الجمهوريــة الجزائريــة الديمقراطيــة الشعبيــة

République Algérienne Démocratique et Populaire

وزارة التعليم العالي والبحث العلمي

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université de Relizane | **جامعة غليزان**

جامعة غليزان
RELIZANE UNIVERSITY

Faculté des Sciences et Technologies

Département d'Informatique

SUPPORT DE COURS

Protocoles de communication : conception et optimisation des réseaux

Pour les étudiants de la 1ère année Master specialité:

Réseaux et Systèmes Distribués

Etabli par :

Dr. Oussama DERNI

oussama.derni@univ-relizane.dz

Année universitaire 2023/2024

Avant-propos

Ce document est un support du cours pour les enseignements du module protocoles de communication. Il a pour objective d'introduire aux étudiants les compétences nécessaires dans la branche de réseaux et protocoles de communication, et d'améliorer leurs compétences dans le domaine de conception et optimisation des réseaux.

Ce cours est adressé aux étudiants de la 1ère année master en informatique, spécialité « Réseaux et Systèmes Distribués ». Il offre les notions de base sur les différentes architectures des réseaux. Puis il discute les principaux protocoles TCP/IP, ainsi que les aspects liés au routage. Ensuite, divers types de routage sont exposés tel que le routage unicast et multicast. En outre le cours présent des notions fondamentales en réseau tel que l'adressage, subnetting et supernetting.

Ce cours est organisé en six chapitres comme suit :

Chapitre 1 : Architecture des réseaux

Dans ce chapitre, nous examinons les dispositions structurelles et logiques d'un réseau. Nous présentons également les différentes couches du modèle OSI, qui sépare les tâches du réseau en sept couches logiques, de l'abstraction la plus basse à la plus élevée.

Chapitre 2 : Protocoles TCP/IP

Ce chapitre introduit le côté logiciel de la mise en réseau. Nous abordons les détails sur le modèle TCP/IP qui est similaire du modèle OSI. Nous fournissons les parties fondamentales du modèle TCP/IP, en examinant les différents protocoles TCP/IP.

Chapitre 3 : Introduction aux principaux aspects liés au routage

Ce chapitre explique comment fonctionnent les routeurs, puis il examine les différentes métriques et coûts de routage. Il présente les divers schémas de routage et ses diversités.

Chapitre 4 : Routage Unicast et Multicast

Dans ce chapitre nous allons concentrer sur les schémas de routage unicast et multicast, en discutant les plus connus protocoles de chacun de ses schémas.

Chapitre 5 : Internet : adressage, subnetting et supernetting (CIDR)

Dans ce chapitre, nous centralisons sur la couche internet du model TCP/IP. Ce chapitre présente les notions fondamentales tel que l'adressage (IPv4, IPv6), le subnetting et le supernetting.

Chapitre 6 : Les techniques modernes de routage

Ce chapitre examine les différentes techniques de routage et les divers classements des protocoles. Il soulève le couvercle sur le protocole BGP qui est le protocole de routage pour Internet.

TABLE DES MATIERES

LISTE DES FIGURES

LISTE DES TABLEAUX

LISTE DES ABREVIATIONS

Address Resolution Protocol
ARP....20
Autonomous Systems
AS....89
Border Gateway Protocol
BGP....89
Carrier Sense Multiple Access/Collision Avoidance
CSMA/CA....20
Carrier Sense Multiple Access/Collision Detection
CSMA/CD....19
Classless Inter-Domain Routing
CIDR....76
Domain Name System
DNS....34
Dynamic Host Configuration Protocol
DHCP....35
Enhanced Interior Gateway Routing Protocol
EIGRP....52
exterior gateway protocols
EGP....47
File Transfer Protocol
FTP....37
HyperText Transfer Protocol
HTTP....32
Institute of Electrical and Electronics Engineers
IEEE....18
interior gateway protocols
IGP....47
Interior Gateway Routing Protocol
IGRP....51
Internet Control Message Protocol
ICMP....23
Internet Engineering Task Force
IETF....81
Internet Group Management Protocol
IGMP....57
Internet Protocol
IP....21
Link State Advertisements
LSA....52
Local Area Network
LAN....8
Media Access Control
MAC....14
Metropolitan Area Network
MAN....9
Network Address Translation
NAT....79
Open Shortest Path First
OSPF....52
Open Systems Interconnection
OSI....1
Peer-To-Peer
P2P....32
Personal Area Network
PAN....8
Port Address Translation
PAT....80
Protocol Independent Multicast
PIM....60
Requests For Comments
RFC....17
Routing Information Protocol
RIP....48
Simple Mail Transfer Protocol
SMTP....36
Synchronize Sequence Number
SYN....28
Terminal Network
Telnet....38
Time To Live
TTL....23
Transmission Control Protocol
TCP....24
Transport Layer Security
TLS....16
Type of Service
TOS....23
User Datagram Protocol
UDP....24
Variable-length subnet mask
VLSM....75
Wide Area Network
WAN....9

Chapitre 1 : Architecture des réseaux

1.1. Introduction

Un réseau est un ensemble des entités interconnecté entre eux à l'aide d'une infrastructure filaire ou radioélectrique, qui nous permet de transmettre des données, partage des ressources, et de communiquer à travers le globe.

L'architecture du réseau fait référence à la disposition structurelle et logique d'un réseau. Il décrit comment les périphériques réseau sont connectés et les règles qui régissent le transfert de données entre eux. L'architecture réseaux diffère et dépend de la taille du réseau ainsi que l'objectif. La plupart des architectures de réseau adoptent le modèle OSI (*Open Systems Interconnection*). Ce modèle conceptuel sépare les tâches du réseau en sept couches logiques, de l'abstraction la plus basse à la plus élevée.

1.2. Définition

L'architecture réseau fait référence à la manière dont les périphériques et services réseau sont structurés pour répondre aux besoins de connectivité des périphériques clients.

- Les périphériques réseau comprennent généralement des commutateurs et des routeurs.
- Les types de services incluent DHCP et DNS.
- Les appareils clients comprennent les appareils des utilisateurs finaux et les serveurs

1.3. Composants du réseau informatique

Les réseaux informatiques partagent des dispositifs, des fonctions et des caractéristiques communs, notamment des serveurs, des clients, des supports de transmission, des données partagées, des imprimantes partagées et d'autres ressources matérielles et logicielles, une carte d'interface réseau, un système d'exploitation local et le système d'exploitation réseau.

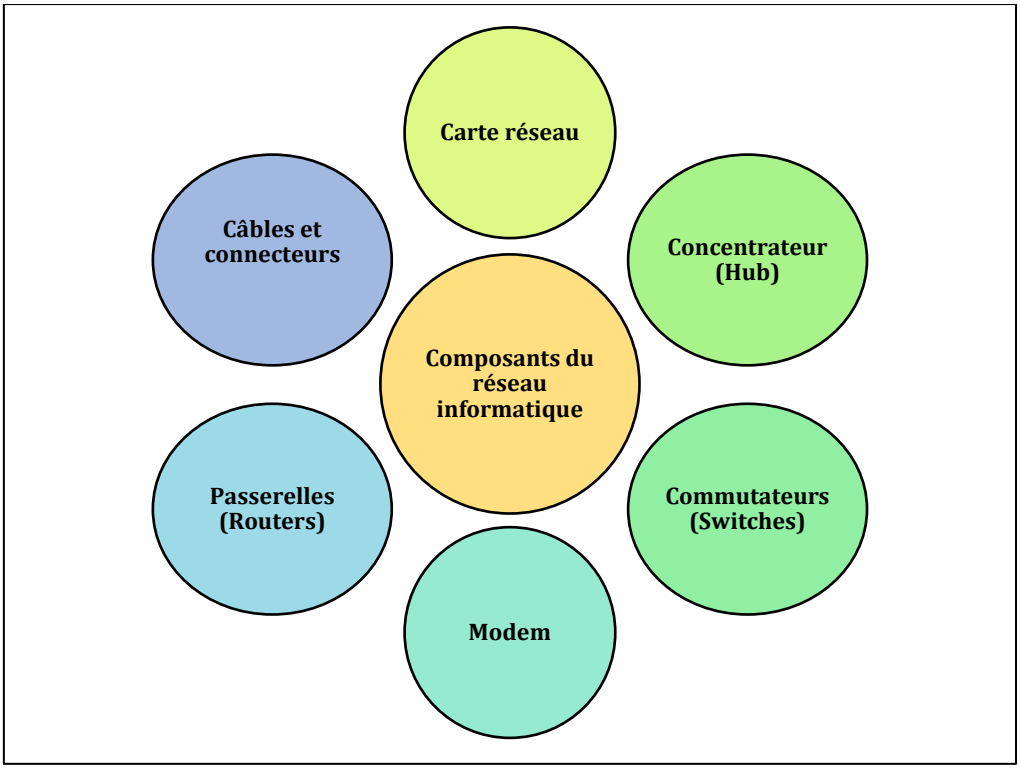


Figure 1.1. Les composants du réseau informatique

1.3.1. Câbles et connecteurs

Pour connecter deux ou plusieurs ordinateurs ou périphériques réseau dans un réseau, des câbles réseau sont utilisés. Il existe trois types de câbles réseau ; coaxial, paire torsadée et fibre optique.

1.3.1.1. Câble coaxial

Le câble coaxial contient un fil conducteur central en cuivre entouré d'un isolant matériau, qui, à son tour, est entouré d'un blindage métallique tressé. (Voir la Figure 1.2)

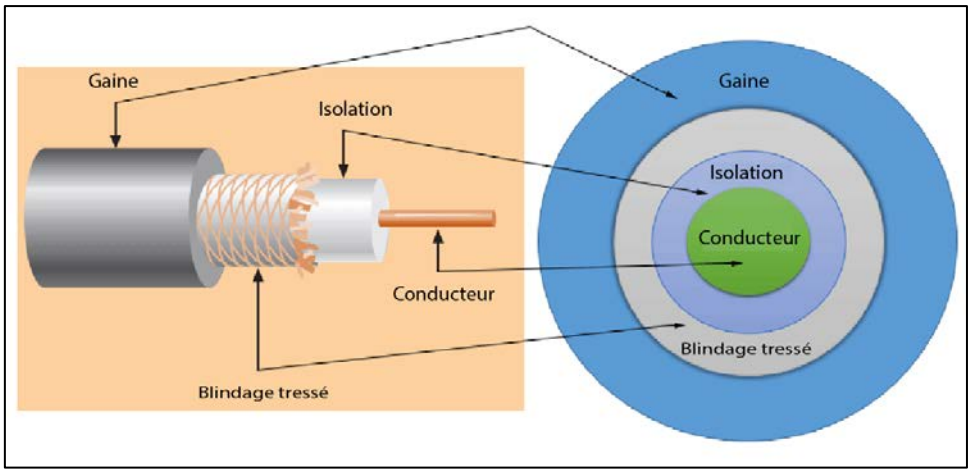


Figure 1.2. Les parties du câble coaxial

Figure 1.3. Le connecteur utilisé en terminaison de câble coaxial

- **Gaine** : C'est la couche externe du câble coaxial. Elle protège le câble des dommages physiques.
- **Blindage tressé** : Ce blindage protège les signaux des interférences externes et du bruit. Ce bouclier est construit à partir du même métal qui est utilisé pour construire le noyau.
- **Isolation :** L'isolation protège le noyau. Il maintient également le noyau séparé du blindage tressé. Étant donné que le noyau et le blindage tressé utilisent le même métal, sans cette couche, ils se toucheront et créeront un court-circuit dans le fil.
- **Conducteur** : Le conducteur transporte des signaux électromagnétiques. Basé sur le conducteur, un câble coaxial peut être classé en deux types ; câble coaxial unipolaire et câble coaxial multipolaire.

1.3.1.2. Paire torsadée

Le type de câblage le plus couramment utilisé dans les réseaux consiste en des paires torsadées de câbles, regroupés dans une veste commune. Chaque paire du câble fonctionne en équipe soit transmettre ou recevoir des données. Utiliser une paire de fils torsadés plutôt qu'un seul fil pour envoyer un signal réduit un type spécifique d'interférence, appelée diaphonie. Plus il y a de torsions par pied, plus moins de diaphonie. Deux types de câblage à paires torsadées sont fabriqués : blindé et non blindé (voir la Figure 1.4)

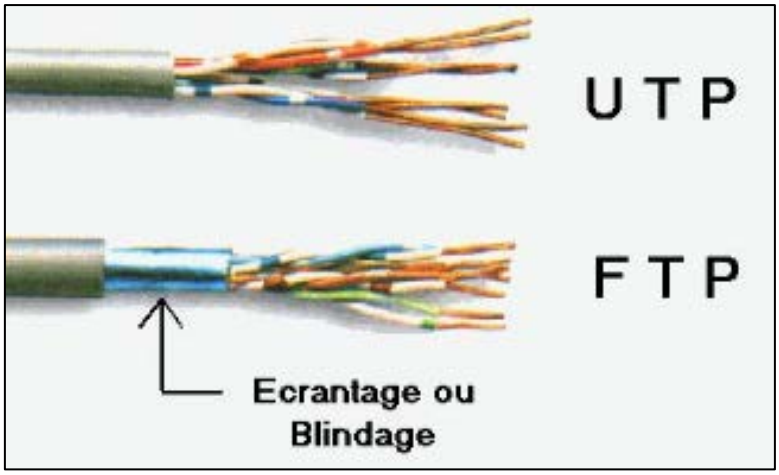


Figure 1.4. Les deux types du câble à paire torsadée

Figure 1.5. RJ45

1.3.1.3. Fibre optique

Le câble à fibre optique transmet la lumière plutôt que l'électricité, ce qui le rend attrayant pour les zones à forte interférence électromagnétique et les transmissions longue distance. Le câble à fibre optique a quatre composants : la fibre de verre elle-même (le noyau) ; le revêtement, qui est la partie qui fait réfléchir la lumière dans la fibre ; matériau tampon pour donner de la force ; et la gaine isolante (voir la Figure 1.6).

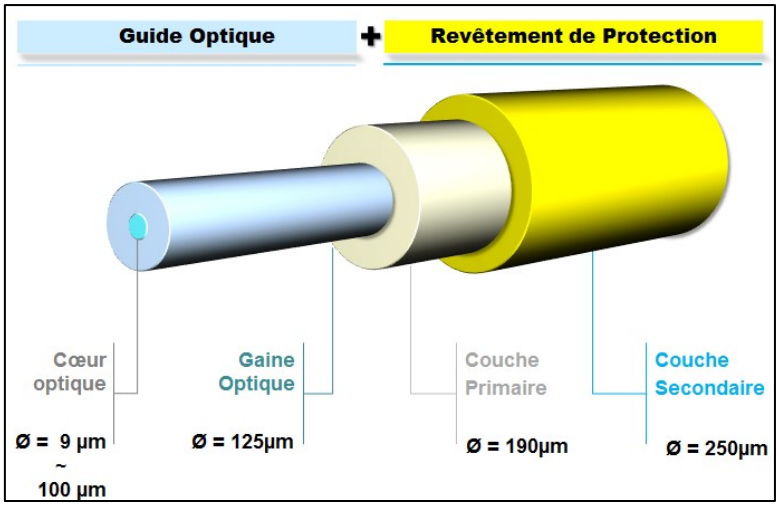


Figure 1.6. La structure de la fibre optique

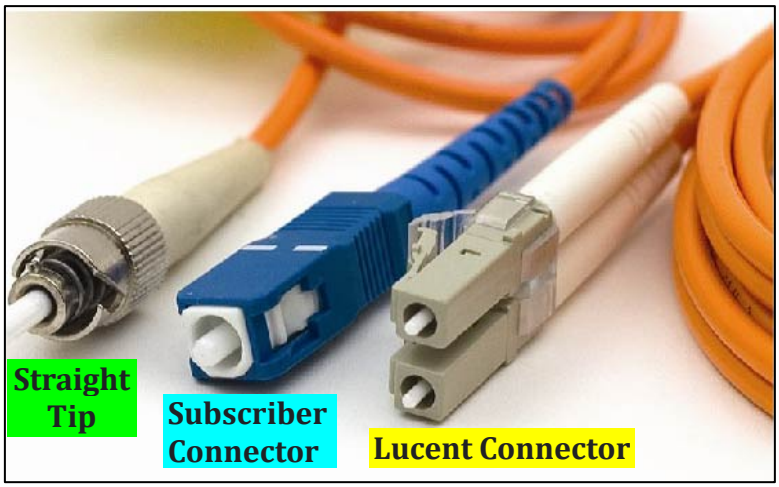


Figure 1.7. De gauche à droite : ST, SC et Fibre optique LC connecteurs

1.3.2. Carte réseau

La carte réseau doit fournir un mécanisme qui donne à chaque système un identifiant unique, comme un matricule de voiture, afin les données sont livrées au bon système. C'est l'une des tâches les plus importantes de la carte réseau. Chaque carte réseau a un identifiant avec une valeur de 48 bits appelée adresse de contrôle d'accès au support ou adresse MAC. Les adresses MAC sont toujours écrites en hexadécimal (exemple : 2E-6E-85-26-9F-48). (Voir la Figure 1.8)

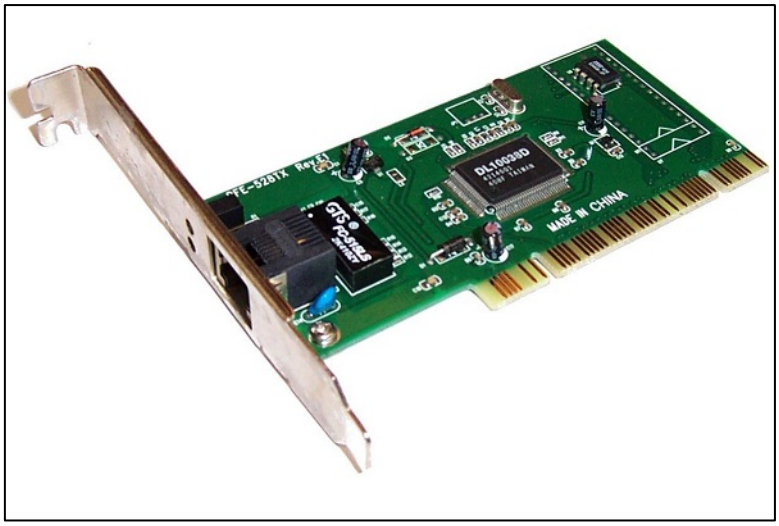


Figure 1.8. Carte réseau

1.3.3. Concentrateur

Un concentrateur (hub) est un périphérique étonné, essentiellement juste un répéteur. Lorsqu'il recevait une trame, le hub en faisait une copie exacte de cette trame, en envoyant une copie de la trame originale sur tous les ports connectés sauf le port d'où provient le message. (Voir la Figure 1.9)

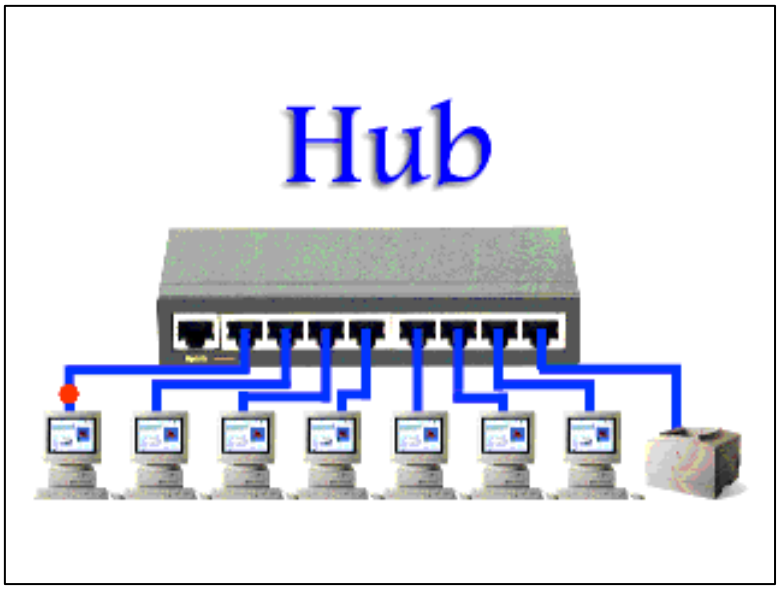


Figure 1.9. Concentrateur

1.3.4. Commutateurs

Un commutateur (Switch) ressemble à un concentrateur, car tous les nœuds s'y connectent. Mais les commutateurs ne fonctionnent pas comme des concentrateurs à l'intérieur. Les commutateurs sont dotés d'intelligences supplémentaires qui permettent d'envoyer des trames au nœud de destination en fonction des adresses MAC. Cela donne

à chaque conversation entre deux ordinateurs la totalité de la bande passante du réseau. (Voir la Figure 1.10)

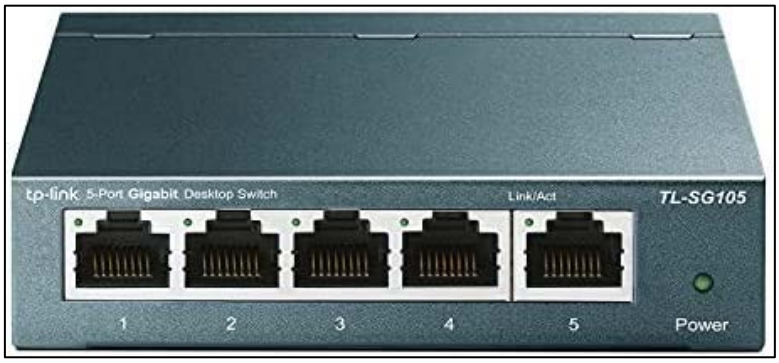


Figure 1.10. Commutateur a cinq ports

1.3.5. Modems

Un modem est un type de matériel qui connecte des périphériques informatiques à votre fournisseur d'internet. Le modem prend les signaux de votre fournisseur d'internet et les traduit en signaux que vos appareils locaux peuvent utiliser, et vice versa. (La Figure 1.11)

Figure 1.11. Modem

1.3.6. Passerelles

Une passerelle (routeur) est un appareil qui connecte au moins deux réseaux ou sous-réseaux à commutation de paquets. Il remplit deux fonctions principales : gérer le trafic entre ces réseaux en transférant les paquets de données vers leurs adresses IP prévues et permettre à plusieurs appareils d'utiliser la même connexion Internet. (Voir la Figure 1.12)

Figure 1.12. Routeur CISCO 7201

1.4. Types de réseaux informatiques

Un réseau informatique peut être classé en fonction de sa taille. Un réseau informatique est principalement de quatre types comme ils sont illustrés dans la Figure 1.13

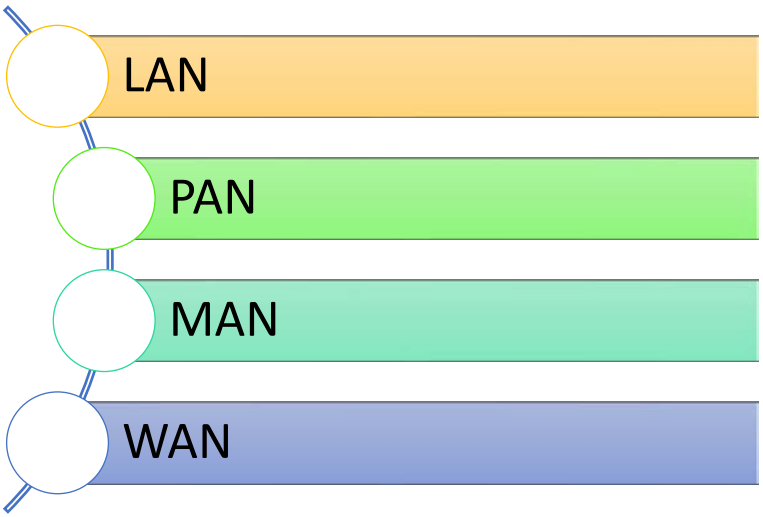


Figure 1.13. Les types de réseaux informatiques

1.4.1. PAN (Réseau personnel)

Le réseau personnel ou PAN (Personal Area Network) est un réseau organisé au sein d'une personne individuelle, généralement dans un rayon de 10 mètres. Le réseau personnel est utilisé pour connecter les périphériques informatiques à usage personnel est connu sous le nom de réseau personnel. Les machines personnelles utilisées dans un réseau personnel sont l'ordinateur portable, les téléphones portables et les lecteurs multimédias.

1.4.2. LAN (Réseau local)

Un réseau local ou LAN (Local Area Network) est un groupe d'ordinateurs connectés les uns aux autres dans une petite zone telle qu'un bâtiment, un bureau. Il est utilisé pour connecter deux ordinateurs personnels ou plus via un support de communication tel qu'une paire torsadée, un câble coaxial, etc. Il est moins coûteux car il est construit avec

du matériel peu coûteux tel que des concentrateurs, des adaptateurs réseau et des câbles Ethernet.

Les données sont transférées à un rythme extrêmement rapide dans le réseau local.

1.4.3. MAN (Réseau métropolitain)

Un MAN (Metropolitan Area Network) est un réseau qui couvre une plus grande zone géographique en interconnectant des réseaux locaux pour former un réseau plus vaste. Les agences gouvernementales utilisent MAN pour se connecter aux citoyens et aux industries privées. Dans MAN, différents réseaux locaux sont connectés les uns aux autres via une ligne de central téléphonique.

1.4.4. WAN (Réseau étendu)

Un WAN (Wide Area Network) est un réseau qui s'étend sur une vaste zone géographique telle que des états ou des pays. Un réseau étendu est un réseau bien plus grand que le MAN. Il n'est pas limité à un seul endroit, mais il s'étend sur une vaste zone géographique via une ligne téléphonique, un câble à fibre optique ou des liaisons par satellite. Internet est l'un des plus grands WAN au monde.

1.5. Les topologies de réseaux

La topologie définit la structure du réseau de la façon dont tous les composants sont interconnectés les uns aux autres. Il existe deux types de topologie : la topologie physique et la topologie logique. La topologie physique est la représentation géométrique de tous les nœuds d'un réseau. La topologie logique reflète la disposition des appareils et leur communication. C'est la transmission de données sur la topologie physique. Il est indépendant de la topologie physique, quelle que soit la disposition des nœuds

1.5.1. Topologie en bus

La topologie en bus (Figure 1.14) est conçue de manière à ce que toutes les stations soient connectées par un seul câble. Lorsqu'un nœud veut envoyer un message sur le réseau, il place un message sur le réseau. Toutes les stations disponibles dans le réseau recevront le message qu'il ait été adressé ou non. La topologie en bus est principalement utilisée dans les réseaux des standards 802.3 (Ethernet) et 802.4. La configuration d'une topologie en bus est assez simple par rapport aux autres topologies. Le câble dorsal est considéré comme une « voie unique » par laquelle le message est diffusé à toutes les stations.

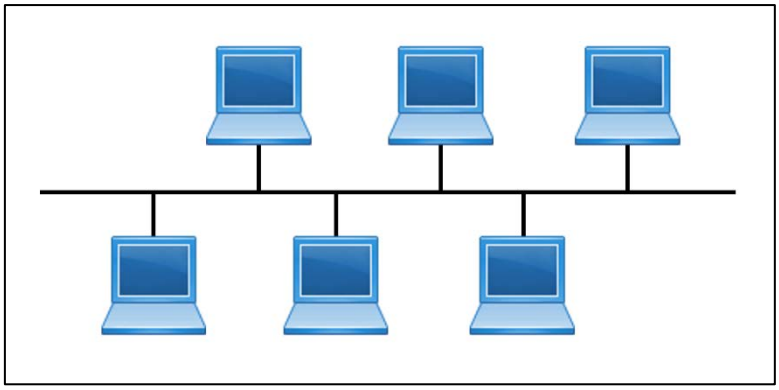


Figure 1.14. La topologie en bus

1.5.2. Topologie en anneau

La topologie en anneau (Figure 1.15) ressemble à une topologie en bus, mais avec des extrémités connectées. Le nœud qui reçoit le message de l'ordinateur précédent le retransmettra au nœud suivant. Les données circulent dans une seule direction (unidirectionnelle). Il n'a pas d'extrémités terminées, c'est-à-dire que chaque nœud est connecté à un autre nœud et n'a pas de point de terminaison. Les données d'une topologie en anneau circulent dans le sens des aiguilles d'une montre. La méthode d'accès la plus courante de la topologie en anneau est le passage de jeton.

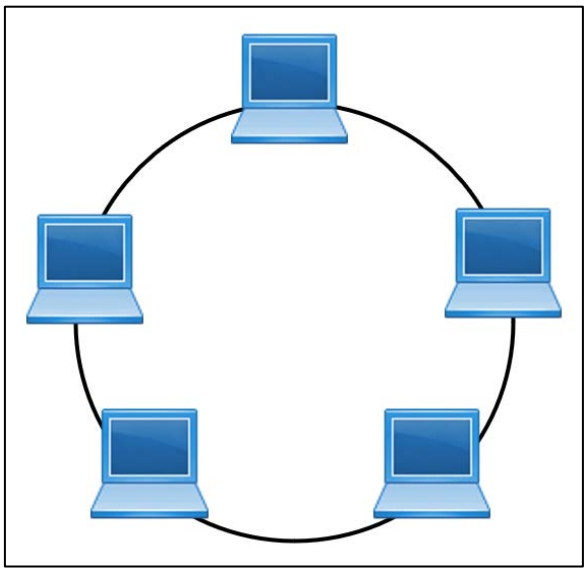


Figure 1.15. La topologie en anneau

1.5.3. Topologie en étoile

La topologie en étoile (Figure 1.16) est un agencement du réseau dans lequel chaque nœud est connecté au concentrateur central, au commutateur ou à un ordinateur central. L'ordinateur central est appelé serveur et les périphériques connectés au serveur sont appelés clients. Les concentrateurs ou les commutateurs sont principalement utilisés

comme dispositifs de connexion dans une topologie physique en étoile. La topologie en étoile est la topologie la plus populaire dans la mise en œuvre du réseau.

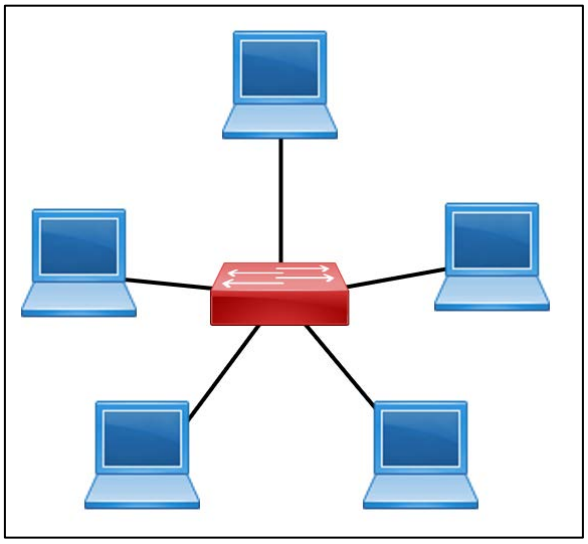


Figure 1.16. La topologie en étoile

1.5.4. Topologie en arbre

La topologie arborescente (Figure 1.17) combine les caractéristiques de la topologie en bus et de la topologie en étoile. Une topologie arborescente est un type de structure dans laquelle tous les ordinateurs sont connectés les uns aux autres de manière hiérarchique. Le nœud le plus haut dans la topologie arborescente est appelé nœud racine, et tous les autres nœuds sont les descendants du nœud racine.

Il n'y a qu'un seul chemin entre deux nœuds pour la transmission de données. Ainsi, il forme une hiérarchie parent-enfant.

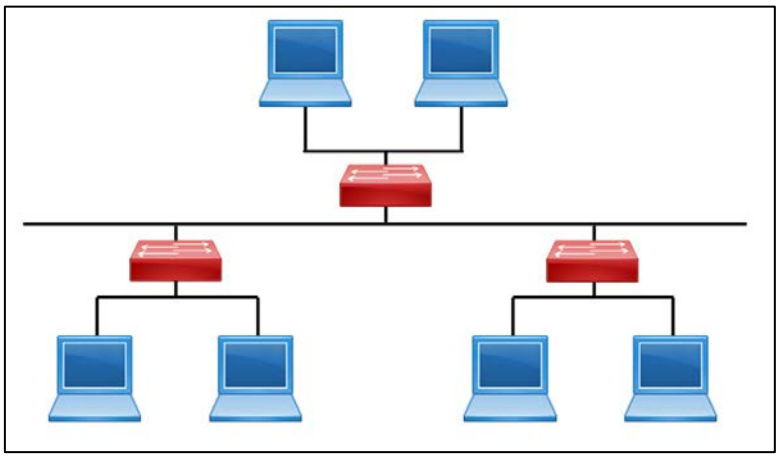


Figure 1.17. La topologie en arbre

1.5.5. Topologies modernes

1.5.5.1. Topologie maillée

Il existe deux types de topologie maillée (entièrement maillée et partiellement maillée), dans une topologie entièrement maillée, chaque ordinateur est connecté à tous les ordinateurs disponibles dans le réseau. Dans une topologie partiellement maillée, tous les ordinateurs, sauf certains, sont connectés aux ordinateurs avec lesquels ils communiquent fréquemment.

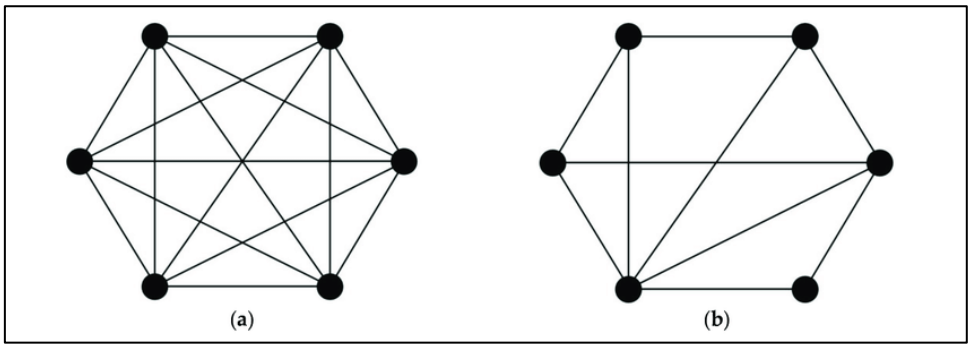


Figure 1.18. (a) entièrement maillée ; (b) partiellement mailée

1.5.5.2. Topologie hybride

La combinaison de différentes topologies est connue sous le nom de topologie hybride. Une topologie hybride est une connexion entre différents liens et nœuds pour transférer les données. Lorsque deux ou plusieurs topologies différentes sont combinées ensemble, on parle de topologie hybride et si des topologies similaires sont connectées les unes aux autres, cela n'entraînera pas une topologie hybride.

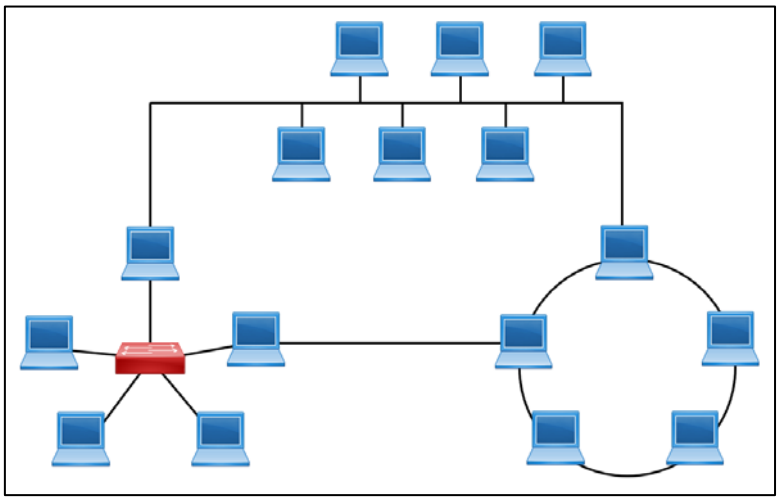


Figure 1.19. Topologie hybride

1.6. Le modèle OSI

Le modèle d'interconnexion de systèmes ouverts (**modèle OSI**) définit et codifie le concept d'architecture de réseau en couches. Les couches d'abstraction sont utilisées pour subdiviser davantage un système de communication en parties gérables plus petites. Une couche est un ensemble de fonctions similaires qui fournissent des services à la couche supérieure et reçoivent des services de la couche inférieure. Sur chaque couche, une instance fournit des services aux instances de la couche supérieure et demande des services à la couche inférieure.

La Figure 1.20 illustre les sept couches du modèle OSI que les systèmes informatiques utilisent pour communiquer sur un réseau. C'était le premier modèle standard pour les communications réseau, adopté par toutes les grandes entreprises informatiques et de télécommunications au début des années 1980.

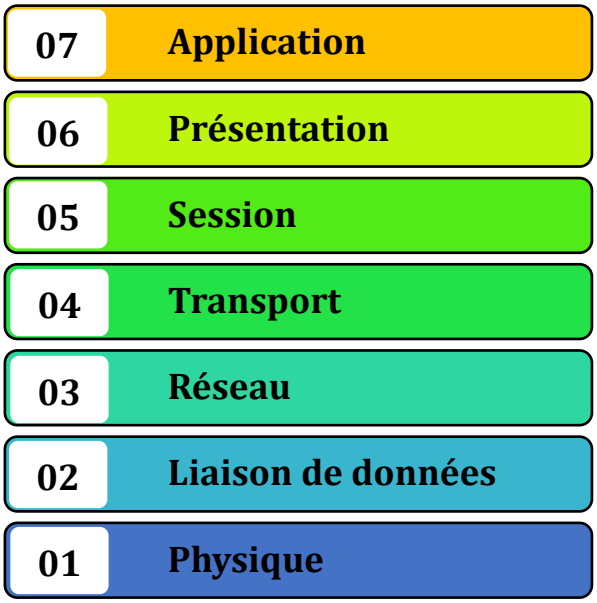


Figure 1.20. Les sept couches du modèle OSI

1.6.1. La couche physique

Le réseau a besoin d'un canal physique par lequel il peut déplacer des bits de données entre les systèmes. La couche physique définit les types d'encodage (c'est ainsi que les 0 et les 1 sont encodés dans un signal). La couche physique est responsable de la communication des flux de données brutes non structurées sur un support physique. Le support physique peut être un câble en cuivre, une fibre optique, ou des ondes électromagnétiques (illustré dans la Figure 1.22)

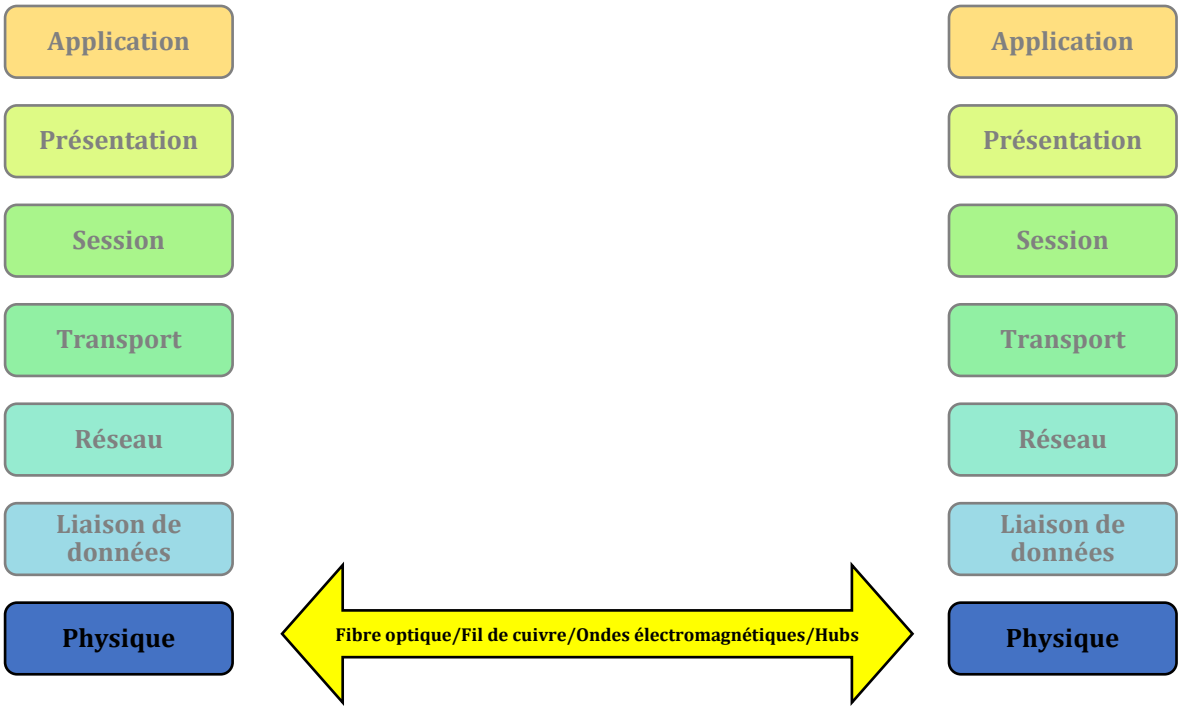


Figure 1.21. La couche physique du modèle OSI

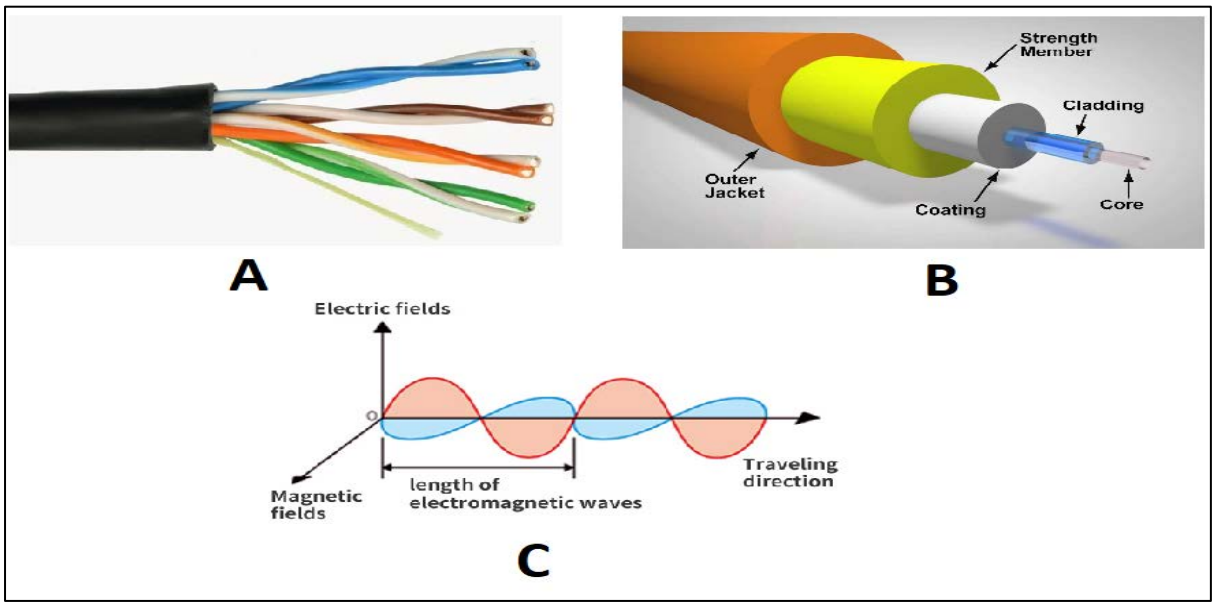


Figure 1.22. Les canaux de communication

1.6.2. La couche liaison de données

La couche liaison de données est la couche qui gère le déplacement des données vers et depuis une liaison physique dans un réseau. Comme il est illustré dans la Figure 1.23, cette couche a deux sous-couches :

- La sous-couche de contrôle de la liaison logique
- La sous-couche de contrôle d'accès au support (Media Access Control)

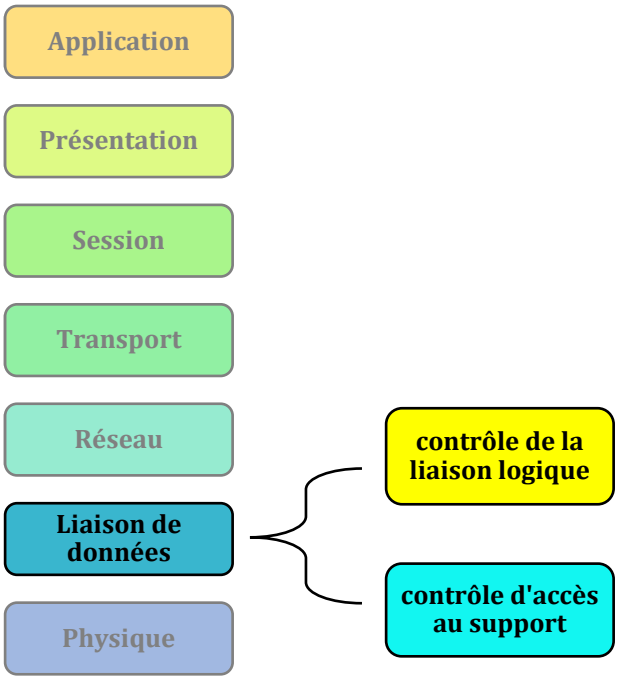


Figure 1.23. Les sous couches de la couche liaison de données

1.6.2.1. La sous-couche de contrôle de la liaison logique

La sous-couche contrôle de la liaison logique fournit la logique pour la liaison de données, elle contrôle les fonctions de synchronisation, de contrôle de flux et de vérification des erreurs de la couche liaison de données.

1.6.2.2. La sous-couche contrôle d'accès au support (MAC)

Cette couche crée et adresse la trame. Elle ajoute la propre adresse MAC de la carte réseau et attache les adresses MAC aux trames. La sous-couche MAC ajoute ou vérifie le FCS. Le MAC assure également que les trames sont envoyées le long du câblage réseau.

1.6.3. La couche réseau

La couche réseau est la cinquième couche du modèle OSI, elle gère les demandes de service de la couche transport et transmet ensuite la demande de service à la couche liaison de données. La couche réseau traduit les adresses logiques en adresses physiques et détermine la route de la source à la destination et gère également les problèmes de trafic tels que la commutation, le routage et contrôle la congestion des paquets de données. Le rôle principal de la couche réseau est de déplacer les paquets de l'hôte d'envoi vers l'hôte de réception.

1.6.4. La couche transport

Le rôle principal de la couche de transport est de fournir les services de communication directement aux processus d'application s'exécutant sur différents hôtes.

La couche de transport fournit une communication logique entre les processus d'application s'exécutant sur différents hôtes. Bien que les processus d'application sur différents hôtes ne soient pas physiquement connectés, les processus d'application utilisent la communication logique fournie par la couche de transport pour s'envoyer les messages. On retrouve dans cette couche les protocoles TCP et UDP qui fournissent un ensemble de services à la couche réseau.

1.6.5. La couche session

La couche session gère la partie de réseau qui connecte les applications entre eux. Elle contrôle les dialogues (connexions) entre ordinateurs. Elle établit, gère et termine les connexions entre les applications (locale et distante).

1.6.6. La couche présentation

La couche présentation traduit les données des couches inférieures dans un format utilisable par **la couche application**, et vice versa. Elle garantit que les communications en transit présentent une forme adaptée au destinataire. Le cryptage des données et la conversion des jeux de caractères (comme ASCII vers EBCDIC) sont généralement associés à cette couche. Par exemple : Le protocole Transport Layer Security (TLS) chiffre et déchiffre les données au niveau de cette couche.

1.6.7. La couche application

La couche application du modèle OSI est la couche la plus familière de l'utilisateur final, ce qui signifie que la couche application et l'utilisateur peuvent interagir directement à l'aide des logicielles (Google chrome, Skype, etc.). Les programmes de la couche application sont basés sur l'architecture client - serveurs. Parmi les protocoles de cette couche on trouve les protocoles HTTP, FTP, SSH, etc.

Chapitre 2 : Protocoles TCP/IP

2.1. Introduction

Ce chapitre introduit le côté logiciel de la mise en réseau. Vous apprendrez les détails sur le modèle TCP/IP qui est similaire au modèle OSI, il s'agit d'un modèle standard de l'industrie qui est efficacement déployé dans des problèmes pratiques de mise en réseau. Le modèle TCP/IP crée un ensemble de règles qui nous permet à tous de prendre un ordinateur (ou un périphérique) prêt à l'emploi, branchez tous les câbles appropriés, allumez-le, connectez et utilisez le réseau. Ce chapitre fournit les parties fondamentales du modèle TCP/IP, il vous apprend les différents protocoles TCP/IP.

2.2. Modèle TCP/IP

Le modèle TCP/IP définit et référence à la fois une grande collection de protocoles qui permettent les ordinateurs à communiquer. Pour définir un protocole, TCP/IP utilise des documents appelés Requests For Comments (RFC). Le modèle évite également de répéter le travail déjà effectué par un autre organisme en se référant simplement aux normes ou aux protocoles créés par ces organismes. Pour aider les gens à comprendre un modèle de mise en réseau, chaque modèle décompose les fonctions en un petit nombre de catégories appelées couches. Chaque couche comprend des protocoles et des normes qui se rapportent à cette catégorie de fonctions.

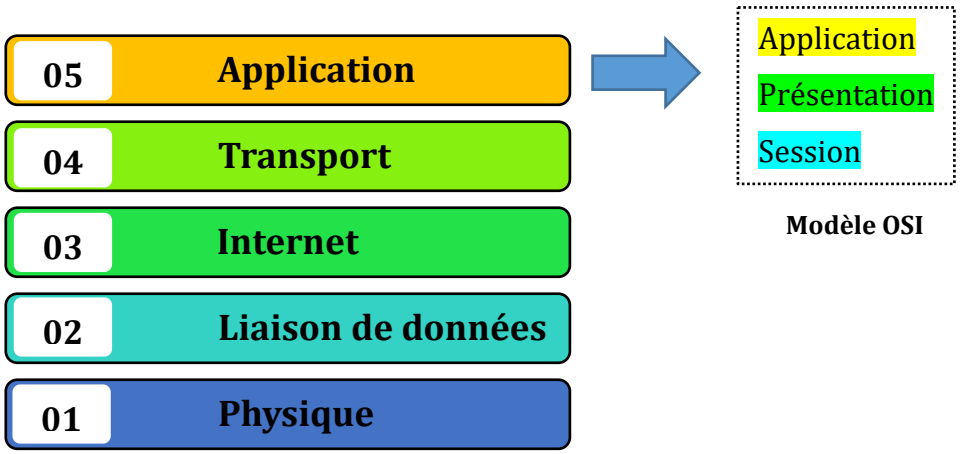


Figure 2.1. Les cinq couches du modèle TCP/IP

Remarques :

- Les trois couches du modèle OSI (application, présentation, et sessions) sont assemblées dans une seule couche du modèle TCP/IP, la couche application.
- Le modèle TCP/IP peut être divisé en quatre couches où la couche physique et la couche liaison sont fusionnées dans une seule couche nommée « accès réseau »

2.2.1. La couche physique

La couche physique définit le câblage et l'énergie (par exemple, les signaux électriques) qui circulent sur les câbles. La couche physique et liaison de données travaillent ensemble assez étroitement. En fait certaines normes définissent à la fois les fonctions de liaison de données et de couche physique.

2.2.2. La couche liaison de données

La couche de liaison de données TCP/IP fournit des services à la couche supérieure (la couche internet). Lorsqu'un hôte ou un routeur choisit d'envoyer un paquet IP à un autre routeur ou hôte, cet hôte ou routeur utilise ensuite les détails de la couche liaison pour envoyer ce paquet au routeur suivant. La couche de liaison comprend toutes les variantes des protocoles Ethernet et des protocoles LAN sans fil.

La couche de liaison de données identifie les périphériques sur la couche physique. Les adresses MAC font partie de la couche de liaison de données. Les commutateurs (switches) fonctionnent au niveau de la couche liaison de données.

2.2.2.1. Protocoles de la couche liaison de données

Parmi les protocoles de cette couche on trouve les protocoles : Ethernet, CSMA/CD, CSMA/CA.

2.2.2.1.1. Ethernet

Le terme Ethernet fait référence à toute une famille de normes. Certaines normes définissent les spécificités de la manière d'envoyer des données sur un type particulier de câblage et à une vitesse particulière. Autres normes définissent les protocoles, ou les règles, que les nœuds Ethernet doivent suivre pour faire partie d'un réseau local Ethernet. Toutes ces normes Ethernet sont issues de l'IEEE (Institute of Electrical and Electronics Engineers) et comportent le numéro **802.3** comme début du nom de la norme.

Tableau 2.1. Les types d'Ethernet

Nom	Vitesse maximale	Nom formel de la norme IEEE
Ethernet	10 Mbps	802.3
Fast Ethernet	100 Mbps	802.3u
Gigabit Ethernet	1000 Mbps	802.3z
10 Gigabit Ethernet	10 Gb	802.3an

L'une des avantages les plus importantes de la famille de protocoles Ethernet est que ces protocoles utilisent la même norme de liaison de données. En fait, les parties centrales de la date standard de liaison de données retour aux normes Ethernet d'origine.
La Figure 2.2 illustre les différents champs d'une trame Ethernet, le rôle de chaque champ est expliqué par la suite.

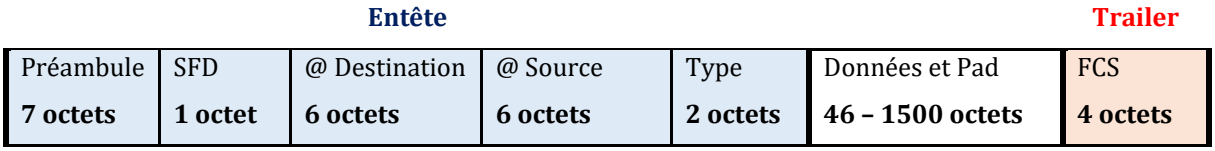


Figure 2.2. Format de la trame Ethernet

- **Préambule :** Permet aux appareils sur le réseau de synchroniser facilement leurs horloges, fournissant une synchronisation au niveau du bit
- **SFD (Start Frame Delimiter) :** Signifie que les six octets suivants contiennent l'adresse MAC de destinataire de trame.
- **@ Destination :** Adresse MAC du destinataire prévu de cette trame
- **@ Source :** Adresse MAC de l'expéditeur de trame
- **Type** : Définit le type de protocole encapsulé à l'intérieur de la trame. Par exemple : IP version 4 (**0x0800**) ; IP version 6 (**0x86DD**).
- **Données et PAD :** Contient les données de la couche supérieure (les PADs sont ajoutés pour atteindre la taille minimale du trame)
- **FCS :** Fournit une méthode permettant à la carte réseau réceptrice de déterminer si la trame a connu des erreurs de transmission.

2.2.2.1.2. CSMA/CD

Le protocole CSMA/CD (**Carrier Sense Multiple Access/Collision Detection)** est utilisé pour détecter une collision dans la couche de contrôle d'accès au support. Une fois la collision détectée, le CSMA/CD immédiatement arrêté la transmission en envoyant le

signal afin que l'expéditeur ne perde pas tout son temps à envoyer le paquet de données. Supposons qu'une collision soit détectée à partir de chaque station lors de la diffusion des paquets. Dans ce cas, ce protocole envoie immédiatement un signal de brouillage pour arrêter la transmission et attend un contexte temporel aléatoire avant de transmettre un autre paquet de données. Si le canal est trouvé libre, il envoie immédiatement les données. Ce protocole est utilisé par les réseaux Ethernet (la norme **802.3**)

2.2.2.1.3. CSMA/CA

CSMA/CA (**Carrier Sense Multiple Access/Collision Avoidance)** s'agit d'un protocole réseau qui évite une collision plutôt que de la laisser se produire, et qu'il ne s'occupe pas de la récupération des paquets après une collision. Il est similaire au protocole CSMA/CD qui fonctionne dans la couche de contrôle d'accès au support. Dans CSMA/CA, chaque fois qu'une station envoie une trame de données à un canal, elle vérifie s'il est utilisé. Si le canal partagé est occupé, la station attend que le canal passe en mode inactif. Par conséquent, nous pouvons dire qu'il réduit les risques de collisions et utilise mieux le support pour envoyer des paquets de données plus efficacement. Ce protocole est utilisé dans les réseaux **802.11** (un ensemble de normes concernant les réseaux sans fil locaux)

2.2.2.1.4. Le protocole ARP

L'objectif du protocole ARP (Address Resolution Protocol) est de convertir l'adresse logique IPv4 en adresse physique (adresse MAC) (voir la Figure 2.3). Ce protocole fonctionne sous la couche 2 du modèle TCP/IP. Ce protocole utilise un format de message de base qui contient soit une demande de résolution d'adresse, soit une réponse de résolution d'adresse. La taille du message ARP dépend de la taille de l'adresse de la couche liaison et de la couche réseau. L'en-tête du message décrit le type de réseau utilisé à chaque couche et la taille de l'adresse de chaque couche. L'en-tête du message est complété à l'aide du code opération, qui est 1 pour la requête et 2 pour la réponse.

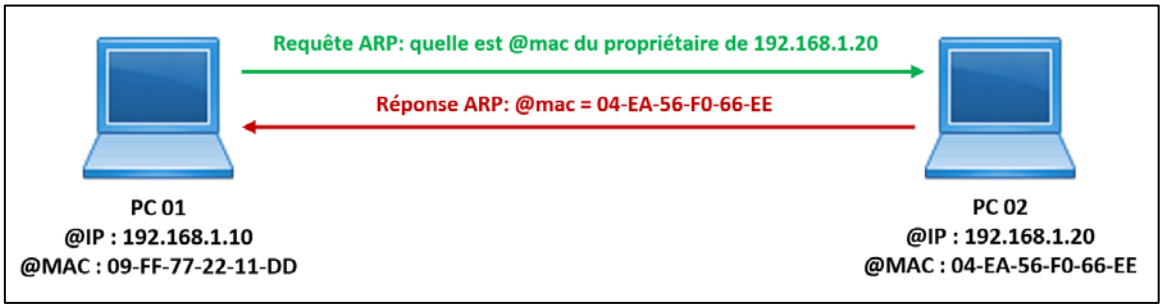


Figure 2.3. Flux de résolution d'adresse physique

2.2.2.1.5. Le protocole RARP

RARP (Reverse Address Resolution Protocol) est un protocole qui se trouve dans la couche liaison des données, il est utilisé pour déterminer les adresses IP lorsque les adresses physiques sont connues.

2.2.3. La couche Internet

La couche internet comprend un petit nombre de protocoles par rapport aux couches supérieures, le protocole IP (Internet Protocol) est le protocole majeur. En fait, le nom TCP/IP est simplement les noms des deux protocoles les plus courants (TCP et IP). IP offre plusieurs fonctionnalités, dont la plus importante est l'adressage et le routage.

Les principales fonctions assurées par la couche Internet sont :

- **Le routage** : Lorsqu'un paquet atteint un routeur, le routeur déplace les paquets vers le lien de sortie du routeur. Ce processus est appelé le ***routage***.
- **L'adressage logique** : la couche liaison de données implémente l'adressage physique et la couche internet implémente l'adressage logique. L'adressage logique est également utilisé pour faire la distinction entre le système source et le système de destination. La couche réseau ajoute un en-tête au paquet qui inclut les adresses logiques de l'expéditeur et du destinataire.
- **L'interconnexion des réseaux** : C'est le rôle principal de la couche internet, elle fournit la connexion logique entre différents types de réseaux.
- **La fragmentation** : la fragmentation est un processus de décomposition des paquets en unités de données individuelles les plus petites qui transitent par différents réseaux.

2.2.3.1. Protocoles de la couche internet

Parmi les protocoles de cette couche nous avons les protocoles : IP (IPv4 et IPv6), ICMP, IGMP.

2.2.3.1.1. IP (Internet Protocol)

IP définit les adresses pour plusieurs raisons importantes. Tout d'abord, chaque appareil qui utilise TCP/IP a besoin d'une adresse unique pour pouvoir être identifié dans le réseau. IP aussi définit comment regrouper les adresses, tout comme le système postal regroupe les adresses en fonction sur les codes postaux.

IP est un protocole utilisé pour envoyer les paquets de la source à la destination. La tâche principale d'IP est de livrer les paquets de la source à la destination en fonction des

adresses IP disponibles dans les en-têtes de paquet. IP définit la structure de paquet qui cache les données à livrer ainsi que la méthode d'adressage qui étiquette le datagramme avec une information de source et de destination.

La première version d'IP était IPv4. Après IPv4, IPv6 est arrivé sur le marché, qui est de plus en plus utilisé sur l'Internet public depuis 2006.

La fonction principale du protocole IP est de fournir un adressage aux hôtes, d'encapsuler les données dans une structure appelée **paquet** et d'acheminer les données de la source à la destination sur un ou plusieurs réseaux IP. Afin de réaliser ces fonctionnalités, le protocole IP définit le format du paquet IP et le système d'adressage.

- **Entête paquet IP :** Avant qu'un paquet IP ne soit envoyé sur le réseau, deux composants principaux sont ajoutés dans un paquet IP, c'est-à-dire un en-tête et les données à envoyer. (Illustré dans la Figure 2.4)

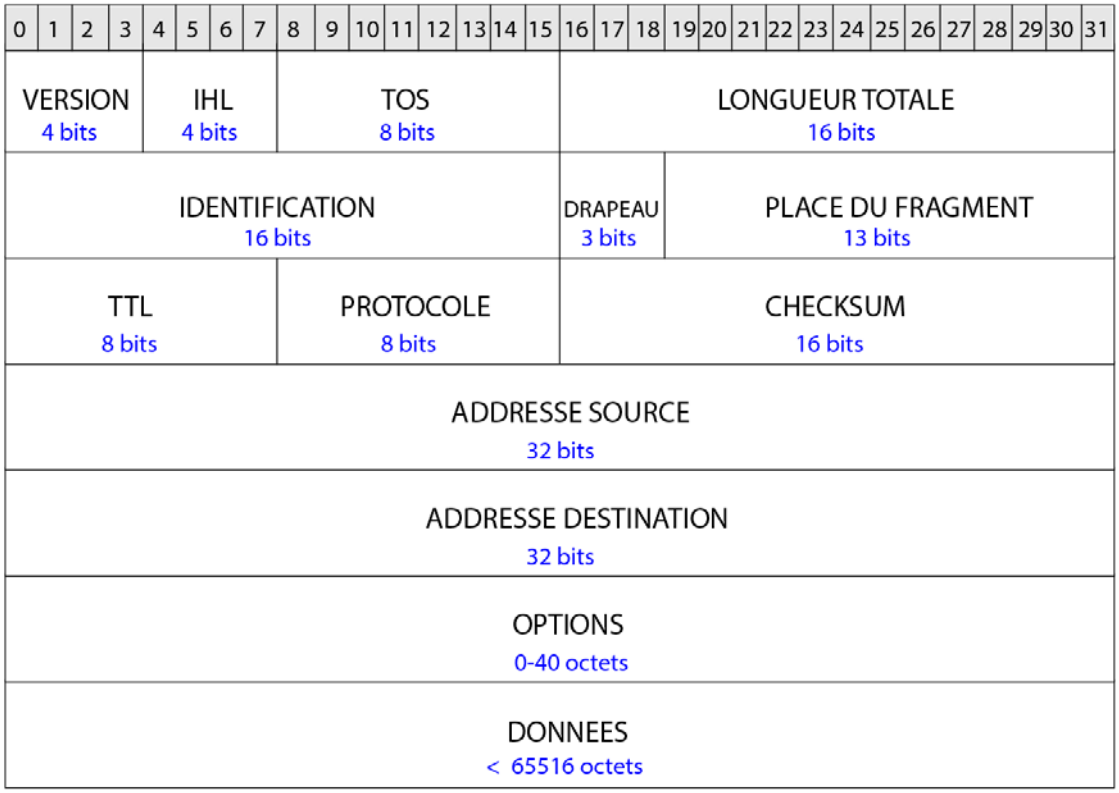


Figure 2.4. Format du paquet IP version 4

Version : c'est la version du protocole IP, pour IPv4 ce champ est toujours égal à 4.

IHL (Internet Header Length) : l'entête IPv4 est de taille variable en raison du champ optionnel (**options**). Ce champ contient la taille de l'entête IPv4, il a 4 bits qui spécifient le nombre de mots de 32 bits dans l'entête.

TOS (Type of Service) : utilisé pour mettre en place de la qualité de service dans un réseau.

Longueur totale : c'est la taille totale du paquet.

Identification : un identifiant qui est utilisé pour numéroter les fragments d'un même paquet.

Drapeau : utilisé pour contrôler ou identifier les fragments.

Place du fragment : position du fragment par rapport au premier fragment du paquet.

TTL (Time To Live) : la durée de vie est le nombre de sauts se produit avant que le paquet ne soit rejeté. Quand le TTL arrive à 0, le paquet est supprimé.

Protocole : précise le protocole de la couche transport. Généralement TCP ou UDP

Checksum : utilisé pour la vérification des erreurs.

Adresse source : La source est celle qui envoie les données.

Adresse destination : la destination est un hôte qui reçoit les données de l'expéditeur.

Options : ce champ est optionnel et il est rarement utilisé.

Données : contiennent les données de l'utilisateur plus les entêtes des couches supérieurs (Transport et Application).

- **Système d'adressage :** Une adresse IP est un identifiant unique attribué à chaque machine connectée à un réseau. L'adresse IP se compose d'une valeur de 32 bits, pour faciliter l'utilisation des adresses IP par les humains, la valeur binaire 32 bits est décomposée en quatre groupes de huit bits, séparés par des points (par exemple : **11000000.10101000.00000001.00000001**). Chacune de ces valeurs 8 bits est convertie en un nombre décimal compris entre 0 et 255 (la valeur binaire est devenue **192.168.1.1**). Chaque paquet IP contient deux adresses, à savoir l'adresse IP de l'appareil qui envoie le paquet et l'adresse IP de l'appareil qui reçoit le paquet.

2.2.3.1.2. Le protocole ICMP

Le protocole ICMP (Internet Control Message Protocol) est un protocole utilisé pour la gestion des erreurs dans la couche internet, il est principalement utilisé sur les périphériques réseau tels que les routeurs. Comme différents types d'erreurs peuvent exister dans la couche réseau, ICMP peut être utilisé pour signaler ces erreurs et pour les déboguer. Par exemple, un expéditeur souhaite envoyer le message à une destination,

mais le routeur n'a pas pu envoyer le message à la destination. Dans ce cas, le routeur envoie le message à l'expéditeur indiquant que je n'ai pas pu envoyer le message à cette destination.

- **Format de message ICMP :** La Figure 2.5 expose les différents champs d'un message ICMP

  Type : C'est un champ de 8 bits. Il définit le type de message ICMP. Les valeurs comprises entre 0 et 127 sont définies pour ICMPv6, et les valeurs comprises entre 128 et 255 sont les messages d'information.

  Code : C'est un champ de 8 bits qui définit le sous-type du message ICMP

  Somme de contrôle : il s'agit d'un champ de 16 bits permettant de détecter si l'erreur existe ou non dans le message.

  Identifiant : un champ d'identification qui peut être utilisé pour aider à faire correspondre les messages d'écho et de réponse d'écho

  Numéro de séquence : un numéro de séquence pour aider à faire correspondre les messages d'écho et de réponse d'écho

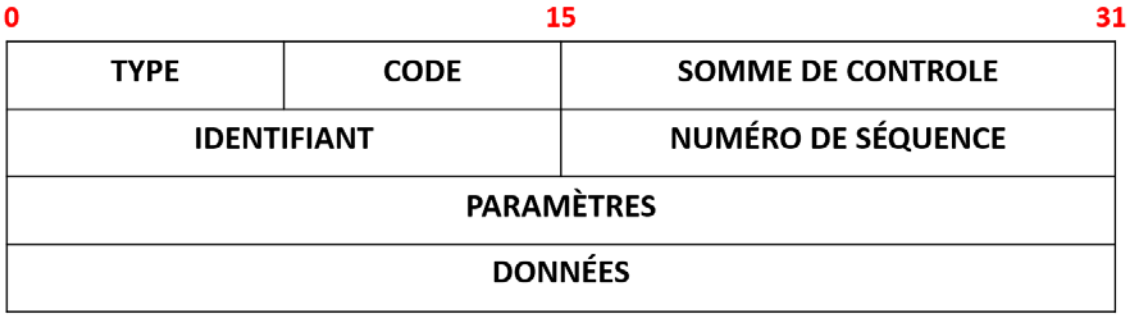


Figure 2.5. Format du message ICMP

Complément :

L'identifiant et le numéro de séquence peuvent être utilisés par l'expéditeur de l'écho pour faciliter la mise en correspondance des réponses avec les demandes d'écho.

2.2.4. La couche transport

Les deux protocoles de couche de transport les plus couramment utilisés sont le TCP (Transmission Control Protocol) et l'UDP (User Datagram Protocol).

Les protocoles de la couche transport fournissent des services aux protocoles de la couche application. Le rôle principal de la couche de transport est de fournir les services de communication directement aux processus d'application s'exécutant sur différents

hôtes. La couche de transport fournit une communication logique entre les processus d'application s'exécutant sur différents hôtes. Bien que les processus d'application sur différents hôtes ne soient pas physiquement connectés, les processus d'application utilisent la communication logique fournie par la couche de transport pour s'envoyer les messages. Chacune des applications de la couche application a la capacité d'envoyer un message en utilisant TCP ou UDP.

Parmi les services fournis par la couche de transport, nous avons les suivants :

- **Livraison de bout en bout :** la couche transport transmet l'intégralité du message à la destination. Par conséquent, il assure la livraison de bout en bout d'un message entier d'une source à la destination.
- **Livraison fiable :** la couche transport fournit des services de fiabilité en retransmettant les paquets perdus et endommagés.
- **Contrôle de flux :** le contrôle de flux est utilisé pour empêcher l'expéditeur de submerger le destinataire. La couche transport est responsable du contrôle de flux. Il utilise le protocole de fenêtre glissante qui rend la transmission de données plus efficace et contrôle le flux de données afin que le récepteur ne soit pas submergé. Le protocole de fenêtre glissante est orienté octet plutôt que trame.
- **Multiplexage :** la couche transport utilise le multiplexage pour améliorer l'efficacité de la transmission.
- **Adressage :** Selon le modèle TCP/IP, la couche transport interagit avec les fonctions de la couche application. Les données générées par une application sur une machine doivent être transmises à la bonne application sur une autre machine. Dans ce cas, l'adressage est assuré par la couche transport, nous parlons des ports plutôt que des adresses IP. L'adressage de la couche de transport TCP/IP est réalisé à l'aide de ports TCP et UDP. Chaque numéro de port identifie un processus logiciel particulier.

2.2.4.1. Le protocole TCP

Il s'agit d'un protocole qui facilite la transmission de paquets de la source à la destination. TCP est un protocole orienté connexion, ce qui signifie qu'il établit la connexion avant la communication qui se produit entre les appareils informatiques d'un réseau. La fonctionnalité principale du TCP est de prendre les données de la couche application. Ensuite, il divise les données en plusieurs paquets nommées (**segments)**, numérote ces

segments et les transmet à la destination. Le TCP, de l'autre côté (destinataire), réassemblera les paquets et les transmettra à la couche application. Comme nous savons que TCP est un protocole orienté connexion, la connexion restera établie jusqu'à ce que la communication ne soit pas terminée entre l'expéditeur et le destinataire.

Dans TCP, la connexion est établie à l'aide de l'établissement de liaison à trois étapes. Le client envoie le segment avec son numéro de séquence. Le serveur, en retour, envoie son segment avec son propre numéro de séquence ainsi que la séquence d'acquittement, qui est le numéro de séquence client **plus 1**. Lorsque le client reçoit l'accusé de réception de son segment, il envoie l'accusé de réception au serveur. De cette façon, la connexion est établie entre le client et le serveur.

Parmi les caractéristiques du protocole TCP :

- **La fiabilité :**

TCP est un protocole fiable car il suit le mécanisme de contrôle de flux et d'erreurs. Il prend également en charge le mécanisme d'accusé de réception, qui vérifie l'état et l'arrivée du son des données. Dans le mécanisme d'accusé de réception, le récepteur envoie un accusé de réception positif ou négatif à l'expéditeur afin que l'expéditeur puisse savoir si le paquet de données a été reçu ou doit être renvoyé.

- **L'ordre des données est maintenu :**

Ce protocole garantit que les données parviennent au destinataire prévu dans le même ordre dans lequel elles sont envoyées. Il ordonne et numérote chaque segment afin que la couche TCP du côté destination puisse les réassembler en fonction de leur ordre.

- **Orienté connexion :**

Il s'agit d'un service orienté connexion, ce qui signifie que l'échange de données n'a lieu qu'après l'établissement de la connexion. Une fois le transfert de données est terminé, la connexion sera interrompue.

- **Un duplex plein :**

C'est un full-duplex signifie que les données peuvent être transférées dans les deux sens en même temps.

- **Orienté flux :**

TCP est un protocole orienté flux car il permet à l'expéditeur d'envoyer les données sous la forme d'un flux d'octets et permet également au récepteur d'accepter les données sous la forme d'un flux d'octets. TCP crée un environnement dans lequel l'expéditeur et le

destinataire sont connectés par un tube imaginaire appelé circuit virtuel. Ce circuit virtuel transporte le flux d'octets sur Internet.

2.2.4.1.1. Format d'entête TCP

Le paquet TCP est appelé **segment**, la Figure 2.6 montre le format de l'entête TCP

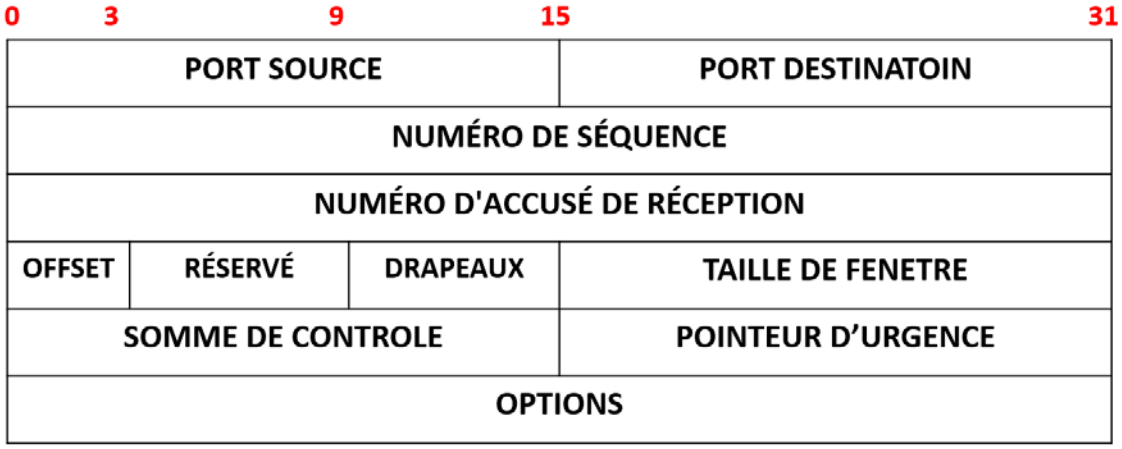


Figure 2.6. Format de l'entête TCP

- **Port source :** Il définit le port de l'application qui envoie les données. Ce champ contient l'adresse du port source, qui est de 16 bits.
- **Port de destination** : Il définit le port de l'application côté réception. Ce champ contient l'adresse du port de destination, qui est de 16 bits.
- **Numéro de séquence :** Ce chiffre sert à représenter le nombre d'octets qui ont été envoyés par la machine émettrice. Cela permet d'informer la machine avec qui nous dialoguons du nombre d'octets envoyés.
- **Numéro d'accusé de réception :** lorsque le drapeau ACK est défini, il contient le numéro de séquence suivant de l'octet de données et fonctionne comme un accusé de réception pour les données reçues précédemment. Par exemple, si le récepteur reçoit le numéro de segment **« x »,** il répond alors **« x+1 »** comme numéro d'accusé de réception.
- **Offset :** Il spécifie la longueur de l'en-tête indiquée par les mots de 4 octets dans l'entête. La taille de l'entête est comprise entre **20** et **60** octets. Par conséquent, la valeur de ce champ serait comprise entre **5** et **15**.
- **Réservé** : C'est un champ de 6 bits réservé pour une utilisation future, et par défaut, tous sont mis à zéro.
- **Drapeaux :** Il y a six bits de contrôle ou drapeaux :

- URG : Il représente un pointeur urgent. S'il est défini, les données sont traitées de manière urgente.
- ACK : si ACK est défini sur 0, cela signifie que le paquet de données ne contient pas d'accusé de réception.
- PSH : si ce champ est défini, il demande à l'appareil récepteur de transmettre les données à l'application réceptrice sans les mettre en mémoire tampon.
- RST : s'il est défini, il demande le redémarrage d'une connexion.
- SYN : Il est utilisé pour établir une connexion entre les hôtes.
- FIN : Il est utilisé pour libérer une connexion, et aucun autre échange de données ne se produira.

- **La taille de la fenêtre :** C'est un champ de 16 bits. Il contient la taille des données que le récepteur peut accepter. La fenêtre indique la quantité de données qu'une machine peut accepter sans exiger d'accusé de réception.
- **Somme de contrôle (checksum) :** C'est un champ de 16 bits. Ce champ est facultatif dans UDP, mais dans le cas de TCP/IP, ce champ est obligatoire.
- **Pointeur d'urgence :** C'est un pointeur qui pointe sur l'octet de données urgentes si le drapeau URG est mis à 1. Il définit une valeur qui sera ajoutée au numéro de séquence pour obtenir le numéro de séquence du dernier octet urgent.
- **Options :** Il offre des options supplémentaires.

2.2.4.1.2. Établissement de connexion TCP

La Figure 2.7 présente les étapes du processus d'établissement de connexion TCP. Nous avons un client avec « @IP : 41.91.1.150 » qui souhaite établir une connexion TCP avec le serveur « @IP : 142.251.37.206 »

- **Étape 1 :** le client envoie donc un segment avec SYN (Synchronize Sequence Number) qui informe le serveur que le client est susceptible de commencer la communication et avec quel numéro de séquence le commencement des segments.
- **Étape 2** : le serveur répond à la demande du client avec les drapeaux SYN-ACK définis. Accusé de réception (ACK) signifie la réponse du segment qu'il a reçu et SYN signifie avec quel numéro de séquence il est susceptible de commencer les segments avec.

- **Étape 3 :** dans la dernière partie, le client accuse une réception de la réponse du serveur et ils établissent tous les deux une connexion fiable avec laquelle ils commenceront le transfert de données proprement dit

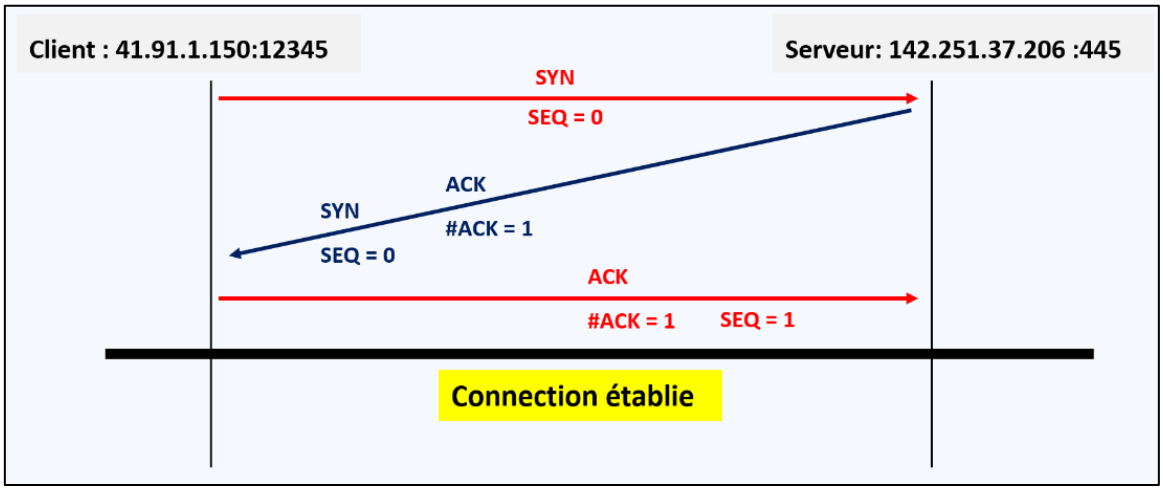


Figure 2.7. Processus d'établissement d'une connexion TCP (3-Way Handshake)

2.2.4.2. Le protocole UDP

L'UDP (User Datagram Protocol) est un protocole de communication alternatif au protocole TCP. L'UDP fonctionne en encapsulant les données dans un paquet (nommé **datagramme**) et en fournissant ses propres informations d'en-tête au datagramme. Ensuite, ce datagramme UDP est encapsulé dans le paquet IP et envoyé à sa destination. Étant donné que UDP envoie les messages sous forme de datagrammes, il est considéré comme le mode de communication le plus efficace. L'UDP est un protocole sans connexion car il ne nécessite aucun circuit virtuel pour transférer les données. UDP fournit également un numéro de port différent pour distinguer les différentes demandes des utilisateurs. Parmi les caractéristiques du protocole UDP :

- **Sans connexion :**

L'UDP est un protocole sans connexion car il ne crée pas de chemin virtuel pour transférer les données. Il n'utilise pas le chemin virtuel, de sorte que les paquets sont envoyés dans des chemins différents entre l'expéditeur et le destinataire, ce qui entraîne la perte de paquets ou une réception dans le désordre.

- **Ports :**

UDP utilise différents numéros de port afin que les données puissent être envoyées à la bonne destination. Il existe 65 535 ports.

- **Transmission rapide :**

UDP permet une transmission plus rapide car il s'agit d'un protocole sans connexion, c'est-à-dire qu'aucun chemin virtuel n'est requis pour transférer les données. Mais il est possible que le paquet individuel soit perdu, ce qui affecte la qualité de transmission.

- **Les segments sont traités indépendamment :**

Chaque segment UDP est géré individuellement car chaque segment emprunte un chemin différent pour atteindre la destination. Les segments UDP peuvent être perdus ou livrés dans le désordre pour atteindre la destination car il n'y a pas d'établissement de connexion entre l'expéditeur et le destinataire.

- **Sans état (Stateless) :**

C'est un protocole sans état, ce qui signifie que l'expéditeur ne reçoit pas l'accusé de réception du paquet qui a été envoyé.

2.2.4.2.1. Format d'entête UDP

Dans UDP, la taille de l'entête est de 8 octets et la taille du datagramme peut atteindre 65 535 octets. Mais cette taille n'est pas possible car les données doivent être encapsulées dans le paquet IP ; par conséquent, le maximum d'UDP serait de 65 535 moins 20 octets. La taille des données que le paquet UDP peut transporter serait de 65 535 moins 28, soit 8 octets pour l'en-tête du paquet UDP et 20 octets pour l'entête IP.

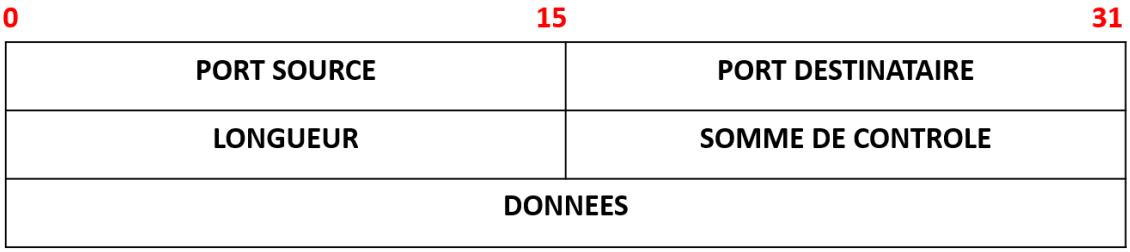


Figure 2.8. Entête UDP

- **Numéro de port source :** il s'agit d'un numéro de 16 bits qui identifie le port qui va envoyer le paquet.
- **Numéro de port de destination :** il s'agit d'un numéro de 16 bits utilisé pour identifier le service au niveau de l'application sur la machine de destination.
- **Longueur** : C'est un champ de 16 bits qui spécifie la longueur totale du paquet UDP qui inclut également l'en-tête. La valeur minimale serait de 8 octets car la taille de l'en-tête est de 8 octets.

- **Somme de contrôle (checksum) :** c'est un champ de 16 bits (optionnel). Ce champ vérifie si les données sont exactes ou non, car il est possible que les données soient corrompues lors de la transmission.

Complément :

Dans UDP, le champ de somme de contrôle est appliqué à l'ensemble du datagramme, c'est-à-dire à l'entête ainsi qu'à la partie donnée, tandis que dans IP, le champ de somme de contrôle est appliqué uniquement à l'en-tête.

2.2.5. La couche application

Dans le modèle TCP/IP la couche application groupe les couches application, présentation et session du modèle OSI. La couche application est la couche la plus proche de l'utilisateur final, ce qui signifie que la couche application et l'utilisateur final peuvent interagir directement.

Parmi les services fournis par la couche application, nous avons les suivants :

- **Terminal virtuel :** Une couche application permet à un utilisateur de se connecter à un hôte distant. Pour ce faire, l'application crée une émulation logicielle d'un terminal sur l'hôte distant. L'ordinateur de l'utilisateur communique avec le terminal logiciel qui, à son tour, communique avec l'hôte. L'hôte distant pense qu'il communique avec l'un de ses propres terminaux, il permet donc à l'utilisateur de se connecter.
- **Transfert, accès et gestion de fichiers :** une application permet à un utilisateur d'accéder à des fichiers sur un ordinateur distant, de récupérer des fichiers sur un ordinateur et de gérer des fichiers sur un ordinateur distant. Nous pouvons définit un fichier virtuel hiérarchique en termes de structure de fichier, d'attributs de fichier et de type d'opérations effectuées sur les fichiers et leurs attributs.
- **Adressage :** Pour obtenir la communication entre le client et le serveur, il y a un besoin d'adressage. Lorsqu'un client fait une demande au serveur, la demande contient l'adresse du serveur et sa propre adresse. La réponse du serveur à la demande du client, la demande contient l'adresse de destination, c'est-à-dire l'adresse du client. Pour réaliser ce type d'adressage, le DNS est utilisé.
- **Services de messagerie :** La couche d'application fournit le transfert et le stockage des e-mails.

- **Services d'annuaire :** une application contient une base de données distribuée qui permet d'accéder à des informations globales sur divers objets et services.
- **Authentification :** Il authentifie le message de l'expéditeur ou du destinataire ou les deux.

2.2.5.1. Architecture des applications réseau

L'architecture applicative est de deux types :

2.2.5.1.1. Architecture client-serveur

Un programme s'exécutant sur la machine locale (client) envoie une demande à un autre programme appelé serveur. Par exemple, lorsqu'un serveur Web reçoit une demande de l'hôte client, il répond à la demande adressée à l'hôte client.

2.2.5.1.2. Architecture P2P (Peer-To-Peer)

Il n'a pas de serveur dédié dans cette architecture. Les pairs sont les ordinateurs qui n'appartiennent pas au fournisseur de services. La plupart des pairs résident dans les maisons, les bureaux, les écoles et les universités. Les pairs communiquent entre eux sans faire passer les informations par un serveur dédié, cette architecture est connue sous le nom d'architecture **peer-to-peer**. Les applications basées sur l'architecture P2P incluent le partage de fichiers et la téléphonie Internet.

2.2.5.2. Protocoles de la couche application

Il existe de nombreux protocoles dans la couche application, parmi les protocoles les plus connues nous avons : HTTP, DNS, DHCP, SMTP, FTP, TELNET.

2.2.5.2.1. Le protocole HTTP

Le protocole HTTP (HyperText Transfer Protocol) est utilisé pour accéder aux données sur le World Wide Web (www). Le protocole HTTP peut être utilisé pour transférer les données sous forme de texte brut, d'hypertexte, d'audio, de vidéo, etc. Il est efficace et nous permet de l'utiliser dans un environnement hypertexte où il y a des sauts rapides d'un document à un autre document. HTTP est similaire au FTP car il transfère également les fichiers d'un hôte à un autre hôte. Mais, HTTP est plus simple que FTP car HTTP utilise une seule connexion, c'est-à-dire aucune connexion de contrôle pour transférer les fichiers. HTTP est utilisé pour transporter les données sous la forme d'un format de type MIME. Nous avons deux types des messages : requête et réponse.

- ***Requête*** : le message de demande est envoyé par le client et se compose d'une ligne de demande, d'en-têtes et parfois d'un corps.
- ***Réponse*** : le message de réponse est envoyé par le serveur au client et se compose d'une ligne d'état, d'en-têtes et parfois d'un corps.

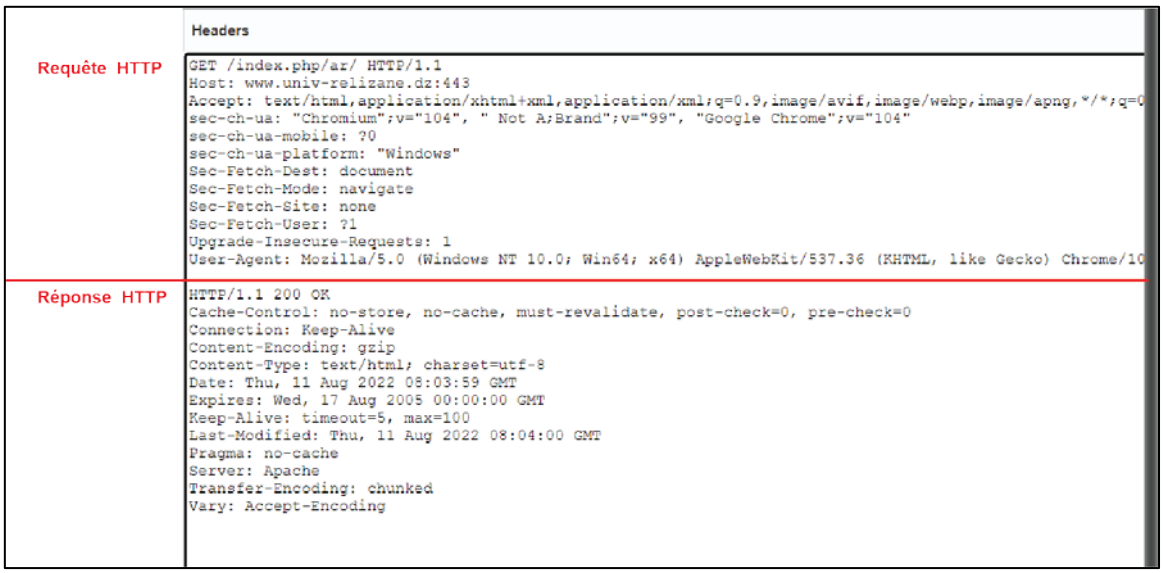


Figure 2.9. Les messages HTTP

Parmi les caractéristiques de ce protocole nous avons les suivantes :

- **Protocole sans connexion :** HTTP est un protocole sans connexion. Le client HTTP lance une requête et attend une réponse du serveur. Lorsque le serveur reçoit la demande, le serveur traite la demande et renvoie la réponse au client HTTP, après quoi le client déconnecte la connexion. La connexion entre le client et le serveur n'existe que pendant la requête en cours et le temps de réponse uniquement.
- **Indépendant du support :** le protocole HTTP est un support indépendant car les données peuvent être envoyées tant que le client et le serveur savent comment gérer le contenu des données. Il est nécessaire que le client et le serveur spécifient le type de contenu dans l'en-tête de type MIME.
- **Sans état :** HTTP est un protocole sans état car le client et le serveur ne se connaissent que pendant la requête en cours. En raison de la nature du protocole, le client et le serveur ne conservent pas les informations entre les différentes requêtes des pages Web.

2.2.5.2.2. Le DNS

Le DNS (Domain Name System) est un service d'annuaire qui fournit un mappage entre le nom d'un hôte sur le réseau et son adresse numérique. Le DNS est nécessaire au fonctionnement d'internet. Chaque nœud d'un arbre à un nom de domaine, et un nom de domaine complet constitué d'une séquence de symboles spécifiés par des points.

Le DNS est un service qui traduit le nom de domaine en adresses IP. Cela permet aux utilisateurs de réseaux d'utiliser des noms conviviaux lorsqu'ils recherchent d'autres hôtes au lieu de se souvenir des adresses IP.

Par exemple, le site web d'université de Relizane a une adresse IP de 193.194.79.72, la plupart des gens accèderaient à ce site en spécifiant https://www.univ-relizane.dz/ . Par conséquent, le nom de domaine est plus fiable que l'adresse IP.

DNS est un protocole de qui se base sur une architecture client/serveur. Les clients DNS envoient des requêtes au serveur tandis que les serveurs DNS envoient des réponses au client. DNS implémente une base de données distribuée pour stocker le nom de tous les hôtes disponibles sur Internet. Si un client tel qu'un navigateur Web envoie une requête contenante un nom d'hôte, un logiciel tel qu'un résolveur DNS envoie une requête au serveur DNS pour obtenir l'adresse IP d'un nom d'hôte. Si le serveur DNS ne contient pas l'adresse IP associée à un nom d'hôte, il transmet la demande à un autre serveur DNS. Si l'adresse IP est arrivée au résolveur, qui à son tour termine la demande via le protocole Internet.

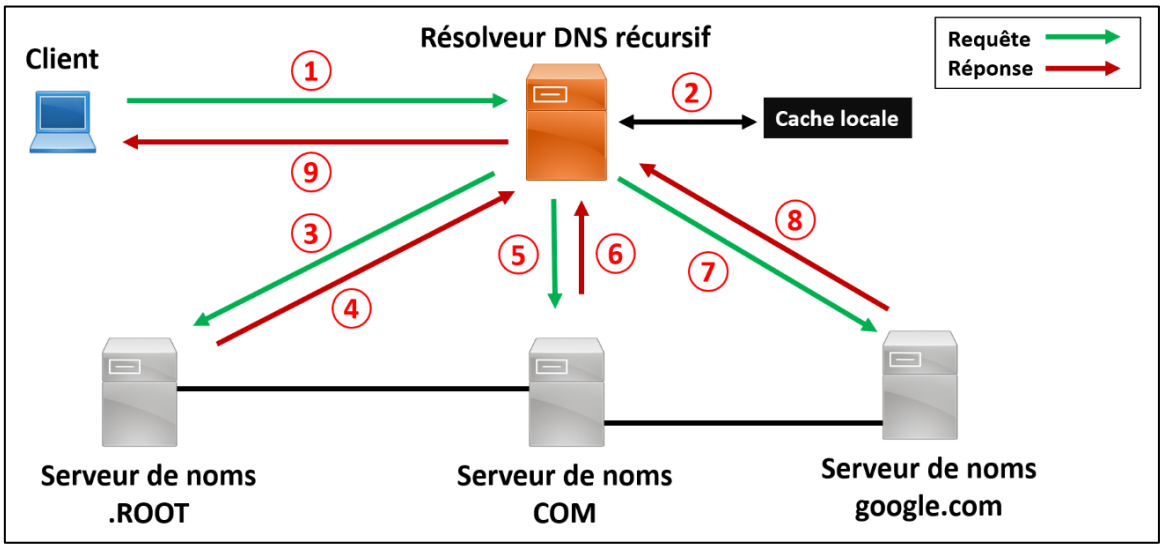


Figure 2.10. Scenario de résolution d'une adresse DNS

2.2.5.2.3. Le DHCP

Le protocole DHCP (Dynamic Host Configuration Protocol) est un protocole client/serveur qui fournit automatiquement à un hôte son adresse IP et d'autres informations de configuration connexes telles que le masque de sous-réseau et la passerelle par défaut. Dans DHCP, le numéro de port 67 est utilisé pour le serveur et 68 est utilisé pour le client. Le DHCP permet à un administrateur réseau de superviser et de distribuer des adresses IP à partir d'un point central et envoie automatiquement une nouvelle adresse IP lorsqu'un ordinateur est branché à un endroit différent du réseau

Format d'entête DHCP :

L'entête DHCP contient les champs suivants :

- **Code d'opération :** spécifie le type général de message. Une valeur de 1 indique un message de demande, tandis qu'une valeur de 2 est un message de réponse
- **Type matériel :** ce champ spécifie le type de matériel utilisé pour le réseau local (Ethernet = 1 ; IEEE 802 = 6 ; Fibre optique = 16)
- **Longueur de l'adresse physique :** spécifie la longueur des adresses matérielles dans ce message. Pour Ethernet ou d'autres réseaux utilisant des adresses MAC IEEE 802, la valeur est 6. C'est également la même chose qu'un champ dans le format de champ ARP, HLN.
- **Sauts :** défini sur 0 par un client avant de transmettre une requête et utilisé par les agents relais pour contrôler le transfert des messages DHCP
- **Identifiant de transaction :** Un champ d'identification de 32 bits généré par le client, pour lui permettre de faire correspondre la demande avec les réponses reçues des serveurs DHCP
- **Secondes :** il est défini comme le nombre de secondes écoulées depuis qu'un client a commencé une tentative d'acquisition ou de renouvellement d'un contrat
- **Adresse IP du client** : le client met sa propre adresse IP actuelle dans ce champ si et seulement s'il a une adresse IP valide lorsqu'il est dans les états BOUND, RENEWING ou REBINDING ; sinon, il définit le champ sur 0.
- **« Votre » adresse IP :** L'adresse IP que le serveur attribue au client.
- **Adresse IP du serveur :** c'est l'adresse du serveur que le client doit utiliser

- **Adresse IP Passerelle :** ce champ n'est pas utilisé par les clients et ne représente pas le serveur donnant au client l'adresse d'un routeur par défaut (cela se fait en utilisant l'option Routeur DHCP)

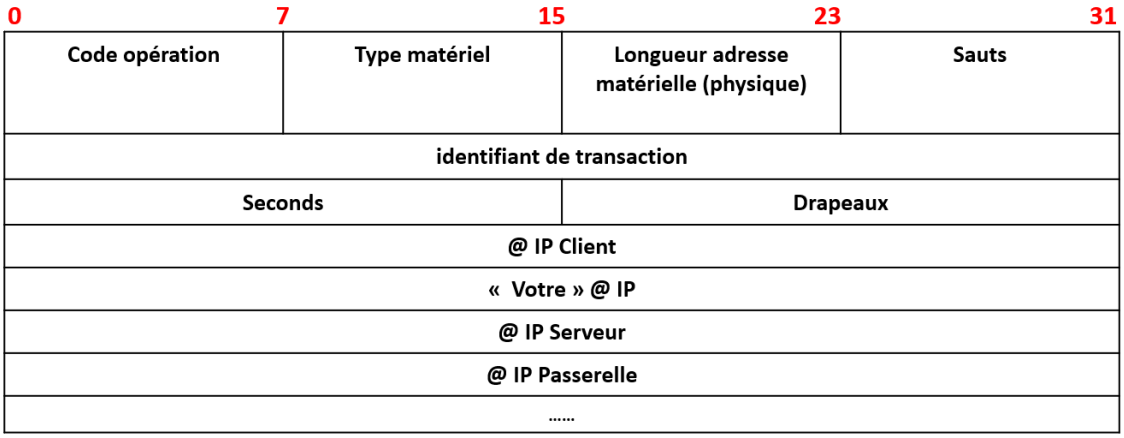


Figure 2.11. Entête DHCP

2.2.5.2.4. Le SMTP

SMTP (Simple Mail Transfer Protocol) est un ensemble de directives de communication qui permettent à un logiciel de transmettre un courrier électronique sur Internet. Il s'agit d'un protocole utilisé pour envoyer des messages à d'autres utilisateurs d'ordinateurs sur la base d'adresse e-mail. Il fournit un échange de courrier entre utilisateurs sur le même ordinateur ou sur des ordinateurs différents, et il prend également en charge :

- L'envoi d'un message unique à un ou plusieurs destinataires.
- L'envoi d'un message peut inclure du texte, de la voix, de la vidéo ou des graphiques.
- Il peut également envoyer les messages sur des réseaux en dehors d'Internet.

Le but principal de SMTP est d'établir des règles de communication entre les serveurs. Les serveurs ont un moyen de s'identifier et d'annoncer le type de communication qu'ils essaient d'effectuer. Ils ont également un moyen de gérer les erreurs telles que l'adresse e-mail incorrecte. Par exemple, si l'adresse du destinataire est erronée, le serveur de réception répond avec un message d'erreur.

Parmi les services fournis par SMTP, nous avons les suivants :

- **Composition du courrier :** un utilisateur envoie un courrier électronique en composant un message de courrier électronique à l'aide d'un ***agent d'utilisateur de messagerie***. L'agent d'utilisateur de messagerie est un programme utilisé pour envoyer et recevoir du courrier. Le message contient deux parties : le corps et l'en-

tête. Le corps est la partie principale du message tandis que l'en-tête comprend des informations telles que l'expéditeur et l'adresse du destinataire. L'en-tête comprend également des informations descriptives telles que l'objet du message. Dans ce cas, le corps du message est comme une lettre et l'en-tête est comme une enveloppe qui contient l'adresse du destinataire.

- **Soumission du courrier :** après avoir composé un courrier électronique, le client de messagerie soumet ensuite le courrier électronique au serveur SMTP en utilisant SMTP sur le port TCP 25.
- **Livraison du courrier :** Les adresses e-mail contiennent deux parties : le nom d'utilisateur du destinataire et le nom de domaine. Par exemple, mohammed@univ-relizane.dz, où « mohammed » est le nom d'utilisateur du destinataire et « univ-relizane.dz » est le nom de domaine. Si le nom de domaine de l'adresse e-mail du destinataire est différent du nom de domaine de l'expéditeur, ***l'agent de soumission de messages*** enverra le courrier à ***l'agent de transfert de courrier***. Pour relayer l'e-mail, l'agent de transfert de courrier trouvera le domaine cible. Il vérifie l'enregistrement MX du système de noms de domaine pour obtenir le domaine cible. L'enregistrement MX contient le nom de domaine et l'adresse IP du domaine du destinataire. Une fois l'enregistrement localisé, l'agent de transfert de courrier se connecte au serveur d'échange pour relayer le message.
- **Réception et traitement du courrier :** Une fois le message entrant reçu, le serveur d'échange le remet au serveur entrant qui stocke le courrier électronique où il attend que l'utilisateur le récupère.
- **Accès et récupération du courrier :** Le courrier électronique stocké peut être récupéré à l'aide de l'agent d'utilisateur de messagerie. L'agent d'utilisateur de messagerie est accessible en utilisant un identifiant et un mot de passe.

2.2.5.2.5. Le protocole FTP

FTP (File Transfer Protocol) est un protocole de transfert de fichiers. Il est utilisé pour transmettre les fichiers d'un hôte à un autre. Il est principalement utilisé pour transférer les fichiers d'un site web de leur créateur vers l'ordinateur qui sert de serveur pour d'autres ordinateurs sur Internet. Il est également utilisé pour télécharger les fichiers sur l'ordinateur à partir d'autres serveurs.

Parmi les caractéristiques du protocole FTP nous avons :

- **Vitesse :** Le FTP est l'un des moyens les plus rapides pour transférer des fichiers d'un ordinateur à un autre.
- **Efficacité** : C'est plus efficace car nous n'avons pas besoin de terminer toutes les opérations pour obtenir l'intégralité du fichier.
- **Sécurité** : Pour accéder au serveur FTP, nous devons nous connecter avec le nom d'utilisateur et le mot de passe. Par conséquent, nous pouvons dire que FTP est plus sécurisé.

2.2.5.2.6. TELNET

Telnet est l'abréviation de **Terminal Network.** Telnet fournit une connexion à l'ordinateur distant de telle sorte qu'un terminal local semble être du côté distant. Lorsque les utilisateurs souhaitent exécuter différents programmes d'application sur un site distant et transfèrent un résultat sur le site local. Cela nécessite un programme client-serveur tel que FTP, SMTP. Mais cela ne nous permettrait pas de créer un programme spécifique pour chaque demande. Une solution consiste à fournir un programme client-serveur général qui permet à l'utilisateur d'accéder à n'importe quel programme d'application sur un ordinateur distant c'est le **Telnet**.

Chapitre 3 : Introduction aux principaux aspects liés au routage

3.1. Introduction

La vraie puissance de TCP/IP tient en un mot : le routage. Le routage nous permet d'interconnecter des LANs individuels dans des WAN. Les routeurs, les boîtes magiques qui agit en tant que points d'interconnexion, avoir toutes les intelligences intégrées pour inspecter les paquets entrants et les transférer vers leur destination LAN éventuelle. Les routeurs sont, pour la plupart, automatiques. Ils nécessitent très peu de maintenance une fois leur configuration initiale terminée car ils peuvent se parler pour déterminer la meilleure façon d'envoyer les paquets IP (couche internet).

3.2. Définition du routage

Le routage est un processus de sélection du chemin le long duquel les données peuvent être transférées de la source à la destination. Le routage est effectué par un dispositif spécial appelé ***routeur***. Un routeur fonctionne au niveau de la couche réseau dans le modèle OSI et de la couche Internet dans le modèle TCP/IP. Un routeur est un périphérique réseau qui transfère le paquet en fonction des informations disponibles dans l'en-tête de paquet et la table de routage.

Les algorithmes de routage sont utilisés pour router les paquets. L'algorithme de routage n'est rien d'autre qu'un logiciel chargé de décider du chemin optimal par lequel les paquets peuvent être transmis. Les protocoles de routage utilisent ***la métrique*** pour déterminer le meilleur chemin pour la livraison des paquets. La métrique est la norme de mesure telle que le nombre de sauts, la bande passante, la charge actuelle sur le chemin, etc. utilisée par l'algorithme de routage pour déterminer le chemin optimal vers la destination. L'algorithme de routage initialise et maintient la table de routage pour le processus de détermination de chemin.

3.3. Métriques et coûts de routage

Les métriques et les coûts de routage sont utilisés pour déterminer le meilleur itinéraire (chemin) vers la destination. Les facteurs utilisés par les protocoles pour déterminer le chemin le plus court, ces facteurs sont connus sous le nom de ***métrique***. Pour certains

protocoles, utiliser les métriques statiques signifie que leur valeur ne peut pas être modifiée et pour certains autres protocoles de routage, utiliser les métriques dynamiques signifie que leur valeur peut être attribuée par l'administrateur système. La Figure 3.1 illustre les métriques les plus couramment utilisées.

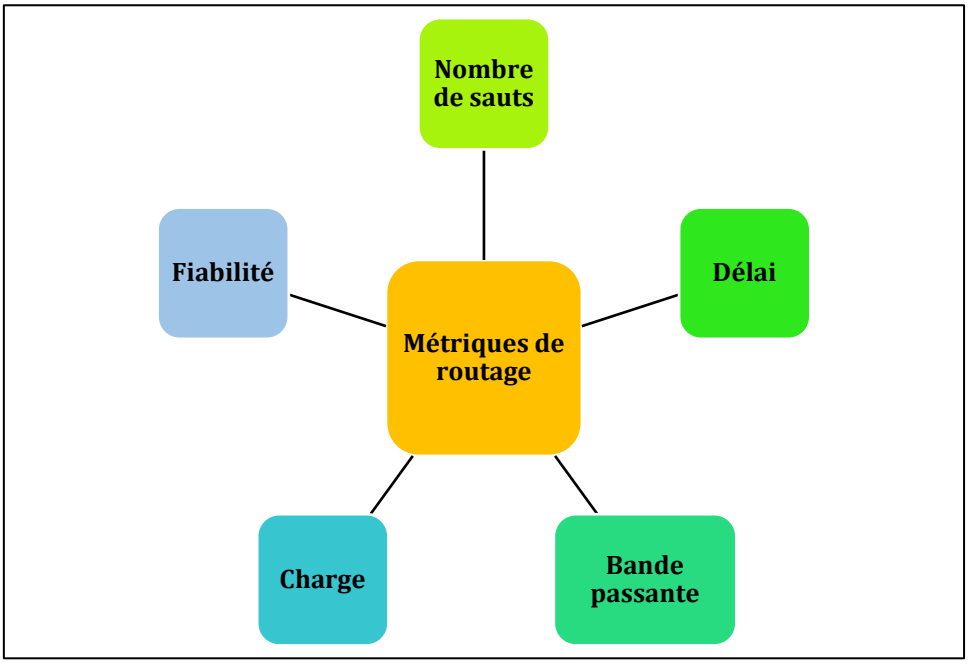


Figure 3.1. Les métriques de routage les plus utilisés

3.3.1.1. Le nombre de sauts

Le nombre de sauts est défini comme une métrique qui spécifie le nombre de passages via des périphériques d'interconnexion de réseaux tels qu'un routeur, un paquet doit circuler dans une route pour se déplacer de la source à la destination. Si le protocole de routage considère le saut comme une valeur de métrique primaire, alors le chemin avec ***le moins de sauts*** sera considéré comme le meilleur chemin pour se déplacer de la source à la destination.

3.3.1.2. Le délai

C'est un temps pris par le routeur pour traiter, mettre en file d'attente et transmettre un paquet à une interface. Les protocoles utilisent cette métrique pour déterminer les valeurs de retard pour toutes les liaisons le long du chemin de bout en bout. Le chemin ayant la valeur de retard la plus faible sera considérée comme le meilleur chemin.

3.3.1.3. La bande passante

La capacité du lien est connue sous le nom de bande passante du lien. La bande passante est mesurée en termes de bits par seconde. Le lien qui a un taux de transfert plus élevé

comme le gigabit est préféré au lien qui a la capacité inférieure. Le protocole déterminera la capacité de bande passante pour tous les liens le long du chemin, et la bande passante globale la plus élevée sera considérée comme la meilleure route.

3.3.1.4. La charge

La charge fait référence au degré d'occupation de la ressource réseau, telle qu'un routeur ou une liaison réseau. Une charge peut être calculée de différentes manières, telles que l'utilisation du processeur et les paquets traités par seconde. Si le trafic augmente, la valeur de charge sera également augmentée. La valeur de charge change en fonction de l'évolution du trafic.

3.3.1.5. La fiabilité

La fiabilité est un facteur métrique pouvant être composé d'une valeur fixe. Elle dépend des liens du réseau, et sa valeur est mesurée dynamiquement. Certains réseaux tombent plus souvent que d'autres. Après une défaillance du réseau, certains liens réseau se réparaient plus facilement que d'autres liens réseau. Tout facteur de fiabilité peut être pris en compte pour l'attribution des cotes de fiabilité, qui sont généralement des valeurs numériques attribuées par l'administrateur système.

3.4. Les types de routage

Le routage peut être classé en trois catégories : Routage statique, Routage dynamique et Routage par défaut.

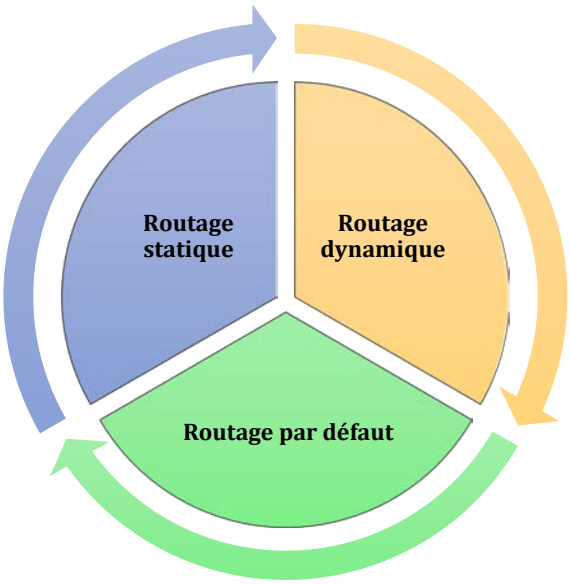


Figure 3.2. Les types de routage

3.4.1.1. Routage statique

Le routage statique est également connu sous le nom de routage non adaptatif. C'est une technique dans laquelle l'administrateur ajoute manuellement les routes dans une table de routage. Un routeur peut envoyer les paquets pour la destination le long de la route définie par l'administrateur. Dans cette technique, les décisions de routage ne sont pas prises en fonction de l'état ou de la topologie des réseaux. Dans ce type de routage l'utilisation du processeur du routeur n'est pas surchargée. Il assure aussi la sécurité car l'administrateur système n'est autorisé qu'à contrôler le routage vers un réseau particulier. Cependant pour un grand réseau, il devient très difficile d'ajouter manuellement chaque route à la table de routage.

3.4.1.2. Routage dynamique

Il est également connu sous le nom de routage adaptatif. C'est une technique dans laquelle un routeur ajoute une nouvelle route dans la table de routage en réponse aux changements de condition ou de topologie du réseau. Dans le routage dynamique, RIP et OSPF sont les protocoles utilisés pour découvrir les nouvelles routes.

Si un itinéraire tombe en panne, l'ajustement automatique sera effectué pour atteindre la destination. Le protocole dynamique doit avoir les fonctionnalités suivantes :

- Tous les routeurs doivent avoir le même protocole de routage dynamique pour échanger les routes.
- Si le routeur découvre un changement dans la condition ou la topologie, le routeur diffuse cette information à tous les autres routeurs.

Ce type de routage est plus efficace dans la sélection du meilleur itinéraire (chemin) en réponse aux changements de topologie. Au contraire au routage statique il est plus coûteux en termes d'utilisation du processeur et de la bande passante.

3.4.1.3. Routage par défaut

Le routage par défaut est une technique dans laquelle un routeur est configuré pour envoyer tous les paquets à la même interface de sortie afin d'atteint un router ou un hôte. Un paquet est transmis au router pour lequel il est configuré en routage par défaut.

Le routage par défaut est utilisé lorsque les réseaux possèdent un point de sortie unique. Il est également utile lorsque la majeure partie des réseaux de transmission doit transmettre les données à la même machine (router, hôte, etc.). Lorsqu'une route spécifique est mentionnée dans la table de routage, le routeur choisira la route spécifique

plutôt que la route par défaut. La route par défaut est choisie uniquement lorsqu'une route spécifique n'est pas mentionnée dans la table de routage.

3.5. Table de routage

Une table de routage est un ensemble de règles, souvent affichées sous forme de tableau, qui est utilisé pour déterminer où les paquets de données circulant sur un réseau IP seront dirigés. Tous les appareils compatibles IP, y compris les routeurs et les commutateurs, utilisent des tables de routage.

La table de routage est remplie par les manières suivantes :

- Les réseaux directement connectés sont ajoutés automatiquement.
- Utilisation du routage statique.
- Utilisation du routage dynamique.

Voir la table de routage ci-dessous :

Tableau 3.1. Exemple d'une table de routage

Destination	Masque de sous-réseau	Métrique	Interface /saut suivant
180.1.5.0	255.255.255.0	2	Eth0
11.12.40.0	255.255.255.0	5	Fe0
55.0.2.0	255.255.255.0	1	GbE0
Défaut	/		Eth1

Une table de routage contient les informations nécessaires pour transmettre un paquet le long du meilleur chemin vers sa destination. Chaque paquet contient des informations sur son origine et sa destination. La table de routage fournit au routeur des instructions pour envoyer le paquet au saut suivant sur son itinéraire à travers le réseau. Chaque entrée de la table de routage se compose des entrées suivantes :

- **Identifiant réseau :** L'adresse réseau ou la destination correspondant à l'itinéraire.
- **Masque de sous-réseau :** Masque utilisé pour faire correspondre une adresse IP de destination à l'adresse réseau.
- **Métrique :** utilisé pour déterminer le meilleur chemin vers la destination.
- **Saut suivant :** L'adresse IP à laquelle le paquet est transféré
- **Interface sortante :** Interface sortante que le paquet doit sortir pour atteindre le réseau de destination.

3.6. Fonctionnement du routage

Les routeurs et les hôtes dans un réseau TCP/IP fonctionnent ensemble pour effectuer le routage. Le système d'exploitation hôte dispose d'un logiciel TCP/IP, y compris le logiciel qui implémente la couche réseau. Les hôtes utilisent ce logiciel pour choisir où envoyer les paquets IP, souvent à un routeur à proximité. Ces routeurs choisissent où envoyer ensuite le paquet IP. Ensemble, les hôtes et les routeurs transmettent le paquet IP à la bonne destination, comme indiqué dans l'exemple de la Figure 3.3.

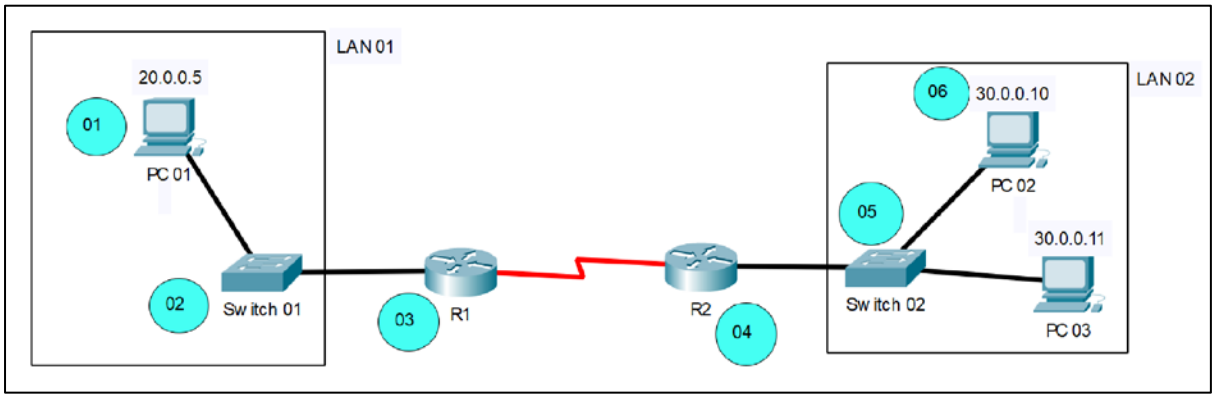


Figure 3.3. Exemple de routage

« Étape 01 » : Le PC 01 créé le paquet IP, l'encapsule dans une trame et le transmettre au switch 01

« Étape 02 » : Le switch 01 reçois la trame et le transmettre au R1 (router 1).

« Étape 03 » : Le R1 examine l'adresse de destination et la compare aux itinéraires de sa table de routage, il trouve un itinéraire vers la destination via R2

« Étape 04 » : Le R2 effectue le même traitement que R1, puis il transmettre le paquet au switch 02.

« Étape 05 » : Le switch 02 envoi le paquet au PC 02.

« Étape 06 » : Le PC 02 reçois le paquet et le trait.

3.7. Les schémas de routage (d'adressage)

Les schémas de routage diffèrent dans la manière dont ils délivrent les messages.

3.7.1. Le routage Unicast

La plupart du trafic sur Internet et sur les intranets, connu sous le nom de trafic unicast, est envoyé avec une destination spécifiée. Le routage des données monodiffusion sur Internet est appelé routage unicast. C'est la forme de routage la plus simple car la

destination est déjà connue. Par conséquent, le routeur n'a qu'à consulter la table de routage et à transmettre le paquet au prochain saut. (Voir la Figure 3.4)

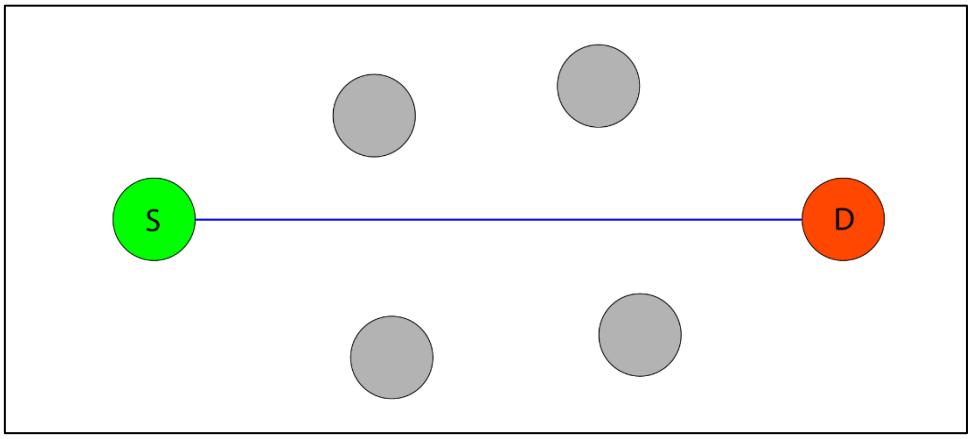


Figure 3.4. Routage unicast

3.7.2. Le routage Broadcast

Par défaut, les paquets broadcast ne sont pas routés et transmis par les routeurs sur aucun réseau. Les routeurs créent des domaines de diffusion. Mais il peut être configuré pour transférer des paquets broadcast dans certains cas particuliers. Le routage de diffusion peut se faire de deux manières (algorithme) :

- Un routeur crée un paquet de données puis l'envoie à chaque hôte un par un. Dans ce cas, le routeur crée plusieurs copies d'un seul paquet de données avec différentes adresses de destination. Tous les paquets sont envoyés en unicast, mais comme ils sont envoyés à tous, cela simule comme si le routeur diffusait.
- Lorsque le routeur reçoit un paquet qui doit être diffusé, il inonde simplement ces paquets de toutes les interfaces. Tous les routeurs sont configurés de la même manière.

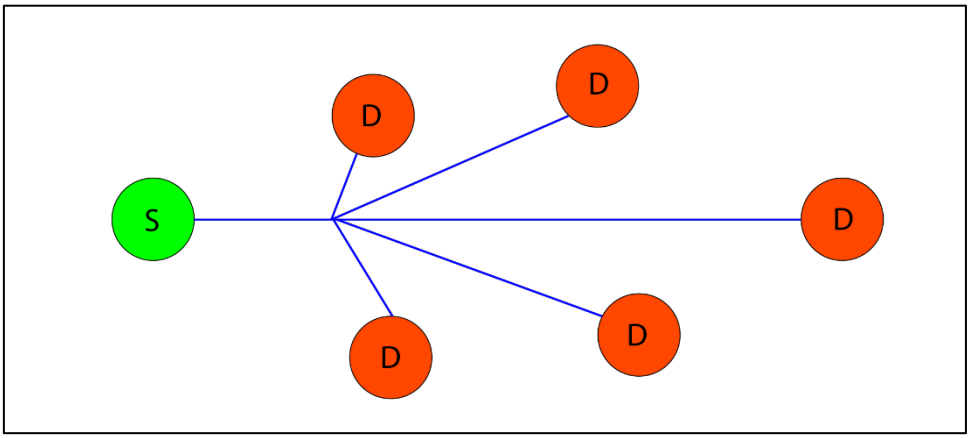


Figure 3.5. Routage Broadcast

3.7.3. Le routage Multicast

Le routage multicast est un cas particulier de routage de diffusion (broadcast) avec une différence d'importance et des défis. Dans le routage broadcast, les paquets sont envoyés à tous les nœuds même s'ils ne le souhaitent pas. Mais dans le routage multicast, les données sont envoyées uniquement aux nœuds qui souhaitent recevoir les paquets.

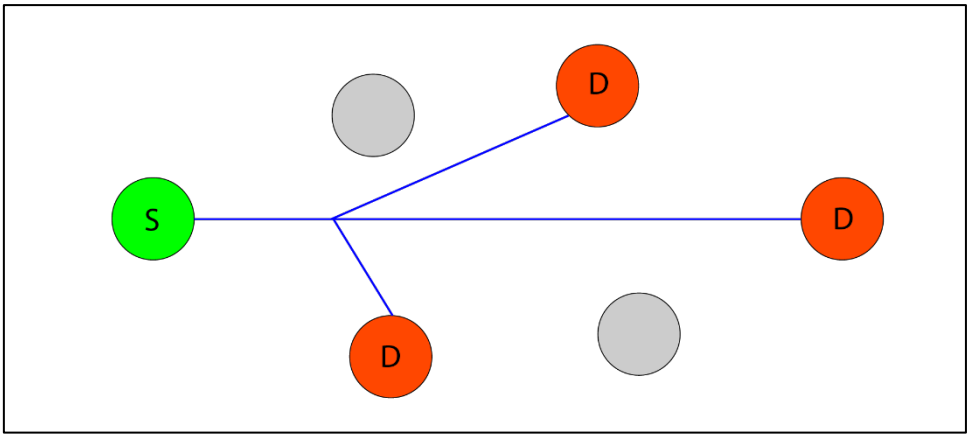


Figure 3.6. Routage Multicast

3.7.4. Le routage Anycast

Le transfert de paquets anycast est un mécanisme dans lequel plusieurs hôtes peuvent avoir la même adresse logique. Lorsqu'un paquet destiné à cette adresse logique est reçu (par un routeur), il est envoyé à l'hôte le plus proche dans la topologie de routage. Le routage anycast est effectué à l'aide du serveur DNS. Chaque fois qu'un paquet anycast est reçu, il est demandé au DNS où l'envoyer. DNS fournit l'adresse IP qui est l'IP la plus proche configurée dessus.

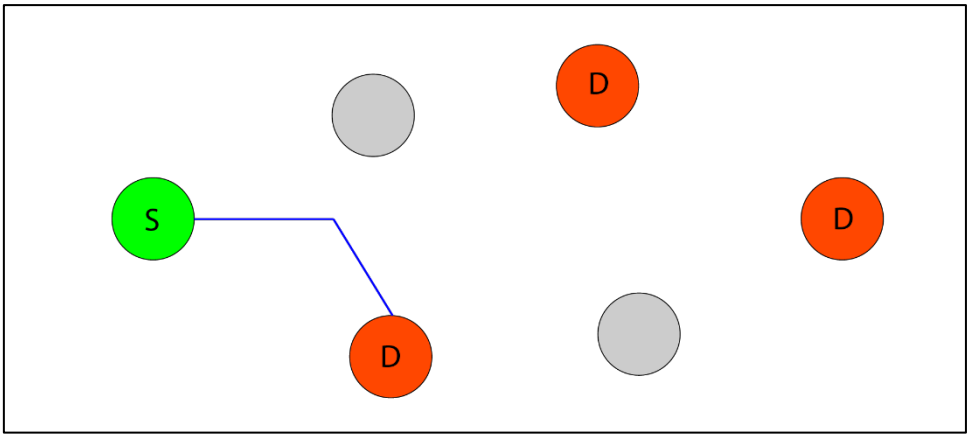


Figure 3.7. Routage Anycast

Chapitre 4 : Routage unicast et multicast

4.1. Introduction

Il existe de nombreux schémas de routage, l'utilisation d'un schéma de routage dépend principalement de la situation et de l'objectif visé. Nous disposons de plusieurs types de schémas de routage ou d'adressage tel que le routage unicast, multicast, broadcast, et anycast. Dans ce chapitre nous allons concentrer sur les schémas de routage unicast et multicast, en discutant les plus connus protocoles de chacun de ces schémas.

4.2. Protocole de routage

Les routeurs ajoutent des routes à leurs tables de routage en utilisant trois méthodes : routes directement connectées, routes statiques et routes apprises à l'aide de protocoles de routage dynamique. Le processus de routage transmet les paquets IP, mais si un routeur n'a pas de routes dans sa table de routage IP qui correspondent à la destination d'un paquet, le routeur rejette le paquet. Parmi les fonctionnalités d'un protocole de routage nous avons les suivantes :

- Découvrez les informations de routage sur les sous-réseaux dès les routeurs voisins.
- Annoncez les informations de routage sur les sous-réseaux aux routeurs voisins.
- S'il existe plusieurs routes possibles pour atteindre un sous-réseau, choisissez la meilleure route en fonction de métrique.
- Si la topologie du réseau change (par exemple, une liaison échoue), réagissez en annonçant que certaines routes ont échoué et choisissez une nouvelle route. (Ce processus est appelé ***convergence***)

Les protocoles de routage appartiennent à l'une des deux principales catégories :

- **IGP** (**interior gateway protocols**) : protocole de routage conçu et destiné à être utilisé à l'intérieur d'un seul système autonome
- **EGP** (**exterior gateway protocols**) : protocole de routage conçu et destiné à être utilisé entre différents systèmes autonomes

Complément :

Un système autonome est un réseau sous le contrôle administratif d'une seule organisation. Chaque fournisseur de services Internet (comme Algérie Télécom) est généralement un seul système autonome.

La Figure 4.1 montre la localisation de chaque catégorie de protocoles.

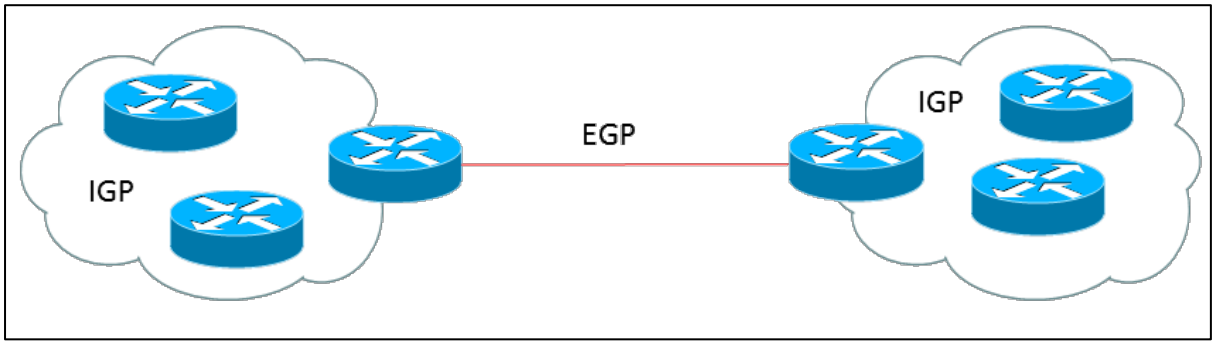


Figure 4.1. Emplacements des IGP et des EGP

4.3. Protocoles de routage unicast

Il existe deux types de protocoles de routage utilisé pour router les paquets unicast

4.3.1. Protocole de routage à vecteur de distance

Ce type de protocole est simple, il prend la décision de routage sur le nombre de sauts entre la source et la destination. Une route avec moins de sauts est considérée comme la meilleure route. Chaque routeur annonce ses meilleures routes aux autres routeurs. En fin de compte, tous les routeurs construisent leur topologie de réseau en fonction des annonces de leurs routeurs voisins, par exemple, nous avons les protocoles : RIP et IGRP.

4.3.1.1. RIP (Routing Information Protocol)

Le RIP est un protocole de routage intra-domaine utilisé au sein d'un système autonome. Pour comprendre le protocole RIP, notre objectif principal est de connaître la structure du paquet, le nombre de champs qu'il contient et comment ces champs déterminent la table de routage. RIP est basé sur la stratégie de vecteur de distance, nous considérons donc la structure entière comme un graphe où les nœuds sont les routeurs et les liens sont les réseaux. Dans une table de routage, la première colonne est la destination, ou on peut dire qu'il s'agit d'une adresse réseau. La métrique de coût est le nombre de sauts pour atteindre la destination, ce nombre de sauts est le nombre de réseaux nécessaires

pour atteindre la destination. Dans RIP, l'infini est défini par la valeur 16, ce qui signifie que le RIP est utile pour les petits réseaux ou les petits systèmes autonomes. Le nombre maximum de sauts que RIP peut contenir est de 15 sauts. Une autre colonne contient l'adresse du routeur auquel le paquet doit être envoyé pour atteindre la destination. Lorsque le routeur envoie le paquet au segment de réseau, il est compté comme un seul saut.

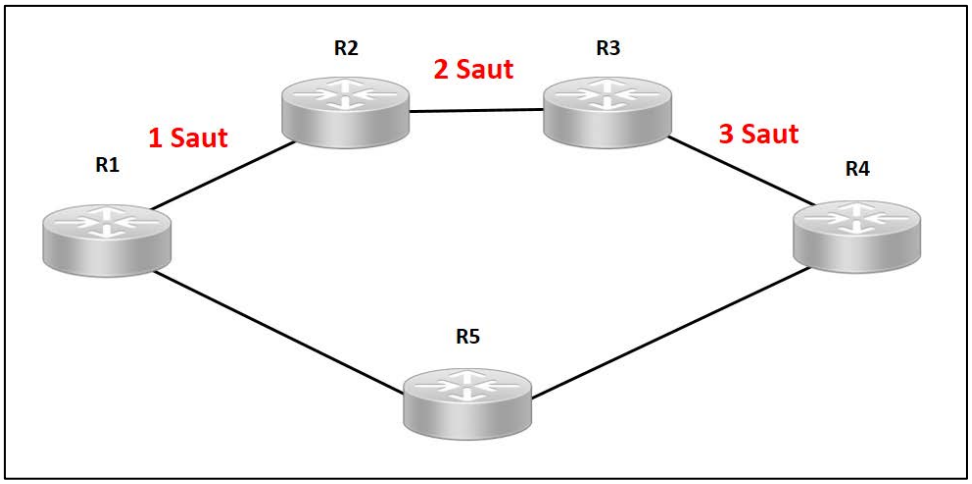


Figure 4.2. Le calcul de nombre de saut par le RIP

Dans la figure ci-dessus, lorsque le routeur 1 transfère le paquet au routeur 2, cela comptera comme 1 saut. De même, lorsque le routeur 2 transmet le paquet au routeur 3, cela comptera comme un nombre de 2 sauts, et lorsque le routeur 3 transmet le paquet au routeur 4, cela comptera comme un nombre de 3 sauts. De la même manière, RIP peut prendre en charge jusqu'à maximum de 15 sauts.

4.3.1.1.1. Format de message RIP

Le format de message est utilisé pour partager des informations entre différents routeurs. Le RIP contient les champs suivants dans un message :

- **Commande :** il s'agit d'un champ de 8 bits utilisé pour la demande ou la réponse. La valeur de la requête est 1 et la valeur de la réponse est 2.
- **Version :** Ici, la version signifie la version du protocole que nous utilisons. Supposons que nous utilisons le protocole de la version 1, alors nous mettons le 1 dans ce champ.
- **Réservé :** il s'agit d'un champ réservé, il est donc rempli de zéros.
- **Famille :** C'est un champ de 16 bits. Comme nous utilisons la famille TCP/IP, nous mettons donc la valeur 2 dans ce champ.

- **Adresse réseau :** Elle est définie comme un champ de 14 octets. Si nous utilisons la version IPv4, nous utilisons 4 octets et les 10 autres octets sont tous des zéros.
- **Distance** : le champ de distance spécifie le nombre de sauts, c'est-à-dire le nombre de sauts utilisés pour atteindre la destination.

4.3.1.1.2. Fonctionnement de RIP

S'il y a 8 routeurs dans un réseau où le routeur 1 veut envoyer les données au routeur 8. Il choisira la route qui a le moins de sauts. Il y a trois routes dans le réseau de la Figure 4.3, la route 1, la route 2 et la route 3. La route 1 a le nombre minimal de sauts, c'est-à-dire 2 où les routes 2 et 3 ayant un nombre de sauts de 3 et 4 respectivement, donc RIP choisira la route 1.

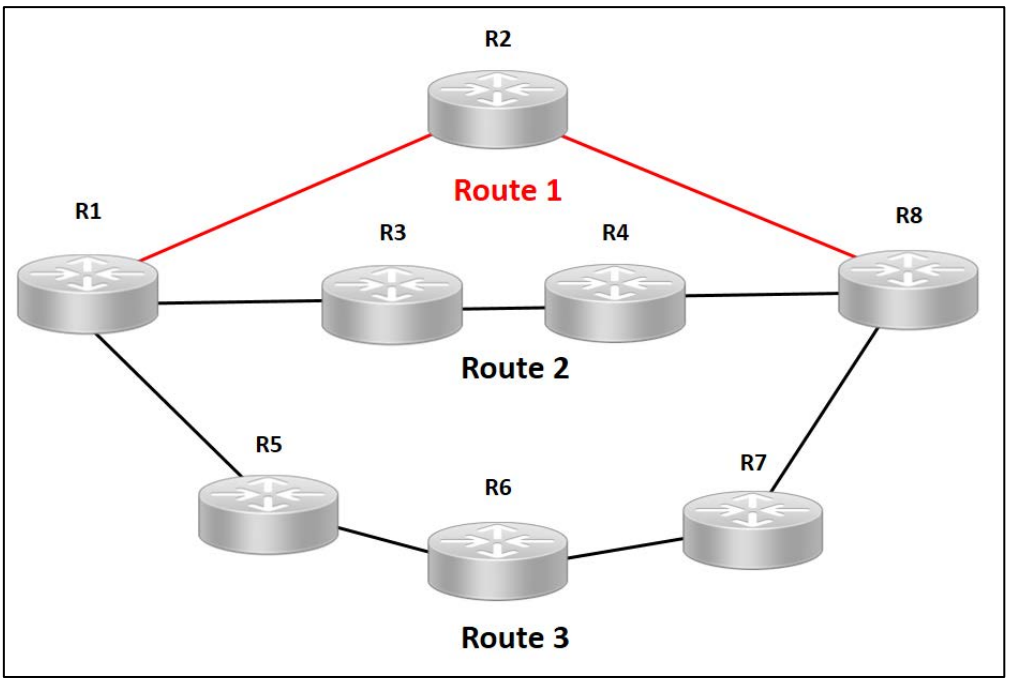


Figure 4.3. La sélection de route par le RIP

Les minuteurs suivants sont utilisés pour mettre à jour la table de routage :

- **Minuterie de mise à jour :** le délai par défaut pour l'échange d'informations de routage par les routeurs utilisant RIP est de 30 secondes. À l'aide d'un temporisateur de mise à jour, les routeurs échangent périodiquement leur table de routage.
- **Minuterie invalide :** si aucune mise à jour n'arrive avant 180 secondes, le routeur de destination la considère comme invalide. Dans ce scénario, le saut de marque du routeur de destination compte comme 16 pour ce routeur.
- **Temps de flush :** C'est le temps après lequel l'entrée de l'itinéraire sera vidée s'il ne répond pas dans le temps de flush. Il est de 60 secondes par défaut. Cette minuterie

démarre après que la route a été déclaré invalide, c'est-à-dire que le temps sera de 180 + 60 = 240 secondes

Complément :

Dans le cas où nous avons que deux routes qui ayant le même nombre de saut, le RIP enverra les données via les deux routes simultanément. De cette façon, il gère l'équilibrage de charge et les données atteignent la destination un peu plus rapidement.

4.3.1.2. IGRP (Interior Gateway Routing Protocol)

Est un protocole propriétaire de routage à vecteur de distance utilisé pour échanger des informations de routage. Le protocole IGRP régule le transfert des informations de routage entre les routeurs liés du réseau hôte ou du système autonome. Le protocole garantit que la table de routage de chaque routeur est tenue à jour avec la route la plus directe disponible. IGRP aide également à minimiser les boucles de routage en se mettant à jour en réponse aux changements qui se produisent sur le réseau et en implémentant la gestion des erreurs.

Parmi les caractéristiques de l'IGRP :

- Protocole de routage à vecteur de distance créé par Cisco.
- La bande passante, le délai (par défaut), la fiabilité, la charge et la MTU sont tous mesurés dans le protocole IGRP.
- Il transmet des mises à jour toutes les 90 secondes, avec un temps de maintien de 280 secondes entre chaque session de diffusion.
- Lorsque des changements de réseau se produisent, des mises à jour déclenchées sont utilisées pour accélérer le processus de convergence.
- La commande de routeur IGRP nécessite l'inclusion d'un numéro de système autonome.
- Pour que les routeurs communiquent des informations de routage, ils doivent être dans le même numéro de système autonome.
- Le nombre maximum de sauts autorisés par IGRP est de 255. Il a une valeur par défaut de 100 et est souvent modifié à 50 ou moins.

4.3.1.3. EIGRP (Enhanced Interior Gateway Routing Protocol)

Le protocole EIGRP est un protocole de routage à vecteur de distance qui comprend des fonctions disponibles dans les protocoles de routage à état de liens. Ce protocole convient à de nombreux supports et topologies différents. Dans un réseau bien conçu, le protocole EIGRP peut mettre à l'échelle pour inclure plusieurs topologies et peut fournir des temps de convergence extrêmement rapides avec un trafic réseau minimal.

4.3.2. Protocole de routage d'état de lien

Les protocoles état de lien sont légèrement plus compliqués que les protocoles à vecteur de distance. Il prend en compte les états des liens de tous les routeurs d'un réseau. Cette technique aide les routeurs à construire un graphe commun de l'ensemble du réseau. Tous les routeurs calculent ensuite leur meilleur chemin à des fins de routage, par exemple, nous avons les protocoles : OSPF et ISIS.

4.3.2.1. OSPF (Open Shortest Path First)

C'est un protocole de routage largement utilisé et pris en charge. C'est un protocole intra-domaine, ce qui signifie qu'il est utilisé au sein d'une zone ou d'un réseau. Il s'agit d'un protocole de passerelle intérieure qui a été conçu au sein d'un seul système autonome. Il est basé sur un algorithme de routage à état de liens dans lequel chaque routeur contient les informations de chaque domaine, et sur la base de ces informations, il détermine le chemin le plus court. Le but du routage est d'apprendre des routes. L'OSPF y parvient en apprenant chaque routeur et sous-réseau de l'ensemble du réseau. Chaque routeur contient les mêmes informations sur le réseau. La façon dont le routeur apprend ces informations en envoyant des LSA (Link State Advertisements). Ces LSA contiennent des informations sur chaque routeur, sous-réseau et autres informations de mise en réseau. Une fois que les LSA ont été inondés, l'OSPF stocke les informations dans une base de données d'état de liens connue sous le nom de LSDB. L'objectif principal est d'avoir les mêmes informations sur chaque routeur dans une LSDB.

OSPF divise les systèmes autonomes en zones (Figure 4.4) où la zone est un ensemble de réseaux, d'hôtes et de routeurs. Les routeurs qui existent à l'intérieur de la zone inondent la zone avec les informations de routage. Chaque zone à des routeurs spéciaux qui sont présents à la frontière de la zone, ces routeurs spéciaux sont connus sous le nom de routeurs frontaliers de zone. Ces routeurs résument les informations sur une zone et partage les informations avec d'autres zones.

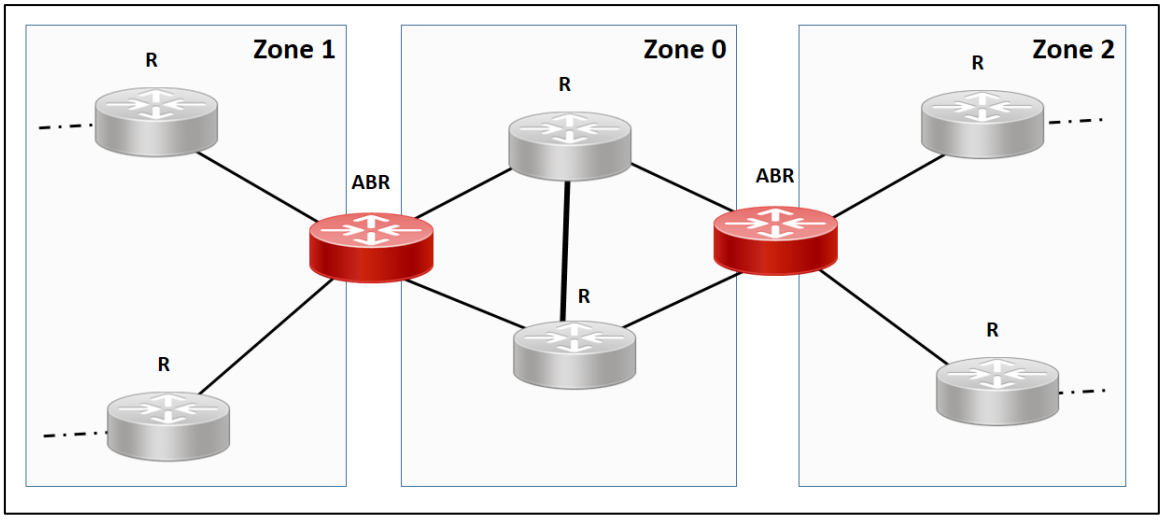


Figure 4.4. OSPF Zones

4.3.2.1.1. Format de message OSPF

Le message du OSPF contient les champs suivants :

- **Version :** Il représente la version du protocole
- **Type** : représente le type (1–5) du message OSPF.
  - Type 1 : message « hello »
  - Type 2 : description
  - Tape 3 : demande
  - Type 4 : mise à jour
  - Type 5 : accuser réception des messages d'état de liaison
- **Longueur** : représente la longueur du message à échanger
- **ID Routeur** : identifie l'expéditeur.
- **ID Zone :** identifiant de 32 bits de la zone dans laquelle se trouve le nœud (routeur)
- **Somme de contrôle :** Somme de contrôle Internet 16 bits.
- **Type d'authentification :** « 0 » signifie qu'aucune authentification n'est disponible, « 1 » (mot de passe normal), « 2 » (authentification cryptographique).
- **Authentification :** Il contient un mot de passe ou une somme de contrôle cryptographique

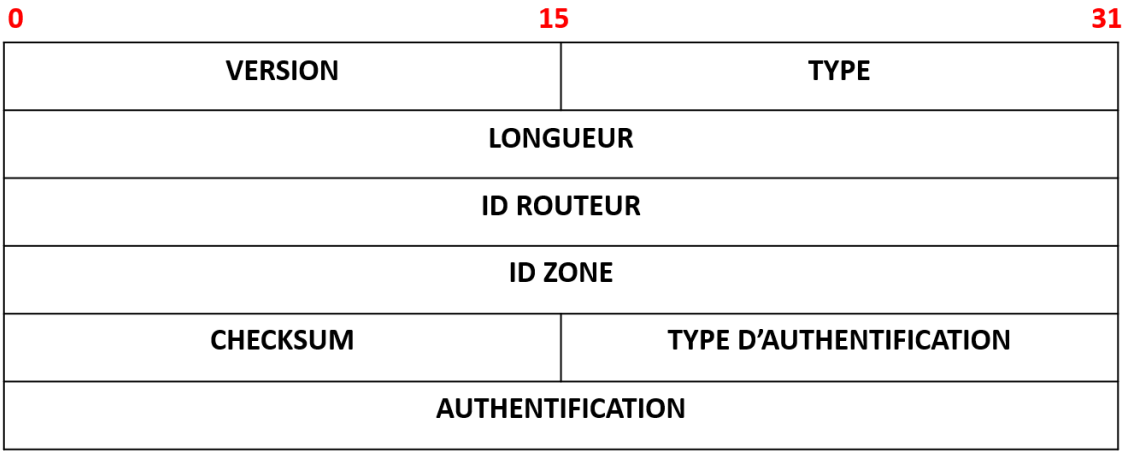


Figure 4.5. Les champs du message OSPF

4.3.2.1.2. Fonctionnement de OSPF

Il y a trois étapes qui peuvent expliquer le fonctionnement d'OSPF :

Étape 1 : La première étape consiste à devenir des voisins OSPF. Les deux routeurs de connexion exécutant OSPF sur le même lien créent une relation de voisinage.

Étape 2 : La deuxième étape consiste à échanger les informations de la base de données. Après être devenus voisins, les deux routeurs échangent les informations LSDB entre eux.

Étape 3 : La troisième étape consiste à choisir la meilleure route. Une fois que les informations LSDB ont été échangées entre elles, le routeur choisit la meilleure route à ajouter à une table de routage en fonction du calcul de plus court chemin.

4.3.2.1.3. La formulation de la relation de voisinage

La première chose qui se passe avant la formation de la relation est que chaque routeur choisit l'ID du routeur.

ID de routeur (RID) : l'ID de routeur est un numéro qui identifie de manière unique chaque routeur sur un réseau. L'ID du routeur est au format de l'adresse IPv4. Il existe plusieurs façons de définir l'ID du routeur, la première consiste à définir l'ID du routeur manuellement et l'autre consiste à laisser le routeur décider lui-même.

Lorsque deux routeurs connectés entre eux point à point, ils ne sont adjacents que lorsque les deux routeurs s'envoient le paquet HELLO. Lorsque les deux routeurs reçoivent l'accusé de réception du paquet HELLO, ils entrent dans un état bidirectionnel. Comme OSPF est un protocole de routage à état de liaison, il permet donc de créer la relation de voisinage entre les routeurs. Les deux routeurs peuvent être voisins uniquement lorsqu'ils appartiennent au même sous-réseau, partagent le même

identifiant de zone, le même masque de sous-réseau, les mêmes minuteries et la même authentification. La relation OSPF est une relation formée entre les routeurs afin qu'ils puissent se connaître. Les deux routeurs peuvent être voisins si au moins l'un d'eux est un routeur désigné ou routeur désigné de secours dans un réseau, ou connecté par une liaison point à point.

Complément :

OSPF choisit un routeur pour servir de routeur désigné et un autre routeur sur le segment pour agir comme routeur désigné de secours. Cela minimise la quantité d'informations répétitives transmises sur le réseau. OSPF transmet tous les messages au routeur désigné.

4.3.2.1.4. Types de liens dans OSPF

Un lien est principalement une connexion, donc la connexion entre deux routeurs est appelée lien. Il existe quatre types de liens dans OSPF :

Point-to-point link : la liaison point à point connecte directement les deux routeurs sans hôte ni routeur entre eux.

Transient link: lorsque plusieurs routeurs sont connectés dans un réseau, on parle de liaison transitoire.

Le lien transitoire a deux implémentations différentes :

- Topologie irréaliste : lorsque tous les routeurs sont connectés les uns aux autres, on parle de topologie irréaliste.
- Topologie réaliste : lorsqu'un routeur désigné existe dans un réseau, il s'agit d'une topologie réaliste. Ici, le routeur désigné est un routeur auquel tous les routeurs sont connectés. Tous les paquets envoyés par les routeurs passeront par le routeur désigné.

Stub link: C'est un réseau qui est connecté au routeur unique. Les données entrent dans le réseau via le routeur unique et quittent le réseau via le même routeur.

Virtual link: Si le lien entre les deux routeurs est rompu, l'administration crée le chemin virtuel entre les routeurs, et ce chemin peut être long également.

4.3.2.1.5. Les types de paquet OSPF

Il existe cinq types de paquets dans OSPF :

- **Hello paquet :** Le paquet Hello est utilisé pour créer une relation de voisinage et vérifier l'accessibilité du voisin. Par conséquent, le paquet Hello est utilisé lorsque la connexion entre les routeurs doit être établie.
- **Description de la base de données :** Après avoir établi une connexion, si le routeur voisin communique avec le système pour la première fois, il envoie les informations de la base de données sur la topologie du réseau au système afin que le système puisse mettre à jour sa base de données.
- **Demande d'état de lien :** La demande d'état de lien est envoyée par le routeur pour obtenir les informations d'une route spécifiée. Supposons qu'il y ait deux routeurs, le routeur 1 et le routeur 2, et que le routeur 1 veuille connaître les informations sur le routeur 2, donc le routeur 1 envoie la demande d'état de lien au routeur 2. Lorsque le routeur 2 reçoit la demande d'état de liaison, alors il envoie les informations d'état des liens au routeur 1.
- **Mise à jour de l'état des liens :** La mise à jour de l'état des liens est utilisée par le routeur pour annoncer l'état de ses liens. Si un routeur souhaite diffuser l'état de ses liens, il utilise la mise à jour de l'état des liens.
- **Reconnaissance de l'état du lien :** L'accusé de réception de l'état des liens rend le routage plus fiable en forçant chaque routeur à envoyer l'accusé de réception à chaque mise à jour de l'état des liens. Par exemple, le routeur A envoie la mise à jour de l'état des liens au routeur B et au routeur C, puis en retour, les routeurs B et C envoient l'accusé de réception de l'état des liens au routeur A, de sorte que le routeur A sache que les deux routeurs ont reçu la mise à jour de l'état des liens.

4.3.2.2. IS-IS (Immediate system-to-immediate system)

IS-IS, classé comme un protocole a état de lien, ce protocole utilise une version modifiée de l'algorithme de Dijkstra. Habituellement, le protocole organise les routeurs en groupes pour créer des domaines plus grands et connecter les routeurs pour le transfert de données. IS-IS utilise fréquemment ces deux types de réseaux :

- Point d'accès au service réseau : Semblable à une adresse IP, il est l'identification d'un point d'accès au service dans les systèmes qui utilisent le modèle OSI.
- Titre d'entité réseau : cela permet d'identifier les routeurs réseau individuels au sein de réseaux informatiques plus importants.

4.4. Protocoles de routage multicast

La multidiffusion (multicast) est une méthode de communication de groupe dans laquelle l'expéditeur envoie simultanément des données à plusieurs récepteurs ou nœuds présents sur le réseau. La multidiffusion est un type de communication un à plusieurs et plusieurs à plusieurs, car elle permet à l'expéditeur ou aux expéditeurs d'envoyer des paquets de données à plusieurs destinataires à la fois sur des LAN ou des WAN.

Un groupe de multidiffusion identifie un ensemble de destinataires intéressés par un flux de données particulier et est représenté par une adresse IP d'une plage bien définie. Les données envoyées à cette adresse IP sont transmises à tous les membres du groupe de multidiffusion.

Les routeurs entre la source et les destinataires dupliquent les paquets de données et transmettent plusieurs copies partout où le chemin vers les destinataires diverge. Les informations d'appartenance au groupe sont utilisées pour calculer les meilleurs routeurs sur lesquels dupliquer les paquets dans le flux de données afin d'optimiser l'utilisation du réseau.

Un hôte source envoie des données à un groupe de multidiffusion en définissant simplement l'adresse IP de destination du paquet comme étant l'adresse du groupe de multidiffusion. N'importe quel hôte peut devenir une source et envoyer des données à un groupe de multidiffusion. Les sources n'ont pas besoin de s'enregistrer avant de pouvoir commencer à envoyer des données à un groupe et n'ont pas besoin d'être elles-mêmes membres du groupe. Il existe de nombreux protocoles et modes de fonctionnement multidiffusion comme : IGMP et PIM.

4.4.1. IGMP (Internet Group Management Protocol)

IGMP est un protocole de communication utilisé par les hôtes et les routeurs adjacents pour la communication multidiffusion avec les réseaux IP et utilise efficacement les ressources pour transmettre les paquets de messages/données. La communication multidiffusion (multicast) peut avoir un ou plusieurs expéditeurs et récepteurs et, par conséquent, IGMP peut être utilisé dans les vidéos en streaming, les jeux ou les outils de conférence Web. Ce protocole est utilisé sur les réseaux IPv4. Comme d'autres protocoles réseau, IGMP est utilisé sur la couche réseau. Le protocole de communication IGMPv1 a été développé en 1989 à l'Université de Stanford. IGMPv1 a été mis à jour vers IGMPv2 en 1997 et à nouveau mis à jour vers IGMPv3 en 2002.

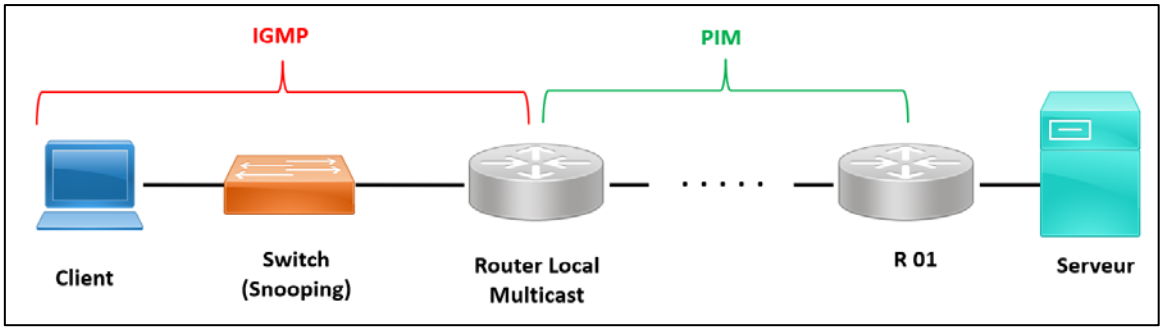


Figure 4.6. L'architecture de IGMP

4.4.1.1. Fonctionnement de IGMP

IGMP fonctionne sur des appareils capables de gérer des groupes de multidiffusion et de la multidiffusion dynamique. Ces appareils permettent à l'hôte de rejoindre ou de quitter l'adhésion au groupe de multidiffusion. Ces appareils permettent également d'ajouter et de supprimer des clients du groupe. Ce protocole de communication est exploité entre l'hôte et le routeur multicast local. Lorsqu'un groupe de multidiffusion est créé, l'adresse du groupe de multidiffusion se trouve dans la plage d'adresses IP de classe D (224-239) et est transmise en tant qu'adresse IP de destination dans le paquet.

Les périphériques de niveau 2 tels que les commutateurs (switches) sont utilisés entre l'hôte et le routeur multicast pour la surveillance (snooping) IGMP. La surveillance IGMP est un processus permettant d'écouter le trafic réseau IGMP de manière contrôlée. Le commutateur reçoit le message de l'hôte et transmet le rapport d'appartenance au routeur multicast local. Le trafic de multidiffusion est ensuite transmis aux routeurs distants à partir de routeurs de multidiffusion locaux à l'aide de PIM (Protocol Independent Multicast) afin que les clients puissent recevoir les paquets de messages/données. Les clients souhaitant rejoindre le réseau envoient un message de jointure dans la requête et le commutateur intercepte le message et ajoute les ports des clients à sa table de routage multidiffusion.

4.4.1.2. Format du message IGMP

Le message du IGMP contient les champs suivants :

- **Type** :
  - 0x11 pour la requête d'adhésion
  - 0x12 pour le rapport d'adhésion IGMPv1
  - 0x16 pour le rapport d'adhésion IGMPv2
  - 0x22 pour le rapport d'adhésion IGMPv3

- 0x17 pour quitter le groupe

- **Temps réponse maximum :** Ce champ est ignoré pour les types de messages autres que la requête d'adhésion. Pour le type de requête d'adhésion, il s'agit du délai maximum autorisé avant l'envoi d'un rapport de réponse. La valeur est en unités de 0,1 seconde
- **Somme de contrôle :** C'est le complément à un de la somme des messages IGMP.
- **Adresse de groupe :** Elle est définie sur 0 lors de l'envoi d'une requête générale, sinon, c'est l'adresse de multidiffusion pour les requêtes spécifiques au groupe ou à la source.

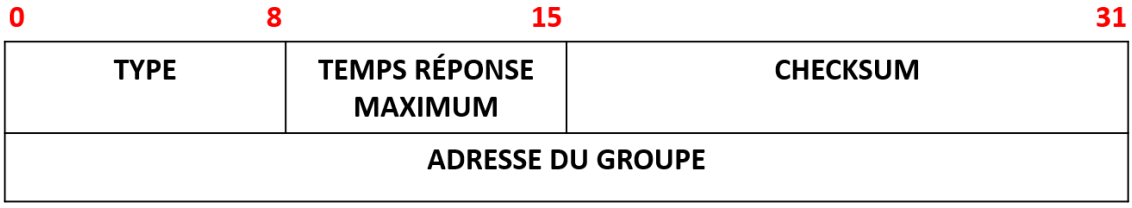


Figure 4.7. Format du message IGMP

4.4.1.3. Types des messages IGMP

- **Rapports d'adhésion :** les appareils les envoient à un routeur multidiffusion afin de devenir membre d'un groupe multidiffusion.
- **Messages « Quitter le groupe » :** ces messages vont d'un appareil à un routeur et permettent aux appareils de quitter un groupe de multidiffusion.
- **Requêtes générales d'adhésion :** un routeur compatible multidiffusion envoie ces messages à l'ensemble du réseau d'appareils connectés pour mettre à jour l'appartenance au groupe multidiffusion pour tous les groupes du réseau.
- **Requêtes d'appartenance spécifiques à un groupe :** les routeurs envoient ces messages à un groupe de multidiffusion spécifique, au lieu de l'ensemble du réseau.

4.4.1.4. La surveillance (Snooping) IGMP

IGMP est un protocole de couche réseau, et seuls les périphériques réseau qui fonctionnent au niveau la couche réseau peuvent envoyer et recevoir des messages. Les commutateurs réseau fonctionne que dans la couche 2. Par conséquent, un commutateur ne sait pas quels périphériques réseau font partie de groupes de multidiffusion et lesquels n'en font pas partie, il peut finir par transférer le trafic multidiffusion vers des

périphériques qui n'en ont pas besoin, ce qui consomme de la bande passante réseau et de la puissance de traitement des périphériques, ralentissant ainsi l'ensemble du réseau. La surveillance « **Snooping** » IGMP résout ce problème en permettant aux commutateurs de « surveiller » les messages IGMP. Généralement, un commutateur de couche 2 ne serait pas au courant des messages IGMP, mais il peut les écouter via la surveillance IGMP.
Cela leur permet d'identifier où les messages de multidiffusion doivent être transférés, de sorte que seuls les appareils appropriés reçoivent le trafic de multidiffusion.

4.4.2. PIM (Protocol Independent Multicast)

PIM est un ensemble de protocoles de routage multidiffusion, chacun optimisé pour un environnement différent. Il existe deux principaux protocoles PIM, le mode PIM Sparse et le mode PIM Dense. Un troisième protocole PIM, PIM bidirectionnel, est moins utilisé.
Généralement soit le mode **PIM Sparse ou le mode PIM Dense** seront utilisés dans un domaine de multidiffusion. Cependant, ils peuvent également être utilisés ensemble au sein d'un même domaine, en utilisant le mode sparse pour certains groupes et le mode dense pour d'autres. Tous les protocoles PIM partagent un format de message de contrôle commun. Les messages de contrôle PIM sont envoyés sous forme de paquet IP bruts.

4.4.2.1. Les composants PIM

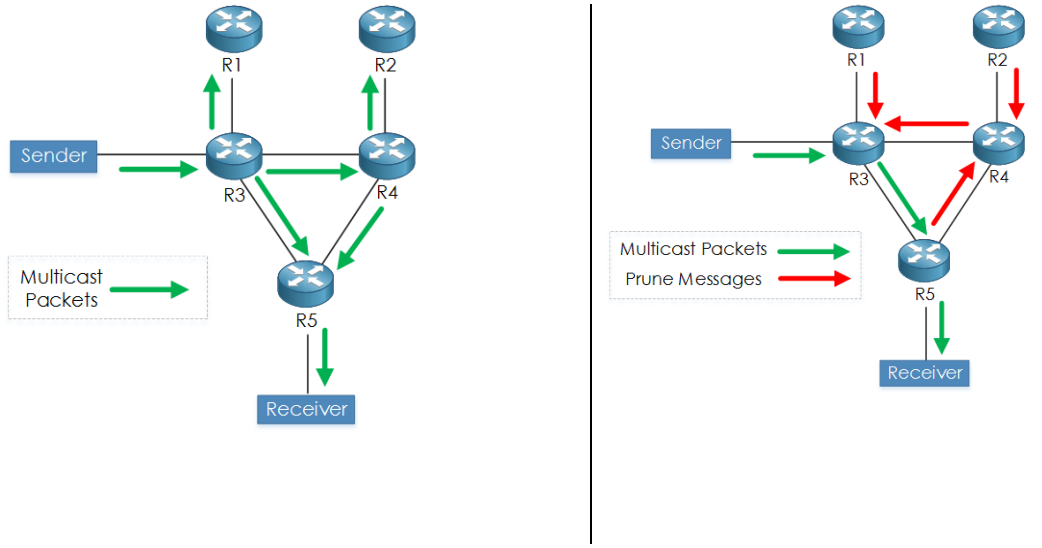
Pour que le trafic multicast soit envoyé via un réseau, il y a deux éléments clés - l'état et l'arbre de distribution multicast.

- **Etat :** L'état est l'information que les périphériques réseau doivent suivre pour que le routeur sache où il doit envoyer le trafic. L'état comprend la composante connue sous le nom de (S, G) ; S (La source multidiffusion), G (groupe multidiffusion).
- **Arbre de distribution :** L'arborescence de distribution est un chemin à travers le réseau utilisé pour distribuer le trafic de multidiffusion. Il existe deux types d'arbres de distribution : le chemin le plus court (également appelé arbre source) et le chemin partagé.

4.4.2.2. Le mode dense PIM (RFC 3973)

Il fonctionne en inondant initialement le trafic de multidiffusion pour tous les groupes de toutes les interfaces activées (Figure 4.8 -- A). Les routeurs qui n'ont pas d'hôtes intéressés envoient des messages PIM Prune pour se retirer de l'arborescence (Figure 4.8 -- B). Sur la base de ce comportement « Inonder et élaguer », le trafic est finalement envoyé uniquement aux routeurs qui nécessitent le trafic. Ceci, à son tour, se traduit par

une arborescence de distribution source, c'est-à-dire un chemin réseau optimal reconstruit vers l'expéditeur.



A **B**

Figure 4.8. Le mode dense PIM

4.4.2.3. Le mode sparse PIM

Avec le mode sparse PIM, aucun trafic multidiffusion n'est transmis à moins que certains le demandent. Ce mode fonctionne via l'utilisation d'un RP (Rendez-vous Point). Ce mode suit le processus suivant :

- **Arbre partagé (RP vers le récepteur)** : Le récepteur envoie un message « IGMP Join » au routeur du premier saut, c'est-à-dire son routeur voisin direct. Ce routeur enverra alors une jointure PIM au RP. Un arbre partagé est ensuite construit du récepteur au RP.
- **Arbre de chemin le plus court (source vers RP)** : La source commence à envoyer du trafic multidiffusion. Le routeur du premier saut encapsule le paquet de multidiffusion dans un message de registre PIM et l'envoie via la monodiffusion au routeur RP. Le RP décapsule le paquet et vérifie le groupe de multidiffusion pour voir s'il a un état pour tous les récepteurs du groupe de multidiffusion. Dans ce cas, le RP renvoie un message « PIM Join » vers la source, afin de reconstruire *un arbre du chemin le plus court* vers la source. La source envoie un autre paquet de multidiffusion, mais il existe maintenant *un arbre du chemin le plus court* (ou arbre source) du RP au routeur du premier saut. Par conséquent, le paquet est maintenant envoyé via

l'arborescence de distribution au RP. Le RP reçoit la nativité du paquet (avec S, G) et, à son tour, renvoie un message d'arrêt de registre au routeur du premier saut pour arrêter de recevoir les messages de registre (via la monodiffusion).

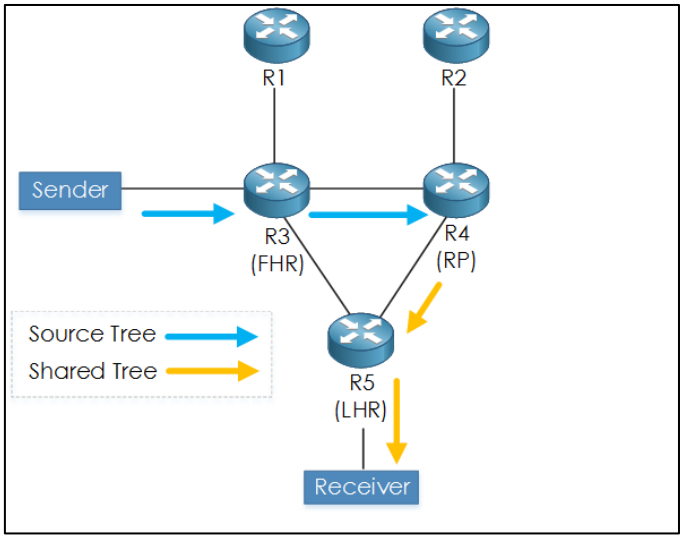


Figure 4.9. PIM Sparse, Arbre de chemin le plus court et arborescence partagée

- **Commutation d'arborescence de chemin le plus court** : Tout d'abord, le routeur du dernier saut (RDS) voit l'adresse source du flux multicast. Maintenant que le routeur du dernier saut connaît l'adresse source, il envoie une jointure (S, G) à la source du flux de multidiffusion. Cela construit un arbre de chemin le plus court de RDS à RPS. Enfin, un message Prune est envoyé du RDS au RP afin de supprimer l'arborescence partagée précédemment utilisée (RP vers RDS).

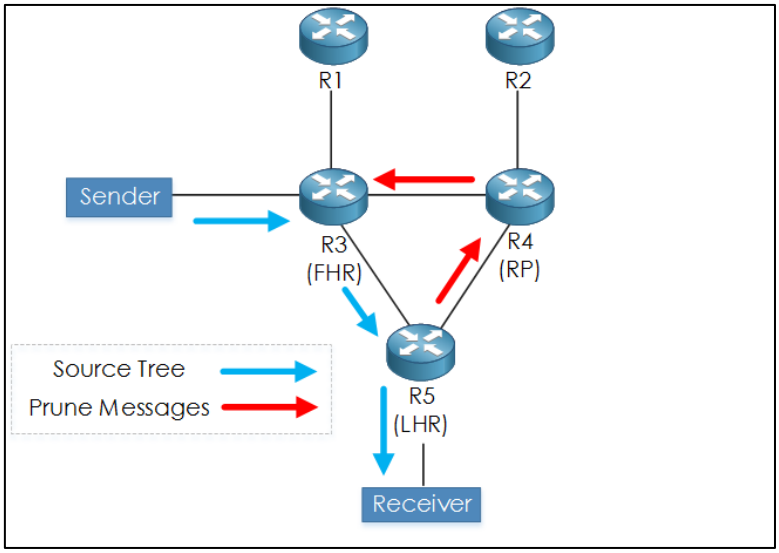


Figure 4.10. Basculement de l'arbre du chemin le plus court

Chapitre 5 : Internet : adressage, subnetting et supernetting (CIDR)

5.1. Introduction

L'internet est une architecture système qui a révolutionné les communications et les méthodes de commerce en permettant l'interconnexion de divers réseaux informatiques à travers le monde. La couche Internet du modèle TCP/IP s'aligne sur la couche 3 (réseau) du modèle OSI, c'est là qu'existent les adresses IP et le routage. Lorsque des données sont transmises d'un nœud d'un réseau local à un nœud d'un autre réseau local, la couche Internet est utilisée. Ce chapitre présente les notions fondamentales tel que l'adressage, le subnetting et le supernetting.

5.2. Adressage

Les adresses Internet sont composées d'une adresse réseau et d'une adresse hôte (ou locale). Cette adresse en deux parties permet à un expéditeur de spécifier le réseau ainsi qu'un hôte spécifique sur le réseau. Une adresse réseau unique et officielle est attribuée à chaque réseau lorsqu'il se connecte à d'autres réseaux Internet.

L'adressage réseau est l'une des principales responsabilités de la couche réseau (Internet). Les adresses réseau sont toujours logiques, c'est-à-dire des adresses IP, pas des adresses physiques comme l'adresse MAC. Un hôte est également connu sous le nom de système final qui a un lien vers le réseau. La frontière entre l'hôte et le lien est connue sous le nom d'interface. Généralement un hôte a une seule interface.

Un routeur est différent de l'hôte en ce qu'il a deux liens ou plus qui s'y connectent. Lorsqu'un routeur transmet le paquet, il transmet le paquet à l'un des liens. La frontière entre le routeur et le lien est connue sous le nom d'interface, et le routeur peut avoir plusieurs interfaces, une pour chacun de ses liens. Chaque interface est capable d'envoyer et de recevoir les paquets IP, donc IP exige que chaque interface ait une adresse.

Chaque adresse IP a une longueur de 32 bits et est représentée sous la forme d'une « notation décimale à points » où chaque octet est écrit sous la forme décimale, et ils sont séparés par des points. Une adresse IP ressemblerait à 10.88.1.213 où 10 représente la notation décimale des 8 premiers bits d'une adresse, 88 représente la notation décimale

des 8 seconds bits d'une adresse. Il existe principalement quatre types d'adresses IP : Public, Privé, Statique et Dynamique.

Parmi eux, les adresses publiques et privées sont basées sur leur emplacement sur le réseau privé, qui doit être utilisé à l'intérieur d'un réseau, tandis que l'adresse IP publique est utilisée à l'extérieur d'un réseau.

5.2.1. Classe d'adresse IP

Une adresse IPv4 a une longueur de 32 bits. Une adresse IP est divisée en sous-classes : Classe A, Classe B, Classe C, Classe D, et Classe E (illustré dans la Figure 5.1)

Une adresse IP est divisée en deux parties :

- **Identificateur réseau** : Il représente le nombre de réseaux.
- **Identificateur hôte** : Il représente le nombre d'hôtes dans chaque réseau.

Chaque classe a une plage spécifique d'adresses IP. La classe d'adresse IP est utilisée pour déterminer le nombre de réseaux et d'hôtes disponibles dans la classe.

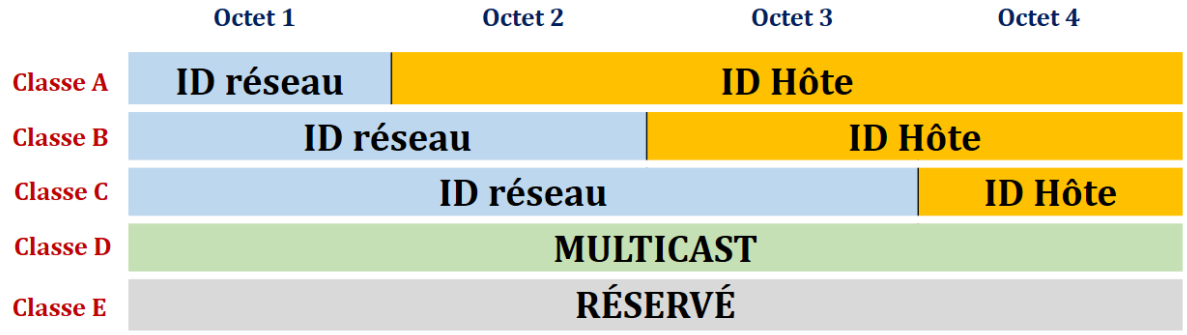


Figure 5.1. Les cinq classes d'adresse IPv4

5.2.1.1. La classe A

Une adresse IP de classe A est attribuée aux réseaux qui contiennent un grand nombre d'hôtes. Dans cette classe nous avons :

- L'ID de réseau a une longueur de 8 bits.
- L'ID d'hôte a une longueur de 24 bits.

En classe A, le premier bit des bits d'ordre supérieur du premier octet contient toujours la valeur « **0** » et les 7 bits restants déterminent l'ID de réseau. Les 24 bits déterminent l'ID d'hôte dans n'importe quel réseau.

Tableau 5.1. Des renseignements sur les adresses classe A

Plage d'adresses réseau	Masque	Nombre total de réseaux	Nombre total d'hôtes
0.0.0.0 à 127.0.0.0	**255.0.0.0**	**2^7 = 128**	**2^24 - 2 = 16777214**

5.2.1.2. La classe B

En classe B, une adresse IP est attribuée aux réseaux allant des réseaux de petite taille aux réseaux de grande taille. Dans cette classe nous avons :

- L'ID réseau a une longueur de 16 bits.
- L'ID d'hôte a une longueur de 16 bits.

En classe B, les bits de poids fort du premier octet contiennent toujours la valeur « **10** » et les 14 bits restants déterminent l'ID de réseau. Les 16 autres bits déterminent l'ID d'hôte.

Tableau 5.2. Des renseignements sur les adresses classe B

Plage d'adresses réseau	Masque	Nombre total de réseaux	Nombre total d'hôtes
128.0.0.0 à 191.255.0.0	**255.255.0.0**	**2^14 = 16384**	**2^16 - 2 = 65534**

5.2.1.3. La classe C

Dans cette classe, une adresse IP est attribuée uniquement aux réseaux de petite taille. Dans cette classe nous avons :

- L'ID réseau a une longueur de 24 bits.
- L'ID d'hôte a une longueur de 8 bits.

Les bits de poids fort du premier octet sont toujours définis sur **110** et les 21 bits restants déterminent l'ID de réseau. Les 8 bits de l'ID d'hôte déterminent l'hôte dans un réseau.

Tableau 5.3. Des renseignements sur les adresses classe C

Plage d'adresses réseau	Masque	Nombre total de réseaux	Nombre total d'hôtes
192.0.0.0 à 223.255.255.0	**255.255.255.0**	**2^21 = 2097152**	**2^8 - 2 = 254**

5.2.1.4. La classe D

La classe D est réservé aux adresses multicast. Il ne possède pas de sous-réseaux. Les bits de poids fort du premier octet sont toujours définis sur « **1110** », et les bits restants déterminent l'ID d'hôte dans n'importe quel réseau.

5.2.1.5. La classe E

Dans la classe E, une adresse IP est utilisée pour une utilisation future ou à des fins de recherche et développement. Il ne possède aucun sous-réseau. Les bits de poids fort du premier octet sont toujours définis sur « **1111** », et les bits restants déterminent l'ID d'hôte dans n'importe quel réseau.

5.2.2. Adresses spéciales

Certains blocs d'adresses ou certaines adresses de chaque bloc ont été réservés à des fins particulières, ils sont appelés des adresses IP spéciales. Les adresses spéciales de l'adressage par classe ont été héritées par l'adressage sans classe lors de son introduction en 1996.

5.2.2.1. Méta-adresse (non-routable)

Le bloc d'adresses composé uniquement de zéros **0.0.0.0/32** est un bloc spécial dans l'espace d'adressage IPv4. Tout hôte ayant cette adresse IP signifie que l'hôte n'est pas connecté au réseau TCP/IP. Lorsque l'hôte souhaite se connecter à Internet, il envoie un paquet de requête au serveur DHCP. Le paquet envoyé par l'hôte au serveur DHCP a pour adresse source 0.0.0.0 et 255.255.255.255 comme adresse de destination. Le serveur DHCP attribue ensuite l'adresse IP à l'hôte et l'hôte se connecte ensuite à Internet (ou réseau).

5.2.2.2. Adresse de diffusion limitée

Le bloc **255.255.255.255/32** est également un bloc spécial dans l'espace d'adressage IPv4. Ici, tous les 32 bits de l'adresse IPv4 sont **« 1 ».** Cette adresse est aussi appelée adresse de diffusion limitée. Si un hôte souhaite envoyer le message à tous les autres hôtes du réseau actuel, cela signifie que l'hôte souhaite diffuser un message dans le réseau actuel. Ensuite, l'hôte utilise cette adresse comme adresse de destination dans le paquet IPv4 et l'envoie sur le réseau. Elle est appelée limitée car le routeur restreint la diffusion du paquet sur le réseau local.

5.2.2.3. Adresses de bouclage

Le bloc spécial **127.0.0.0/8** a des adresses qui sont utilisées comme adresses de bouclage. La longueur du préfixe ici est de 8 bits, donc le nombre d'adresses peut être calculé comme $\mathbf{2^{24}}$. Ce bloc spécial a 16777216 adresses. Si nous considérons cette adresse dans l'adressage par classe, alors ce bloc est le dernier bloc de la classe A.

Toutes les adresses commençant par **« 127. »** doivent être considérées comme des adresses de bouclage. L'adresse de bouclage ne peut pas être que l'adresse de destination d'un paquet. Le paquet avec l'adresse de bouclage ne quitte jamais la machine à partir de laquelle il est envoyé, il revient simplement à la source. Elle peut être utilisée pour vérifier si la carte réseau fonctionne correctement ou non.

5.2.2.4. Adresses de lien local

Ces adresses sont dites « lien local », ce qui signifie que les paquets avec ces adresses sont envoyés au réseau, mais ne doivent jamais être transmis à d'autres parties du réseau. Ils sont conçus pour être utilisé pour l'adressage sur une seule liaison à des fins telles que la configuration automatique d'adresse ou la découverte de voisins. Vous verrez souvent des adresses de cette plage si un périphérique ne parvient pas à obtenir une adresse via DHCP. Ensuite, il prend simplement une adresse de cette plage et l'utilise pour essayer de communiquer au moins localement. La plage de ces adresses est de **169.254.0.0** à **169.254.255.255**

5.2.2.5. Adresses privées

Un paquet avec une adresse IP privée n'est pas acheminé (routé) sur Internet. Les adresses IP privées sont configurées par l'administrateur du réseau. Les appareils sur le même réseau utilisent des adresses IP privées pour communiquer entre eux.

Les plages d'adresses à utiliser par les réseaux privés sont :

- **Classe A** : 10.0.0.0 à 10.255.255.255
- **Classe B** : 172.16.0.0 à 172.31.255.255
- **Classe C :** 192.168.0.0 à 192.168.255.255

5.2.3. Masque réseau

Chaque classe de réseau a un masque par défaut associé qui définit la taille du réseau et les parties hôtes d'un réseau de classe A, B et C. Pour ce faire, le masque contient des **« 1 »** binaires pour les bits considérés être dans la partie réseau et des **« 0 »** binaires pour les bits considérés comme étant dans la partie hôte.

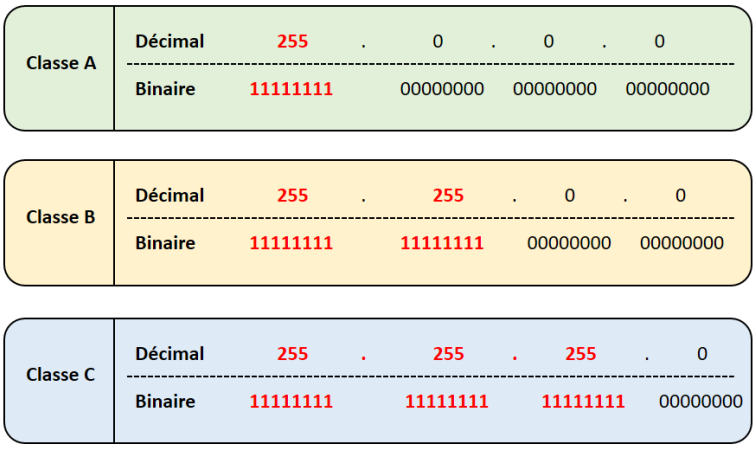


Figure 5.2. Les masques par défaut pour les classes A, B et C

5.2.4. Calcul et dérivation

Dans cette section, nous allons apprendre à calculer certains éléments importants, qui nous aident à mieux comprendre l'adressage.

5.2.4.1. Nombre d'hôtes par réseau

Les bits hôtes existent pour le but de donner à chaque hôte une adresse IP unique en vertu d'avoir une valeur différente dans la partie hôte des adresses. Ainsi, avec H bits hôtes, 2^H combinaisons uniques existent.

Cependant, le nombre d'hôtes dans un réseau n'est pas 2^H ; au lieu de cela, c'est **$2^H - 2$**. Chaque réseau réserve deux adresses IP qui auraient autrement été utiles en tant qu'adresses hôtes mais qui ont à la place ont été réservés à un usage spécial : un pour l'ID réseau et un pour l'adresse de diffusion réseau. Par conséquent, la formule pour calculer le nombre d'adresses hôtes pour la classe A, B ou C est :

$2^H - 2$ (Où H est le nombre de bits hôtes)

5.2.4.2. Adresse réseau

L'ID réseau ou adresse réseau, identifie le réseau. Cette adresse ne peut pas être attribuée en tant qu'adresse IP d'hôte. Ainsi, le nombre le plus bas d'une adresse IP d'un réseau est l'identifiant réseau. Pour trouver l'adresse réseau, remplacez les bits de l'hôte de l'adresse IP par des « 0 ».

Par exemple si nous avons l'IP d'hôte : 15.20.3.5 ➔ l'adresse réseau est 15.0.0.0

5.2.4.3. Adresse de diffusion (broadcast)

L'adresse de diffusion peut être utilisée comme adresse de destination dans un paquet, et les routeurs transmettraient une copie de ce paquet à tous les hôtes de ce réseau. Numériquement, une adresse de diffusion réseau est toujours le numéro le plus élevé (le dernier) du réseau. Pour trouver l'adresse de diffusion, remplacez les bits de l'hôte de l'adresse IP par des « 1 ».

Par exemple si nous avons l'adresse réseau : 15.0.0.0 ➔ l'adresse broadcast est 15.255.255.255

5.2.4.4. Première adresse utilisable (adresse d'hôte)

C'est l'adresse qui suit l'adresse réseau. Par exemple si nous avons l'adresse réseau : 15.0.0.0 ➔ la première adresse utilisable est 15.0.0.1

5.2.4.5. Dernière adresse utilisable (adresse d'hôte)

C'est l'adresse avant l'adresse de diffusion par exemple si nous avons l'adresse broadcast : 15.255.255.255 ➔ la dernière adresse utilisable est 15.255.255.254

La Figure 5.3 illustre les étapes à suivre pour dériver l'adresse réseau et d'autres adresses à partir d'une adresse IP

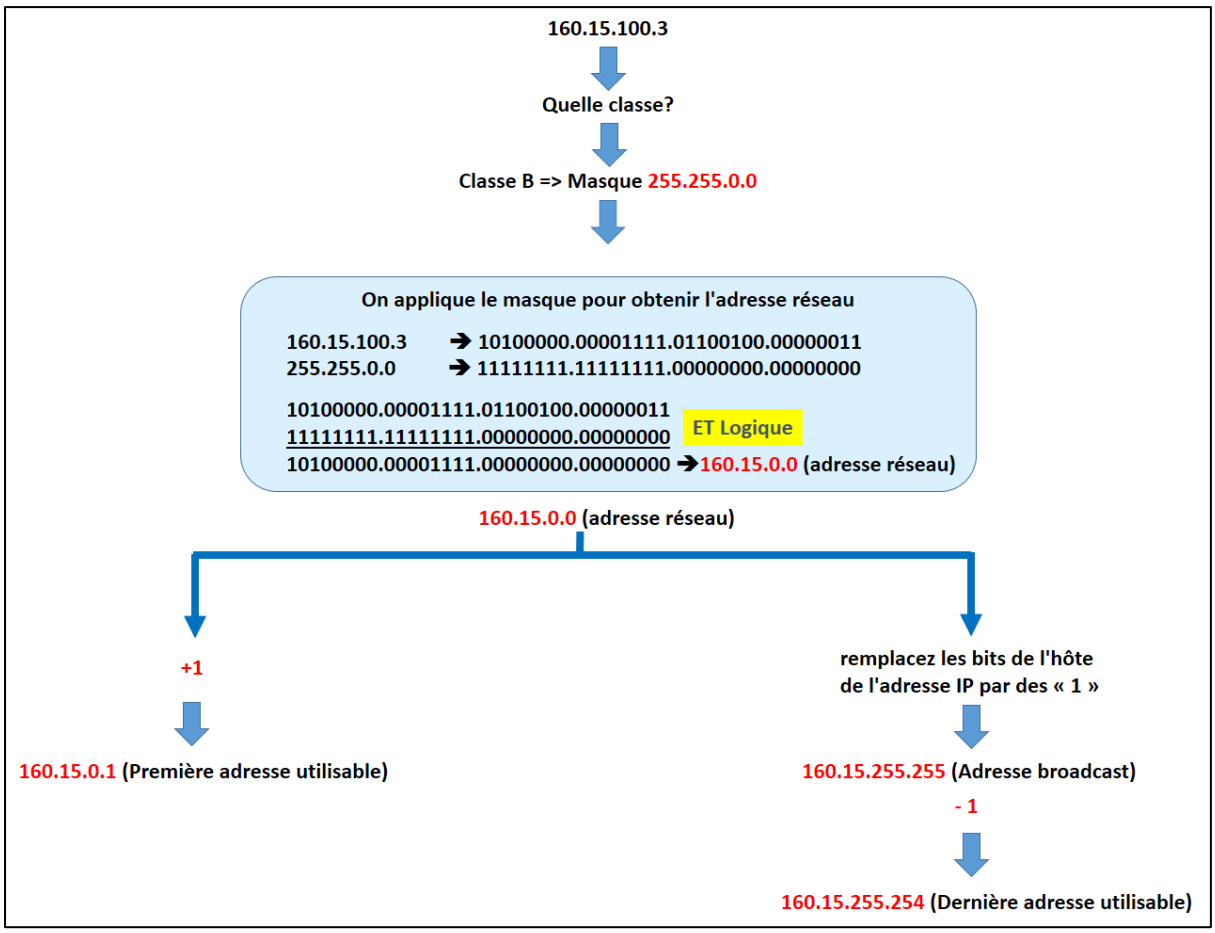


Figure 5.3. Exemple de dérivation de l'ID réseau et d'autres valeurs à partir d'une adresse

5.2.5. Différents formats de masques

Les masques de sous-réseau peuvent être écrits sous forme de nombres binaires de 32 bits, mais pas n'importe quel nombre binaire. En particulier, le masque de sous-réseau binaire doit suivre ces règles :

- La valeur ne doit pas entrelacer les 1 et les 0.
- Si des 1 existent, ils sont à gauche.
- Si des 0 existent, ils sont à droite.

Deux formats de masque de sous-réseau existent pour que nous, les humains, n'ayons pas à travailler avec nombres binaires de 32 bits.

- **Notation décimale pointée :** convertir chaque ensemble de 8 bits dans l'équivalent décimal en les séparant par des points. Par exemple :
  11111111 11111111 11111111 00000000
  255 . 255 . 255 . 0
- **Le format de préfixe :** Ce format tire parti de la règle selon laquelle le masque de sous-réseau commence par un certain nombre de 1, puis le reste des chiffres sont des 0. Le format de préfixe répertorie une barre oblique « / » suivie du nombre de « 1 » binaires du masque. Par exemple :
  11111111 11111111 11111111 00000000 ➔ **/24**
  11111111 00000000 00000000 00000000 ➔ **/8**

5.2.6. Parties d'adresse IP

Le masque de sous-réseau subdivise les adresses IP d'un sous-réseau en deux parties : la partie sous-réseau (préfixe), et la partie hôte.

- La partie préfixe identifie les adresses qui résident dans le même sous-réseau car toutes les adresses IP du même sous-réseau ont la même valeur dans la partie préfixe de leurs adresses.
- La partie hôte d'une adresse identifie l'hôte de manière unique à l'intérieur du sous-réseau.

Pour résumer ces comparaisons clés :

Partie sous-réseau (préfixe) : égale dans toutes les adresses du même sous-réseau.

Partie hôte : différente dans toutes les adresses du même sous-réseau.

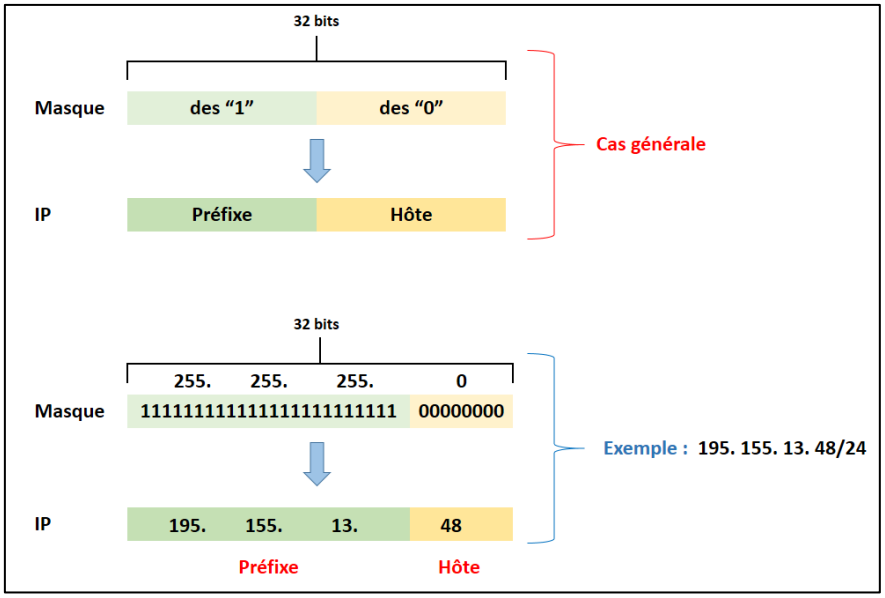


Figure 5.4. Préfixe (sous-réseau) et parties d'hôte définies par des masques

5.2.7. Adressage sans classe et par classe

Les termes adressage sans classe (*Classless*) et adressage par classe (*Classful*) font référence aux deux manières différentes de penser aux adresses. L'adressage par classe signifie que vous pensez aux règles de classe A, B et C, de sorte que le préfixe est séparé en parties réseau et sous-réseau. L'adressage sans classe signifie que vous ignorez les règles de classe A, B et C et traitez la partie préfixe comme une seule partie. Les définitions plus formelles suivantes sont répertoriées pour référence et étude :

- **Adressage sans classe (Classless) :** le concept selon lequel une adresse IPv4 comporte deux parties : la partie préfixe plus la partie hôte - telle que définie par le masque, sans tenir compte de la classe (A, B, ou C).
- **Adressage par classe (Classful) :** le concept selon lequel une adresse IPv4 comporte trois parties : réseau, sous-réseau, et hôte, tel que défini par le masque et les règles de classe A, B et C.

5.3. Subnetting

La segmentation du réseau (subnetting) est la stratégie utilisée pour partitionner un seul réseau physique en plusieurs sous-réseaux logiques plus petits (sous-réseaux). Une adresse IP comprend une partie de réseau et une partie d'hôte. Les sous-réseaux sont conçus en acceptant des bits de la partie hôte de l'adresse IP et en utilisant ces bits pour attribuer un certain nombre de sous-réseaux plus petits à l'intérieur du réseau d'origine. Les sous-réseaux permettent à une organisation d'ajouter des sous-réseaux sans avoir besoin d'acquérir une nouvelle adresse réseau via le fournisseur de services Internet. Les sous-réseaux aident à réduire le trafic réseau et masquent la complexité du réseau. La création de sous-réseaux est essentielle lorsqu'une seule adresse de réseau doit être attribuée sur de nombreux segments d'un réseau local. Les sous-réseaux ont été initialement conçus pour résoudre le manque d'adresses IP sur Internet.

Le subnetting offre les avantages suivants :

- Réduit le trafic réseau en réduisant le volume des diffusions
- Aide à dépasser les contraintes dans un réseau local, par exemple, le nombre maximum d'hôtes autorisés.
- Offre utilisation beaucoup plus efficace des adresses IP par rapport aux blocs de classe

- Il vous permet également de séparer un réseau pour la sécurité et pour le contrôle de la bande passante.

Le subnetting est basé sur la manipulation du masque de sous-réseau. Deux choses à garder à l'esprit lorsque vous créez des sous-réseaux :

- Commencez par le masque par défaut de sous-réseau et déplacez-le vers la droite (en changeant les bits zéros de la partie hôte en uns) jusqu'à ce que vous ayez le nombre de sous-réseaux dont vous avez besoin.
- Négligez les points. Ils ne définissent plus les sous-réseaux.

Complément :

N'essayez jamais de créer un sous-réseau sans d'abord convertir en binaire.

Le subnetting divisé le préfixe en deux parties : la partie réseau et la partie sous-réseau. La classe définit la longueur de la partie réseau, la partie sous-réseau étant simplement le reste du préfixe. La figure suivante montre l'idée.

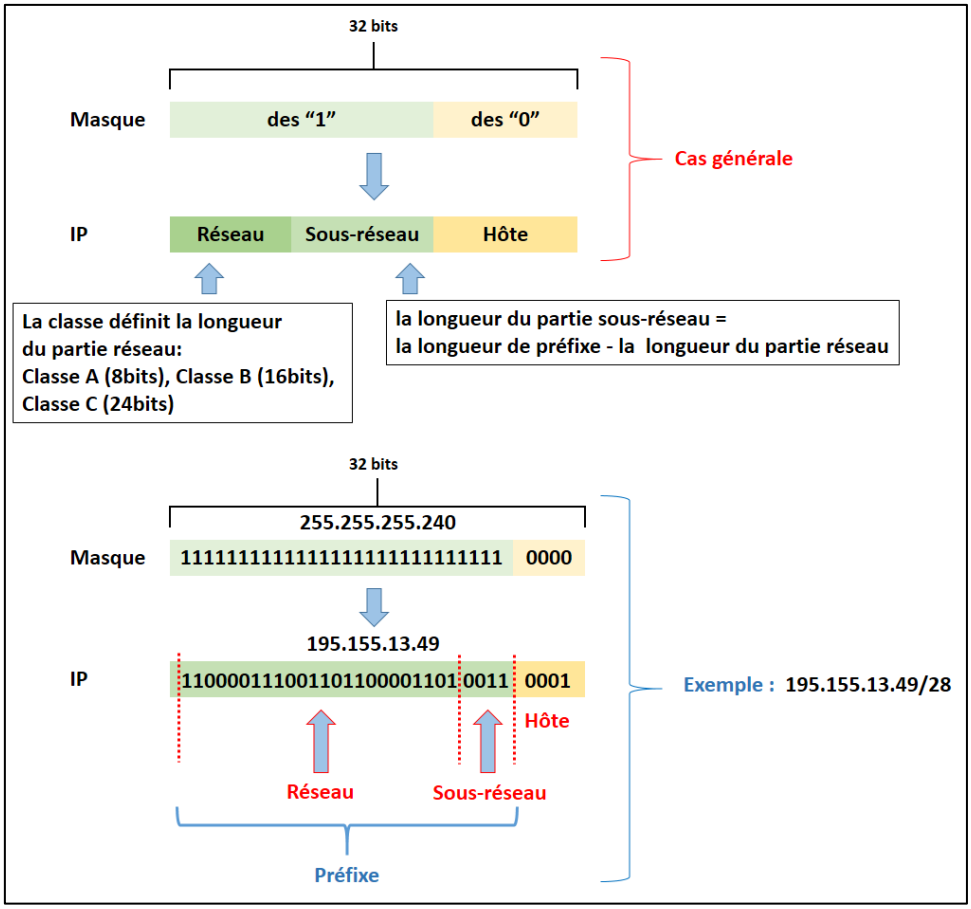


Figure 5.5. Les trois parties d'adresse IP (réseau, sous-réseau et hôte)

Les parties réseau et sous-réseau combinées agissent comme le préfixe car toutes les adresses du même sous-réseau doivent avoir des valeurs identiques dans les parties réseau et sous-réseau. La taille de la partie hôte reste inchangée.

5.3.1. Calcul des hôtes

La formule suivante est utilisée pour le calcul de nombre des hôtes :

$\mathbf{2^x - 2}$, où x représente le nombre de zéros dans le masque de sous-réseau.

Soustrayez deux pour l'ID réseau et l'adresse de diffusion.

Si vous vous souvenez de cette formule simple, vous pouvez toujours déterminer le nombre d'hôtes pour un sous-réseau donné.

Exemple :

Si vous avez un masque de sous-réseau **/26**, quel est le nombre maximum de hôtes que vous pouvez avoir sur ce réseau ?

1. Nombre des bits hôte = 32 – 26 = 6
2. On utilise la formule, 2^6 - 2 = 62 hôtes

5.3.2. Exemple de création des sous-réseaux

Imaginez que vous ayez une société de développement des jeux vidéo et que vous deviez séparer chaque équipe dans un sous-réseau distinct. Il y a 3 équipes comme illustré dans la figure suivante.

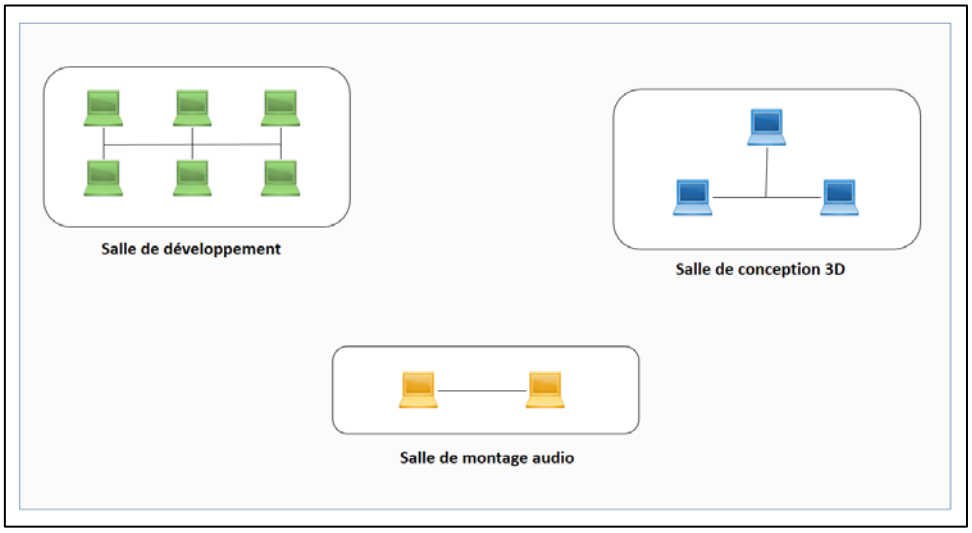


Figure 5.6. Disposition du réseau

Votre adresse réseau est 172.16.0.0/16. Vous devez attribuez un sous-réseau à chaque réseau local. Tous les sous-réseaux commencent par un seul ID de réseau.

Dans ce scénario, vous devez convertir l'ID réseau 172.16.0.0/16 en trois ID réseau : un pour la salle de développement, un pour la salle de conception 3D et un pour la salle de montage audio. Pour cela nous allons suivre les étapes suivantes :

- **ETAPE 01 :** Le principal outil de création de sous-réseaux est le masque de sous-réseau existant. Écrivez-le en binaire. Placez une ligne à la fin de dernier bit de 1, comme indiqué dans la Figure 5.7
- **ETAPE 02 :** Elle consiste à décaler la ligne à droite par X bits, tel que :

  $$2^X \geq NB$$

  Avec NB c'est le nombre des sous-réseaux nécessaire, X le plus petit nombre entier qui satisfaite la condition.

  Dans notre cas nous avons : **NB = 3** ➔ $2^2 \geq 3$ ➔ **X = 2**

  $2^2 = 4$ c'est-à-dire nous avons 4 sous réseaux
- **ETAPE 03 :** Il faut remplacer les X bits de 0 par des 1 pour obtenir le nouveau masque des sous-réseaux. C'est le masque : **255.255.192.0**

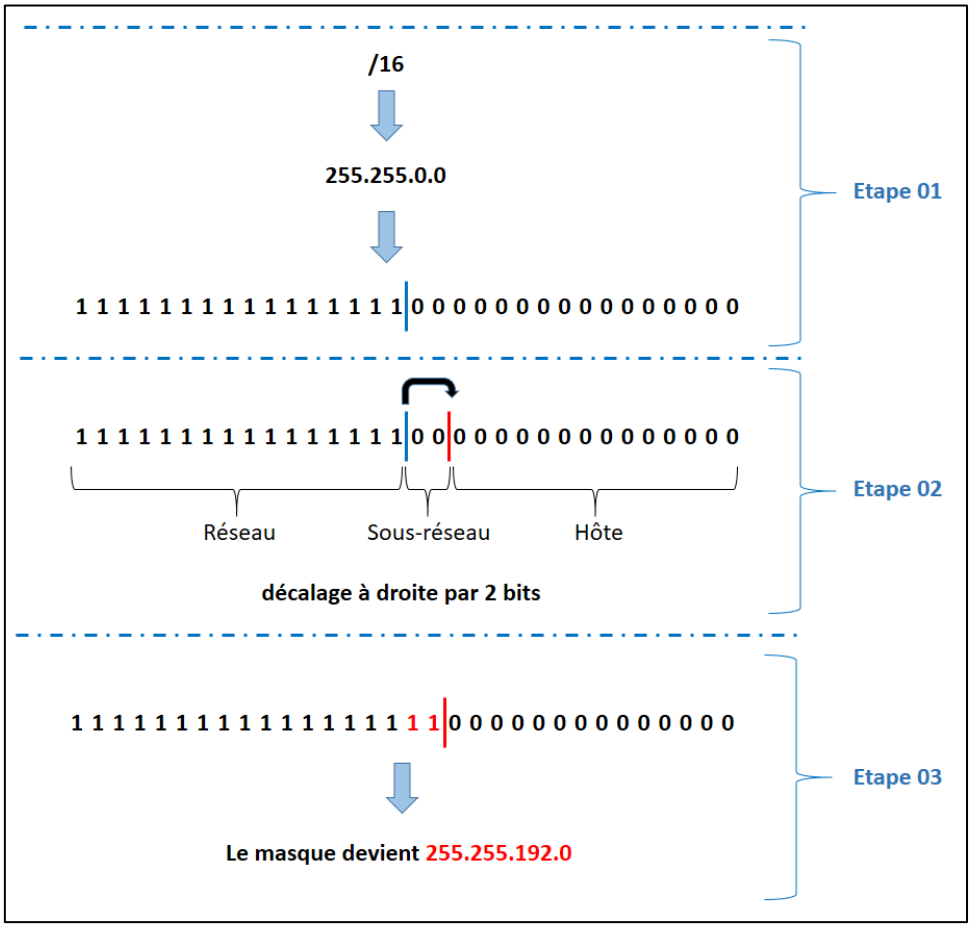


Figure 5.7. Les étapes de subnetting

Tableau 5.4. Les sous-réseaux obtenus de l'exemple

ID réseau (adresse réseau)	Plage d'hôtes	Adresse de diffusion (broadcast)
10101100000100000**00**000000000000 172.16.0.0/18	172.16.0.1 ➔ 172.16.63.254	10101100000100000**00**1111111111111 172.16.63.255
10101100000100000**01**000000000000 172.16.64.0/18	172.16.64.1 ➔ 172.16.127.254	10101100000100000**01**1111111111111 172.16.127.255
10101100000100001**0**000000000000 172.16.128.0/18	172.16.128.1 ➔ 172.16.191.254	10101100000100001**0**1111111111111 172.16.191.255
10101100000100001**1**000000000000 172.16.192.0/18	172.16.192.1 ➔ 172.16.255.254	10101100000100001**1**1111111111111 172.16.255.255

Complément :

Étant donné que les sous-réseaux sont créés par puissances de deux, vous créerez souvent plus de sous-réseaux que nécessaire.

5.4. Subnetting (VLSM)

VLSM (Variable-length subnet mask) est une stratégie de conception de sous-réseau qui permet à tous les masques de sous-réseau d'avoir des tailles variables. Les administrateurs réseau peuvent diviser un espace d'adressage IP en sous-réseaux de différentes tailles et l'allouer en fonction des besoins individuels sur un réseau. Ce type de sous-réseau permet une utilisation plus efficace d'une plage d'adresses IP donnée VLSM est la norme de facto pour la façon dont chaque réseau est conçu aujourd'hui.

5.4.1. Les étapes du VLSM

- Organisez les réseaux du plus grand au plus petit
- Mettre en œuvre le sous-réseau VLSM pour le plus grand réseau
- Mettre en œuvre le sous-réseau VLSM pour le deuxième plus grand réseau
- Mettre en œuvre le sous-réseau VLSM pour le n-ème plus grand réseau

5.4.2. Exemple du VLSM

Soit les réseaux présentés dans la figure suivante

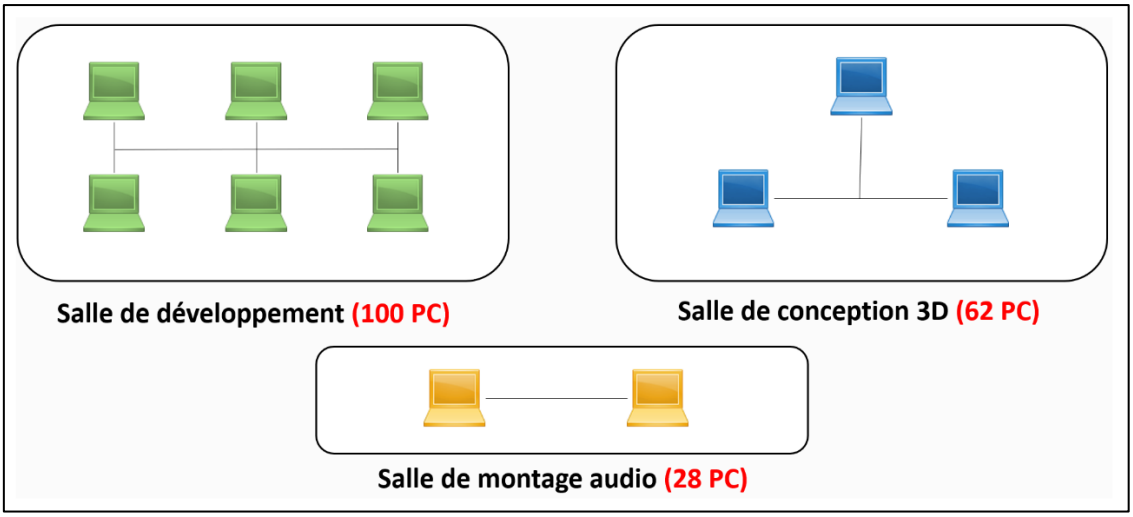


Figure 5.8. Disposition du réseau (VLSM)

On se fait attribuer la configuration suivante : **192.168.1.0/24**

- La 1ere étape consiste a ordonné les sous-réseaux du plus grand au plus petit.
    1) Sous réseau 01 : 100
    2) Sous réseau 02 : 62
    3) Sous réseau 03 : 28
- On réalise le subnetting comme il est illustré dans la figure suivante :

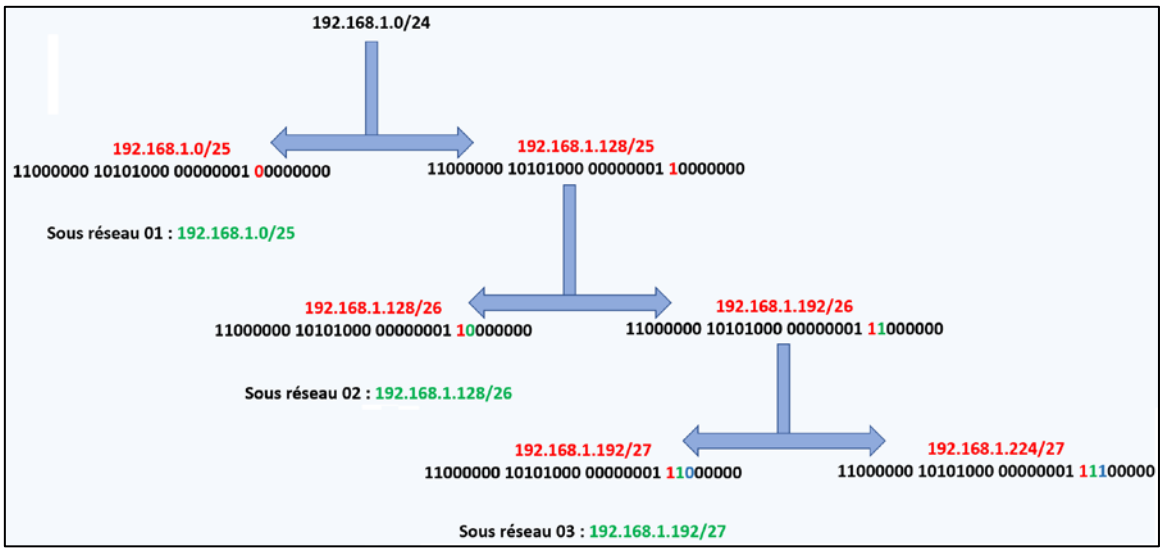


Figure 5.9. Les étapes de subnetting (VLSM)

5.5. Supernetting

Supernetting ou CIDR (Classless Inter-Domain Routing), est un schéma d'adressage IP qui améliore l'attribution des adresses IP. Il remplace l'ancien système basé sur les classes A, B et C. Ce schéma a également contribué à prolonger considérablement la durée de vie d'IPv4 et à ralentir la croissance des tables de routage.

Supernetting est utilisé pour combiner plusieurs réseaux de classe C en groupes, que le routeur, à son tour, traite comme un seul grand réseau. Supernetting fait le contraire de subnetting, ce qui signifie que nous prenons les bits de la partie ID réseau et les donnons à la partie ID hôte.

5.5.1. Règles de supernetting

Il y a quelques points qui doivent être gardés à l'esprit lors du supernetting :

- Déterminez le nombre de réseaux à agréger et assurez-vous que ce nombre est d'ordre 2.
- Tous les réseaux doivent être contigus
- La taille de bloc de chaque réseau doit être égale et doit être sous la forme 2^n
- La valeur de l'octet non commun dans le premier bloc « réseau » est zéro ou un multiple du nombre de réseaux à agréger

5.5.2. Fusion des sous-réseaux

Imaginez que vous ayez une société avec 4 sous-réseaux distincts, comme illustré dans la figure suivante :

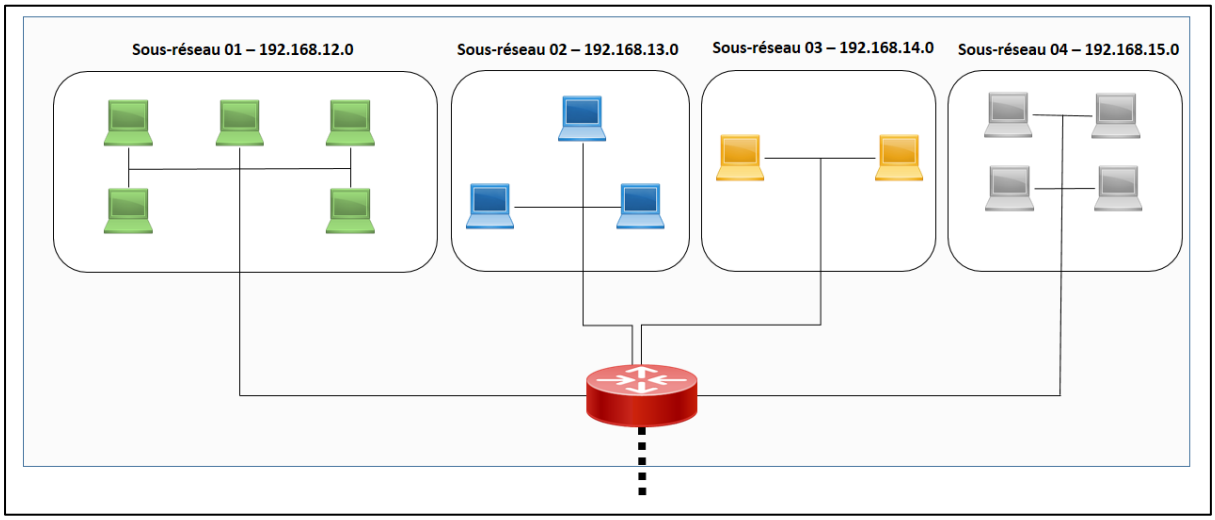


Figure 5.10. Les sous-réseaux d'une société

Nous voulons fusionner ces 4 sous-réseaux en un seul grand réseau. Avant de commencer le processus de supernetting, nous devons vérifier si les conditions sont satisfaites.

1. Le nombre de réseaux à agréger est d'ordre 2 : 2^2 = 4 sous réseaux
2. Tous les réseaux doivent être contigus :

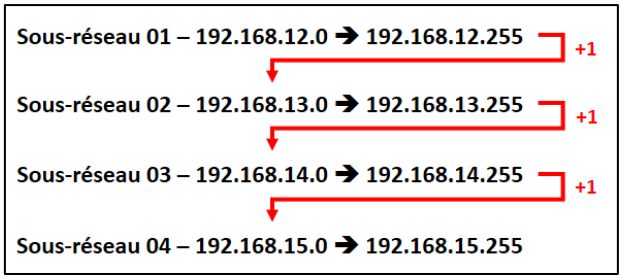


Figure 5.11. La première condition pour le Supernetting

3. La taille de bloc de chaque réseau doit être égale et doit être sous la forme 2^n :
   - Sous-réseau 01 : 256 = 2^8
   - Sous-réseau 02 : 256 = 2^8
   - Sous-réseau 03 : 256 = 2^8
   - Sous-réseau 04 : 256 = 2^8

   Dans ce cas n = 8
4. La valeur de l'octet non commun dans le premier bloc « réseau » est zéro ou un multiple du nombre de réseaux à agréger
   - Premier block de réseau : 192.168.12.0
   - La valeur de l'octet non commun est **12** car :

     192.168.**12**.0

     192.168.**13**.0

     192.168.**14**.0

     192.168.**15**.0

   12 est multiple du nombre de réseaux à agréger (c'est-à-dire 4)

Nous pouvons maintenant entamer le processus de supernetting.

- **ETAPE 01 :** Écrivez le masque en binaire. Placez une ligne à la fin de dernier bit de 1, comme indiqué dans la Figure 5.12
- **ETAPE 02 :** Elle consiste à décaler la ligne à gauche par X bits, tel que :

  $$2^{H+X} = TS$$

  Avec TS la taille de supernet, H c'est le nombre des bits de la partie hôte de sous-réseau, X le plus petit nombre entier qui satisfaite la condition.

  Dans notre cas nous avons : $TS = 2^8 * 4 = 2^{10} \rightarrow 2^{8+X} = 2^{10} \rightarrow X = 2$
- **ETAPE 03 :** Il faut remplacer les X bits de 1 par des 0 pour obtenir le nouveau masque de supernet. C'est le masque : **255.255.252.0**

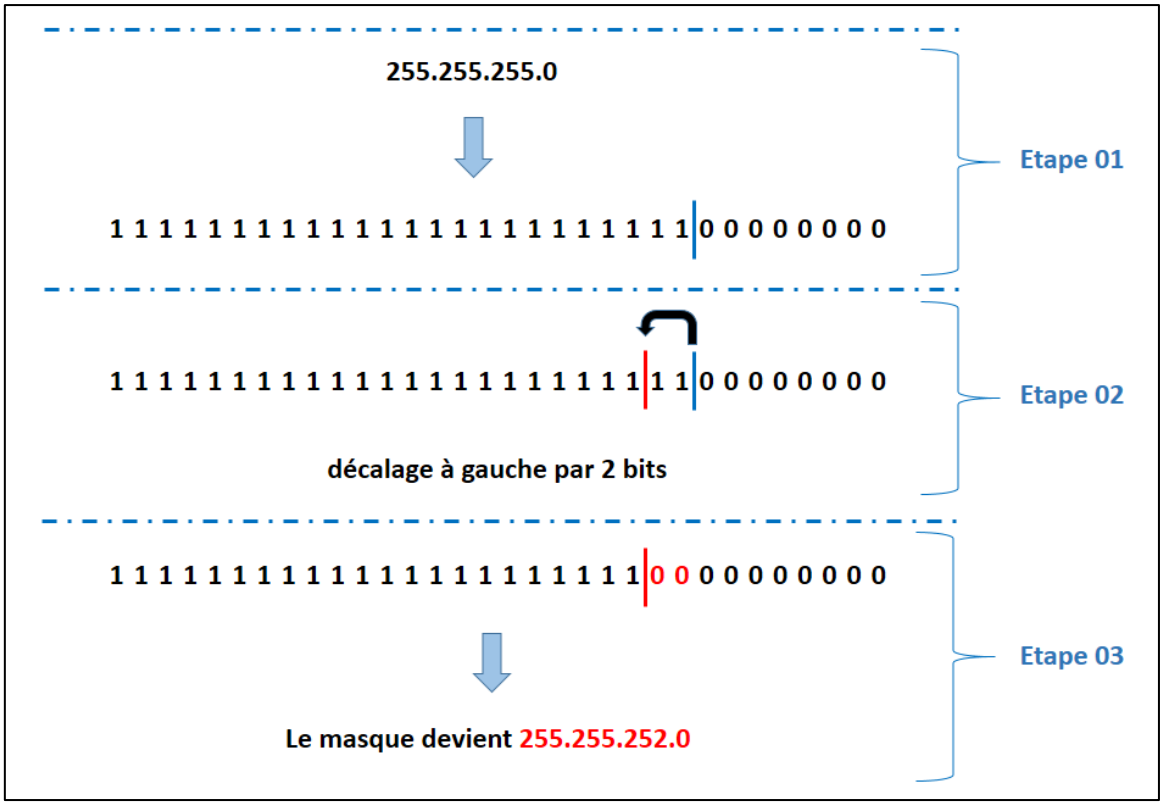


Figure 5.12. Les étapes de supernetting

Tableau 5.5. Le supernet obtenu de l'exemple

ID réseau (adresse réseau)	Plage d'hôtes	Adresse de diffusion (broadcast)
11000000101010000000110000000000 192.168.12.0/22	192.168.12.1 ➔ 192.168.15.254	11000000101010000000111111111111 192.168.15.255

Complément :

Le supernetting nécessite que les routeurs du réseau doivent exécuter un routage statique ou utiliser un protocole de routage sans classe tel que RIP2 ou OSPF

5.6. NAT (Network Address Translation)

NAT (Network Address Translation) est un moyen de mapper plusieurs adresses privées locales à une adresse publique avant de transférer les informations. Les organisations qui souhaitent que plusieurs appareils utilisent une seule adresse IP utilisent NAT, comme la plupart des routeurs domestiques. NAT permet à un appareil unique d'agir comme un intermédiaire ou un agent entre le réseau local privé et le réseau public (Internet). L'objectif principal de NAT est de conserver le nombre d'adresses IP publiques utilisées, à des fins de sécurité et économiques.

5.6.1. Fonctionnement

Un étudiant utilise un ordinateur portable connecté à un modem afin d'accéder au site web de son université. L'ordinateur portable envoie cette demande dans un paquet au modem (routeur), qui la transmet au site web. Mais d'abord, le routeur change l'adresse IP sortante d'une adresse locale privée en une adresse publique. En utilisant NAT, les informations seront renvoyées à l'ordinateur portable en utilisant l'adresse publique du routeur, et non l'adresse privée de l'ordinateur portable.

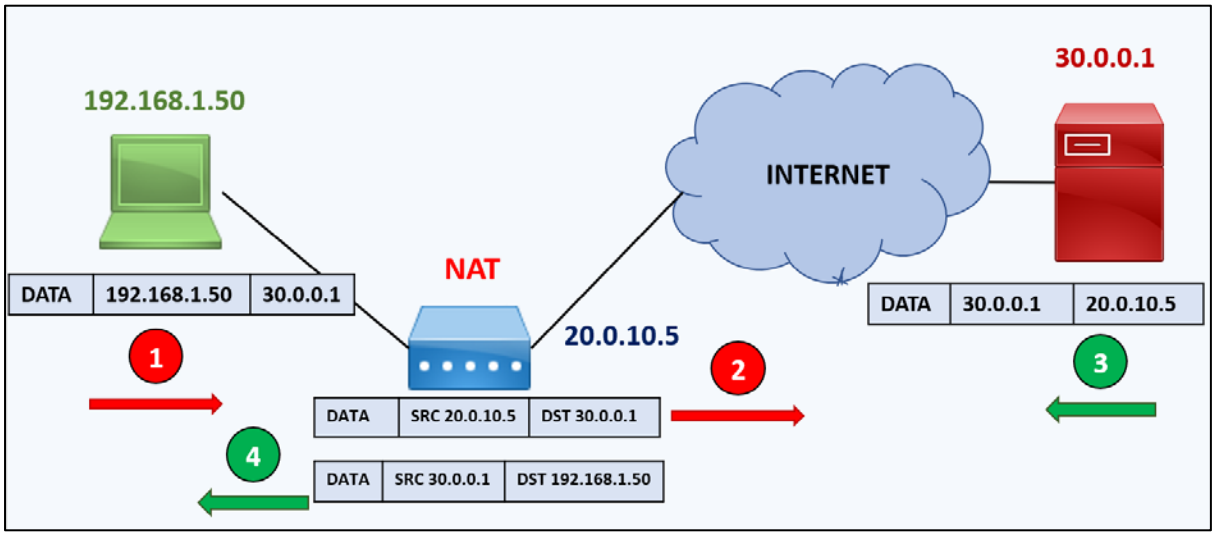


Figure 5.13. Le fonctionnement du NAT

5.6.2. Les types de NAT

5.6.2.1. NAT statique

Lorsque l'adresse locale est convertie en adresse publique, ce NAT choisit la même. Cela signifie qu'il y aura une adresse IP publique cohérente associée à ce routeur ou à ce périphérique NAT

5.6.2.2. NAT dynamique

Au lieu de choisir la même adresse IP à chaque fois, ce NAT passe par un pool d'adresses IP publiques. Il résulte que le routeur ou le périphérique NAT obtient une adresse différente chaque fois que le routeur traduit l'adresse locale en adresse publique

5.6.2.3. PAT

PAT (Port Address Translation) signifie traduction d'adresse de port. C'est un type de NAT dynamique, mais il regroupe plusieurs adresses IP locales en une seule publique. Les organisations qui souhaitent que toutes les activités de leurs employés utilisent une

adresse IP unique utilisent un PAT, souvent sous la supervision d'un administrateur réseau.

5.7. IPv6

Internet Engineering Task Force (IETF) a développé le système d'adressage Internet Protocol version 6 (IPv6). La fonction principale d'IPv6 est de permettre la création d'un plus grand nombre d'identifiants d'adresse TCP/IP uniques. IPv6 a étendu l'espace d'adressage IP de 32 bits à 128 bits, autorisant jusqu'à 2^128, c'est-à-dire près de 3.4 × 10^38 adresses. Les réseaux d'appareils mobiles et l'Internet des objets (IoT) sont tous IPv6.

5.7.1. Notation des adresses IPv6

IPv6 a 128 bits, nous n'avons pas des octets comme IPv4. IPv6 utilise deux-points comme séparateur, au lieu du point utilisé dans le format décimal à points d'IPv4. Chaque groupe de 16 bits, appelé quatuor (hextet), est un nombre hexadécimal compris entre 0000 et FFFF. Les adresses IPv6 s'écrivent comme suite : **2001:0db8:85a3:0000:0000:8a2e:0370:7334**

5.7.1.1. Notation abrégée

Les zéros non significatifs peuvent être supprimés de n'importe quel groupe. Par exemple 0010 devient 10, 0a66 devient a66 et 0000 devient 0.

2001:0db8:85a3:0051:0000:8a2e:0370:0004 ➔ 2001:db8:85a3:51:0:8a2e:370:4

On utilise « **::** » pour représenter un ou plusieurs groupes consécutifs de zéro. Par exemple : 2001:0:0:0:0:8a2e:0370:0004 ➔ 2001**::**8a2e:0370:4

Remarque : un seul « :: » est autorisé par adresse

5.7.2. Composants d'une adresse IPv6

Une adresse IPv6 se divise généralement en deux parties de 64 bits:

- Le préfixe réseau est les 64 premiers bits et est utilisé pour le routage
- La deuxième 64 bits est la partie utilisateur, appelée ID d'interface

Le préfixe réseau est en outre divisé en **un préfixe de routage** et **un ID de sous-réseau**

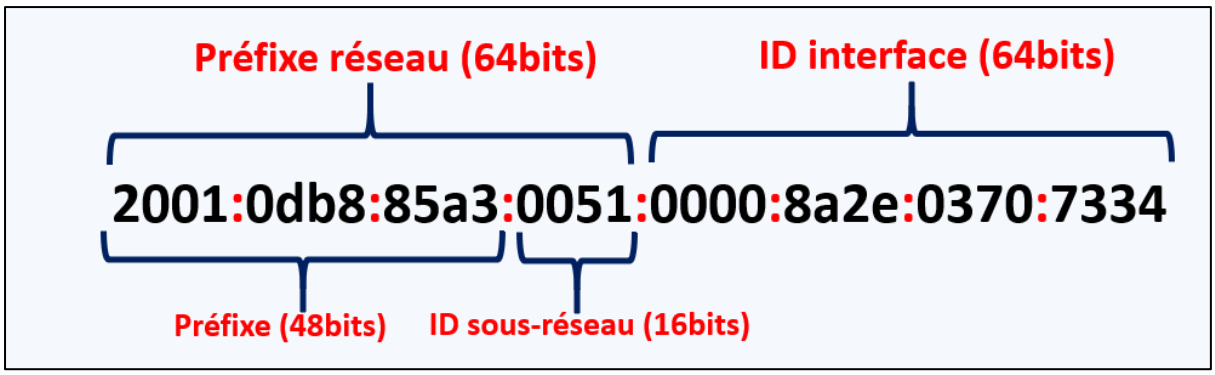


Figure 5.14. Les composants d'une adresse IPv6

5.7.2.1. Identificateur d'interface

La seconde partie de l'adresse (64 derniers bits) est toujours utilisée pour l'ID d'interface. L'adresse MAC d'un système est composée de 48 bits et représentée en hexadécimal. Un hôte peut configurer automatiquement son ID d'interface en utilisant le format d'identifiant unique étendu (EUI-64) de l'IEEE. Un hôte divise sa propre adresse MAC en deux parties de 24 bits. Ensuite, la valeur hexadécimale « 0xFFFE » est mis en place entre les deux parties ce qui donne l'ID d'interface EUI-64.

5.7.2.1.1. Conversion de l'ID d'interface EUI-64 en ID d'interface IPv6

Le 7ème bit le plus significatif d'une adresse mac représente le bit unique universel. Une adresse MAC aura toujours ce bit défini sur 0. On définit le 7ème bit le plus significatif de l'ID EUI-64 avec la valeur de « 1 ».

5.7.3. Types d'adresses IPv6

Il existe trois types d'adresses IPv6

5.7.3.1. Les addresses Unicast

Dans cette catégorie, nous trouvons les types suivants :

5.7.3.1.1. Adresse Unicast globale

Équivalent à l'adresse publique d'IPv4. Les adresses monodiffusion (Unicast) globale dans IPv6 sont globalement identifiables et adressables de manière unique.

- **Préfixe de routage global :** les 48 bits les plus significatifs sont désignés comme préfixe de routage global qui est attribué à un système autonome spécifique. Les trois bits les plus significatifs du préfixe de routage global sont toujours définis sur « **001** »

Le première hextet de 2000::/3 ➔ 3FFF::/3. Les 16 bits restantes sont pour l'ID de sous-réseau

5.7.3.1.2. Adresse lien-local

Le plus gros élément à comprendre est qu'un hôte n'a plus une seule adresse IP à moins que le réseau ne soit connecté à un routeur. Lorsqu'un ordinateur configuré par IPv6 démarre pour la première fois, il se donne une adresse lien-local. Considérez une adresse lien-local comme l'équivalent d'une adresse zeroconf d'IPv4. Les 10 premiers bits de l'adresse lien-local sont toujours définis sur « **1111111010** ». Les 54 bits suivants sont mis à « **0** ». Cela signifie que chaque adresse lien-local commence toujours par « **fe80:0000:0000:0000 ».**

5.7.3.1.3. Adresse de bouclage

Adresse de bouclage (loopback) est utilisé par un nœud pour s'envoyer un paquet IPv6. Une adresse de bouclage IPv6 fonctionne de la même manière qu'une adresse de bouclage IPv4. Une adresse de bouclage ne peut pas être attribuée à une interface physique. L'adresse de bouclage IPv6 est « **0000:0000:0000:0000:0000:0000:0000:0001/128 »**, qui peut également être représentée par « **::1 ».**

5.7.3.1.4. Adresses non spécifiées

Une adresse non spécifiée est une adresse entièrement composée de « **0** ». Une adresse unicast non spécifiée est utilisée comme adresse source pour indiquer l'absence d'adresse. Elle ne peut pas être affecté à une interface. Un routeur ne transmettra jamais un paquet dont l'adresse source n'est pas spécifiée **« 0000:0000:0000:0000:0000:0000:0000:0000 »** ou **« :: »**

5.7.3.1.5. Adresse locale unique

Semblable à une adresse privée IPv4 et non destinée à être routable dans Internet IPv6
Ce type d'adresse IPv6 doit être utilisé dans les communications locales. La seconde partie de cette adresse contient l'ID d'interface et la première partie est divisée entre : le préfixe ; le bit local (drapeau); ID global; ID de sous-réseau. Elles sont destinées à un usage privé et ne doivent pas être acheminées sur l'Internet. Ces adresses ne doivent être utilisées que dans une zone plus limitée, comme au sein d'un site ou routées entre un nombre limité de domaines administratifs. Elles sont destinées aux appareils qui n'ont jamais besoin d'accéder à Internet et qui n'ont jamais besoin d'être accessibles depuis Internet. Les adresses locales uniques ont le préfixe **fc00::/7**, ou les 7 premiers bits comme « **1111110x** ». La plage d'adresses est de **fc00::/7 ➔ fdff::/7.** Le 8eme bit (x) est

connu sous le nom de drapeau, et il peut être « 0 » ou « 1 ». Cela signifie que la plage d'adresses est divisée en deux parties :

- **fc00::/8** (11111100): Lorsque le drapeau est défini sur 0
- **fd00::/8** (11111101) : Lorsque le drapeau est défini sur 1, l'adresse est affectée localement

Les identifiants globaux (ID global) (40bits) peuvent être générés à l'aide d'un algorithme pseudo-aléatoire qui leur donne une très forte probabilité d'être uniques. Il est important que tous les sites générant des identifiants globaux utilisent le même algorithme pour garantir cette forte probabilité d'unicité.

5.7.3.2. Les addresses Multicast

ff00::/8, les 8 premiers bits sont des bits « 1 », réservés pour la multidiffusion IPv6. Les 4 bits suivants sont alloués pour les drapeaux. Les trois premiers drapeaux sont : 0 (réservé), R (point de rendez-vous) et P (préfixe de réseau). Le quatrième drapeau est le drapeau transitoire (drapeau T), qui désigne deux types d'adresses multidiffusion : Permanent (0) et Non permanent (1), ils sont attribués par des applications multicast. Les 4 bits suivants sont alloués pour le champ portée qui définit la plage à laquelle les routeurs peuvent transférer le paquet de multidiffusion. Les 112 bits suivants représentent l'ID de groupe.

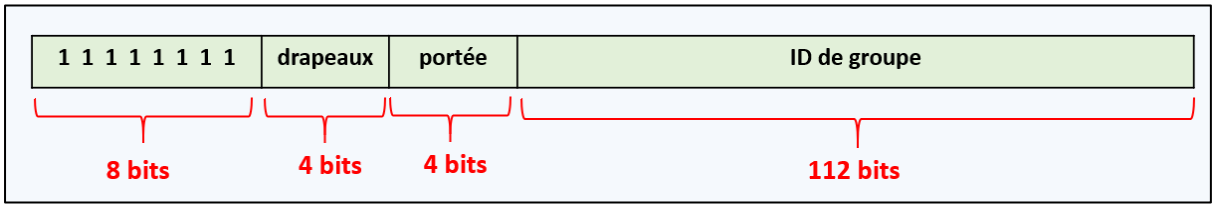


Figure 5.15. Structure d'une adresse Multicast

5.7.3.3. Les addresses Anycast

Il n'y a pas de préfixe spécial pour une adresse anycast d'IPv6. Une adresse IPv6 anycast utilise la même plage d'adresses que les adresses unicast globales. Chaque appareil participant est configuré pour avoir la même adresse anycast.

5.7.4. Entête IPv6

Dans IPv4, la taille de l'en-tête peut aller de 20 à 60 octets selon le champ d'options, mais dans IPv6, la taille de l'en-tête est fixée à 40 octets.

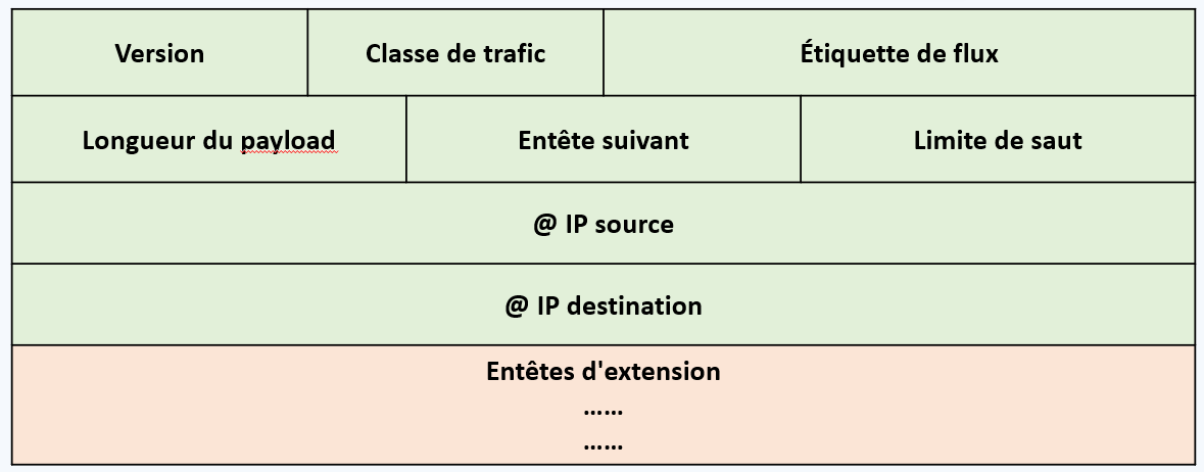


Figure 5.16. Entête IPv6

- **Version (4 bits) :** Il représente la version du protocole Internet il a une valeur de « 6 »
- **Classe de trafic (8 bits) :** Indique la classe ou la priorité du paquet IPv6. Il aide les routeurs à gérer le trafic en fonction de la priorité du paquet. Si une congestion se produit sur le routeur, les paquets les moins prioritaires seront rejetés.
- **Étiquette de flux (20 bits) :** Cette étiquette est utilisée pour maintenir le flux séquentiel des paquets appartenant à une communication. La source étiquette la séquence pour aider le routeur à identifier qu'un paquet particulier appartient à un flux d'informations spécifique. Il permet d'éviter la réorganisation des paquets de données. Il est conçu pour le streaming/les médias en temps réel.
- **Longueur de la charge utile (payload) (16 bits) :** Utilisé pour indiquer aux routeurs la quantité d'informations qu'un paquet particulier contient dans sa charge utile.
- **En-tête suivant (8 bits) :** Il indiquer le type d'entête d'extension, si l'en-tête d'extension n'est pas présent, il indique la PDU de couche supérieure. Les valeurs pour le type de PDU de couche supérieure sont identiques à celles d'IPv4 (6 (TCP) ;17 (UDP), etc.)
- **Hop Limit (8-bits) :** C'est le même que TTL dans les paquets IPv4. Il indique le nombre maximum de nœuds intermédiaires que le paquet IPv6 est autorisé à acheminer.
- **Adresse source (128 bits) :** ce champ indique l'adresse de l'expéditeur du paquet.
- **Adresse de destination (128 bits) :** il fournit l'adresse du destinataire du paquet.
- **En-têtes d'extension :** Le champ d'en-tête suivant de l'entête fixe IPv6 pointe vers le premier en-tête d'extension et ce premier entête d'extension pointe vers le deuxième entête d'extension et ainsi de suite.

Chapitre 6 : Les techniques modernes de routage

6.1. Introduction

Un protocole de routage est le langage qu'un routeur parle avec d'autres routeurs afin de partager des informations sur l'accessibilité et l'état des réseaux. Les protocoles de routage dynamique effectuent non seulement ces fonctions de détermination de chemin et de mise à jour de la table de routage, mais déterminent également le meilleur chemin suivant si le meilleur chemin vers une destination devient inutilisable. La capacité à compenser les changements de topologie est l'avantage le plus important qu'offre le routage dynamique par rapport au routage statique. Dans ce chapitre nous allons examiner les différentes techniques de routage, classements des protocoles, et nous examinons un protocole de routage extérieur, le BGP.

6.2. Classification des protocoles de routage

Nous pouvons classer les protocoles de routage en fonction de différents critères.

6.2.1. Classification 1

Il existe 3 catégories dans cette classification :

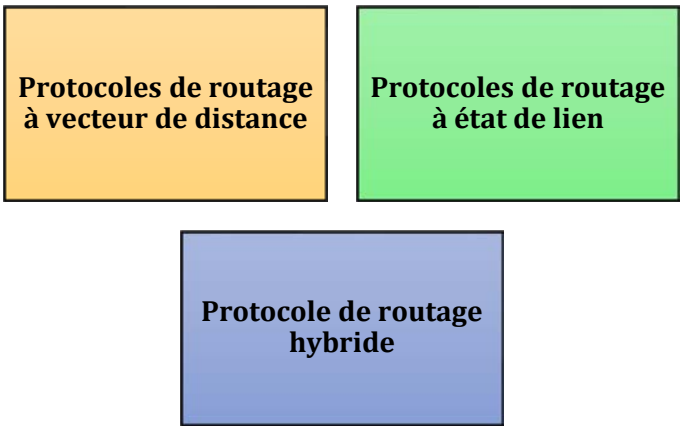


Figure 6.1. Classification 01 des protocoles de routage

6.2.1.1. Protocoles de routage à vecteur de distance

Le vecteur de distance signifie que les itinéraires sont annoncés en tant que vecteurs de distance et de direction

- **Distance :** identifie la distance jusqu'au réseau de destination et est basée sur une métrique telle que le nombre de sauts, le coût, la bande passante, le délai, etc.
- **Vecteur :** spécifie la direction du routeur de saut suivant ou de l'interface de sortie pour atteindre la destination

Les routeurs ne connaissent pas le paysage exact et les blocs possibles, ils ne connaissent que le prochain point vers leur destination. Les protocoles à vecteur de distance fonctionnent mieux dans les situations où :

- Le réseau est simple et plat
- Les temps de convergence les plus défavorables dans un réseau ne sont pas un problème

6.2.1.2. Protocoles de routage à état de lien

Les protocoles à état de lien ont généralement une vue complète de la topologie, ils connaissent généralement les meilleurs chemins ainsi que les chemins de secours vers les réseaux. Les protocoles d'état des liens utilisent l'algorithme du chemin le plus court pour trouver le meilleur chemin vers un réseau. Ils fonctionnent mieux dans les situations où :

- La conception du réseau est hiérarchique
- Une convergence rapide du réseau est cruciale

6.2.1.3. Protocoles de routage hybride :

C'est la combinaison des techniques précédents, il est chargé de rapporter des informations sur le routage lorsque des modifications se produisent dans la topologie. Le protocole de routage hybride améliore également le protocole de routage de la passerelle intérieure.

6.2.2. Classification 2

Il existe 2 catégories dans cette classification :

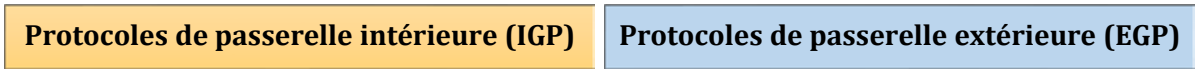


Figure 6.2. Classification 02 des protocoles de routage

6.2.2.1. Protocoles de passerelle intérieure (IGP)

Les protocoles de passerelle intérieure (IGP) sont utilisés pour le routage intra-système autonome - routage à l'intérieur d'un système autonome.

6.2.2.2. Protocoles de passerelle extérieure (EGP)

Les protocoles de passerelle extérieure (EGP) sont utilisés pour le routage inter-système autonome - routage entre systèmes autonomes.

6.2.3. Classification 3

Il existe 2 catégories dans cette classification :

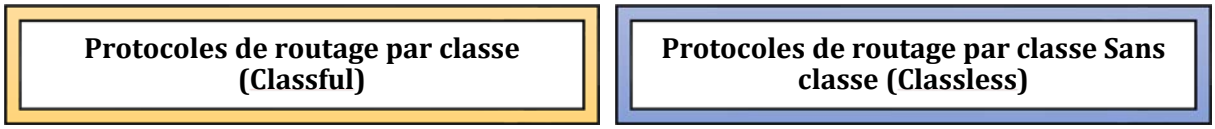


Figure 6.3. Classification 03 des protocoles de routage

6.2.3.1. Protocoles de routage par classe

Les protocoles de routage par classe n'incluent pas le masque de sous-réseau dans leurs mises à jour de routage. En effet, ils ont été conçus avant l'introduction du CIDR, puisqu'ils n'incluent pas le masque de sous-réseau dans leurs mises à jour de routage, ils ne peuvent pas fonctionner là où les réseaux ont été divisés en sous-réseaux.

6.2.3.2. 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. La plupart des réseaux modernes utilise les protocoles de routage sans classe.

6.2.4. Exemples de protocoles de routage

Tableau 6.1. Classification des protocoles de routage

	Protocoles de passerelle intérieure (IGP)			Protocoles de passerelle extérieure (EGP)
	À vecteur de distance	À état de lien	Hybride	
Par classe	**RIPv1** **IGRP**			**EGP**
Sans classe	**RIPv2** **RIPng (IPv6)**	**OSPFv2** **OSPFv3 (IPv6)** **IS-IS** **IS-IS (IPv6)**	**EIGRP** **EIGRP (IPv6)**	**BGP (IPv4, IPv6)**

6.2.5. Le protocole BGP

BGP (Border Gateway Protocol) est le protocole qui sous-tend le système de routage global d'Internet. Il gère la manière dont les paquets sont acheminés d'un réseau à l'autre via l'échange d'informations de routage et d'accessibilité entre les routeurs périphériques. BGP dirige les paquets entre les systèmes autonomes (autonomous systems (AS)), qui sont des réseaux gérés par une seule entreprise ou un seul fournisseur de services. Il crée aussi la stabilité du réseau en garantissant que les routeurs peuvent s'adapter aux échecs de route : lorsqu'un chemin tombe en panne, un nouveau chemin est rapidement trouvé. BGP prend des décisions de routage basées sur des chemins, définis par des règles ou des politiques réseaux conduits par les administrateurs réseau. La Figure 6.4 illustre les domaines d'utilisation du protocole BGP.

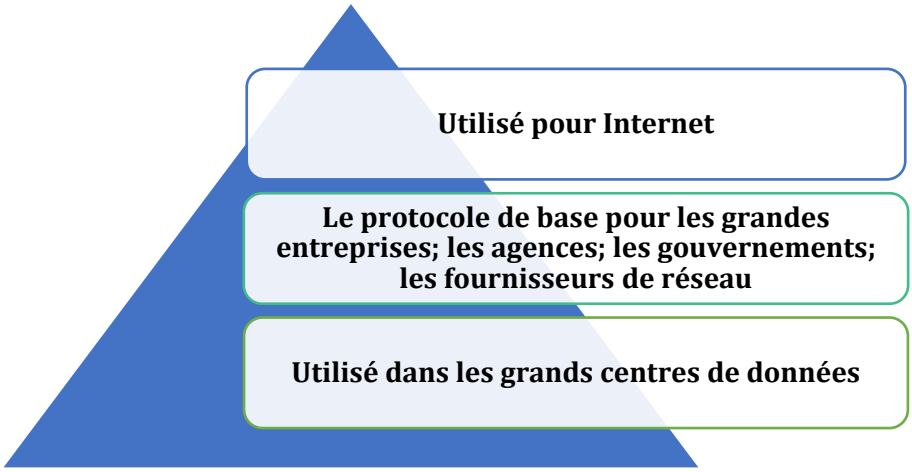


Figure 6.4. Les domaines d'utilisation du BGP

6.2.5.1. Les opérations

BGP n'envoie que des messages unicast et forme une connexion point à point distincte avec chacun de ses pairs. Il est un protocole de couche application utilisant TCP (port 179) pour cette connexion point à point et s'appuie sur les propriétés de TCP pour les fonctions de maintenance de session (l'accusé de réception, la retransmission et le séquencement). BGP est un protocole vectoriel, bien qu'il soit appelé vecteur de chemin plutôt que vecteur de distance, car il considère la route vers une destination comme un chemin à travers une série de systèmes autonomes plutôt que comme une série de sauts de routeurs.

Une route BGP décrit le vecteur de chemin à l'aide d'un attribut de route appelé **« AS_PATH »**, qui répertorie séquentiellement les numéros de système autonome comprenant le chemin vers la destination. L'attribut **« AS_PATH »** est un déterminant du

chemin le plus court. Étant donné plusieurs routes vers la même destination, la route avec un **« AS_PATH »** listant le moins de numéros de système autonome, est supposée être le chemin le plus court. Les numéros des systèmes autonomes de la liste AS_PATH sont utilisés pour la détection de boucle. Un routeur recevant une route BGP avec son propre numéro du système autonome dans AS_PATH assume une boucle et rejette la route. Si un routeur a une session BGP avec un voisin avec un numéro du système autonome différent, la session est appelée BGP externe (eBGP), autrement si le voisin a le même numéro du système autonome que le routeur, la session est appelée BGP interne (iBGP), les voisins sont appelés, respectivement, voisins externes ou internes.

6.2.5.2. Fonctionnement

La métrique entre deux systèmes autonomes adjacents est implicitement supposée n'être qu'un saut. Il utilise une métrique de nombre de sauts comme distance entre deux systèmes autonomes adjacents, le chemin le plus court d'un système autonome à un autre distant est essentiellement compté en termes de nombre le plus court de sauts. BGP permet également des liaisons virtuelles parallèles entre les systèmes autonomes adjacents. Un mécanisme est également fourni pour l'échange des informations local afin de décider d'une liaison préférée.

Dans chaque système autonome, certaines entités sont désignées comme agents BGP pour la communication avec les systèmes autonomes voisins. Ces agents sont des routeurs spécialement désignés appelés (BGP Speakers). Cela signifie que la session BGP basée sur TCP est en fait établie entre 2 locuteurs (speakers) BGP adjacents, donc chaque locuteur est considéré comme le pair de l'autre.

6.2.5.3. Types de messages

BGP utilise différents types de messages, comme indiqué ci-dessous :

6.2.5.3.1. Le message OPEN

Est le premier message envoyé pour établir une session BGP après l'établissement de la connexion TCP. Cela est lancé par les speakers BGP qui agissent en tant qu'agents désignés de systèmes autonomes pour parler à d'autres speakers BGP voisins. Souvent en pratique, chaque speaker BGP est configuré à l'avance avec l'adresse IP de l'autre speaker BGP afin que chaque extrémité puisse initier cette connexion TCP. C'est possible que différents speakers BGP utilisent différents numéros de version BGP. Le message OPEN contient le numéro de version ainsi que le numéro du système autonome.

6.2.5.3.2. Le message UPDATE

Envoyé entre deux speakers BGP pour échanger des informations des sous réseaux. Il fonctionne généralement en mode push, c'est-à-dire qu'à chaque fois qu'un speaker BGP a de nouvelles informations concernant un sous réseau à communiquer à son speaker BGP d'appairage, un message UPDATE est envoyé. En état stable, les speakers BGP génèrent des messages UPDATE chaque fois que l'une ou l'autre des extrémités a déterminé une nouvelle meilleure route pour un sous réseau spécifique. Si une extrémité de la session BGP était l'annonceur d'une route vers un sous réseau particulier vers son autre extrémité, elle doit générer un retrait si ce speaker ne peut plus atteindre ce sous réseau particulier.

6.2.5.3.3. Le message KEEPALIVE

Sont échangés périodiquement entre deux speakers BGP pour confirmer que la session est toujours active. Chaque extrémité apprend et s'accorde sur un temps maximum acceptable, appelé temps de maintien, lors de l'échange initial des messages OPEN. Les messages KEEPALIVE sont générés environ une fois tous les tiers du temps de maintien, mais pas plus d'une fois par seconde. S'il y a déjà un UPDATE envoyé dans cette fenêtre de temps, un message KEEPALIVE n'est pas nécessaire puisque l'autre extrémité sait que l'état est actif. Les messages KEEPALIVE ne doivent pas être générés s'il est convenu que le temps de maintien est égal à zéro, ce cas suppose que, d'une manière ou d'une autre, la session est totalement fiable.

6.2.5.3.4. Le message NOTIFICATION

Le message NOTIFICATION est envoyé pour fermer une session BGP. Utilisé lorsqu'une erreur survient nécessitant la fermeture de la session. Un lien virtuel entre deux speakers BGP est considéré comme indisponible :

- Si le message NOTIFICATION est envoyé par une extrémité
- Lorsqu'il y a absence de messages KEEPALIVE ou UPDATE dans une attente temps.

6.2.5.3.5. Le message ROUTE–REFRESH

À tout instant au cours d'une session, une extrémité peut envoyer ROUTE–REFRESH à son speaker BGP voisin demandant de réannoncer l'état de routage dans sa base d'informations de routage. ROUTE–REFRESH peut être considéré comme une demande d'extraction à laquelle on répond à l'aide d'un message UPDATE.

6.2.5.4. Les minuteries du BGP

6.2.5.4.1. Minuterie Connect Retry

Il définit l'intervalle de temporisation avant de réessayer une demande de connexion. Alors que la valeur recommandée est de 120 secondes, elle peut être définie sur zéro pour certaines conditions d'événement.

6.2.5.4.2. Minuterie de maintien

Il indique le temps maximum qui peut s'écouler sans recevoir de message UPDATE ou KEEPALIVE d'un speaker BGP avant de déclarer que le pair n'est pas joignable. L'expiration de ce temp indique que le lien virtuel entre deux speakers est en panne
La valeur recommandée est fixée à 90s tandis que la valeur positive minimale doit être de 3s. Le temps est autorisé à être défini sur zéro, qui est utilisé comme indicateur que la session n'expirera jamais.

6.2.5.4.3. Minuterie Garder en vie (Keep Alive)

Ce temporisateur se rapporte à la fréquence de génération des messages KEEPALIVE. La valeur de la minuterie est réglée sur un tiers de la valeur de temps de maintien. Si le temps de maintien est de 60 secondes via l'échange de messages OPEN au début d'une connexion BGP, alors garder en vie est défini sur 20 secondes.

Bibliographie

[1] 5.1.1 - IGMP | CCIE Docs. (n.d.). http://www.bscottrandall.com/5.1.1.html

[2] Burke, J. (2023, June 1). BGP (Border Gateway Protocol). Networking. https://www.techtarget.com/searchnetworking/definition/BGP-Border-Gateway-Protocol

[3] Donato, R. (2018, June 24). What is PIM (Protocol Independent Multicast)? Packet Coders. https://www.packetcoders.io/what-is-pim-protocol-independent-multicast/

[4] Doyle, J., & Carroll, J. (2016). Routing TCP/IP: CCIE Professional Development, Volume 2.

[5] Dynamic Host Configuration Protocol (DHCP). (n.d.). https://www.tutorialspoint.com/dynamic-host-configuration-protocol-dhcp

[6] Dynamic routing protocols | CCNA Blog. (n.d.). https://www.ccnablog.com/dynamic-routing-protocols/

[7] GeeksforGeeks. (2023, March 14). Introduction of Internetworking. https://www.geeksforgeeks.org/introduction-of-internetworking

[8] Graziani, R. (2017). IPv6 Fundamentals: A Straightforward Approach to Understanding IPv6. Cisco Press.

[9] IPCISCO. (2020, December 8). ARP Protocol Overview | What is ARP? | ARP Process ⋆ IpCisco. IPCisco. https://ipcisco.com/lesson/address-resolution-protocol-arp/

[10] Medhi, D., & Ramasamy, K. (2017). Network Routing: Algorithms, Protocols, and Architectures. Morgan Kaufmann.

[11] Meyers, M. (2022b). CompTIA Network+ Certification All-in-One Exam Guide, Eighth Edition (Exam N10-008). McGraw-Hill Education.

[12] Network Address Translation Definition | How NAT Works | Computer Networks | CompTIA. (n.d.). Default. https://www.comptia.org/content/guides/what-is-network-address-translation

[13] Odom, W. (2019). CCNA 200-301 Official Cert Guide, Volume 1. Cisco Press.

[14] Odom, W. (2019b). CCNA 200-301 Official Cert Guide, Volume 2. Cisco Press.

[15] OSPF Protocol | Open Shortest Path First Protocol - javatpoint. (n.d.). www.javatpoint.com. https://www.javatpoint.com/ospf-protocol

[16] RFC 1058: Routing Information Protocol. (1988, June 1). IETF Datatracker. https://datatracker.ietf.org/doc/html/rfc1058

[17] RFC 2236: Internet Group Management Protocol, Version 2. (1997, November 1). IETF Datatracker. https://datatracker.ietf.org/doc/html/rfc2236

[18] RFC 2328: OSPF Version 2. (1998, April 1). IETF Datatracker. https://datatracker.ietf.org/doc/html/rfc2328

[19] RFC 2460: Internet Protocol, Version 6 (IPV6) specification. (1998, December 1). IETF Datatracker. https://datatracker.ietf.org/doc/html/rfc2460

[20] The TCP/IP Guide - DHCP Message Format. (n.d.). http://www.tcpipguide.com/free/t_DHCPMessageFormat.htm

[21] Upravnik. (2022, December 18). ARP (Address Resolution Protocol) explained. Study CCNA. https://study-ccna.com/arp/

[22] What is Network Architecture? | VMware Glossary. (2022, September 20). VMware. https://www.vmware.com/fr/topics/glossary/content/network-architecture.html

[23] Welekwe, A., & Welekwe, A. (2023, January 25). Variable Length Subnet Mask (VLSM) Tutorial. Comparitech. https://www.comparitech.com/net-admin/variable-length-subnet-mask-vlsm-tutorial/ [Original source: https://studycrumb.com/alphabetizer]