IP et 0 si la demande concerne la table de routage complète.
Adresse IP	Adresse de la route de destination, qui peut être un réseau, un sous-réseau ou une adresse d'hôte.
Mesure	Nombre de sauts compris entre 1 et 16. Le routeur émetteur augmente la mesure avant d'envoyer le message.

Tableau III.4 : Format de message RIPv1.

III.7.3 : Fonctionnement du protocole RIPv1

a. Processus de requête/réponse IP

Le protocole RIP utilise deux types de messages spécifiés dans le champ Commande : un message de requête et un message de réponse.

Chaque interface configurée sous RIP envoie un message de requête au démarrage, demandant à ce que tous les voisins RIP envoient leurs tables de routage complètes. Un message de réponse est renvoyé par les voisins RIP. Lorsque le routeur à l'origine de la requête reçoit les réponses, il évalue chaque entrée de route. Si une entrée de route est nouvelle, le routeur de réception installe cette route dans la table de routage. Si la route existe déjà dans la table, l'entrée existante est remplacée par la nouvelle si son nombre de sauts est meilleur. Le routeur qui vient de démarrer envoie ensuite une mise à jour déclenchée via toutes les interfaces RIP contenant sa propre table de routage pour communiquer les nouvelles routes aux voisins RIP.

b. Classes d'adresses IP et routage par classe

RIP est un protocole de routage par classe. Le protocole RIPv1 n'envoie pas d'informations de masque de sous-réseau dans la mise à jour. Par conséquent, un routeur utilise le masque de sous-réseau configuré sur une interface locale ou applique le masque de sous-réseau par défaut de la classe de l'adresse. Du fait de cette limite, les réseaux RIPv1 ne peuvent pas être discontinus.

III.8 : Protocole RIP VERSION 2

RIPv2 est un protocole de routage sans classe à vecteur de distance qui est défini dans le document RFC 1723. S'agissant d'un protocole de routage sans classe, RIPv2 inclut le masque de sous-réseau aux adresses réseau des mises à jour de routage. À l'instar des autres protocoles de routage sans classe, RIPv2 prend en charge les réseaux discontinus.

RIPv2 est en fait une amélioration des fonctions et des extensions du protocole RIPv1 plutôt qu'un nouveau protocole à part entière. Ces fonctions améliorées comprennent :

- Les adresses de tronçon suivant comprises dans les mises à jour de routage ;
- L'utilisation d'adresses de multidiffusion pour l'envoi de mises à jour ;
- L'option d'authentification disponible.

III.8.1 Configuration de RIPv2

a. Comparaison des formats des messages RIPv1 et RIPv2

À l'instar de la version 1, RIPv2 est encapsulé dans un segment UDP via le port 520 et peut transporter jusqu'à 25 routes. Bien que RIPv2 possède le même format de message de base que RIPv1, deux modifications majeures ont été apportées.

La première modification apportée au format de message RIPv2 se situe au niveau du champ du masque de sous-réseau, qui permet d'inclure un masque 32 bits dans l'entrée de route RIP. En conséquence, le routeur récepteur ne dépend plus du masque de sous-réseau de l'interface entrante ou du masque par classe lors de la détermination du masque de sous-réseau d'une route.

La deuxième modification significative apportée au format du message RIPv2 concerne l'ajout de l'adresse de tronçon suivant. L'adresse de tronçon suivant permet, le cas échéant, d'identifier une adresse de tronçon suivant mieux adaptée que l'adresse du routeur

émetteur. Si le champ contient uniquement des zéros (0.0.0.0), l'adresse du routeur émetteur constitue la meilleure adresse de tronçon suivant.

Tableau III.5 : Comparaison des formats des messages RIPv1et RIPv2.

III.8.2 RIPv2 et l'Authentification

La plupart des protocoles de routage envoient leurs mises à jour de routage et d'autres informations de routage à l'aide du protocole IP (sous forme de paquets IP). Le problème de sécurité propre à tout protocole de routage est le risque d'accepter des mises à jour de routage invalides. La source de ces mises à jour de routage invalides peut être une personne malveillante qui tente d'interrompre le fonctionnement du réseau ou de capturer des paquets en indiquant au routeur une mauvaise destination d'envoi des mises à jour. Un routeur incorrectement configuré peut constituer une autre source de mises à jour invalides. Il peut arriver également qu'un hôte soit relié au réseau et qu'à l'insu de l'utilisateur, l'hôte exécute le protocole de routage du réseau local.

Par exemple dans la **figure 3.13**, R1 propage une route par défaut dans tous les autres routeurs de ce domaine de routage. Cependant, une personne a ajouté par erreur le routeur R4 au réseau, qui propage également une route par défaut. Certains routeurs peuvent transférer le

trafic par défaut vers R4 au lieu du véritable routeur de passerelle, à savoir R1. Ces paquets peuvent entrer dans un « trou noir » et disparaître à jamais.

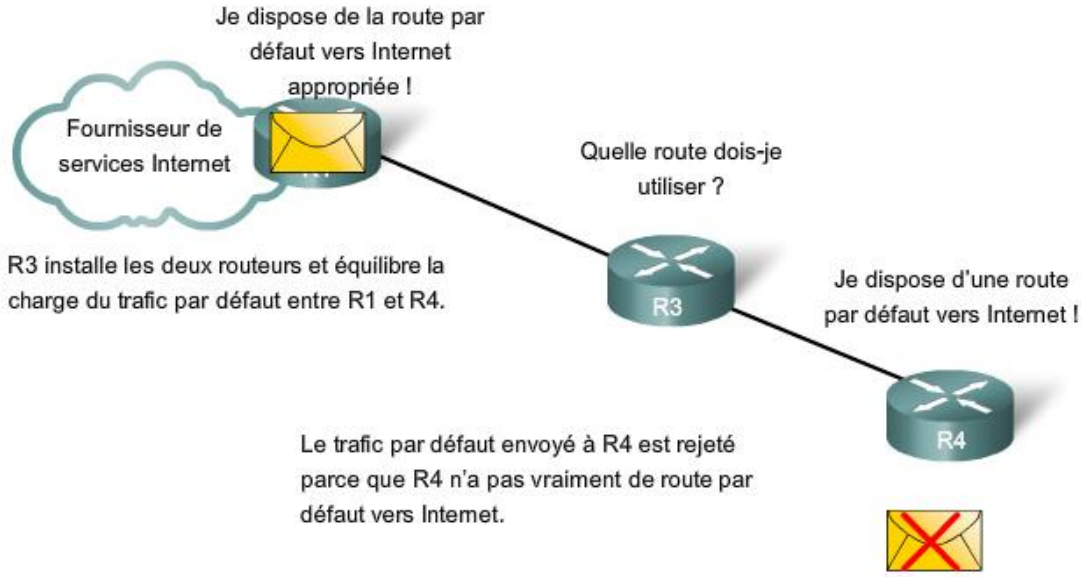


Figure III.13 : Authentification par RIPv2.

Quelle que soit la raison, il est recommandé d'authentifier les informations de routage transmises entre les routeurs. Le protocole RIPv2 peut être configuré pour authentifier les informations de routage. Ainsi, les routeurs n'acceptent que les informations de routage des autres routeurs qui ont été configurés avec le même mot de passe ou les mêmes informations d'authentification.

Remarque : l'authentification ne chiffre pas la table de routage.

CHAPITRE IV

Configuration du protocole RIP sur un réseau

IV.1 Introduction

Ce chapitre décrit la simulation du protocole de routage dynamique RIP avec le logiciel Packet Tracer.

IV.2 Le logiciel « PACKET TRACER V5.1 »

Packet Tracer est un logiciel permettant de construire un réseau physique virtuel et de simuler le comportement des protocoles sur ce réseau.

L'utilisateur construit son réseau à l'aide d''´equipements tels que des routeurs, des commutateurs ou des ordinateurs. Ces équipements sont ensuite reliés via des connexions (câbles divers, fibre optique). Une fois l'ensemble des équipements reliés, il est possible de configurer pour chacun d'entre eux, les adresses IP, les services disponibles, etc.…..

Packet Tracer fonctionne sous les systèmes d'exploitation WIN 98, XP, WIN7.
A l'ouverture du logiciel, la fenêtre de la figure IV.1 apparaît.

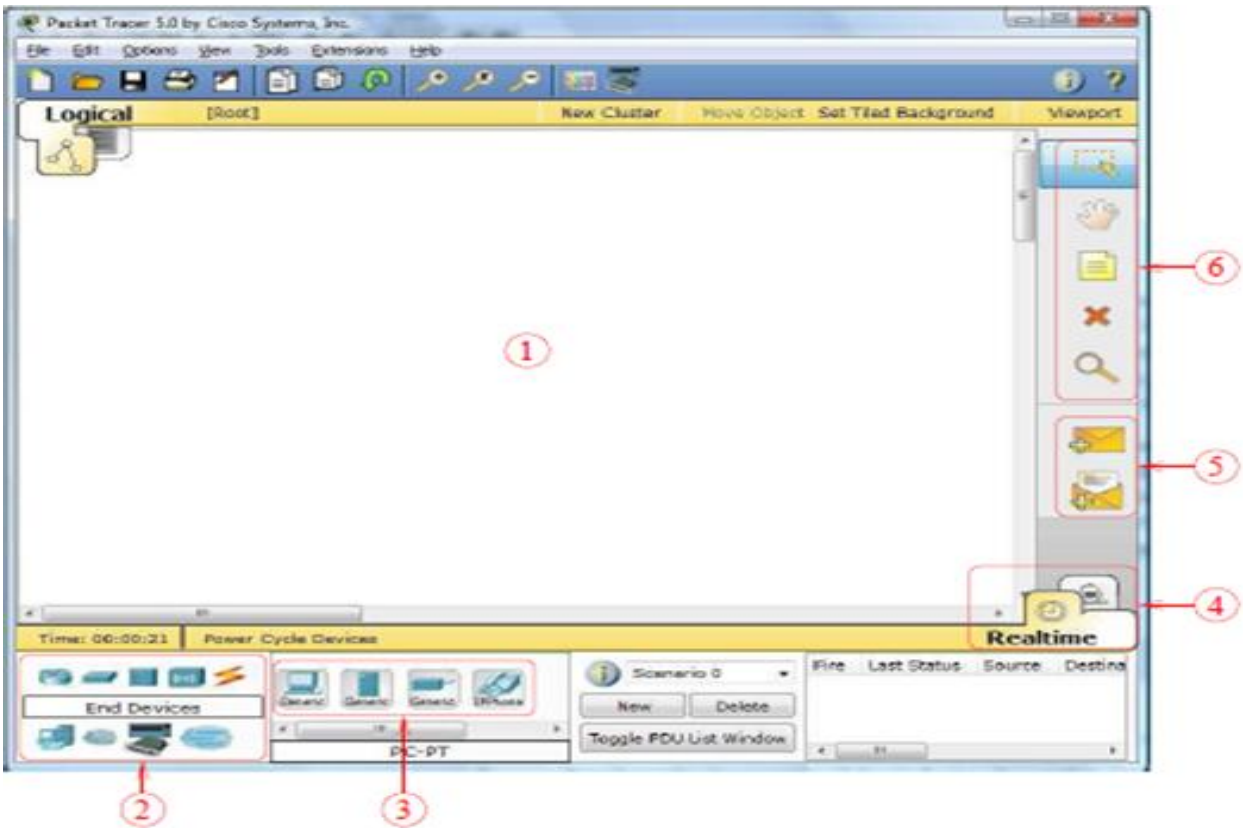


Figure IV.1: La page principale du Packet Tracer.

Un ensemble d'éléments de la barre d'outils sont visibles :

La zone (1) : est la partie dans laquelle le réseau est construit. Les équipements sont regroupés en catégories accessibles.

La zone (2) : Une fois la catégorie sélectionnée, le type d'´equipement peut être sélectionné qans La zone (3).

La zone (3) : elle contient les différents modèles d'appareils.

La zone (4) permet de passer du mode temps réel au mode simulation

La zone (5) : permet d'ajouter des indications dans le réseau

La zone (6) : contient un ensemble d'outils :

Select : permet de déplacer ou éditer des équipements

Move Layout : permet de déplacer le plan de travail

Place Note : place des notes sur le réseau

Delete : supprime un équipement ou une note

Inspect : permet d'ouvrir une fenêtre d'inspection sur un équipement (table ARP, routage)

IV.2.1 Construction d'un réseau

Pour construire un réseau, l'utilisateur doit choisir parmi huit catégories proposées par Packet Tracer : les routeurs, les switchs, les hubs, les équipements sans-fil, les équipements dits terminaux (ordinateurs, serveurs) et enfin, une connexion multi utilisateurs. Lorsqu'une catégorie est sélectionnée, l'utilisateur a le choix entre plusieurs équipements différents. Pour ajouter un équipement, il suffit de cliquer dessus.

Pour relier deux équipements, on choisit la catégorie **"Connections"** puis on clique sur la connexion désirée pour choisir le câble approprié, comme par exemple des câbles droits (Copper Straight-Through) ou des câbles croisés (Copper Cross-Over), qui sont visibles en position 1 et 2 sur la figure IV.2.

Figure IV.2 : Les équipements réseau.

Dès qu'un équipement a été ajouté, on clique dessus pour le configurer. Une nouvelle fenêtre comportant trois onglets (figure IV.3) s'ouvre :

Physical (aperçu réel de la machine et de ses modules).

Config (configuration passerelle, DNS et adresse IP).

Desktop (ligne de commande ou navigateur Web).

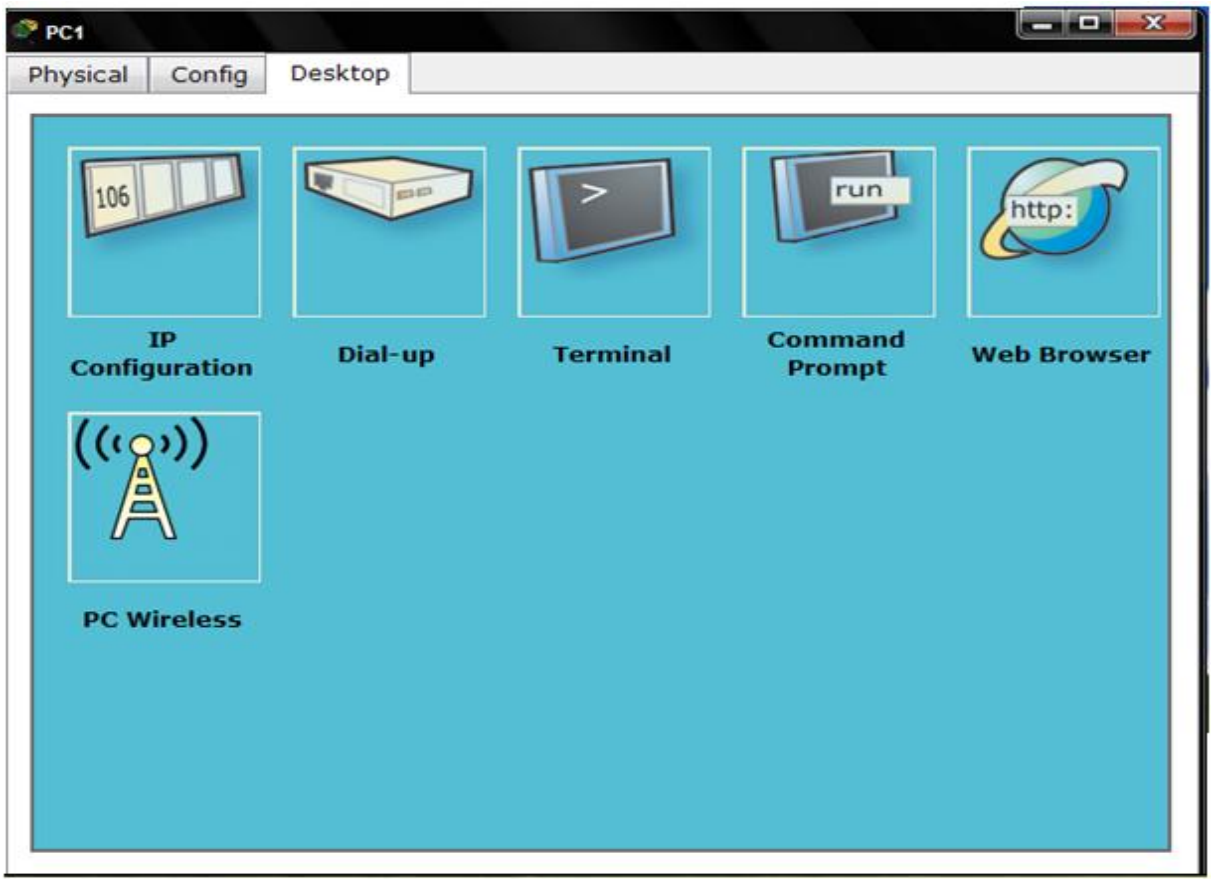


Figure IV.3 : Accès au différent mode.

Dans l'onglet Config, il est possible de configurer la passerelle par défaut, ainsi que l'adresse du serveur DNS. Il est aussi possible de configurer l'adresse IP et le masque de sous-réseau.

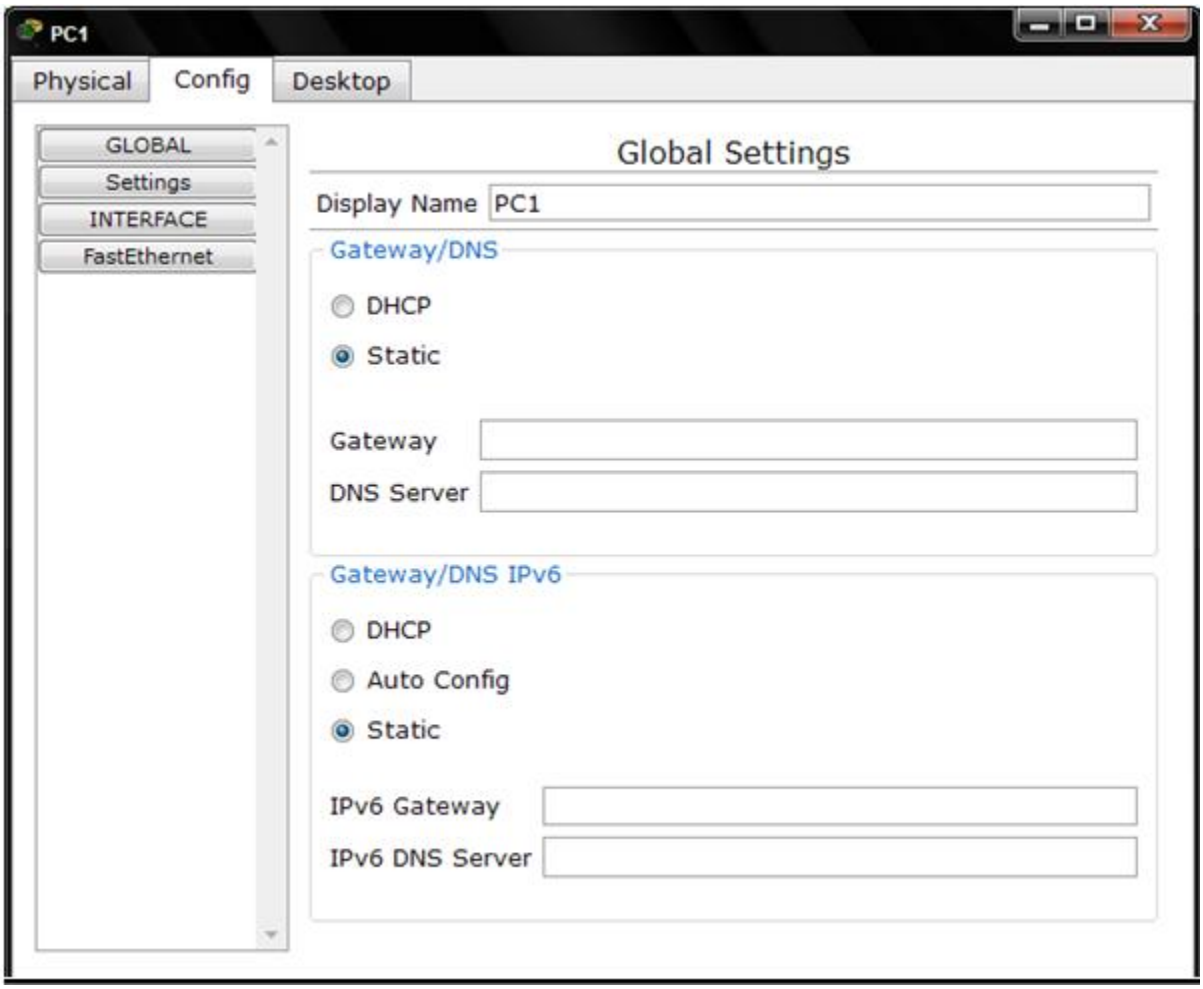


Figure IV.4 : Configuration passerelle et DNS.

IV.2.2 Le mode simulation

Une fois le réseau crée et prêt à fonctionner, on passe en mode simulation pour tester les différentes situations configurées.

On peut créer de nouveaux scénarios en cliquant sur le bouton « NEW». Pour ajouter un paquet en clique sur  et on peut ainsi voir le parcours de ce paquet dans les différentes couches du modèle OSI, ainsi que sa durée de vie.

L'arrivée d'un paquet avec succès est représentée par :  .

L'arrivée d'un paquet sans succès est représentée par :  .

Si un paquet entre dans la file d'attente il sera représenté comme suit :  .

IV.3 Présentation du réseau

La figure IV.5 suivante illustre la topologie choisie pour représenter notre réseau. Le réseau comprend trois routeurs R1, R2 et R3 connectés par deux liaisons de réseau étendu. Chaque routeur est connecté à un réseau local Ethernet différent, représenté par un commutateur et un PC. Les routeurs sont de type Cisco 1841, disposant de :

- Deux interfaces FastEthernet : FastEthernet 0/0 et FastEthernet 0/1
- Deux interfaces série : Serial 0/0/0 et Serial 0/0/1

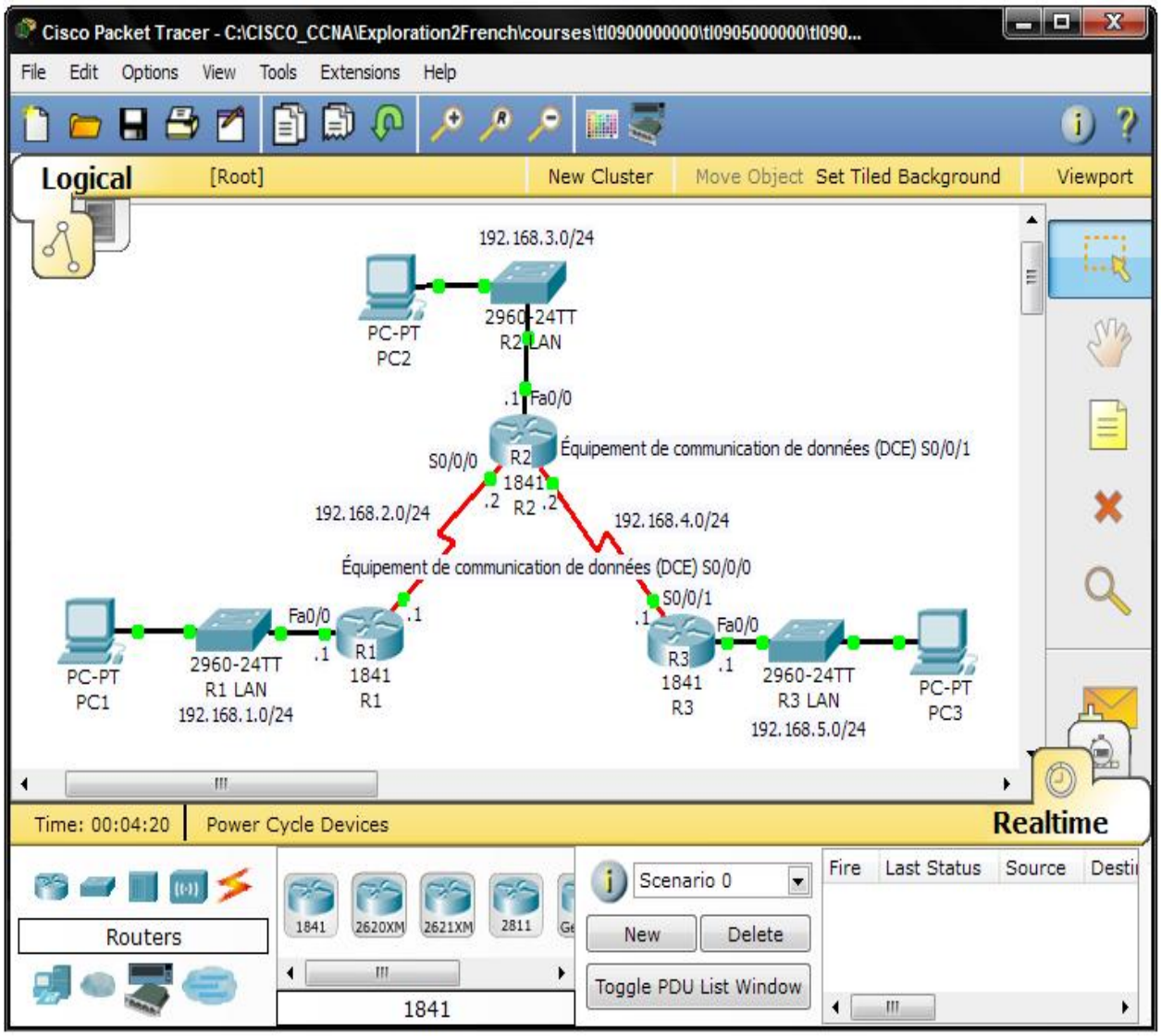


Figure IV.5 : Diagramme de topologie.

IV.4 Construction du réseau

On positionne les périphériques dans l'espace de travaille logique puis on place trois commutateurs, trois ordinateurs et trois routeurs et on définit leurs nom d'affichage pour chaque routeurs et chaque ordinateur dans l'ongle config. puis on connecte chaque périphériques avec un câble approprié de la manière suivante :

1) **Connections routeurs R aux commutateurs S**

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

2) **Connections les PCs aux commutateurs S**

On utilise un câble Ethernet droit pour relier la carte réseau du PC à l'interface FastEthernet du commutateur S.

3) **Câblage de la liaison série entre les routeurs R**

On connecte l'extrémité ETCD du câble série null à l'interface Serial du routeur R1 et l'extrémité ETTD du câble série null à l'interface Serial du routeur R2.

Ø **Information des adresses de chaque périphérique :**

Périphérique	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
R1	Fa0/0	192.168.1.1	255.255.255.0	N/D
	S0/0/0	192.168.2.1	255.255.255.0	N/D
R2	Fa0/0	192.168.3.1	255.255.255.0	N/D
	S0/0/0	192.168.2.2	255.255.255.0	N/D
	S0/0/1	192.168.4.2	255.255.255.0	N/D
R3	Fa0/0	192.168.5.1	255.255.255.0	N/D
	S0/0/1	192.168.4.1	255.255.255.0	N/D
PC1	Carte réseau	192.168.1.10	255.255.255.0	192.168.1.1
PC2	Carte réseau	192.168.3.10	255.255.255.0	192.168.3.1
PC3	Carte réseau	192.168.5.10	255.255.255.0	192.168.5.1

Tableau IV.1 : adresses des périphériques.

IV.5 Configuration d'un routeur

Ø Modes d'accès

Pour atteindre le menu de configuration d'un routeur, on utilise :

Ø Soit le port console du routeur.

Ø Soit des terminaux virtuels en émulation Telnet.

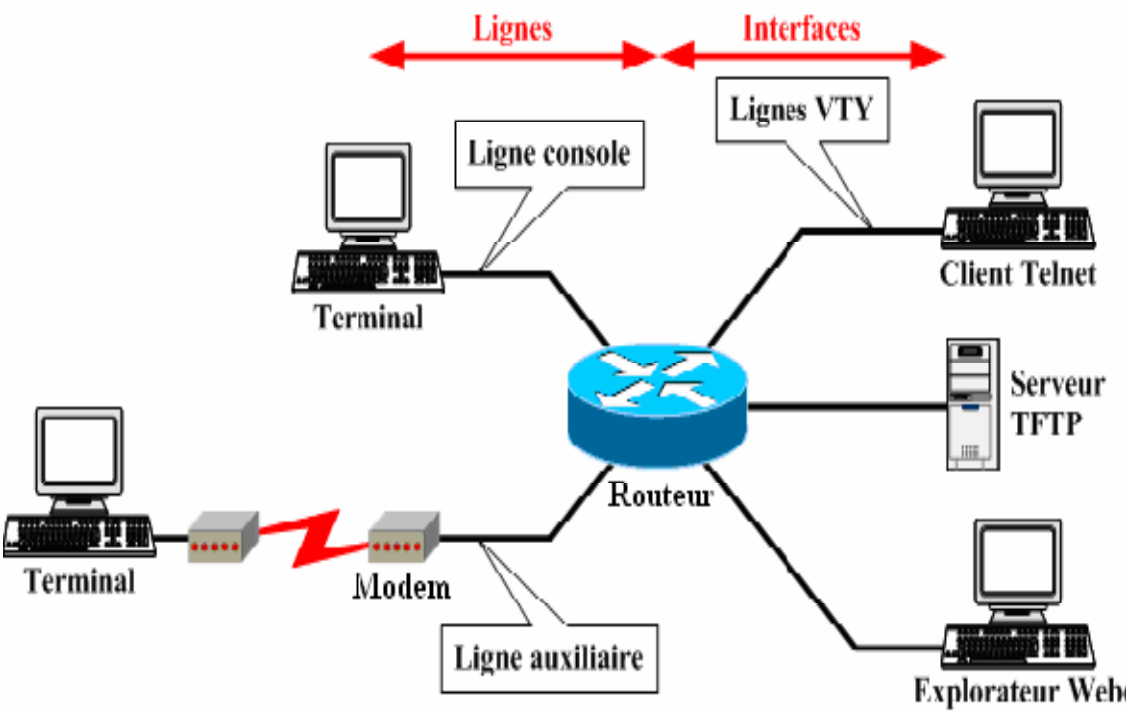


Figure IV.6 : Moyens d'accès pour la configuration.

Un routeur peut être configuré à partir des sources externes suivantes

- **Ligne console** : Accès primaire, à utiliser si aucun autre accès de configuration n'est disponible.
- **Ligne auxiliaire** : Permet de connecter un terminal distant au routeur via une ligne RTC par le biais de modems interposés.
- **Ligne(s) VTY** : Accès au routeur par l'intermédiaire de sessions Telnet (5 ou 16 lignes disponibles par routeur en fonction du modèle).
- **Explorateur Web** : Accès utilisant le serveur HTTP interne du routeur.
- **Serveur TFTP** : Import/export de fichiers de configuration.
- **Serveur FTP** : Import/export de fichiers de configuration.

La ligne console est l'accès de configuration à utiliser lorsque aucune configuration n'est chargée ou si cette dernière ne permet pas l'accès par un autre moyen (Telnet, etc.).

- **Les routeurs Cisco fonctionnent dans trois modes différents :**

Mode	Invite de commande
Utilisateur	Router >
Privilégié	Router #
Configuration globale	Router (config) #
Interface	Router (config-if) #
Ligne	Router (config-line) #
Routeur	Router (config-router) #

Tableau IV.2 : Mode de fonctionnement.

- **Le mode ligne de commande 'exec'**

Permet d'exécuter quelques commandes de base, mais sans modifier la configuration du routeur.

- **Le mode administrateur 'exec privilégié'**

Permet de modifier certains paramètres du routeur et d'accéder à des commandes complémentaires.

- **Le mode 'global configuration'**

Permet lui de modifier complètement la configuration du routeur.

Lorsque l'on se connecte à un routeur **Cisco** (via console ou via Telnet) on se retrouve dans le mode ligne de commande. Le prompt est alors > précédé du nom du routeur :

Routeur1 >

Pour passer en mode administrateur, il suffit de rentrer l'instruction **enable** et de donner s'il existe, le mode de passe pour passer dans ce mode. Le prompt change alors pour devenir #:

Routeur1 >**enable**

Routeur1#

Les deux lignes précédentes nous ont permis de passer en mode administrateur, nous allons maintenant passer en mode configuration du routeur :

Routeur1**#config terminal**

Routeur1 (config) #

Pour ressortir de ce mode de configuration, il suffit de taper la commande **<ctrl> Z** et l'on revient au mode privilégié. Pour remonter les niveaux d'accès ou pour sortir du mode privilégié, on utilise la commande **disable** ou tout simplement la commande **exit**.

1) Nommer un routeur:

Routeur1(config)**#hostname R1**

R1(config) #

2) Définir des mots de passe:

R1(config) **# enable password <password>**

R1(config) **# enable secret <password>**

R1(config)**#service password-encryption**//* Pour encrypter les mots de passe *//

Les commandes suivantes permettent de définir un mot de passe facultatif mais recommandé sur :

a) La line de Console :

R1(config) **#line console 0**

R1(config-line) **#password <password>**

R1(config-line) **#login**

b) La Line Telnet:

R1(config) **#line vty 0 4**

R1(config-line) **#password<password>**

R1(config-line) **#login**

3) Configuration des Interfaces Ethernet :

La configuration des interfaces se fait interface par interface. Pour configurer l'interface Ethernet 1/0 d'un routeur, on doit accéder à la configuration de l'interface en question à l'aide de la commande: R1(config)**#interfaceEthernet1/0**

Le résultat de cette commande est le changement de l'invite en :

R1(config-if) #

Pour spécifier l'adresse IP de cette interface ainsi que son masque de sous-réseau

R1(config-if) **#ip address <ip address> <net mask>**

Pour activer/désactiver une interface on utilise la commande :

R1(config-if) **#no shutdown/shutdown**

Sur les routeurs Cisco, la commande **no *commande paramètres*** permet de supprimer l'effet d'une commande antérieure.

IV.6 Configuration du routeur R1

Étape 1 : on définie le non du routeur puis on doit le sécurisé a l'aide du mot de passe secret, de la console et le mot de passe vty.

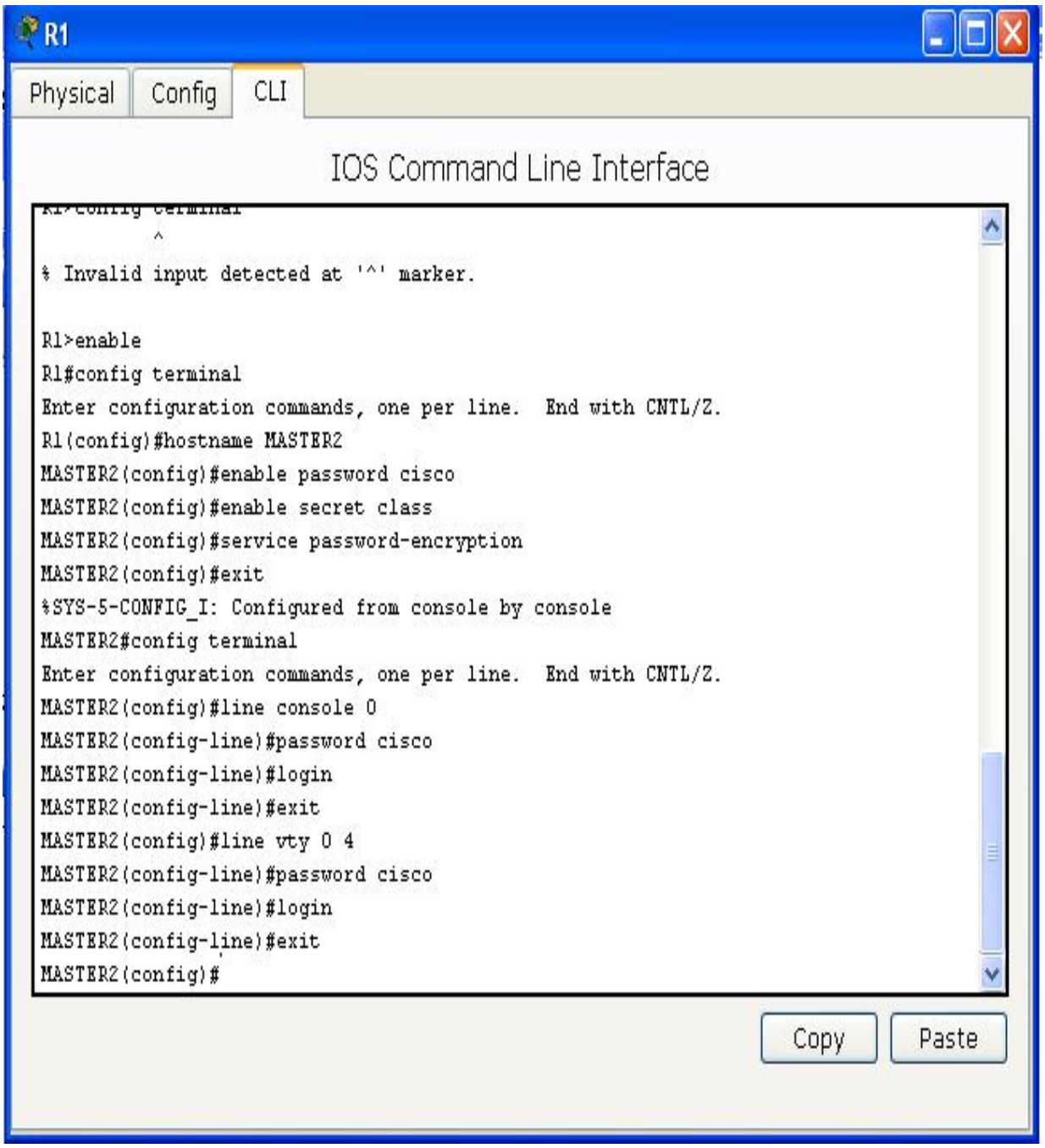


Figure IV.7 : Configuration du nom du routeur et les mots de passes.

Ø Le programme de configuration du routeur R1

R1>enable //*pour le passage en mode privilégié*//
R1#config t //*pour le passage en mode de configuration globale*//
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#hostname MASTER2 //* configuration du nom du routeur *//
MASTER2(config)#enable password cisco //* configuration du mot de passe secret *//
MASTER2(config)#enable secret class
MASTER2(config)#service password-encryption //* Pour encrypter les mots de passe *//
MASTER2(config)#exit
%SYS-5-CONFIG_I: Configured from console by console
MASTER2#config t
Enter configuration commands, one per line. End with CNTL/Z.
MASTER2(config)#line consol 0 //* configuration mot de passe sur la ligne de console *//
MASTER2(config-line)#password cisco
MASTER2(config-line)#login
MASTER2(config-line)#exit
MASTER2(config)#line vty 0 4 //* configuration mot de passe sur la ligne vty *//
MASTER2(config-line)#password cisco
MASTER2(config-line)#login
MASTER2(config-line)#exit
MASTER2(config)#^Z
%SYS-5-CONFIG_I: Configured from console by console
MASTER2#copy run start //* pour enregistrez la configuration *//
Destination filename [startup-config]?

On applique la même configuration pour les routeurs **R2** et **R3.**

Ø Resultat de la configuration

Le mode passe est demandé avant l'accès au mode priviligié pour configuré les interfaces.

Étape 2 : On configure l'interface fastEthernet0/0 et l'interface série serial0/0/0 avec les adresses IP affichés dans le Tableau VI.1 puis on les activent à l'aide de la command**e** **no shutdown**

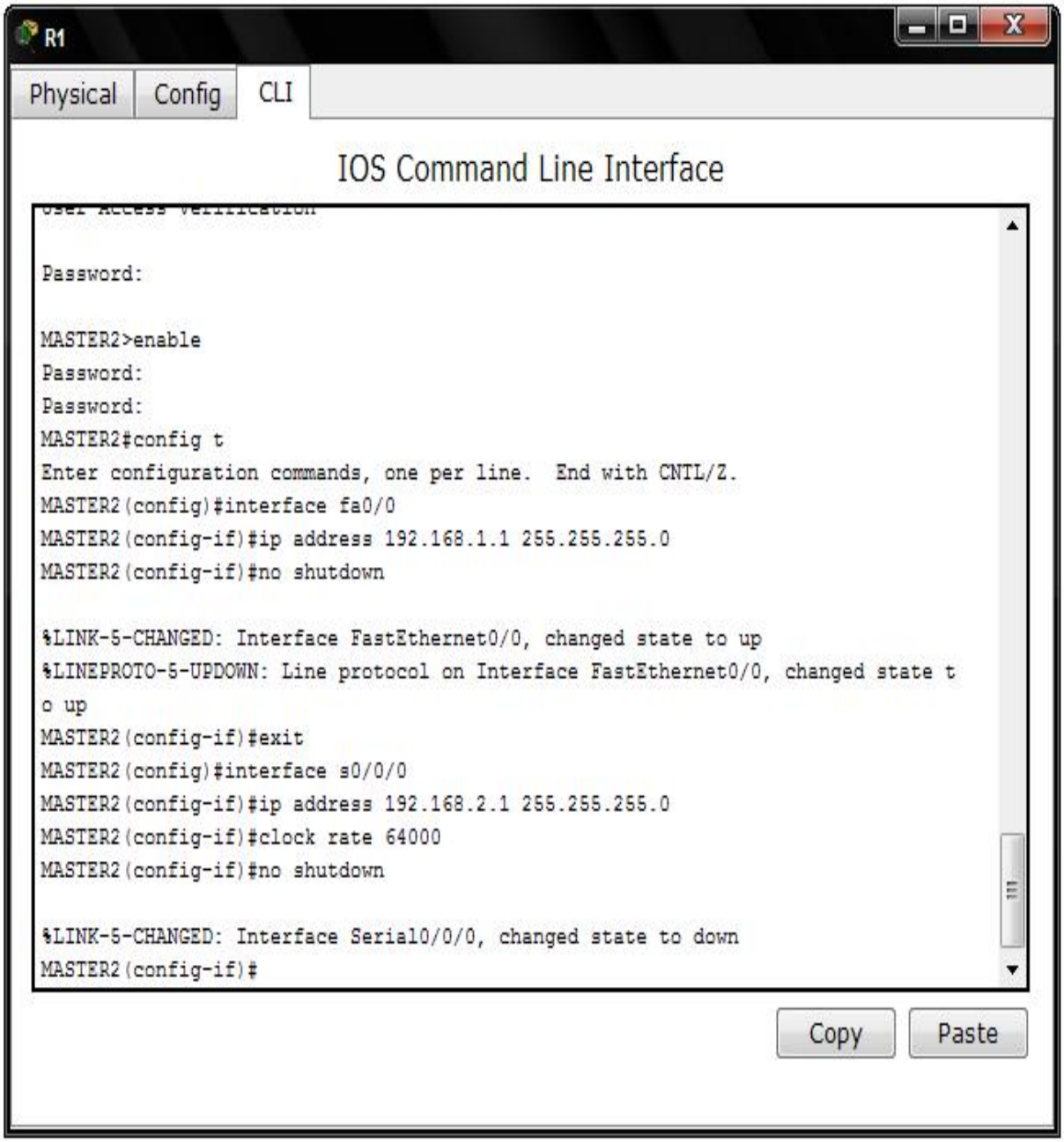


Figure IV.8 : Configuration des interfaces du routeur.

Le programme de configuration des interfaces de routeur R1

User Access Verification

Password: //*le mode passe cisco est demandé pour l'accès au mode utilisateur *//

MASTER2>enable

Password: //*le mode passe cisco et class sont demandés pour l'accès au mode privilégié *//

Password:

MASTER2#config t

Enter configuration commands, one per line. End with CNTL/Z.

MASTER2(config)#interface fa0/0 / /* pour configurer l'interface *//

MASTER2(config-if)#ip address 192.168.1.1 255.255.255.0

MASTER2(config-if)#no shutdown / /* pour activer l'interface *//

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

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

MASTER2(config-if)#exit

MASTER2(config)#interface s0/0/0

MASTER2(config-if)#ip address 192.168.2.1 255.255.255.0

MASTER2(config-if)#clock rate 64000

MASTER2(config-if)#no shutdown

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

- **Le programme de configuration des interfaces de R2**

User Access Verification

Password:

R2>enable

R2#config t

Password:

Password:

Enter configuration commands, one per line. End with CNTL/Z.

R2(config)#interface fa0/0

R2(config-if)#ip address 192.168.3.1 255.255.255.0

R2(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

R2(config-if)#exit

R2(config)#interface s0/0/0

R2(config-if)#ip address 192.168.2.2 255.255.255.0

R2(config-if)#clock rate 64000

R2(config-if)#no shutdown

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

R2(config-if)#

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

R2(config-if)#exit

R2(config)#interface s0/0/1

R2(config-if)#ip address 192.168.4.2 255.255.255.0

R2(config-if)#clock rate 64000

R2(config-if)#no shutdown

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

R2(config-if)#^Z

%SYS-5-CONFIG_I: Configured from console by console

R2#copy run start

Destination filename [startup-config]?

Building configuration...

[OK]

R2#

- **Le programme de configuration des interfaces de R3**

User Access Verification

Password:

R3>enable

Password:

Password:

R3#config t

Enter configuration commands, one per line. End with CNTL/Z.

R3(config)#interface fa0/0

R3(config-if)#ip address 192.168.5.1 255.255.255.0

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

R3(config-if)#exit

R3(config)#interface s0/0/1

R3(config-if)#ip address 192.168.4.1 255.255.255.0

R3(config-if)#clock rate 64000

R3(config-if)#no shutdown

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

R3(config-if)#

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up

R3(config-if)#exit

R3(config)#^Z

%SYS-5-CONFIG_I: Configured from console by console

R3#copy run start

Destination filename [startup-config]?

Building configuration...

[OK]

R3#

IV.7 Configuration du routage sur le réseau

a) avant de mettre on œuvre le protocole RIP sur les routeurs R1, R2 et R3**,** on exécute la commande **no router Rip** sur le router **R1** puis on sort du mode de configuration du terminal a l'aide de la commande **ctrl z,** en fin on vérifie sa table de routage a l'aide de la commande **show ip route.**

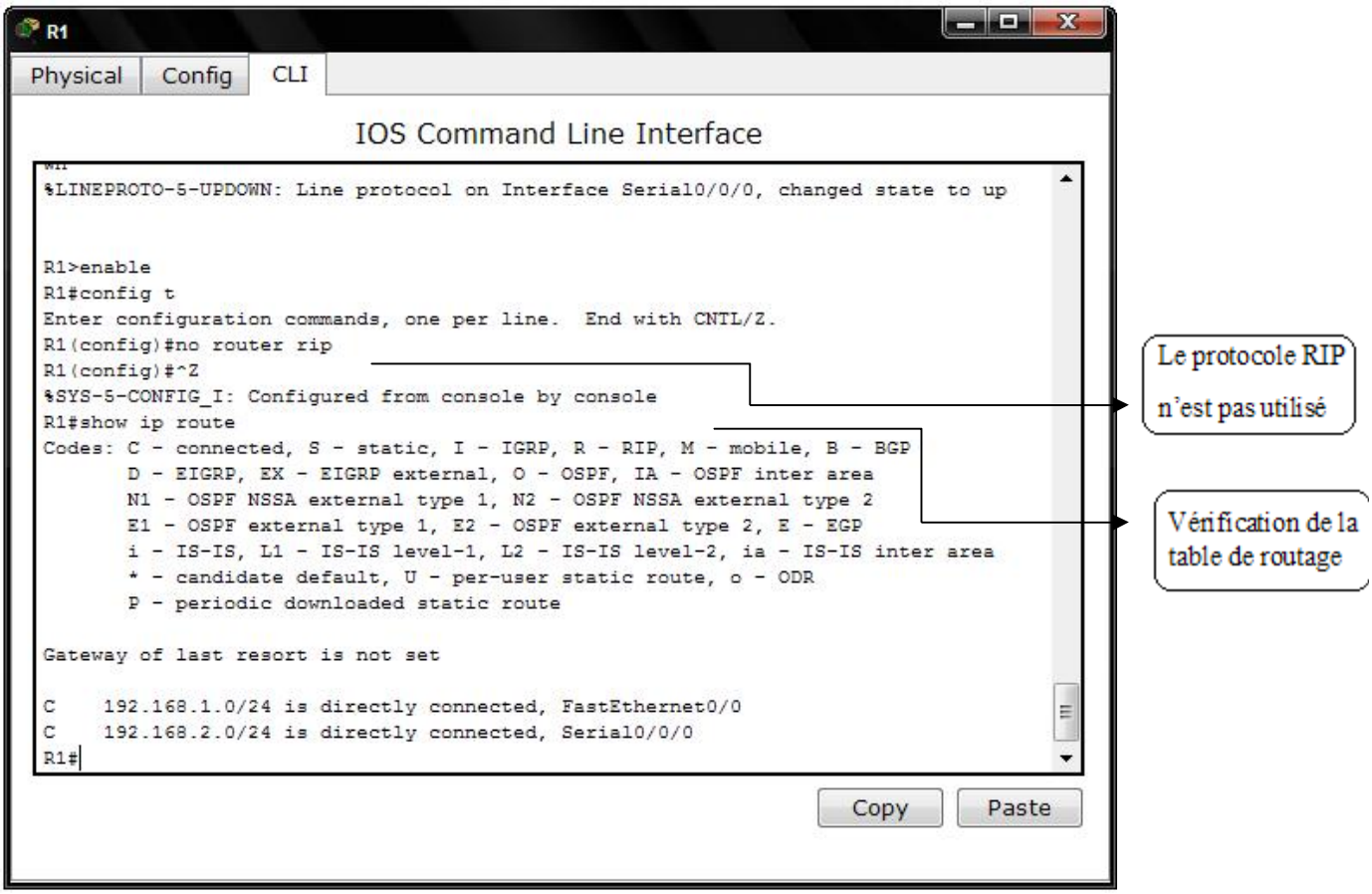


Figure IV.9 : Vérification de la table de routage de R1.

On constate qu'il ya que les réseaux directement connectées, ils sont codées par la lettre **C**:

C 192.168.1.0/24 is directly connected, FastEthernet0/0

C 192.168.2.0/24 is directly connected, Serial0/0/0

- **Resultat de la commande « show ip route » sur R2**

R2#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

C 192.168.2.0/24 is directly connected, Serial0/0/0

C 192.168.3.0/24 is directly connected, FastEthernet0/0

C 192.168.4.0/24 is directly connected, Serial0/0/1

R2#

- **Resultat de la commande « show ip route » sur R3**

R3#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

C 192.168.4.0/24 is directly connected, Serial0/0/1

C 192.168.5.0/24 is directly connected, FastEthernet0/0

R3#

Ø Vérification de la connectivité :

On Vérifie la connectivité du réseau en exécutant une requête **Ping** depuis chaque ordinateur vers les deux autres.

Exemple : du pc1 vers le pc3 dont l'adresse est 192.168.5.10

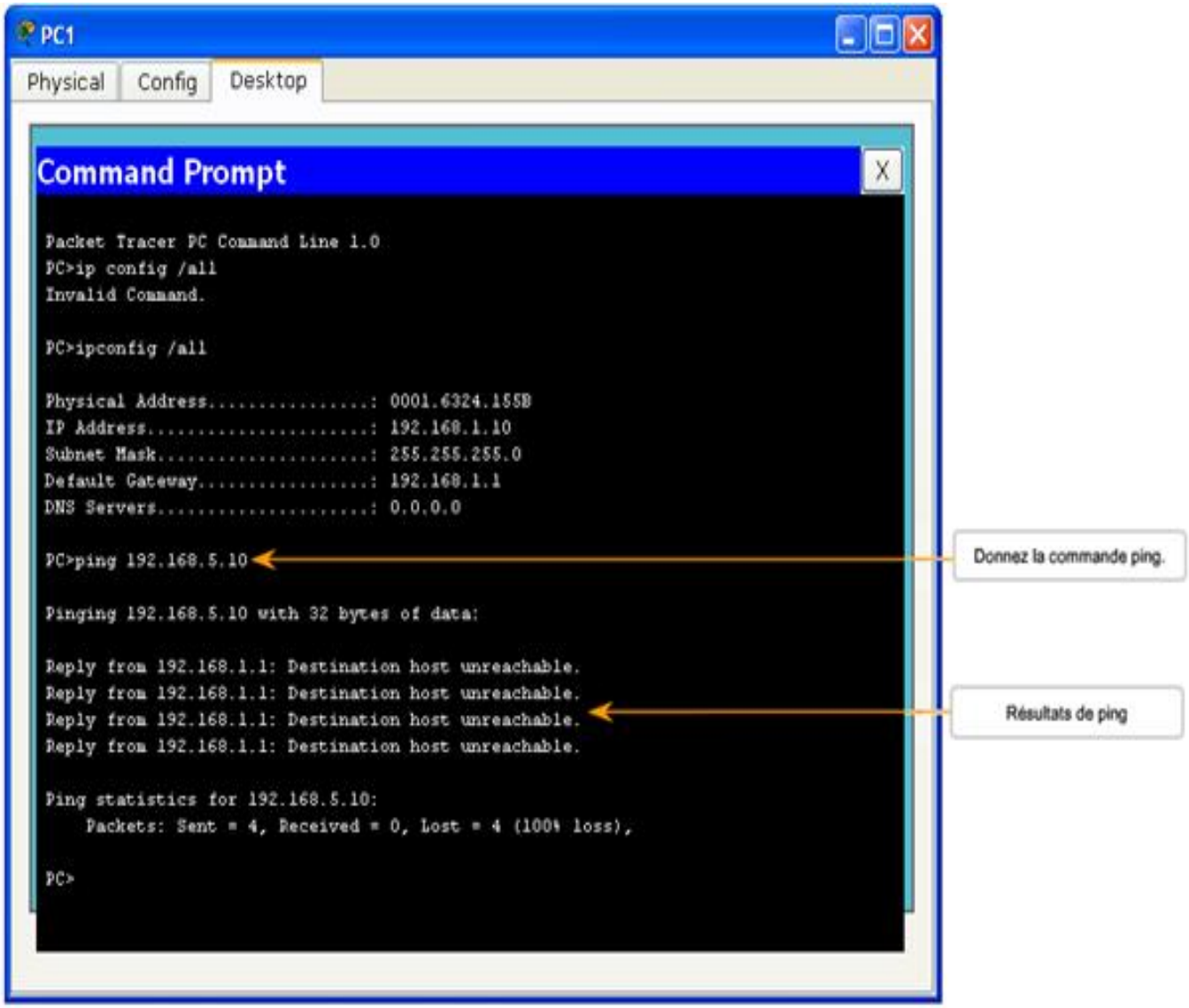


Figure IV.10 : Test avant la configuration du protocole RIP.

Les requêtes **Ping** échouent, parce que R1 ne contient pas dans sa table de routage la route qui correspond à 192.168.5.10 à savoir l'adresse IP de destination du paquet de requêtes **Ping.**, or dans la table de routage de R1 il ya que les réseaux connecté directement.

C 192.168.1.0/24 is directly connected, FastEthernet0/0

C 192.168.2.0/24 is directly connected, Serial0/0/0

Donc on doit configurer le protocole RIP pour qu'il reçoive des mises à jour sur les réseaux distants.

b) Après la configuration du protocole RIP sur les routeurs R1, R2 et R3, On passe en mode de configuration du routeur en tapant la commande **router rip.**

Dans ce mode, on doit spécifier les réseaux directement connectés au routeur afin de démarrer le processus de routage pour ces réseaux.

Deux réseaux sont directement connectés au routeur R1 : 192.168.1.0/24 et 192.168.2.0/24.

Trois réseaux sont directement connectés au routeur R2 : 192.168.2.0/24 , 192.168.3.0/24 et 192.168.4.0/24.

Deux réseaux sont directement connectés au routeur R3 : 192.168.4.0/24 et 192.168.5.0/24.

- on Configure le premier réseau à l'aide de la commande **network 192.168.1.0** et le deuxième avec la commande **network 192.168.2.0. (**Pour le routeur R1).
- on Configure le premier réseau à l'aide de la commande **network 192.168.2.0/24**, le dexième avec la commande **network 192.168.3.0/24** et le troixieme avec **network 192.168.4.0/24** . (Pour le routeur R2).
- on Configure le premier réseau à l'aide de la commande **network 192.168.4.0/24** et le deuxième avec la commande **network 192.168.5.0/24 .** (Pour le routeur R3).

Voir la figure IV.11.

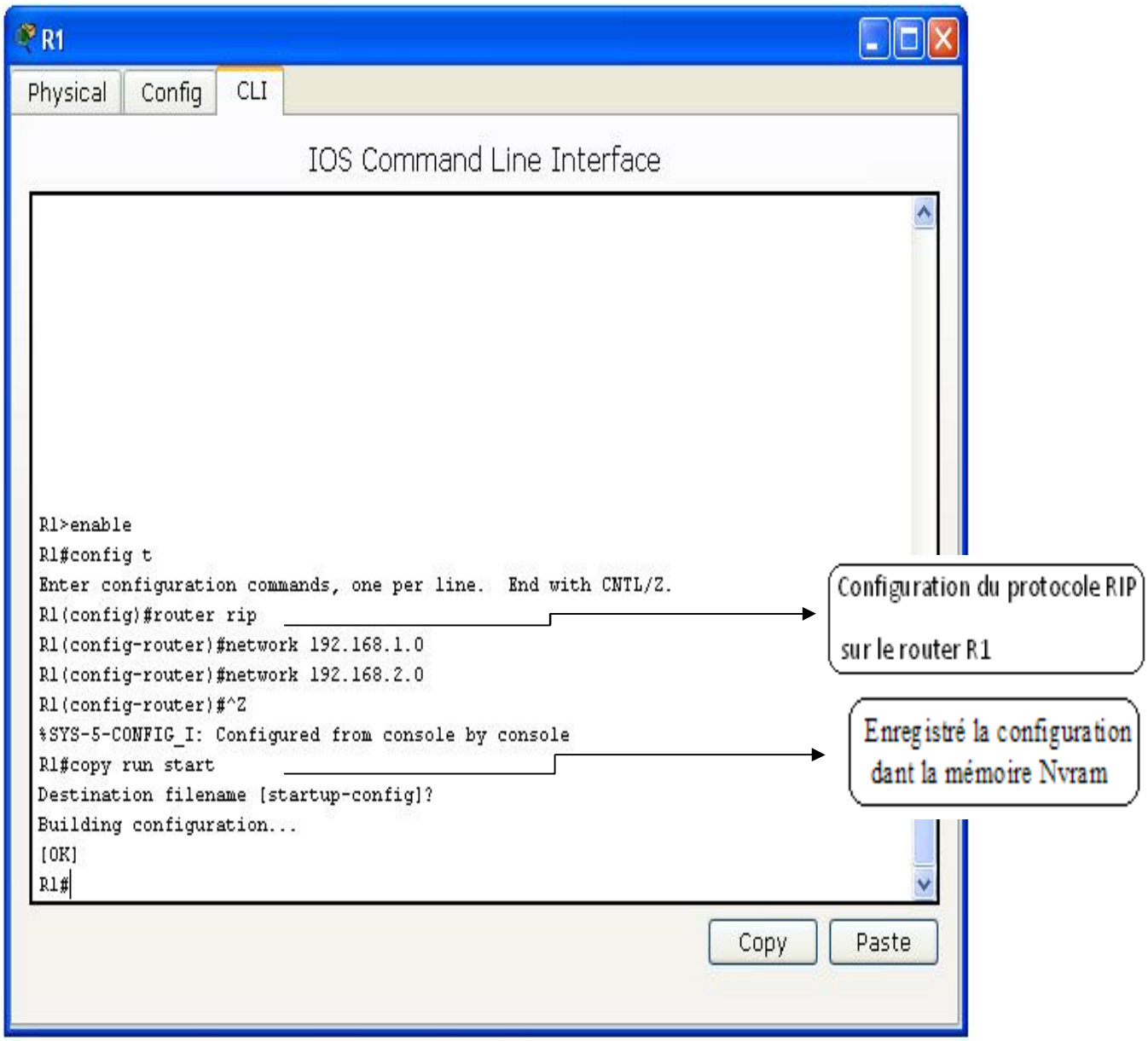


Figure IV.11 : Configuration du protocole RIP sur R1.

Ø Vérification du routage RIP sur le router R1

On a utilisé la commande **show ip route** pour vérifier la table de routage de **R1**

Résultat de la commande :

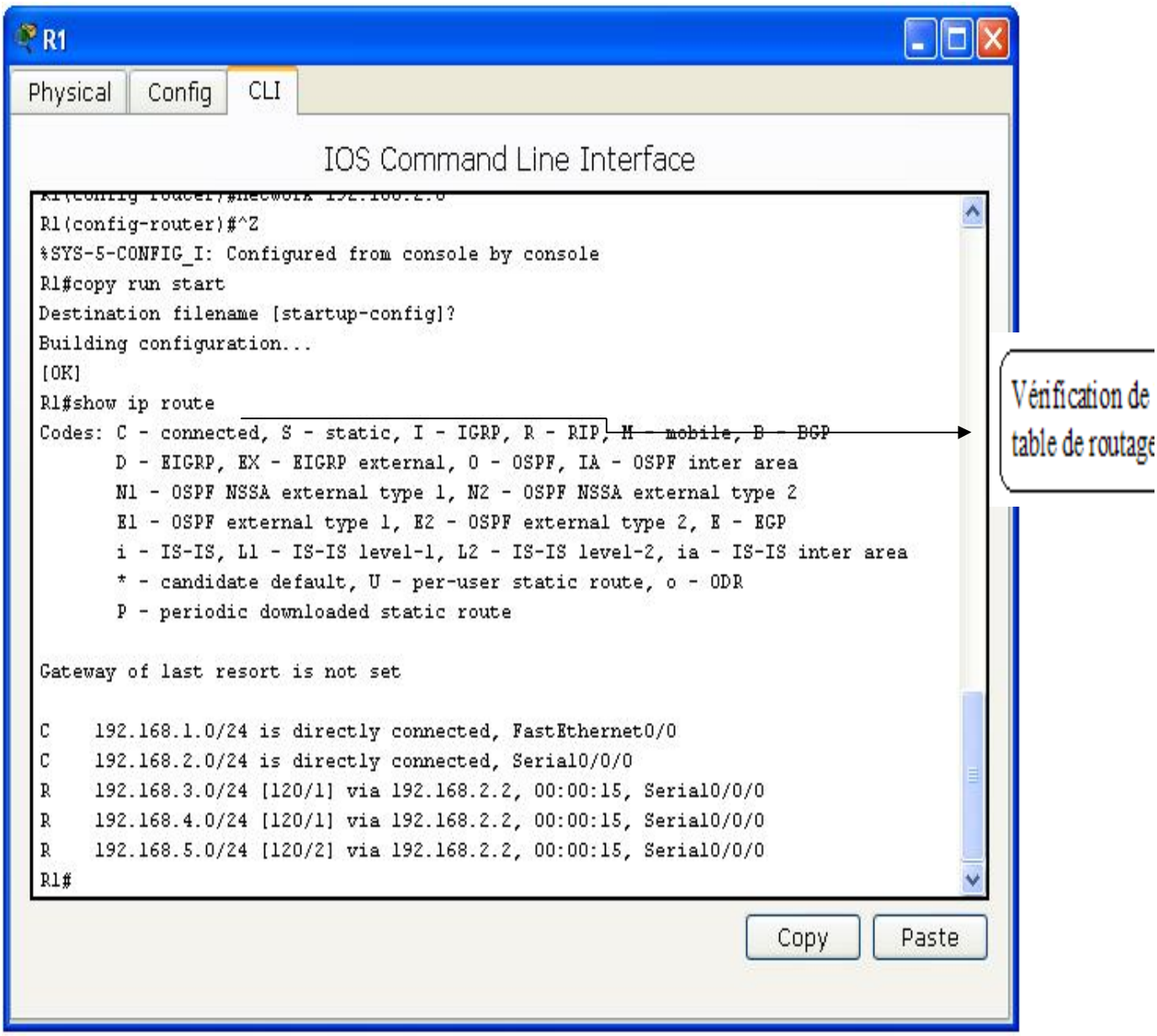


Figure IV.12 : Vérification de création des nouvelles routes sur R1.

Les routes acquises via le protocole RIP sont codées avec un **R** dans la table de routage.

- **Résultat de la commande show ip route sur R1**

R1#**show ip route**

C 192.168.1.0/24 is directly connected, FastEthernet0/0

C 192.168.2.0/24 is directly connected, Serial0/0/0

R 192.168.3.0/24 [120/1] via 192.168.2.2, 00:00:15, Serial0/0/0

R 192.168.4.0/24 [120/1] via 192.168.2.2, 00:00:15, Serial0/0/0

R 192.168.5.0/24 [120/2] via 192.168.2.2, 00:00:15, Serial0/0/0

R1#

- **Résultat de la commande show ip route sur R2**

R2#**show ip route**

R 192.168.1.0/24 [120/1] via 192.168.2.1, 00:00:22, Serial0/0/0

C 192.168.2.0/24 is directly connected, Serial0/0/0

C 192.168.3.0/24 is directly connected, FastEthernet0/0

C 192.168.4.0/24 is directly connected, Serial0/0/1

R 192.168.5.0/24 [120/1] via 192.168.4.1, 00:00:23, Serial0/0/1

R2#

- **Résultat de la commande show ip route sur R3**

R3#**show ip route**

R 192.168.1.0/24 [120/2] via 192.168.4.2, 00:00:18, Serial0/0/1

R 192.168.2.0/24 [120/1] via 192.168.4.2, 00:00:18, Serial0/0/1

R 192.168.3.0/24 [120/1] via 192.168.4.2, 00:00:18, Serial0/0/1

C 192.168.4.0/24 is directly connected, Serial0/0/1

C 192.168.5.0/24 is directly connected, FastEthernet0/0

R3#

On constate que chaque routeurs contient tous les réseaux dans sa table de routage et cela grâce au protocole RIP qui a acquis des nouvelles routes qui sont codés par la lettre R

Ø Vérification de la connectivité

On vérifie la connectivité du réseau en exécutant une requête **Ping** depuis chaque ordinateur vers les deux autres.

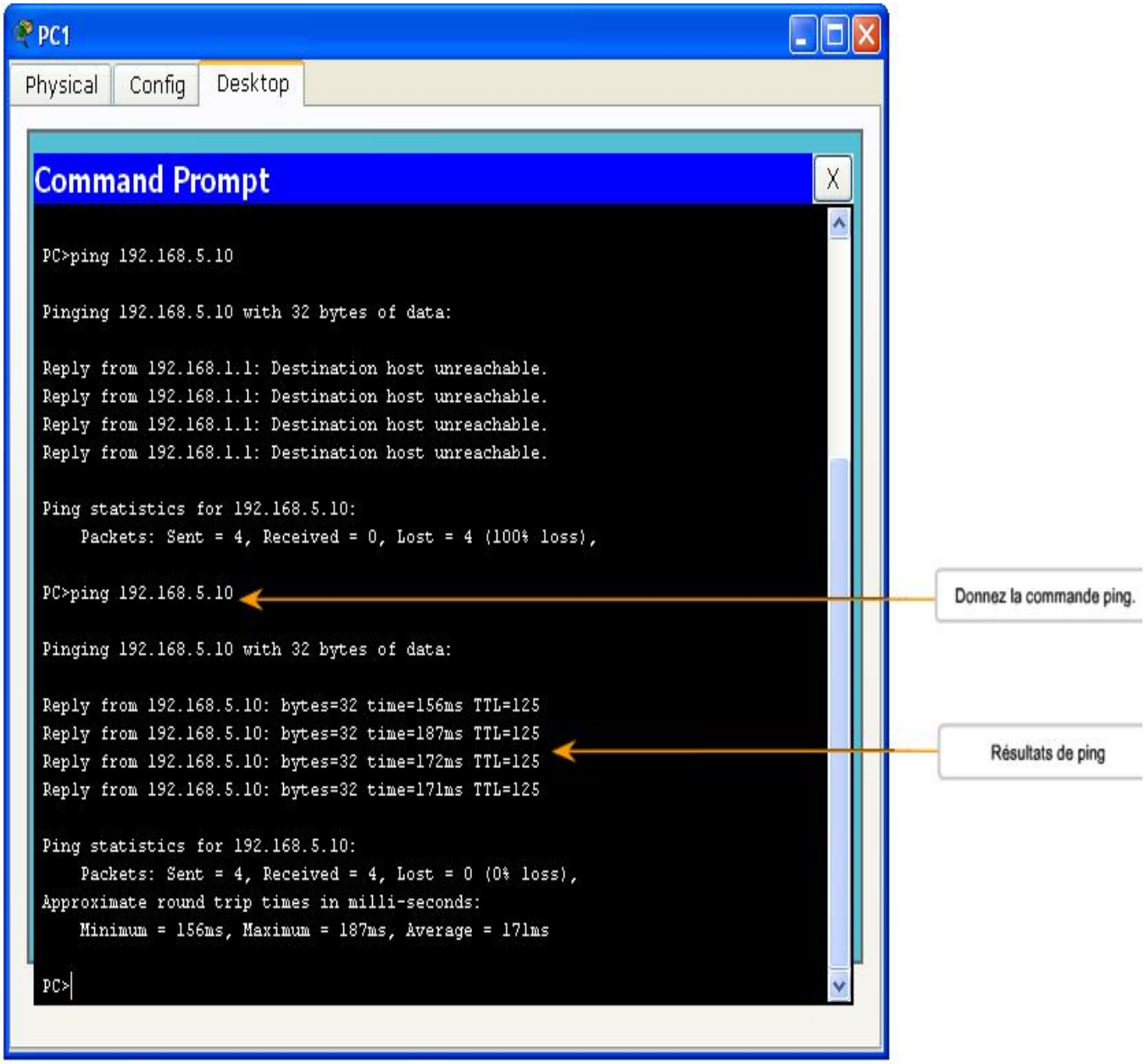


Figure IV.13 : Teste après configuration du protocole RIP.

En constate que la requête Ping aboutie parce que le routeur R1 contient dans sa table de routage une route qui correspond a 192.168.5.10 à savoir l'adresse IP de destination du paquet de requêtes ping.et cela grâce au protocole de routage dynamique RIP qui a découvert automatiquement des réseaux distants via d'autres routeurs.

IV.8 Conclusion

D'après les résultats de la simulation obtenus, on constate que Le protocole RIP constitue un excellent moyen pour aborder la problématique du routage dynamique. Il a permis de bien administré le réseau et d'acquérir des informations de manière dynamique sur les réseaux distants, il est aussi pratique car avec très peu de commandes de configuration on arrive à une solution qui fonctionne correctement et qui est même capable de prendre en compte automatiquement des modifications de la topologie.

.

Conclusion générale

Conclusion générale

Le développement technologique dans le monde informatique, en particulier le réseau informatique nous a amené à choisir un thème sur le protocole de routage dynamique à vecteur de distance.

Ce travail nous a permis d'acquérir beaucoup de connaissance dans le domaine des réseaux. Nous avons pu comprendre, l'interconnexion entre couches dans le modèle OSI et celui du TCP/IP, les différents protocoles, le routage statique et dynamique, le fonctionnement des routeurs cisco.la configuration du routeur ainsi que les différentes commandes ; et nous avons utilisé le logiciel de simulation Packet Tracer V 5.1 pour mettre en application le protocole de routage dynamique à vecteur de distance RIP.

Vu les inconvénients que présentent les réseaux filaire tel que les problèmes de câblage qui sont parfois très encombrants et trop ennuyeux à réaliser, ajouté a cela un autre problème est celui posé par l'explosion de la taille des tables de routage dans l'Internet. le WIFI peut être la meilleur technologie que l'on puisse utiliser pour résoudre les problèmes de câblage et la nécessité de mettre on œuvre de nouveau protocole de routage à savoir RIPng (RIP next generation) qui est le premier protocole de routage dynamique propose pour Ipv6. Il est identique au protocole RIPng dans Ipv4, seule la fonction d'authentification car elle est inutile puisque RIPng peut s'appuyer sur les mécanismes de sécurité disponibles en Ipv6.

Enfin, nous espérons avoir été à la hauteur du travail qui nous a été confié.

Bibliographie

Bibliographie

I. Ouvrages

- **[Rou 05]** A. Roux, Cisco Entrainez-vous à configurer routeurs et commutateurs, Ed ENI ,2005.
- **[Par 05]** B.Parkhurst, Les Routeurs, Ed. CampusPress, 2005.
- **[Par 05]** D. Paret, Réseaux multiplexés pour systèmes embarqués Ed .Dunod, 2005.
- **[Dro 09]** D.Dromard, D .Seret, Architectures des Réseaux, Ed.PEARSON, 2009.
- **[Puj 02]** G. Pujolle, Initiation aux réseaux, Ed. EYROLLES, 2002.
- **[Puj 04]** G. Pujolle, Réseaux et Télécoms, Ed. EYROLLES, 2004.
- **[Rud 05]** I.Rudenko, configuration IP des routeurs Cisco, Ed .EYROLLES, 2005.
- **[Dor 05]** J.Dordoigne, Réseaux Locaux et Etendus Notions Fondamentales, Ed ENI.2005.
- **[Mon 08]** J.Montagnier, Réseaux d'entreprise par la pratique, Ed EYROLLES, 2008.
- **[Hav 05]** J.Havez, Routage Statique, Dynamique avec Ripv1, Ripv2 et OSPF, Ed UTBM ,2005.

II. Thèses

- **[Sha 10]** R. Sharrock, Gestion autonomique de performance, d'énergie et de qualité de service. Application aux réseaux filaires, réseaux de capteurs et grilles de calcul, Mémoire de doctorat .INP Toulouse ,2010.
- **[Ham 07]** M.Hammar, Interactions entre le protocole MAC et les protocoles de couche hautes (routage et transport) pour l'optimisation et la performance dans un MANET, Mémoire de Magister, Dpt Informatique, UMMTO, 2007.
- **[Kab, Aid 07]** N.kabeche, N.Aid, Interconnexion du réseau TCP/IP a base des routeurs CISCO, Mémoire de fin d'étude Ingénieur, Dpt Electronique, UMMTO ,2007.
- [**Oul, Bou 05**] M.Oulcd, A.Bouklouch, Etude des protocoles pour Réseaux Informatiques, Mémoire de fin d'étude Ingénieur, Dpt Electronique, ITO, 2005.

Ø **[Oum, Dou 05]** S. Oumarou, Y.Doutoum, Interface de gestion SNMP d'un réseau local, Mémoire de fin d'étude Ingénieur, Dpt Electronique, ITO, 2005.

III. Sites web

Ø http://kheops.unice.fr/deneire/cours.pdf
Ø http://www.cisco.fr
Ø http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_configuration_guide_book09186a0080172852.html :
Ø http://www.siliconvalleyccie.com/cisco-hn/dsl-pix.htm
Ø http://www.zebra.org/
Ø http://perso.ens-lyon.fr/eric.fleury/CPS/ART/slides/M1_ART_02-routage.pdf
Ø http://memoireonline.free.fr/
Ø http://www.commentçamarche.fr
Ø www.Supinfo.com
Ø http://www.supinfo-projects.com/fr/2003/ip_networks
Ø http://www.springer.fr
Ø http://www.hsc.fr/ressources/cours/tcpip/html