MODULE : LES PROTOCOLES DES RESEAUX INFORMATIQUES

OBJECTIF DU MODULE : A l'issue de ce module, le stagiaire doit être capable d'identifier les types, les structures et les protocoles des réseaux Informatiques.

LEÇON N°01 : LES TOPOLOGIES DES RESEAUX

OBJECTIF DE LA LEÇON N°01 : A la fin de cette leçon, le stagiaire doit être capable d'identifier la classification des réseaux selon leur taille (LAN, MAN, WAN…).

INTRODUCTION :

Un réseau désigne un ensemble d'équipements interconnectés qui servent à échanger des flux d'information, et pour permettre la communication de données entre applications, quelles que soient les distances qui les séparent. Un réseau s'appuie sur deux notions fondamentales :
L'interconnexion qui assure la transmission des données d'un nœud à un autre.
La communication qui permet l'échange des données entre processus.

Les caractéristiques de base d'un réseau sont :

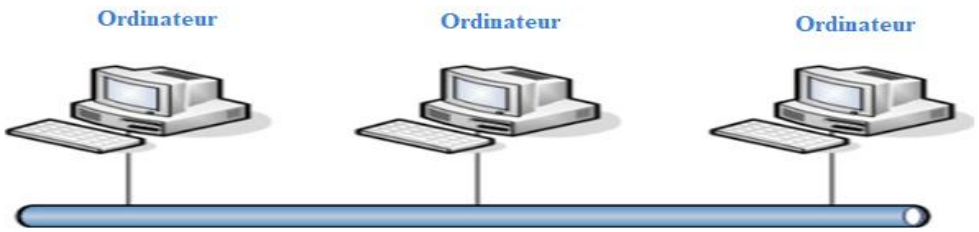
- **La topologie** qui définit l'architecture d'un réseau ;
- **Le débit** exprimé en bits/s (ou bps) qui mesure une quantité de données numériques (bits) transmises par seconde (s) ;
- **La distance maximale** (ou portée) qui dépend de la technologie mise en œuvre ;
- **Le nombre de nœuds maximum** que l'on peut interconnecter.

I. TOPOLOGIE DES RESEAUX :

Pour connecter deux (02) ordinateurs, un fil suffit. Comment connecter N ordinateurs pour que chaque ordinateur puisse communiquer avec n'importe quel ordinateur ?
On distinguera la topologie physique qui définit la manière dont les équipements sont interconnectés entre eux, de la topologie logique qui précise la manière dont les équipements communiquent entre eux (comment les informations circulent sur les réseaux).

1. Les différentes topologies physiques :

1.1. La topologie en Bus:



a. Définition :

La **topologie en bus** est une architecture réseau où tous les périphériques sont connectés à un **câble principal unique** (appelé **"backbone"** ou **"bus"**). Les données sont diffusées à tous les appareils, mais seul le destinataire prévu les traite.

- **Communication** : Les signaux voyagent dans les deux sens et sont **terminés aux extrémités** par des bouchons (terminateurs) pour éviter les réflexions.
- **Exemple historique** : **Ethernet 10BASE2** (câble coaxial) et **10BASE5** (thick Ethernet).

b. Fonctionnement

- **BROADCAST** : Quand un nœud envoie des données, elles sont transmises à **tous les autres nœuds**.
- **CSMA/CD** (*Carrier Sense Multiple Access with Collision Detection*) :

- Si deux nœuds envoient des données en même temps → **collision**.
- Le protocole force une attente aléatoire avant retransmission.

c. Avantages

- **Coût faible :** Moins de câblage que l'étoile ou l'anneau.
- **Simplicité d'installation :** Connexion en série sur un seul câble.

- **Adapté aux petits réseaux :** Idéal pour des configurations temporaires ou peu étendues.

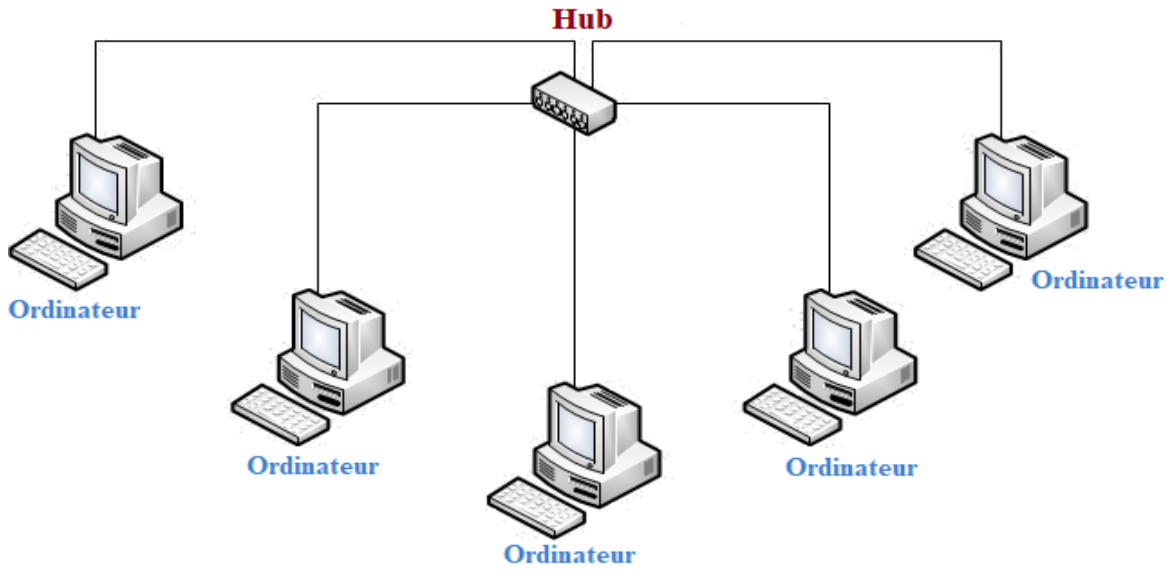
d. Inconvénients :

- **Risque élevé de collisions** : Plus il y a de nœuds, plus le réseau ralentit (CSMA/CD inefficace à grande échelle).
- **Panne globale en cas de rupture** : Si le câble principal est coupé, **tout le réseau tombe**.
- **Difficulté de dépannage** : Localiser un problème de connexion ou une interruption est complexe.
- **Débit limité** : Partage de la bande passante entre tous les appareils.

e. Applications :

- **Réseaux locaux anciens** (années 1980-1990) : Ethernet coaxial (10BASE2).
- **Réseaux industriels simples** : Automatisation basique.
- **Réseaux temporaires** : Configurations rapides pour des événements.

1.2. La topologie en Étoile:



a. Définition : La **topologie en étoile** est une architecture de réseau où tous les périphériques (ordinateurs, imprimantes, serveurs, etc.) sont connectés à un **nœud central unique**, appelé **concentrateur (hub)** ou **commutateur (switch)**.

- **Communication** : Toutes les données passent par le nœud central avant d'atteindre leur destination.
- **Exemple courant** : Les réseaux domestiques (box Internet comme point central).

b. Fonctionnement :

- **Hub (ancienne technologie)** : Diffuse les données à tous les périphériques (risque de collisions).
- **Switch (technologie moderne)** : Achemine les données uniquement vers le destinataire (moins de congestion).

c. Avantage :

- **Facilité d'installation et de maintenance** : Ajout/suppression de périphériques sans perturber le réseau.
  Détection simple des pannes : Si un périphérique tombe en panne, le reste du réseau fonctionne.
- **Performances stables** : Pas de collisions (avec un switch).
- **Sécurité** : Isolation des problèmes (une connexion compromise n'affecte pas les autres).

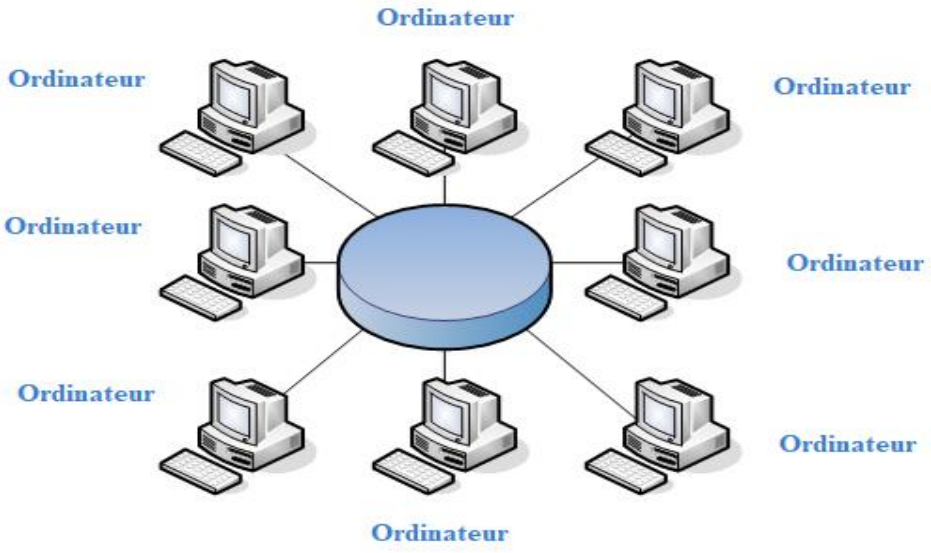
d. Inconvénients :

- **Dépendance au nœud central** : Si le hub/switch tombe en panne, **tout le réseau est coupé**.
- **Coût élevé** (pour les grands réseaux) : Nécessite des câbles et un équipement central performant.
- **Débit limité par le nœud central** : Risque de saturation si le trafic est intense.

e. Applications :

- **Réseaux locaux (LAN)** : Entreprises, écoles.
- **Réseaux domestiques** : Box Internet connectée à plusieurs appareils.
- **Réseaux sans fil (Wi-Fi)** : Le routeur agit comme nœud central.

1.3. La topologie en Anneau:



a. **Définition :**

La **topologie en anneau** est une architecture où tous les périphériques (nœuds) sont connectés en **forme de boucle fermée**, chaque appareil étant relié à **deux voisins**. Les données circulent dans **un seul sens** (anneau unidirectionnel) ou parfois dans **les deux sens** (anneau bidirectionnel).

- **Communication** : Les données voyagent de nœud en nœud sous forme de **jetons (token)**.
- **Exemple historique** : Les anciens réseaux **Token Ring** (IBM) ou **FDDI** (fibre optique).

b. **Fonctionnement :**

- **Token Passing (Anneau à jeton)** :

- Un **jeton** circule dans l'anneau.
- Un nœud ne peut envoyer des données que s'il **possède le jeton**.
- Après transmission, le jeton est libéré pour le nœud suivant.

- **Bidirectionnel** :

- Certains anneaux permettent un flux dans les deux sens pour la redondance.

c. **Avantages**

- **Équité** : Pas de collisions (contrôle par jeton).
- **Performances prévisibles** : Délais constants, adapté aux réseaux chargés.
- **Évolutivité** : Ajout de nœuds sans perturber le trafic (avec gestion appropriée).
- **Redondance (en FDDI)** : Double anneau pour la tolérance aux pannes.

d. **Inconvénients :**

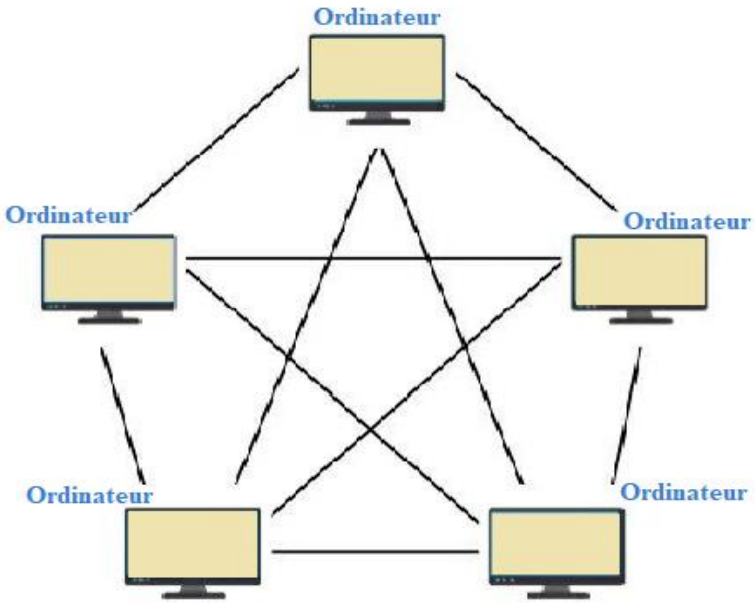
- Si une machine tombe en panne, le réseau est coupé.

e. **Applications :**

- **Réseaux industriels** : Automatisation (Profibus, Token Ring).
- **Anciens réseaux d'entreprise** : IBM Token Ring (années 1980-1990).
- **Réseaux haute disponibilité** : FDDI (double anneau en fibre optique).

1.4. La topologie maillée :

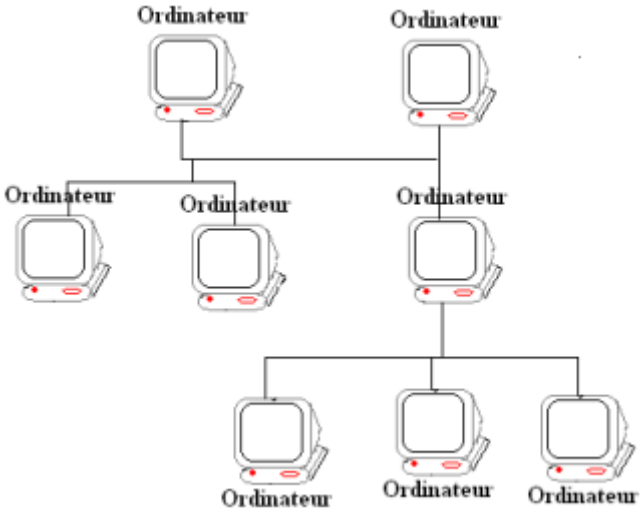
Avec cette topologie, chaque poste est reliée directement à tous les postes du réseau.



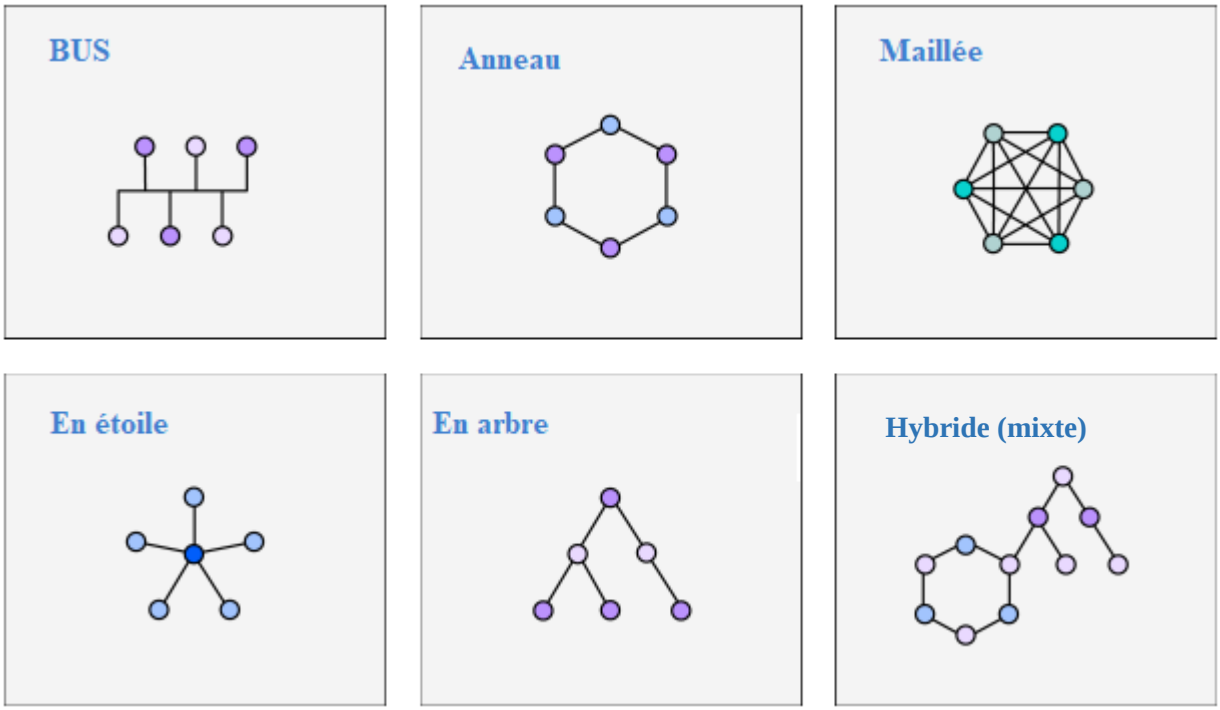
- **Avantages:** garantie d'une meilleure stabilité du réseau en cas d'une panne du nœud.
- **Inconvénients:** difficile à mettre en œuvre et ne peut pas être utilisé dans les réseaux internes Ethernet. Il peut facilement devenir très coûteux.

1.5. La topologie en arbre :

Dans une topologie en arbre appelée aussi topologie hiérarchique, le réseau est divisé en niveau et on a tendance à voir qu'on est en face d'un arbre généalogique.



Comparaison avec d'autres topologies



Critère	Étoile	Bus	Anneau
Fiabilité	Élevée (sauf nœud central)	Faible (casse du câble principal)	Moyenne (panne en cascade)
Coût	Modéré	Économique	Élevé
Maintenance	Simple	Complexe	Complexe

II.LES DIFFERENTES TOPOLOGIES LOGIQUES :

1. Topologie Ethernet :

Ethernet est aujourd'hui l'un des réseaux les plus utilisés en local. Il repose sur une topologie physique de type bus linéaire, c'est-à-dire tous les ordinateurs sont reliés à un seul support de transmission.

Dans un réseau Ethernet, la communication se fait à l'aide d'un protocole appelé CSMA/CD (Carrier Sense Multiple Access with Collision Detect), ce qui fait qu'il aura une très grande surveillance des données à transmettre pour éviter toute sorte de collision. Par un conséquent un poste qui veut émettre doit vérifier si le canal est libre avant d'y émettre.

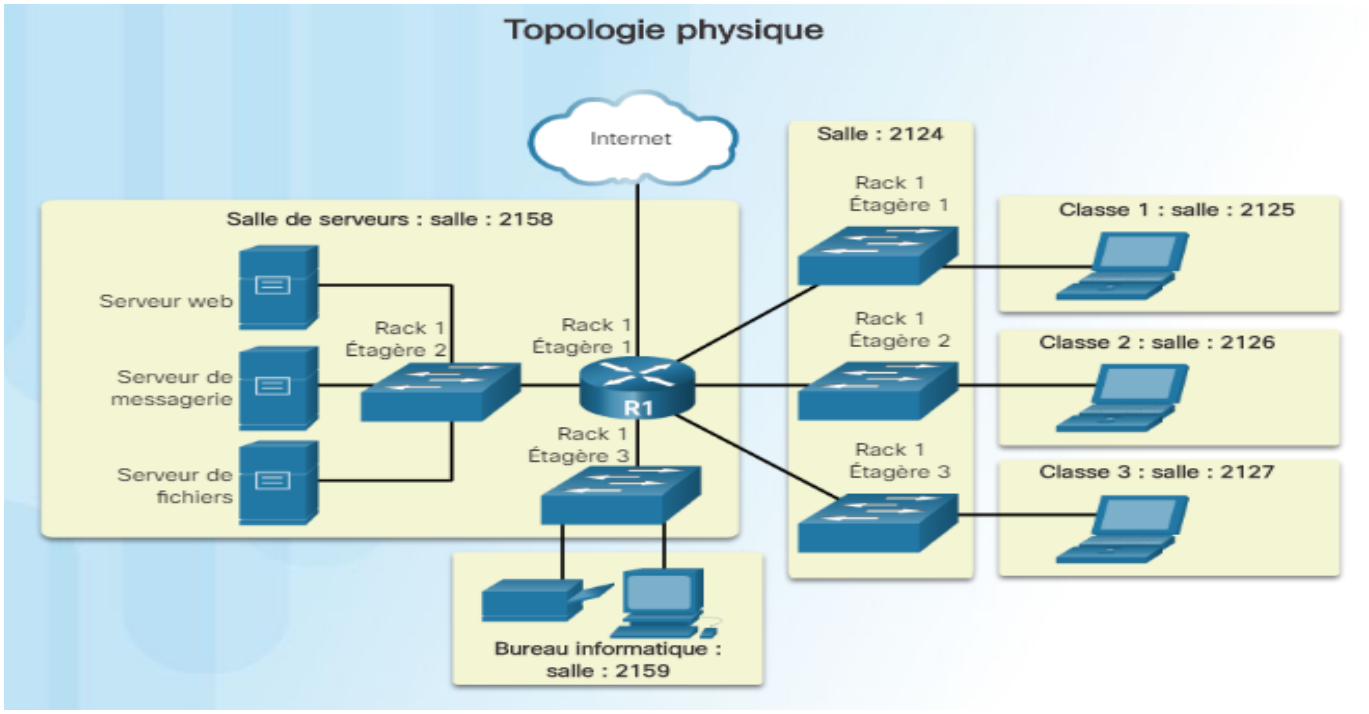
2. Le Token Ring :

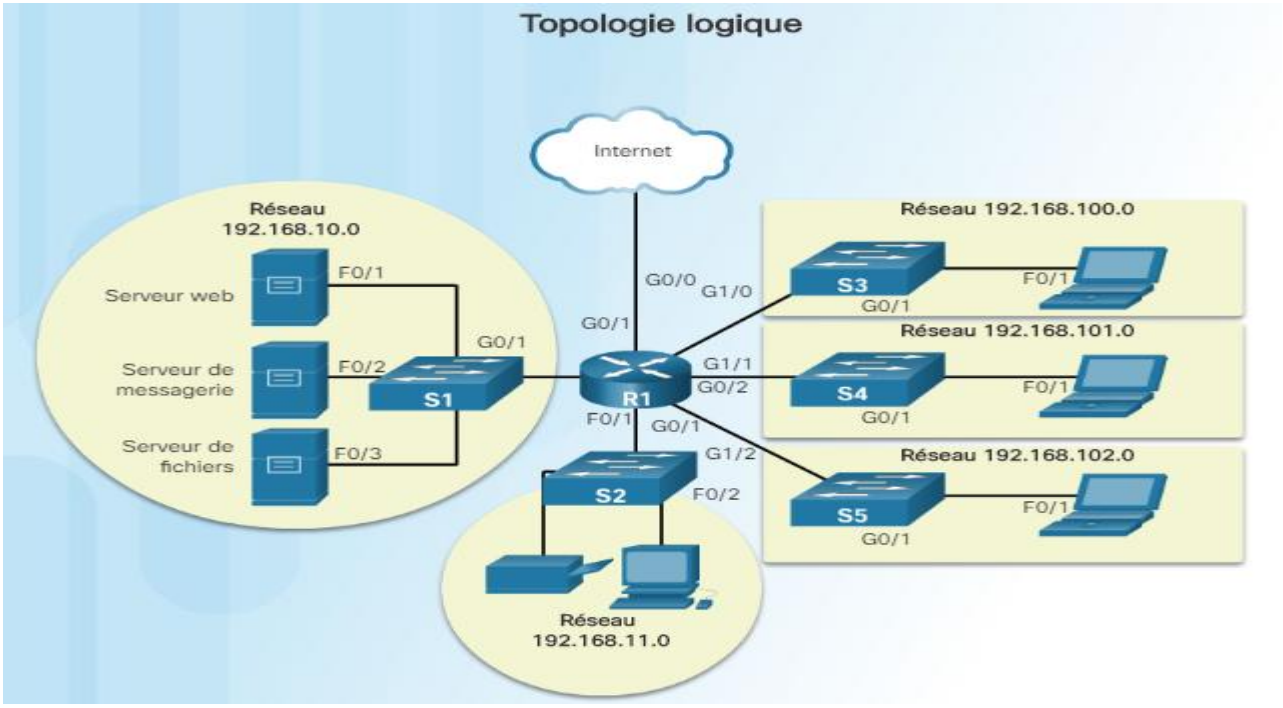
Token Ring repose sur une topologie en anneau (ring). Il utilise la méthode d'accès par jeton (token). Dans cette technologie, seul le poste ayant le jeton a le droit de transmettre. Si un poste veut émettre, il doit attendre jusqu'à ce qu'il ait le jeton.

Dans un réseau Token ring, chaque nœud du réseau comprend un MAU (Multi station Access Unit) qui peut recevoir les connexions des postes. Le signal qui circule est régénéré par chaque MAU.
Mettre en place un réseau token ring coûte chers, malgré que la panne d'une station MAU provoque le disfonctionnement du réseau.

3. Le FDDI :

La technologie LAN FDDI (Fiber Distributed Data Interface) est une technologie d'accès réseau utilisant des câbles fibres optiques. Le FDDI est constitué de deux anneaux : un anneau primaire et anneau secondaire. L'anneau secondaire sert à rattraper les erreurs de l'anneau.





III. LES TYPES DE RESEAU

Les infrastructures réseau peuvent considérablement varier en fonction des paramètres suivants :

- la taille de la zone couverte.
- le nombre d'utilisateurs connectés.
- le nombre et les types de services disponibles.

Les différents types de réseau sont :

1. LAN (Local Area Network) ou réseau local:

Un réseau local est une infrastructure réseau qui couvre une zone peu étendue. Les fonctionnalités spécifiques offertes par les LAN sont les suivantes :

- Les LAN relient des périphériques finaux dans une zone limitée telle qu'une maison, une école, un immeuble de bureaux ou un campus.
- En règle générale, un réseau local est administré par une seule entreprise ou une seule personne. Le contrôle administratif qui gère les stratégies de sécurité et de contrôle d'accès s'applique au niveau du réseau.
- Le réseau local fournit une bande passante très élevée aux périphériques finaux et aux périphériques intermédiaires internes.

2. MAN (Metropolitain Area Network) ou réseau métropolitain :

Infrastructure réseau qui couvre une zone plus vaste qu'un LAN, mais moins étendue qu'un WAN -(par exemple, une ville). Les MAN sont généralement gérées par une seule entité, comme une grande entreprise

Un MAN est formé de commutateurs ou de routeurs interconnectés par des liens hauts débits (en général en fibre optique).

3. WAN (Wide Area Network) ou réseau étendu :

Un réseau étendu (WAN) est une infrastructure réseau qui couvre une zone étendue. Les réseaux étendus sont généralement gérés par des prestataires de services ou des fournisseurs d'accès à Internet (FAI).

Les fonctionnalités spécifiques offertes par les WAN sont les suivantes :

- Les WAN relient des LAN sur des zones étendues couvrant des villes, des états, des provinces, des pays ou des continents.
- Les WAN sont habituellement gérés par plusieurs prestataires de services.
- Les réseaux WAN fournissent généralement des liaisons à plus bas débit entre les réseaux locaux.

4. LAN sans fil (WLAN) :

Infrastructure similaire à un réseau local, mais sans fil. Elle relie des utilisateurs et des terminaux situés dans une zone peu étendue.

5. Réseau de stockage SAN :

Infrastructure réseau conçue pour prendre en charge des serveurs de fichiers et pour fournir des fonctionnalités de stockage, de récupération et de réplication de données.

IV. LES TYPES D'ARCHITECTURES D'UN RESEAU INFORMATIQUE :

1. Définition d'une architecture d'un réseau informatique :

En informatique, architecture désigne la structure générale inhérente à un système informatique, l'organisation des différents éléments du système (logiciels, matériels, informations) et des relations entre les éléments.

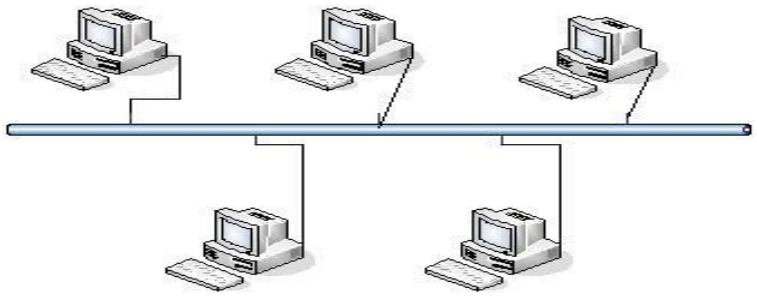
2. Les types d'architectures d'un réseau (poste à poste, client/serveur) :

Les premiers réseaux étaient constitués de matériels et de logiciels issus d'une seule société (IBM) qui cumulait les rôles de constructeur, d'architecte et d'éditeur, … Ces réseaux étaient vendus clefs en main, mais ils ne fonctionnaient pas avec d'autres réseaux, ils étaient compatibles avec eux même et c'était déjà beaucoup.

Les réseaux sont dits soit « **de postes à postes** », soit de type « **client/serveur** ».

Les réseaux Clients Serveurs ou Postes à Postes peuvent fonctionner sur toutes les topologies (en bus ou en étoile,…) et toutes les architectures (Ethernet, FDDI,…).

2.1. Architecture poste à poste :

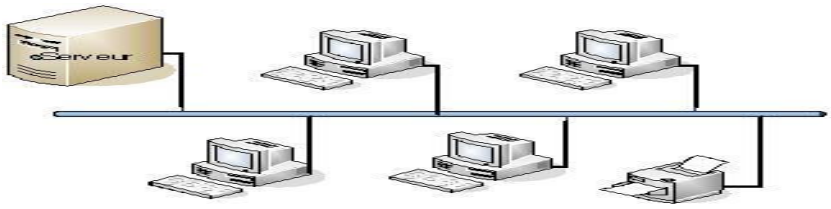


Un réseau poste à poste

Les réseaux postes à postes ne comportent en général que peu de postes, moins d'une dizaine de postes, parce que chaque utilisateur fait office d'administrateur de sa propre machine, il n'y a pas d'administrateur central, ni de super utilisateur, ni de hiérarchie entre les postes, ni entre les utilisateurs.
Chaque utilisateur décide lui-même des partages sur son disque dur et des permissions qu'il octroie aux autres utilisateurs.
Les réseaux Postes à Postes permettent de travailler en équipe, ou en « groupe de travail »

Les réseaux Postes à Postes sont faciles et pas cher à installer au départ mais deviennent très difficiles à gérer avec le temps.

2.2. Architecture client/serveur :



Un réseau client/serveur

Les réseaux Client/serveur comportent en général plus de dix postes. La plupart des stations sont des « **postes serveurs** », c'est à dire des ordinateurs dont se servent les utilisateurs, les autres stations sont dédiées à une ou plusieurs tâches spécialisées, on dit alors qu'ils sont des serveurs.

Les « **postes serveurs** » sont en général de puissantes machines, elles fonctionnent à plein régime et sans discontinuité.

Les serveurs peuvent être réservés ou dédiés à une certaine tâche :

- Les serveurs de fichiers et d'impression
- Les serveurs d'applications (applications bureautiques, applications de base de données)
- Les serveurs de messagerie
- Les serveurs de télécopies
- Les serveurs PROXY pour accéder aux services de l'Internet
- Les serveurs web pour publier le site Internet et servir les internautes
- Les serveurs RAS pour les accès à distance

Dans une organisation Clients Serveurs, les clients ne « voient » que le serveur.

Le système d'exploitation du serveur peut être différent de celui des stations clientes.

En tout cas, le système d'exploitation du serveur doit être véritablement multitâche afin de pouvoir servir un grand nombre de requêtes en même temps et de façon équitable, c'est à dire en octroyant le même temps processeur à chaque client.

2.3. L'avantage des réseaux Client/serveur :

L'avantage des réseaux Client/serveur est de réunir deux avantages complémentaires, l'indépendance et la centralisation :

- **L'indépendance :**

- Les stations peuvent travailler en mode autonome et ouvrir des sessions locales.
- Les communications se passent directement de clients à serveurs (sauf pour la connexion et le contrôle des droits et des permissions qui s'effectuent par l'intermédiaire d'un serveur d'authentification (qui peut être une machine dédiée), le Contrôleur Principal de Domaine dans un réseau NT).

- **La centralisation :**

- L'administration du réseau est réalisée par un administrateur ou un super utilisateur qui gère le réseau et qui a tous les droits…
- La standardisation des installations et des mises à jour des applications sur un très grand nombre de postes permet d'uniformiser la configuration d'un grand nombre de postes.
- La planification du réseau, son évolution, sa croissance, ses changements, etc.…
- La stratégie de sécurité
- Les sauvegardes

LEÇON N°02 : LES DIFFERENTES COUCHES DU MODELE OSI

OBJECTIF DE LA LEÇON N°02 : A la fin de cette leçon, le stagiaire doit être capable de caractériser les différentes couches du modèle OSI.

I. DESCRIPTION DU MODELE OSI :

1. Introduction :

Pour établir une communication entre deux ordinateurs il faut tenir compte des différences entre le matériel et le logiciel de chaque machine. Ces difficultés pour établir une communication se multiplient lorsqu'il s'agit d'interconnecter des réseaux mettant en jeu des matériels et des systèmes informatiques très différents. Pour créer un réseau, il faut utiliser un grand nombre de composants matériels et logiciels souvent conçus par des fabricants différents.

Pour que le réseau fonctionne, il faut que tous ces appareils soient capables de communiquer entre eux. Pour faciliter cette interconnexion, il est apparu indispensable d'adopter des normes. Ces normes sont établies par différents organismes de normalisation.

2. Les principaux organismes normalisateurs internationaux européens nationaux industriels :

- **AFNOR** : Association Française de Normalisation
- **ANSI :** American National Standard Institute
- **BSI** : British Standard Institute
- **UTT-T** : Union Internationale des Télécommunications
- **CCITT :** Comité Consultatif International pour le Télégraphe et le Téléphone
- **CEN** : Comité Européen de Normalisation
- **CENELEC** : CEN ELECtrotechnique
- **CEPT** : Conférence Européenne des Postes et Télécommunications

- **DIN** :Deusche Industry Norm
- **ECMA** :European Computer Manufactures Association
- **ISO** :International Standard Organization
- **IEEE :**Institute of Electrical and Electronics Engineers

Le modèle OSI (**O**pen **S**ystems **I**nterconnection) définit de quelle manière les ordinateurs et les périphériques en réseau doivent procéder pour communiquer :

• Il spécifie le comportement d'un système dit ouvert ;

• Les règles de communication constituent les protocoles normalisés ;

• Le modèle OSI est normalisé par l'ISO.

3. Description du modèle OSI :

Créé dans les années 80, se décompose en 7 parties appelées couches et suit les préceptes suivant :

- Chaque couche est responsable de l'un des aspects de la communication ;
- Une couche de niveau N communique avec les couches N+1 et N-1 par le biais d'une interface ;
- Une couche inférieure transporte les données delà couche supérieure sans en connaître la signification ;
- Les couches N de 2 systèmes communiquent à l'aide de protocoles de communication commun.

Les couches sont réparties selon les utilisations suivantes :

- Les couches 1 à 3 sont **orientées transmission** ;
- La couche 4 est **une couche intermédiaire** ;
- Les couches 5 à 7 **sont orientées traitement**.

II. LES 7 COUCHES DU MODELE OSI :

1.La couche application :

Cette couche définit les services Internet standard et les applications réseau à la disposition des utilisateurs. Ces services fonctionnent conjointement avec la couche transport pour assurer l'envoi et la réception de données. Les messages qui doivent être envoyés sur le réseau entrent dans le modèle OSI par cette couche (courrier électronique, transfert de fichiers).

2. La couche présentation :

Cette couche concerne la façon dont les systèmes différents représentent les données informatiques. Par exemple, elle définit ce qui se passe lorsqu'on essaie d'afficher des données provenant d'Unix sur un écran MS-DOS. Elle se charge également de la compression et du cryptage des données à transmettre puis du décryptage et de la décompression de celles-ci sur l'ordinateur destinataire.

3. La couche session :

Cette couche gère les connexions courantes entre systèmes. Elle tient compte de l'ordre des paquets de données et des communications bidirectionnelles. Les fonctions de cette couche permettent aux applications fonctionnant sur deux stations de travail de coordonner leurs communications en une seule session (qui peut être considérée comme un dialogue très structuré). La couche Session est responsable de la création de la session, de la gestion des paquets envoyés dans un sens et dans l'autre durant celle-ci ainsi que de sa clôture.

4. La couche transport :

Cette couche est l'équivalent du système de courrier recommandé. Elle s'assure que le courrier est bien remis à son destinataire. Si un paquet n'atteint pas sa destination, elle gère le processus consistant à prévenir l'expéditeur et à solliciter l'émission d'un autre exemplaire. En fait, elle s'assure que les trois couches situées au-dessous d'elle (c'est-à-dire les couches 1.2.3) font leur travail correctement. A défaut, le logiciel de la couche 4 peut intervenir et gérer la correction des erreurs en renvoyant les paquets altérés ou manquants. Les protocoles TCP et UDP fournissent également des services à la plupart des applications.

5. La couche réseau :

Cette couche gère l'adressage et l'acheminement des données (en les envoyant dans la bonne direction au bon destinataire lors des transmissions sortantes et en recevant les transmissions entrantes au niveau du paquet) Alors que, la couche Liaison de données ne connaît que l'ordinateur immédiatement adjacent, la couche Réseau est responsable de la ROUTE COMPLETE d'un paquet, de la source à la destination. IPX **et** IP sont des exemples de protocoles de la couche réseau**.**

IPX (Internetwork Packet eXchange).

6. La couche liaison de données :

La couche Liaison de données assure un transit fiable des données sur une liaison physique. Du fait de sa complexité, la couche de liaison de données est souvent subdivisée en une couche de *contrôle d'accès au support* (MAC) et une couche de *contrôle de liaison logique* (LLC).

- La couche de contrôle d'accès au support (MAC) régit l'accès au réseau (passage de jetons et détection de collisions) et contrôle ce réseau.
- La couche de contrôle de liaison logique(LLC), a pour rôle d'envoyer et de recevoir les messages de données de l'utilisateur. Ethernet et Token Ring sont des protocoles de la couche de liaison de données.

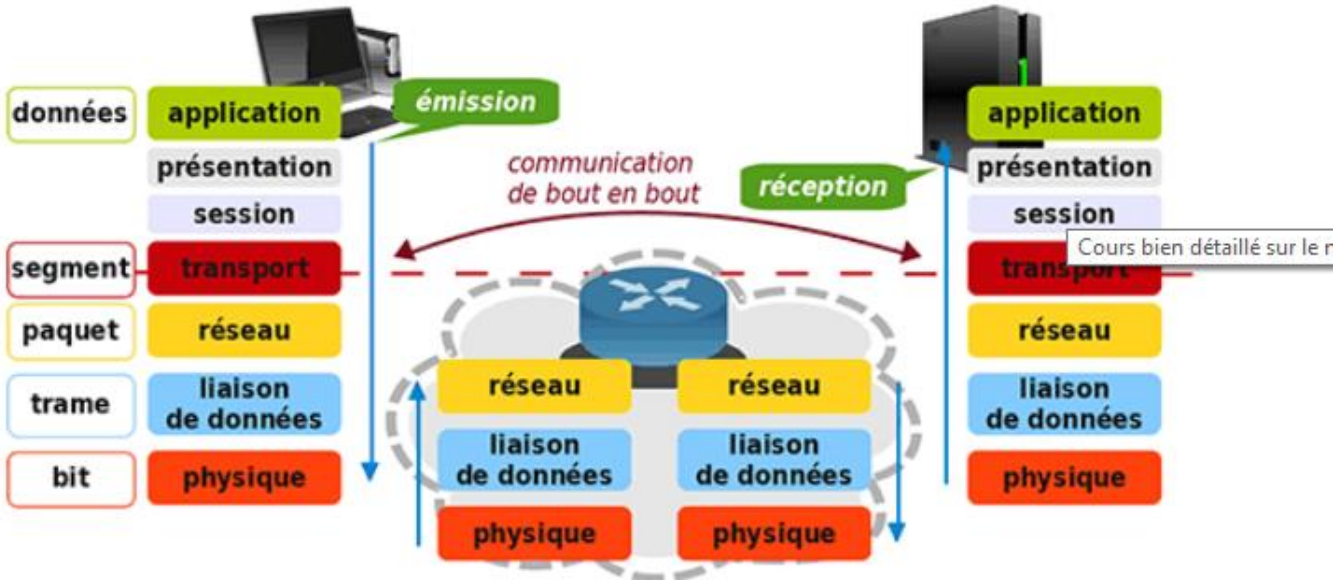
C'est l'endroit où les adresses des cartes réseau (**adresses MAC**) deviennent importantes. La couche 2 se charge en outre de reconditionner les paquets dans des cadres (frames), qui correspondent au format de transmission des données par les équipements matériels opérant aux niveaux inférieurs à la couche 3.

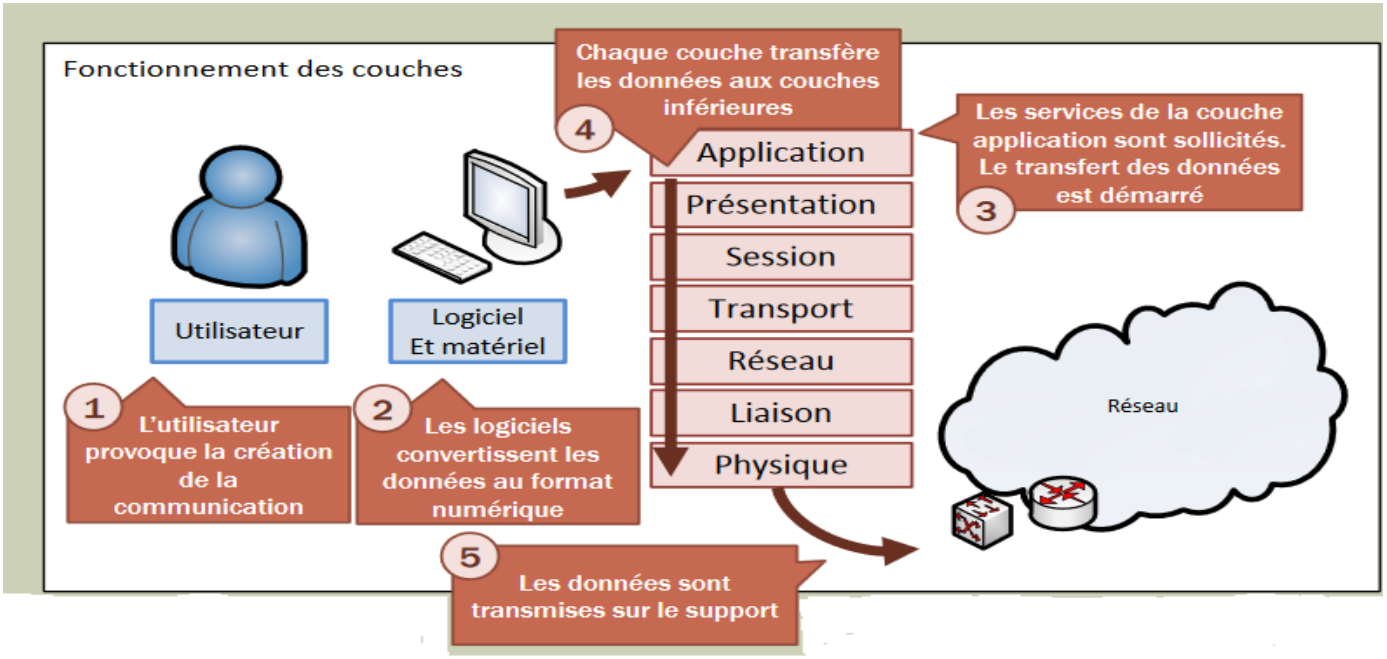
7. La couche physique :

Cette couche est chargée de la transmission des bits sur le réseau au niveau électrique, optique ou radio. Elle fournit les moyens matériels pour l'envoi et la réception de données (c'est l'équivalent des camions, des trains et des avions transportant le courrier).

TABLEAU RECAPITULATIF DES COUCHES

7	Application	Fournit un point d'accès aux services réseaux. Le modèle ne donne aucune spécification à cette couche
6	Présentation	Chargée du codage et de la conversion des données applicatives transmises
5	Session	Gère la synchronisation des échanges et des transactions par ouverture ou fermeture de session
4	Transport	Gère les communications de bout en bout entre processus
3	Réseau	Gère les communications de proche en proche à travers des réseaux physiques différents
2	Liaison	Gère les communication entre 2 hôtes reliés directement par un support physique.
1	Physique	Chargée de transmettre les données à envoyer sur le support physique. Service limité à l'envoi d'un bit



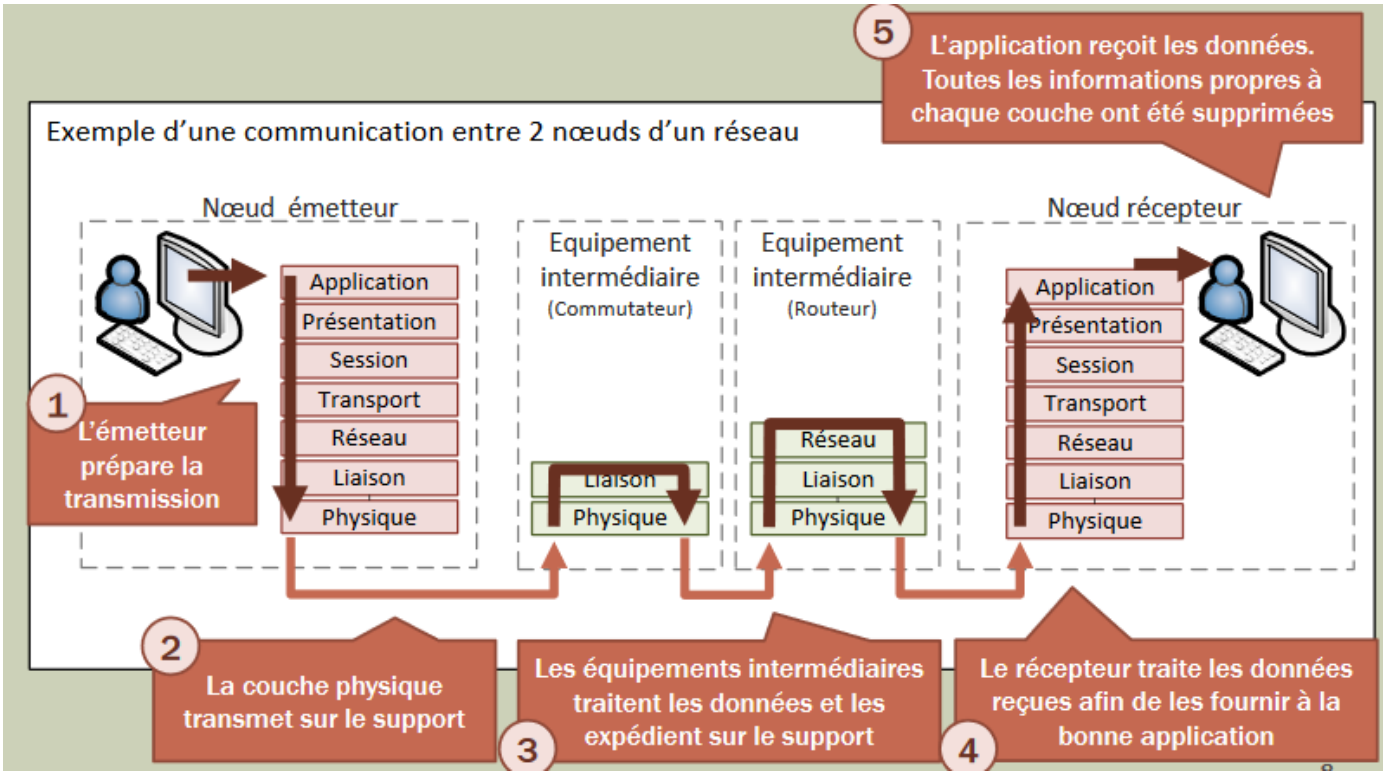


III. LES REGLES SUR LES DIFFERENTES COUCHES DU MODELE OSI :

Le modèle OSI définit deux règles. En plus du fait d'avoir des rôles spécifiques, chaque couche doit respecter deux conditions.

Chaque couche doit être indépendante l'une de l'autre. Les informations qu'utilisera une couche ne pourront donc pas être utilisées par une autre couche. Cette règle permet d'assurer l'évolution des communications au travers du temps. Cela permet de mettre en place des évolutions du réseau de façon transparente sans impacter fortement les utilisateurs et les constructeurs. Le fait qu'elles soient indépendantes l'une de l'autre permet également de les interchanger si besoin.

La deuxième règle du modèle OSI est que chaque couche ne peut communiquer uniquement qu'avec les couches adjacentes. La couche trois pourras donc communiquer avec la couche deux mais pas avec la couche cinq ou encore la couche six.



IV.TERMINOLOGIE LIEE AU MODELE OSI :

1. Encapsulation des données :

- **Message :** c'est un regroupement logique de données au niveau de la couche 7 (application), souvent composé d'un certain nombre de groupes logiques de couches inférieures, par exemple des paquets.
- **Segment** : c'est un terme utilisé pour décrire une unité d'information de la couche de transport.
- **Paquet** : c'est un regroupement logique d'informations comportant un en-tête qui contient les données de contrôle et (habituellement) les données utilisateur. Le terme paquets est le plus souvent utilisé pour désigner les unités de données au niveau de la couche réseau
- **Trame** : c'est un regroupement logique de données envoyé comme unité de couche liaison de données par un média de transmission.
- **Datagramme** : c'est un regroupement logique de données envoyé comme unité de couche réseau par un média de transmission, sans établissement préalable d'un circuit virtuel. Les datagrammes
- **IP** sont les principales unités d'information sur Internet.

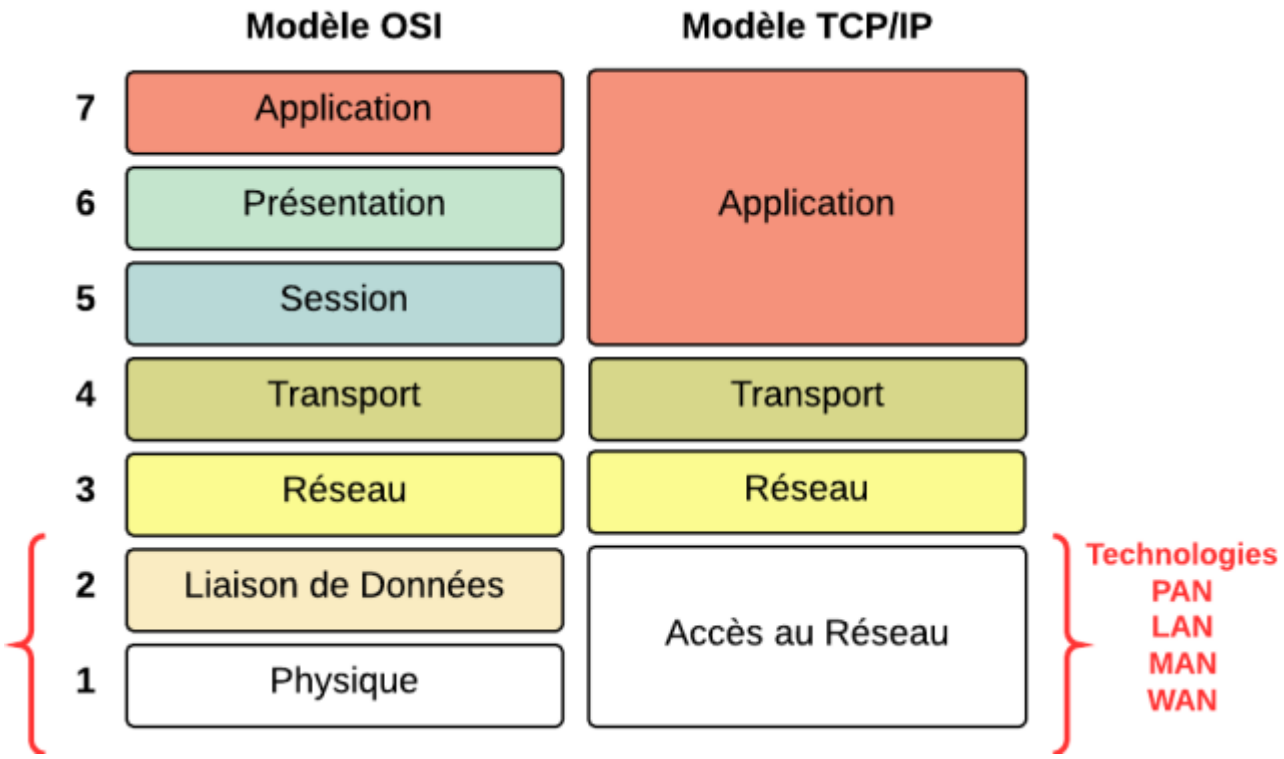
- **SDU** : **(Service data unit) unité de données de service**. Unité d'information d'un protocole de couche supérieure qui définit une demande de service à un protocole de couche inférieure.
- **PDU** : **(Protocol data unit) unité de données de protocole**. Terme OSI désignant un paquet.

2. Le modèle TCP /IP :

Ce protocole de communication est un ensemble de règles permettant à plusieurs ordinateurs de dialoguer entre eux. A la manière des humains, les ordinateurs doivent parler le même langage afin de se comprendre
TCP/IP: «Protocole de communication pour la transmission de données».

- **TCP** : Transmission Control Protocol.
- **IP** : Internet Protocol.

2.1. Description des quatre couches du modèle TCP/IP :



Le ministère américain de la Défense a créé le modèle de référence TCP/IP parce qu'il avait besoin d'un réseau pouvant résister à toutes les conditions, même à une guerre nucléaire. Le ministère de la Défense veut que ses paquets se rendent à chaque fois d'un point quelconque à tout autre point, peu importe les conditions. C'est ce problème de conception très épineux qui a mené à la création du modèle TCP/IP qui, depuis lors, est devenu la norme sur laquelle repose Internet.

Le modèle TCP/IP comporte quatre couches : la couche application, la couche transport, la couche Internet et la couche d'accès au réseau. Comme vous pouvez le constater, certaines couches du modèle TCP/IP portent le même nom que des couches du modèle OSI. Il ne faut pas confondre les couches des deux modèles, car la couche application comporte des fonctions différentes dans chaque modèle.

- **La couche application :**

La couche application gère les protocoles de haut niveau : représentation codage et contrôle du dialogue.

Le modèle TCP/IP regroupe en une seule couche tous les aspects liés aux applications et suppose que les données sont préparées de manière adéquate pour la couche suivante.

- **La couche transport :**

La couche transport est chargée des questions de qualité de service touchant la fiabilité, le contrôle de flux et la correction des erreurs. L'un de ses protocoles, TCP (Transmission Control Protocol – protocole de contrôle de transmission), fournit d'excellents moyens de créer, en souplesse, des communications réseau fiables, circulant bien et présentant un taux d'erreurs peu élevé. Le protocole TCP est orienté connexion. Il établit un dialogue entre l'ordinateur source et l'ordinateur de destination pendant qu'il prépare les informations de couche application en unités appelées segments.

- **La couche Internet :**

Le rôle de la couche Internet consiste à envoyer des paquets source à partir d'un réseau quelconque de l'inter- réseau et à les faire parvenir à destination, indépendamment du trajet et des réseaux traversés pour y arriver. Le protocole qui régit cette couche est appelé protocole IP (Internet Protocol).

L'identification du meilleur chemin et la commutation de paquets ont lieu au niveau de cette couche.

- **La couche d'accès au réseau :**

Cette couche se charge de tout ce dont un paquet IP a besoin pour établir une liaison physique, puis une autre liaison physique. Cela comprend les détails sur les technologies LAN et WAN, ainsi que tous les détails dans les couches « physique et liaison de données » du modèle OSI.

2.2. Vue d'ensemble des applications TCP/IP :

- **Modèle client / serveur :**

La plupart des applications TCP/IP fonctionnent sur le modèle client / serveur. Un serveur est une machine TCP/IP sur laquelle tourne un logiciel serveur qui a pour rôle principal d'attendre un message de la part d'un client. Il analyse la requête du client, formate sa réponse et la renvoie au client.

L'exemple typique est le navigateur web, qui demande au serveur de lui envoyer une page. La demande se fait sous la forme d'une chaîne de caractères : « http ://www.google.fr/index.html». Le serveur (en l'occurrence la machine qui a pour nom « www» dans le domaine « google.fr ») renvoie le contenu de la page « index.html » --(<html><body> ... </html></body>), et le logiciel client l'interprète et l'affiche en retour.

- **Telnet (Terminal Emulation Protocol) :**

Telnet permet à un utilisateur de se connecter à distance sur un hôte. L'utilisateur travaille sur l'hôte distant comme s'il était directement connecté dessus. Les séquences de touche tapées sur l'ordinateur sont envoyées à l'hôte qui les interprète et renvoie les réponses à l'ordinateur appelant.

- **Ftp (File Transfert Protocol) :**

Ftp permet de transférer des fichiers entre deux machines sur un réseau TCP/IP. Le client se connecte au serveur distant et établi une session interactive. Il peut alors visualiser les fichiers et les répertoires distants et lancer des commandes de transfert.

- **Smtp (Simple Mail Transfert Protocol) :**

Smtp permet à un utilisateur d'envoyer un message à un destinataire connecté à un réseau TCP/IP. Le message est composé sous forme de texte, et l'utilisateur tape l'adresse électronique du destinataire, l'objet du message et le texte lui-même. Smtp utilise TCP/IP pour envoyer ce message à un serveur de messagerie. Les serveurs de messagerie agissent comme des relais et délivrent leurs messages au destinataire.

- **Snmp (Simple Network Management Protocol) :**

Snmp permet la gestion à distance de périphériques tels que les ponts, routeurs ou switch. Un agent Snmp doit tourner sur ces périphériques. Une station Snmp envoie des requêtes pour lire ou modifier les paramètres d'un périphérique. Il utilise UDP et IP.

- **Dns (Domain Name System) :**

Dns constitue un annuaire électronique permettant de nommer les différentes ressources d'un réseau. Dns associe les noms des périphériques à leur adresse IP. Par exemple l'hôte **www.google.com** a pour adresse IP : 216.239.51.101. Les noms Dns jouent un rôle prépondérant dans tous les protocoles TCP/IP, car ils permettent de travailler avec des mots plutôt que des chiffres.

- **Http (Hyper Text Transfert Protocol):**

Http est un protocole permettant d'envoyer des pages web à un ordinateur équipé d'un navigateur. Ce navigateur peut lire des documents textes, graphiques, audio ou vidéo.

LEÇON N°03 : LES TYPES D'INTERFACES DE COMMUTATION DES DONNEES

OBJECTIF DE LA LEÇON N°03 : A la fin de cette leçon, le stagiaire doit être capable de reconnaître les différents Protocoles de commutation.

I. INTRODUCTION A LA COMMUTATION :

A l'invention du téléphone par Alexandre Graham Bell, uniquement deux postes peuvent être en liaison dans deux pièces d'une même habitation Conséquence : un certain nombre de postes reliés en dérivation sur une même ligne et impossibilité de communiquer avec un poste raccordé sur une autre ligne. La solution était de trouver un moyen avec lequel chaque téléphone peut être connecté ou commuté (connecter temporairement) avec n'importe quel autre téléphone. Une des solutions était de connecter chaque ligne avec tous les autres. Si on a par exemple six postes il nous faudrait 15 lignes, pour N abonnés il nous faut N (N-1)/2 lignes. Cette solution n'est pas pratique si N est grand. Une solution pratique dans le temps était de faire emmener les lignes téléphoniques vers un centre où elles seront commutées entre elles à l'aide d'un opérateur, le premier standard manuel.

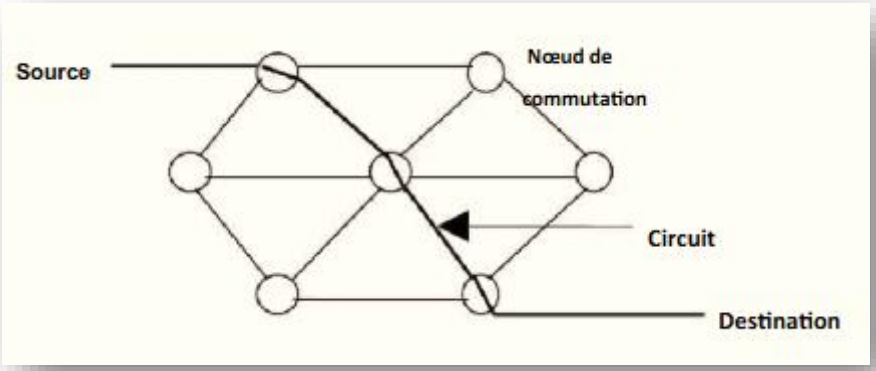
DEFINITION

Un réseau peut être défini comme étant un ensemble complexe de moyens techniques permettant le transfert d'un signal correspondant à une information codée ; il peut être géré par un opérateur public ou privé. Le réseau est donc constitué d'un ensemble de voies de transmission et de moyens nécessaires pour les relier entre elles afin de les attribuer aux usagers. L'attribution des voies de transmission, appelée aussi assignation, peut être fixe ou variable suivant le type de service rendu. Dans le cas où l'assignation est variable une opération de commutation est nécessaire.

II. LES MODES DE COMMUTATION :

1.LA COMMUTATION DE CIRCUITS :

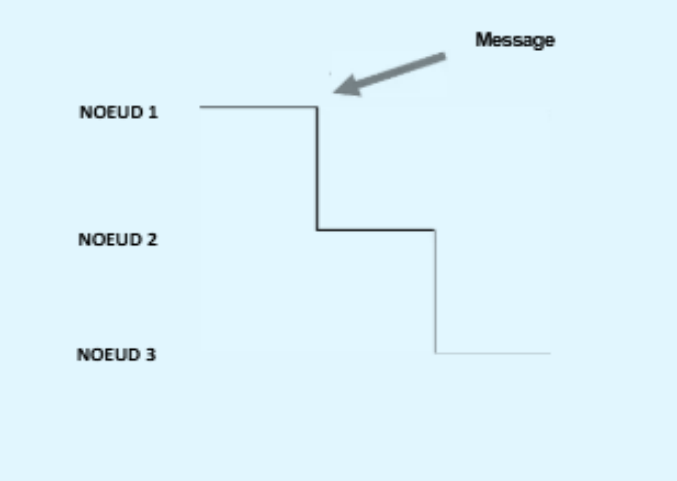
Cette technique a été utilisée pour la transmission de données avant l'apparition de réseaux spécialisés pour les données. Un circuit matérialisé est construit entre la source et la destination. Ce circuit n'appartient qu'aux deux entités qui se communiquent.



1.1. Principe de la commutation de circuit :

Le circuit doit être établi avant que des informations puissent transiter. Il dure jusqu'au moment où l'un des deux abonnés interrompt la communication. Si les deux correspondants n'ont plus de données à transmettre pendant un certain temps la liaison reste inutilisée. La commutation de circuits ne fait intervenir que des circuits de jonction et la connexion peut être spatiale ou temporelle. La communication par commutation de circuits est fondée sur la négociation et la construction d'un chemin unique exclusif d'une machine A à une machine B, lors de l'établissement d'une séquence de dialogue entre ces deux machines. Le chemin ainsi créé perdure jusqu'à la clôture de la séquence de dialogue qu'il sous-entend. Ce chemin est appelé un circuit, d'où le nom de cette méthode de communication. La technique de commutation par commutation de circuits, très utilisée en télécommunication, a pendant longtemps été réalisée à l'aide de centraux téléphoniques établissant physiquement les connexions lors de la construction des circuits, d'abord grâce aux petites mains des employées des téléphones qui établissaient des liaisons entre des paires de connecteurs sur un tableau électrique, puis de façon automatisée. Actuellement, la tendance s'oriente vers les circuits virtuels construits sur des réseaux à commutation de paquet

Un message est une suite d'informations logique formant un ensemble non dé coupable logiquement aussi bien pour l'expéditeur que pour le destinataire, par exemple : un fichier complet, une ligne tapée sur un terminal, un secteur de disque (exemple de boite aux lettres). La commutation de message est un processus d'acheminement de messages dans un réseau de télécommunication sans établissement préalable d'un circuit de bout en bout, par réception, mise en mémoire et retransmission des messages complets de proche en proche vers leur destination Un réseau de commutation de messages se présente sous la forme suivante



1.2. Principe de transfert d'un message :

C'est un réseau maillé de nœud de commutation, le message y est envoyé de nœud en nœud jusqu'au destinataire. Il ne pas être envoyé au nœud suivant tant qu'il n'a pas été reçu complètement et correctement dans le nœud précédant. Il faut des mémoires au niveau des nœuds intermédiaires pour le stockage des messages tant que ceux-ci ne sont pas correctement reçus. Un système de gestion des transmissions permet d'acquitter les messages correctement reçus et demande la retransmission des messages erronés : Il faut donc un système de contrôle de flux dans les nœuds. Une des difficultés est la transmission correcte de très long message. Pour un taux d'erreurs de 10 Bit (1 bit erroné sur 10 sur le réseau téléphonique) un message de longueur 100 000 octets n'a qu'une possibilité de 0,0003 d'arriver correctement. La communication est unidirectionnelle et la réception d'un message nécessite une longue durée.

2. LA COMMUTATION DE PAQUETS :

Avec l'évolution rapide des besoins des utilisateurs dans le domaine de la transmission de données et pour accélérer la vitesse de transmission, les réseaux de commutation de paquets sont nés. Le paquet est une suite d'informations binaire ne pouvant pas dépasser une longueur de valeur fixée à l'avance. Ainsi les messages des utilisateurs sont découpés en paquets qui ont couramment une longueur maximale de l'ordre de 1000 à 2000 bits.

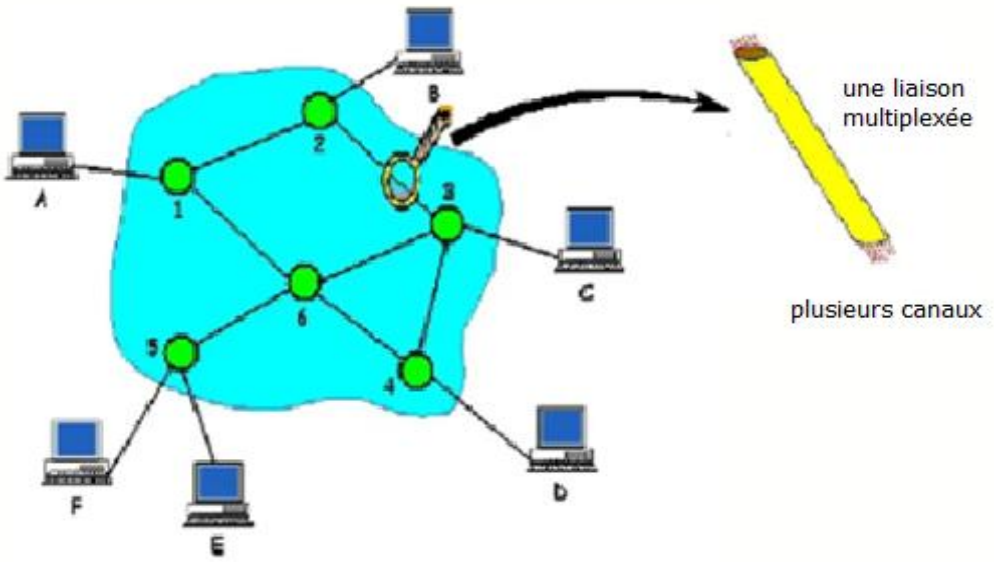
La commutation de paquets est un processus d'acheminement dans lequel les messages sont découpés en paquets, chaque paquet comportant les adresses nécessaires à son routage. Dans les nœuds du réseau, ces paquets sont reçus dans une file d'attente et retransmis, après analyse des adresses, sur la voie de transmission appropriée ; à l'arrivée, on reconstitue les messages à partir des paquets reçus.

Puisqu'un paquet n'occupe une voie que pendant sa transmission, la voie est ensuite disponible pour la transmission d'autres paquets appartenant soit au même message, soit à d'autres messages.

Le point de différenciation essentiel entre la commutation de paquets et la commutation de circuits est le schéma de gestion/réservation des ressources au niveau des unités d'acheminement intermédiaires.

La commutation de circuits nécessite la réservation de ressources de communication durant toute la durée de la conversation et sur un trajet complet entre les deux machines impliquées dans le dialogue. A l'opposé, dans le cas de la commutation de paquets, la réservation de ressources ne concerne pour un paquet donné que la liaison reliant deux unités d'acheminement sur laquelle le paquet considéré est actuellement en cours de transit, et uniquement pendant la durée de transit de ce paquet entre les deux unités d'acheminement considérées. Un avantage évident de la commutation de paquets sur la commutation de circuits est donc une utilisation beaucoup plus rationnelle des ressources de communication : les ressources ne sont réservées que durant leur utilisation.

Les paquets de plusieurs messages peuvent donc être multiplexés temporellement sur une même liaison. Le rôle des nœuds de commutation est d'aiguiller les paquets vers la bonne sortie ce qui peut être donné par une table de routage.



LEÇON N°04: LE MODE D'ADRESSAGE INTRANET /INTERNET ET LES PROTOCOLES DE ROUTAGE

Objectif de la leçon n°04 : A la fin de cette leçon, le stagiaire doit être capable de reconnaître le mode d'adressage et les protocoles de routage.

I.ADRESSAGE DANS UN INTRANET ET INTERNET :

Les adresses réseau (IP) sont utilisées pour identifier les appareils aussi bien dans un **Intranet** (réseau privé) que sur l'**Internet** (réseau public). Cependant, leur attribution et leur gestion diffèrent.

1. Adressage dans un Intranet (Réseau Privé)

Un **Intranet** est un réseau local (LAN) ou étendu (WAN) interne à une organisation, utilisant des **adresses IP privées**.

Caractéristiques :

- **Plages d'adresses privées** (définies par la RFC 1918) :
  - **Classe A** : `10.0.0.0` → `10.255.255.255` (16 millions d'adresses)
  - **Classe B** : `172.16.0.0` → `172.31.255.255` (1 million d'adresses)
  - **Classe C** : `192.168.0.0` → `192.168.255.255` (65 000 adresses)

- **Pas routables sur Internet** : Ces adresses ne peuvent pas être utilisées directement sur le web.
- **Attribution** :
  - **Manuelle** : Configuration statique (ex: serveurs locaux).
  - **Automatique** : Via **DHCP** (Dynamic Host Configuration Protocol) pour les postes clients.

- **NAT (Network Address Translation)** : Permet à plusieurs appareils d'utiliser une seule IP publique pour accéder à Internet.

Exemple :

- Un PC dans un réseau d'entreprise a l'IP `192.168.1.10`.
- Le routeur utilise le NAT pour traduire cette IP en une adresse publique (ex: `203.0.113.5`) lorsqu'il communique avec Internet.

2. Adressage sur Internet (Réseau Public)

Internet utilise des **adresses IP publiques**, uniques et routables globalement.

Caractéristiques :

- **Plages d'adresses publiques** :
- Attribuées par l'**IANA** (Internet Assigned Numbers Authority) et les **RIR** (RIR : RIPE, ARIN, APNIC…).
- **IPv4 vs. IPv6** :
- **IPv4** (ex: 203.0.113.5) : Limité à ~4,3 milliards d'adresses (épuisement progressif).
- **IPv6** (ex: 2001:0db8:85a3::8a2e:0370:7334) : 340 undécillions d'adresses (solution à long terme).
- **Attribution** :
- **Fournisseurs d'accès (FAI)** : Attribuent dynamiquement (DHCP) ou statiquement des IP publiques.
- **Serveurs dédiés** : IP fixes pour les sites web (ex: 93.184.216.34 pour example.com).
- **DNS (Domain Name System)** : Convertit les noms de domaine (ex: google.com) en IP publiques.

Exemple :

- Un serveur web a l'IP publique 93.184.216.34.
- Un utilisateur y accède via le nom de domaine example.com.

3. L'adresse IP :

L'adresse IP identifie l'emplacement d'un hôte sur le réseau. Une adresse IP doit être unique et présenter un format normalisé.

Chaque adresse IP comporte deux parties : un **ID de réseau** et **un ID d'hôte.**

- Tous les hôtes d'un même réseau doivent avoir le même **ID réseau**, unique dans l'inter-réseau.
- L'ID d'hôte identifie une station de travail, un serveur, un routeur ou tout autre hôte TCP/IP du réseau. L'ID d'hôte doit être unique pour chaque ID de réseau.

Chaque hôte TCP/IP est identifié par une adresse IP logique. Tous les hôtes et les composants du réseau qui communiquent à l'aide de TCP/IP doivent posséder une adresse IP unique.

Deux formats permettent de faire référence à une adresse IP le format binaire et la notation décimale pointée.

Chaque adresse IP a une longueur de **32 bits** et est composée de **quatre champs de 8 bits (d'octets).** Les octets sont séparés par des points et représentent un nombre décimal compris entre 0 et 255.

Les 32 bits de l'adresse IP sont alloués à l'ID de réseau et à l'ID d'hôte.

Exemple :

Format binaire format décimal à points Format décimal

11000000 10101000 00000001 00001111 192.168.1.15

Conversion d'adresses IP du format binaire en format décimal

Le bit de poids faible représente la valeur décimale 1, le bit de poids fort la valeur décimale 128. La valeur décimale la plus élevée d'un octet est 255 c'est à dire tous les bits sont mis à 1.

Le tableau suivant indique comment les bits d'un octet sont convertis d'un code binaire en une valeur décimale

Code binaire	Valeurs binaires	Valeur décimale
00000000	0	0
00000001	1	1
00000011	1+2	3
00000111	1+2+4	7
00001111	1+2+4+8	15
00011111	1+2+4+8+16	31
00111111	1+2+4+8+16+32	63
01111111	1+2+4+8+16+32+64	127
11111111	1+2+4+8+16+32+64+128	255

- La partie réseau est appelée aussi **préfixe**, et le nombre de bits de la partie réseau définit la longueur de préfixe qui définit le nombre des 1 pour le masque sous réseau.

Exemple : 192.168.10.0/24

Masque sous réseau

Pour que le réseau Internet puisse router (acheminer) les paquets de données, il faut qu'il connaisse l'adresse du réseau de destination. Pour déterminer cette adresse réseau à partir de l'adresse IP de destination, on utilise le masque de sous réseau.

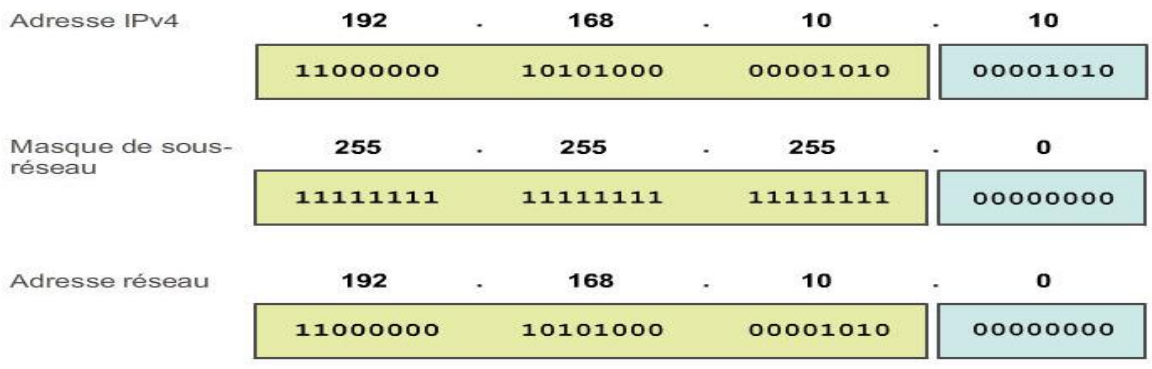
Format du masque : Le masque de réseau, ou Netmask, est constitué de 32 bits. Les bits à « 1 » sont tous à gauche alors que les « 0 » sont tous à droite. On dit que les bits à « 1 » sont contigus (c'est-à-dire collés).

Exemples de masques : 11111111.00000000.00000000.00000000 = 255.0.0.0

11111111.11111111.11111111.00000000 = 255.255.255.0

Exemple de masque invalide : 11111111.01111111.00000000.00000000

Calcul de l'adresse réseau : Un « ET » logique appliqué entre le masque de réseau et l'adresse IP permet d'obtenir l'adresse d'un réseau correspondant.



1 AND 1 = 1 1 AND 0 = 0 0 AND1 =0 0 AND 0 = 0

3.1. Classes d'adresse IP:

Il existe différentes classes d'adresse IP. Chaque classe définit la partie de l'adresse IP qui identifie l'ID de réseau et celle qui identifie l'ID d'hôte.

La communauté Internet a défini 5 classes d'adresse IP pour les différentes tailles de réseau (A, B, C, D et E). Microsoft TCP/IP prend en charge les adresses de classe **A**, **B** et **C** affectées aux hôtes.

La classe d'adresse définit les bits utilisés pour l'ID de réseau et pour l'ID d'hôte. Elle définit également le nombre de réseaux et le nombre d'hôtes par réseau autorisés.
On peut identifier la classe d'adresse par le nombre contenu dans le premier octet. Le schéma d'adressage IP **32 bits** prend en charge un nombre total de **3 720 314 628 hôtes (2^{32}).**

Classe A : Les adresses de classe A sont attribuées aux réseaux de grande taille « un nombre élevé d'hôtes ».

Dans un réseau de classe A : - les 8 premiers bits (dits bits de poids fort) sont affecté à la partie réseau

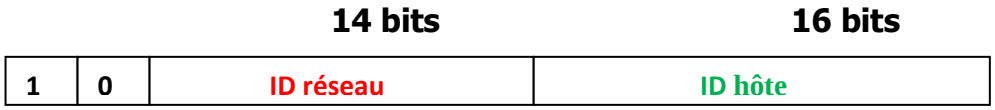
- les 24 bits restants sont pour la partie hôte.

Cette classe autorise **126 réseaux (2^{7} -2)** et environ **17 millions d'hôtes** par réseau **(2^{24} – 2).**

Ses adresses IP : 0.0.0.0 à 127.255.255.255 (adresses privées et publiques). **Préfixe** =8

Classe B : Les adresses de classe B sont attribuées à des réseaux de taille moyenne à grande. Dans un réseau de classe B : - les 16 premiers bits (dits bits de poids fort) sont affecté à la partie réseau

- les 16 bits restants représentent la partie hôte.

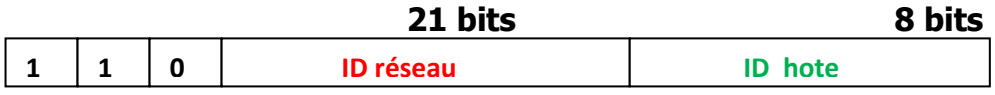


Cette classe autorise **16384 réseaux (2^{14})** contenant chacun **65 000 hôtes** environ **(2^{16} – 2).**

Ses adresses IP : 128.0.0.0 à 191.255.255.255 (adresses privées et publiques). **Préfixe** = 16

Classe C : Les adresses de classe C sont généralement employées pour de petits réseaux locaux. Dans un réseau de classe C : - les 24premiers bits (dits bits de poids fort) sont affecté à la partie réseau

- les 8 bits restants représentent la partie hôte.



Cette classe autorise environ **2 millions de réseaux (2^{21})** contenant chacun **254 hôtes (2^{8} – 2).**

Ses adresses IP : 192.0.0.0 à 223.255.255.255 (adresses privées et publiques). **Préfixe** = 24

Classe D : Les adresses de classe D sont réservées aux groupes de diffusion multipoint. Un groupe de diffusion multipoint peut contenir un, plusieurs ou aucun hôte. Les 4 bits de poids forts ont toujours les valeurs binaires 1110.
Les bits restants sont attribués de manière unique à chaque groupe d'hôtes. Il n'y a aucun bit de réseau ou d'hôte dans des opérations de diffusion multipoint. Les paquets sont passés à un sous-ensemble sélectionné d'hôtes sur un réseau. Seuls les hôtes enregistrés pour l'adresse de diffusion multipoint acceptent le paquet.
Ses adresses IP : 224.0.0.0 à 239.255.255.255 (adresses de multicast).

Classe E : Les adresses de classe E sont expérimentales, elles sont réservées par IANA à un usage non déterminé. Les bits de poids fort ont toujours la valeur binaire 1111.
Ses adresses IP : 240.0.0.0 à 255.255.255.255 (adresses réservées par l'IETF).

4. Adressage ipv4 :

4.1. Les adresses ipv4 publiques et privées

À l'origine, un organisme portant le nom d'InterNIC (Internet Network Information Center) était chargé de la vérification de l'unicité des adresses IP. Celui-ci n'existe plus et a été remplacé par l'IANA
(Internet Assigned Numbers Authority).

Chaque adresse IP publique étant unique, deux ordinateurs connectés à un réseau public ne peuvent pas avoir la même adresse IP publique.

Les adresses IP publiques doivent être obtenues auprès d'un fournisseur d'accès Internet (FAI) ou d'un registre moyennant une participation.

Blocs d'adresses privées :

Les hôtes qui n'ont pas besoin d'accéder à Internet peuvent utiliser des adresses privées

- 10.0.0.0 à 10.255.255.255 (10.0.0.0/8)
- 172.16.0.0 à 172.31.255.255 (172.16.0.0/12)
- 192.168.0.0 à 192.168.255.255 (192.168.0.0/16)

4.2. Les adresses ipv4 réservées :

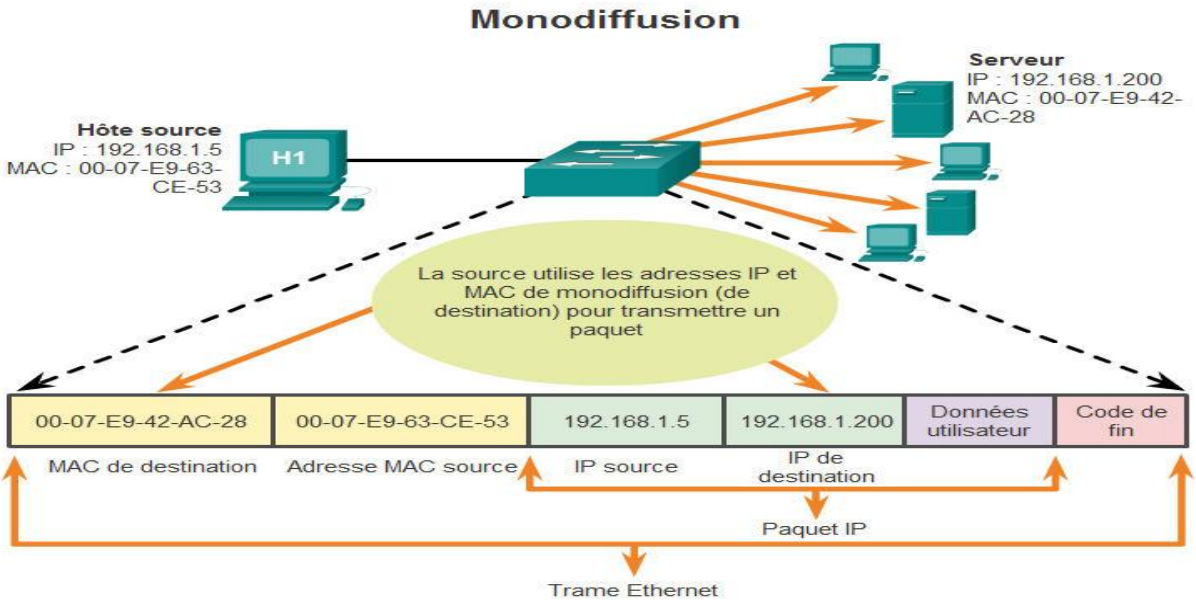
- **Adresses réseau et de diffusion :** dans chaque réseau, les première et dernière adresses ne peuvent pas être attribuées à des hôtes

  L'adresse de diffusion « broadcast »permet à une machine d'envoyer un datagramme à toutes les machines d'un réseau. Cette adresse est celle obtenue en mettant tous les bits de l'host-id à 1.
- **Adresse de bouclage :** 127.0.0.1 est une adresse spéciale utilisée par les hôtes pour diriger le trafic vers eux-mêmes (les adresses de 127.0.0.0 à 127.255.255.255 sont réservées)
- **Adresse Link-local :** les adresses de 169.254.0.0 à 169.254.255.255 (169.254.0.0/16) peuvent être automatiquement attribuées à l'hôte local
- **Adresses TEST-NET :** les adresses de 192.0.2.0 à 192.0.2.255 (192.0.2.0/24) sont réservées à des fins pédagogiques et utilisées dans la documentation et dans des exemples de réseau
- **Adresses expérimentales :** les adresses de 240.0.0.0 à 255.255.255.254 sont indiquées comme étant réservées

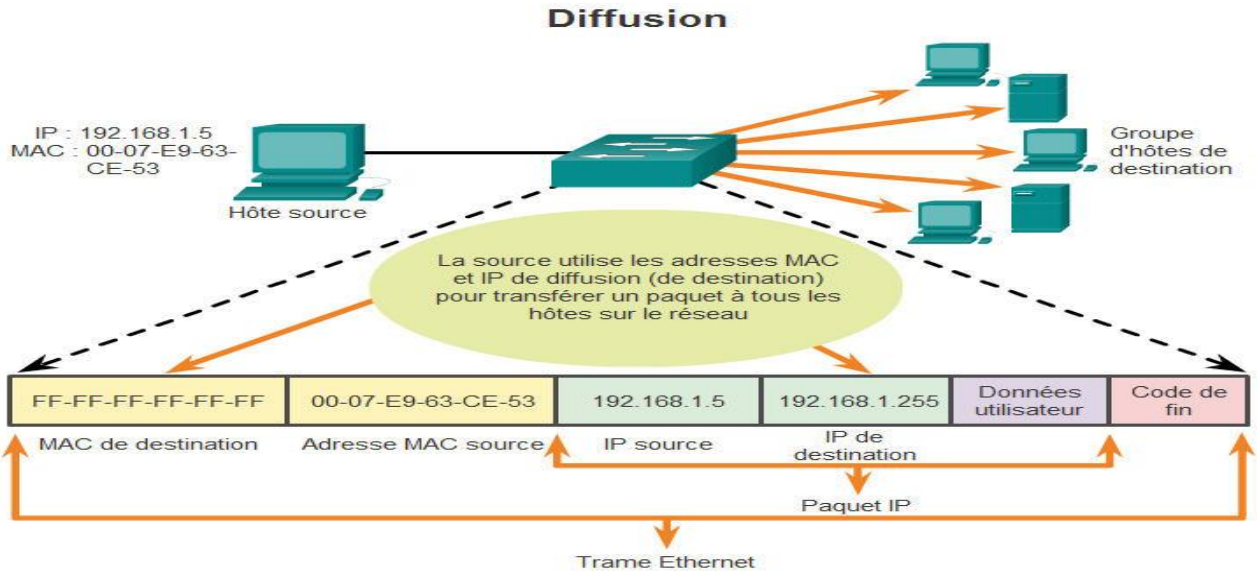
4.3. Adresses IPv4 de monodiffusion, et de diffusion et de multidiffusion

Dans un réseau IPv4, les hôtes peuvent communiquer de trois façons :

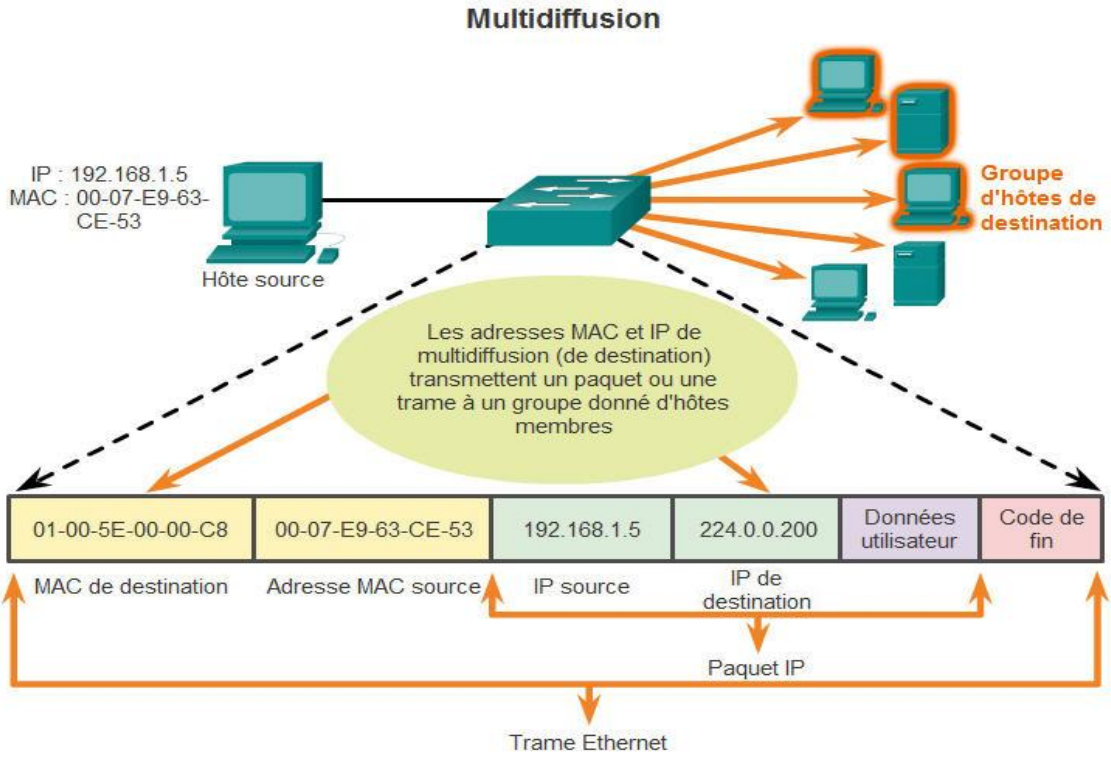
a. Monodiffusion (unicast) : consiste à envoyer un paquet d'un hôte à un autre



b. Diffusion (broadcast) : consiste à envoyer un paquet d'un hôte à tous les hôtes du réseau



c. Multidiffusion (multicast) : consiste à envoyer un paquet d'un hôte à un groupe d'hôtes en particulier, même situés dans des réseaux différents.



L'adresse MAC de multidiffusion est une valeur spécifique qui commence par **01-00-5E** au format hexadécimal

La plage d'adresses de multidiffusion IPv4 est comprise entre 224.0.0.0 et 239.255.255.255

II. PROTOCOLES DE ROUTAGE :

1. Généralités :

- Pour qu'un paquet IP puisse atteindre sa destination, il doit traverser des routeurs qui l'acheminent.
- Un routeur est un équipement qui possède donc plusieurs interfaces
- Il contient des tables déterminant l'interface de sortie en fonction de l'IP de destination.

2. Routage statique et dynamique :

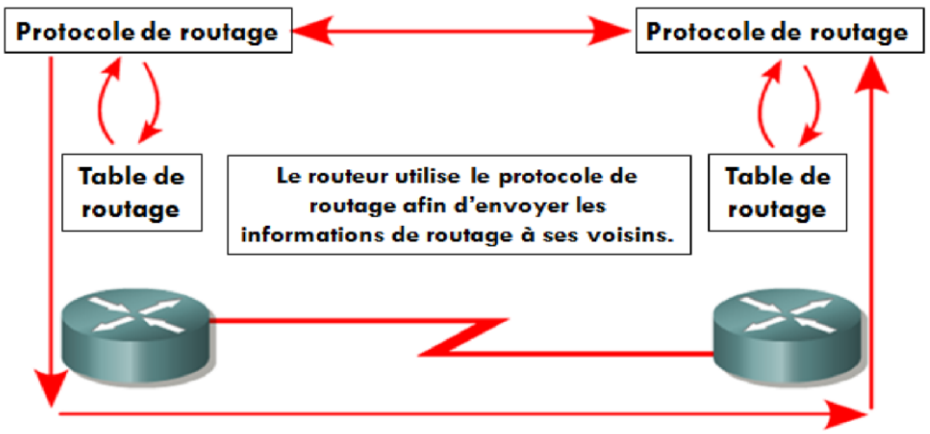
2.1. Routage Statique : Utilise une route entrée manuellement par un administrateur réseau dans le routeur

Le routage statique est inadapté si :

- Le nombre de réseaux à connecter est important
- La topologie du réseau change
- Plusieurs routeurs existent et la reconfiguration doit être automatique en cas de panne.

2.2. Routage dynamique: protocole de communication inter-routeurs qui va permettre de construire automatiquement les tables de routages.

Routage dynamique : utilise une route corrigée automatiquement par un protocole de routage selon les modifications de topologie ou de trafic



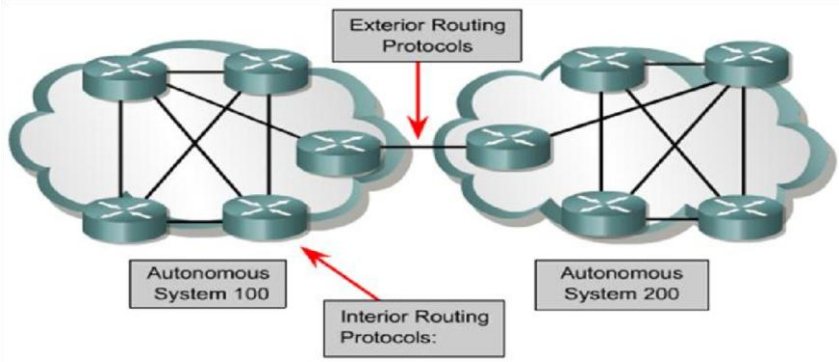
- **Protocole de communication inter-routeurs** : chaque routeur informe ses voisins des réseaux directement accessibles.
- Processus qui exécute le protocole de routage sur un routeur et qui communique avec les routeurs voisins. Il met à jour la table de routage du noyau avec les informations reçues des routeurs voisins.
- Le principe du routage ne change pas, c'est uniquement la façon de renseigner et de mettre à jour la table de routage qui change, puisqu'elle n'est plus manuelle mais dynamique.

- **Politique de routage** : Choix de la meilleure route parmi celles conduisant à une même destination (Distance administrative et coût).
- En cas de panne sur cette route, le démon la supprime et choisit une alternative pour atteindre la destination.

3. Système autonome :

Aucune autorité ne gère l'Internet. C'est pour cette raison que l'on introduit la notion de systèmes autonomes (AS : Autonomous System). Chaque système est donc administré par une seule autorité administrative (société, campus universitaire…) .

IGP ET EGP :



Le système autonome: est un ensemble de réseaux placés dans un domaine administratif unique
Protocoles IGP : Fonctionnent au sein d'un système autonome
Protocoles EGP : Connectent différents systèmes autonomes

Protocole de routage intérieur IGP :

Pour chaque AS, on définit des protocoles de routage interne (**IGP)** qui permettent le dialogue entre les routeurs du système, Il existe deux familles :

- Protocole de routage à vecteur de distance
- Protocole de routage à état de lien ou Link-state

Protocole de routage extérieur EGP:

Pour l'échange de données entre les domaines autonomes, on utilise des protocoles de routages extérieurs (EGP) exemple :
- EGP, du même nom, la première génération.
- BGP, Border Gateway Protocol, qui remplace EGP.

Choix de la meilleure route :

Distance administrative : Les routeurs choisissent la source de routage ayant la meilleure distance administrative

Source de la route	Distance administrative
Interface connectée	0
Route statique	1
RIP	120
OSPF	110
EIGRP	90

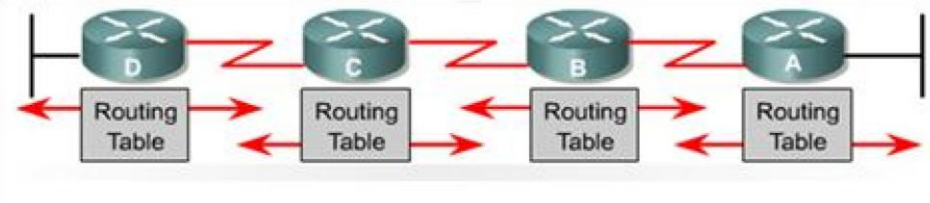
Mesures : Les routeurs choisissent la route ayant la meilleure mesure

RIP
Nombre de sauts

OSPF
Cout

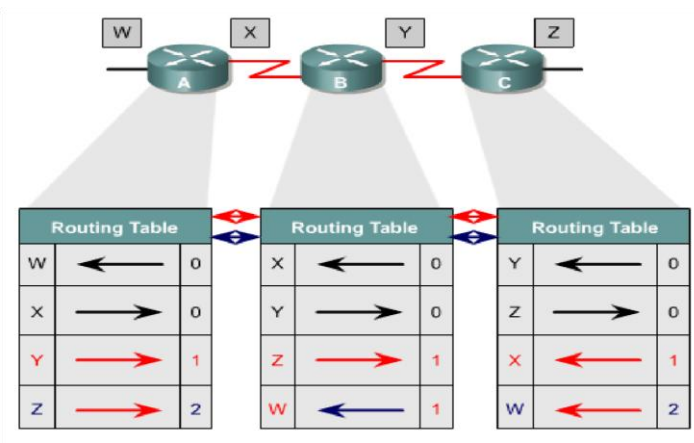
EIGRP
Bande Passante
Délai
Charge
Fiabilité

Protocole de routage à vecteur de distance :

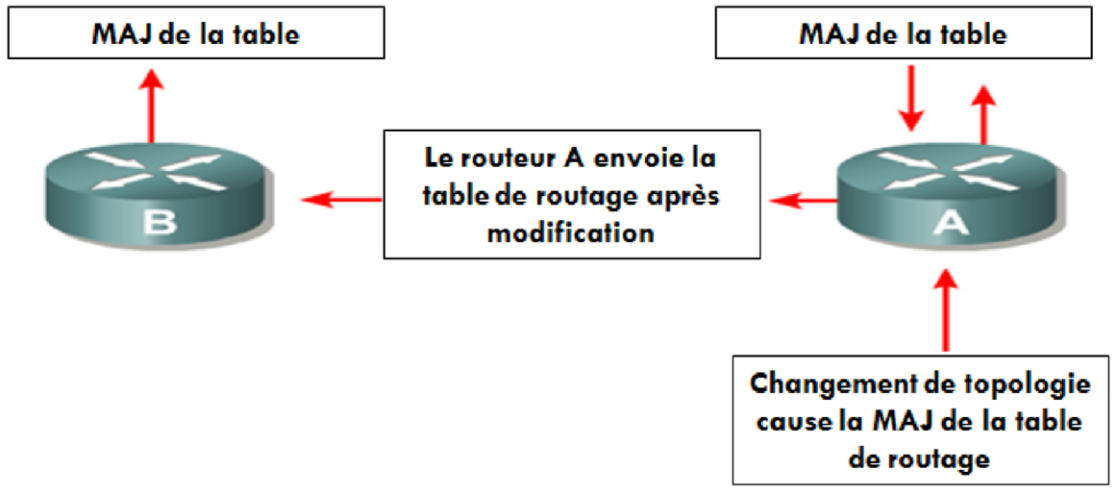


Les routeurs envoient régulièrement des copies de leur table de routage aux routeurs voisins et accumulent les vecteurs de distances.

Découverte des routes



M.A.J Protocol vecteur de distance :



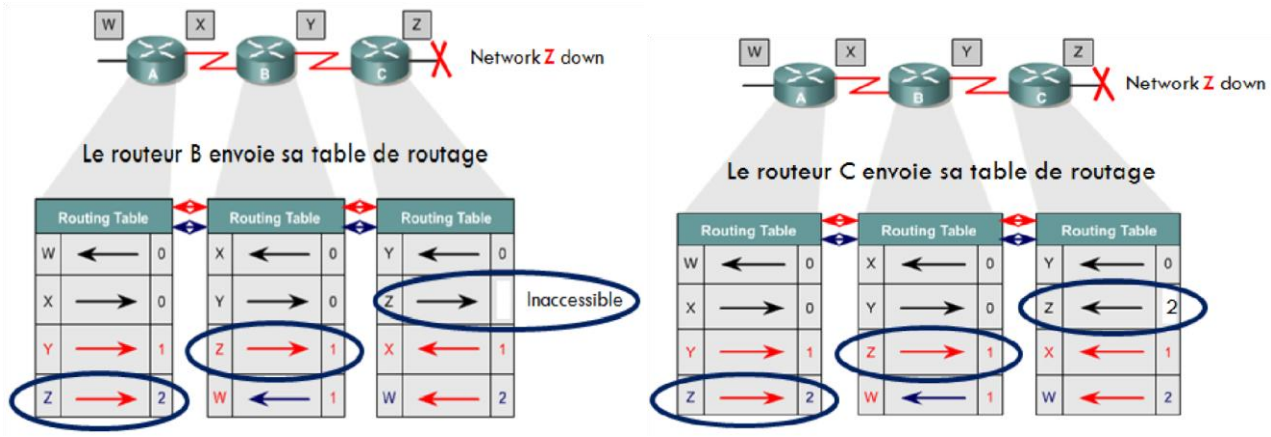
Problèmes :

Les boucles de routages peuvent apparaitre quand une table de routage n'est pas mise à jour suite à un changement de topologie, à cause de la lenteur de convergence du protocole utilisé

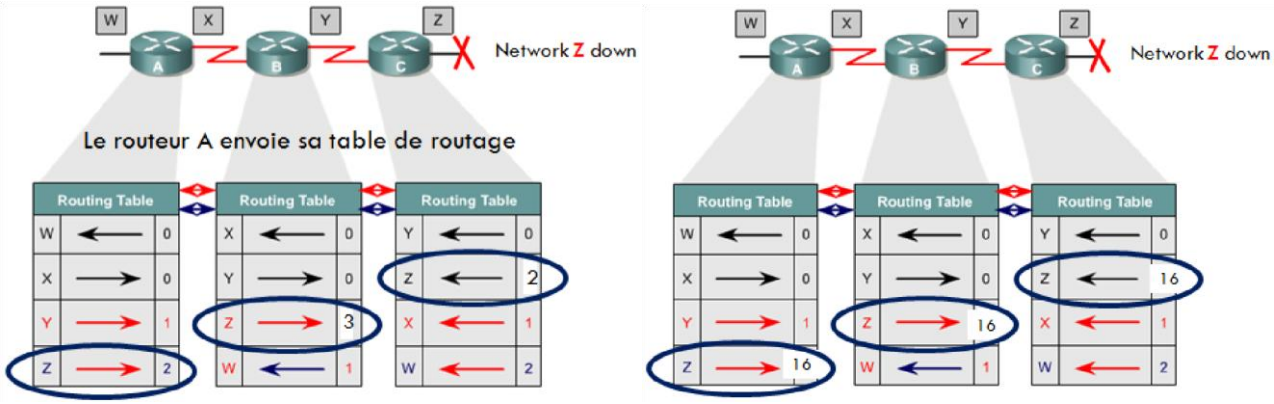
Solutions :

- Limitation du nombre de sauts.
- Le découpage d'horizon.
- Empoisonnement du routage.
- Mise à jour déclenchée.
- ……..

Problème du comptage à l'infini :



Solution du comptage à l'infini :

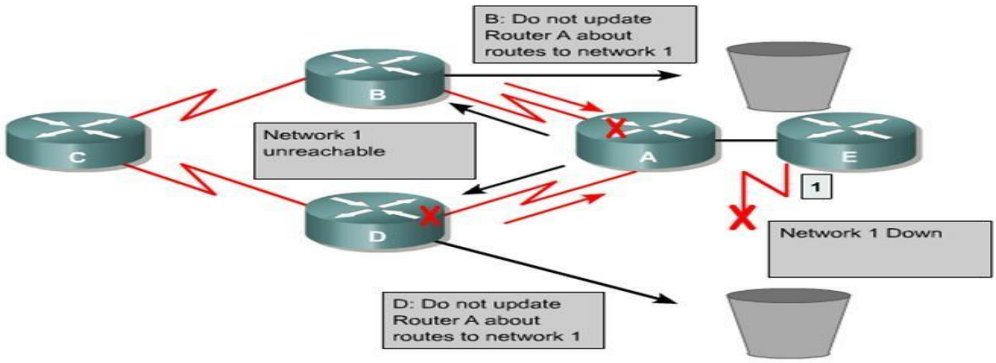


Une limite est fixée au nombre de sauts (Valeur 16) afin d'éviter les boucles infinies.

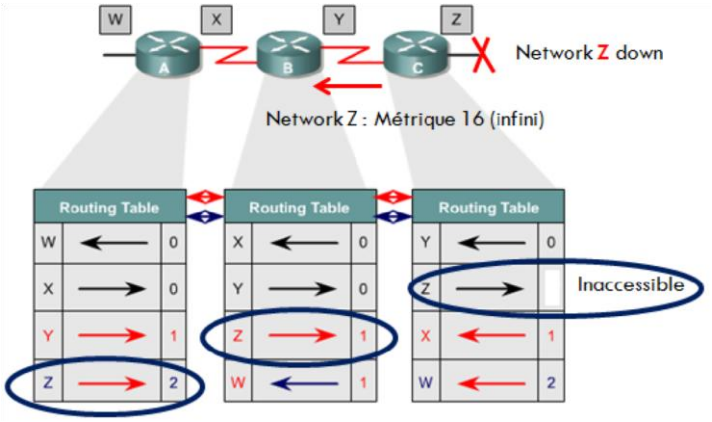
Solution aux boucles de routage :

Le découpage d'horizon

Il est toujours inutile de renvoyer des informations relatives à une route dans la direction dont les informations d'origine proviennent

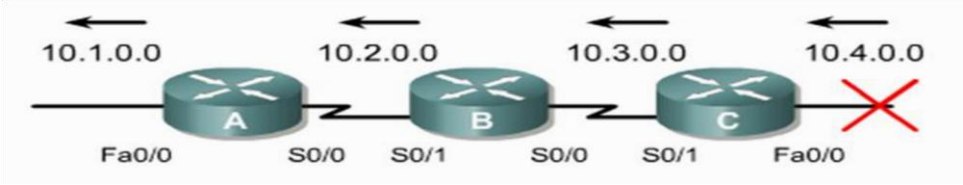


Empoisonnement du routage



Mise à jour déclenchées

Le routeur envoie des mises à jour lorsqu'une modification survient dans sa table de routage.



LEÇON N°05: SERVICES DES RESEAUX INFORMATIQUES

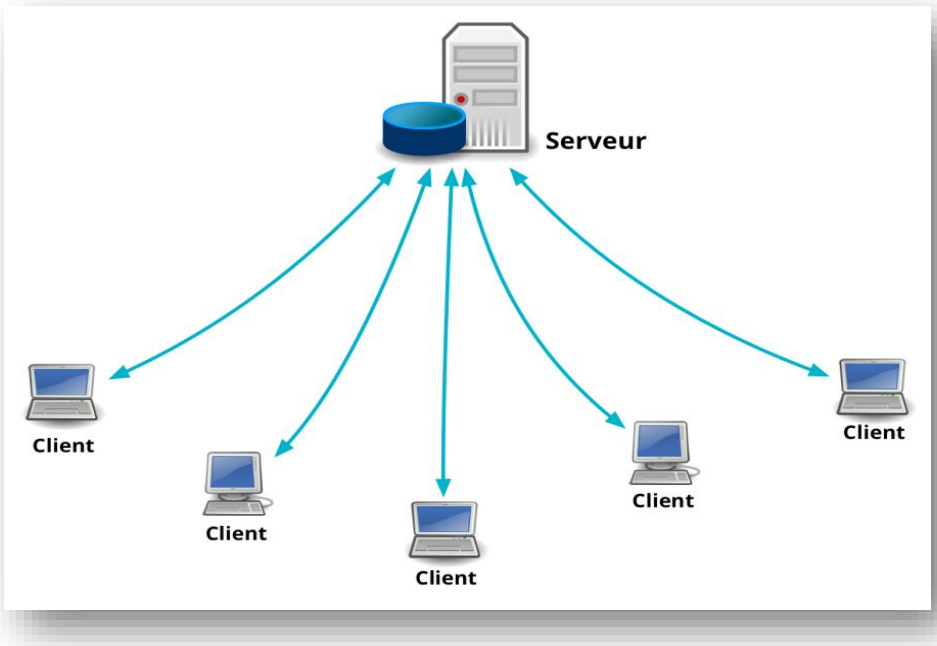
Objectif de la leçon n°05 : A la fin de cette leçon le stagiaire doit être capable de :

- Définir la notion de service réseau ;
- Caractériser les types standards des services réseau (DNS, WINS, NIS, DHCP, SMTP, POP MIME, RARP, BOOTP…) ;
- Caractériser les méthodes d'accès aux réseaux (méthode déterministe (802.5), méthode aléatoire CSMA/CD (802.3))

I. UN RESEAU : POUR FAIRE QUOI ?

Mettre en réseau des équipements informatique permet de les faire communiquer de façon à ce que certains d'entre eux puisse offrir leurs ***services*** aux autres (« partage de ressources » et de compétences).

C'est le schéma de fonctionnement client/serveur



DÉFINITIONS :

Un **logiciel serveur** donne à un ordinateur la compétence d'offrir un service à d'autres machines.

Un **logiciel client** donne à un ordinateur la compétence d'utiliser les services offerts par un serveur.

Un logiciel serveur en cours de fonctionnement est appelé : **service**. (ex : service de messagerie)

un logiciel client en cours de fonctionnement est appelé : **client**. (ex : client de messagerie)

Un ordinateur peut être à la fois serveur et client (pour un autre service) ;

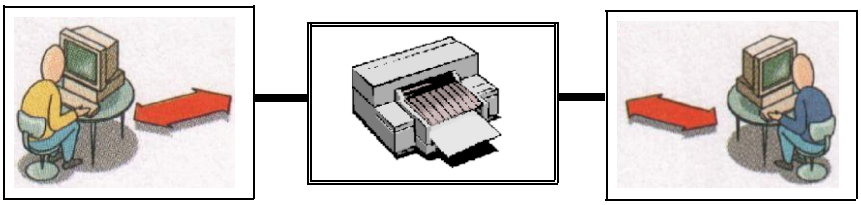
Le *protocole* est un langage spécifique à un type de service ; il permet le dialogue entre le logiciel client et le logiciel serveur.

Remarque :

Les services sont parfois interdépendants ; ex : le service de partage de fichier utilise le service d'authentification.

II. QUELS SERVICES SUR LE RESEAU ?

1. Service de partage d'imprimante

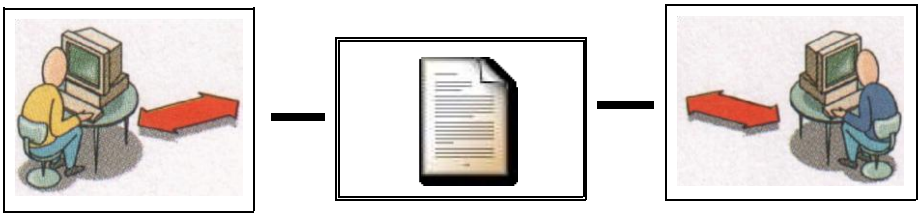


Une même imprimante peut être utilisée depuis *tous* les ordinateurs du réseau

Protocole	***description fonctionnelle***	***A***	***M***
Netbios	Ce système intégré dans le S.E. Windows permet de partager une imprimante reliée à l'ordinateur local (LPT ou USB)		
CUPS	Common Universal Printing System		

2. Les services de partage de fichier

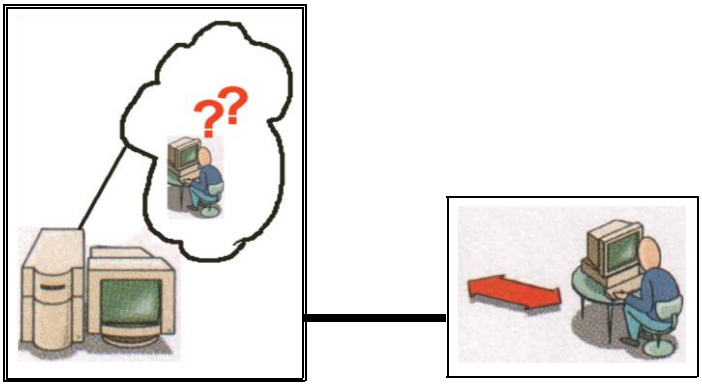
Le partage d'information est la raison d'être des réseaux! les formats et modes de partage sont multiples.



Un fichier inscrit sur un ordinateur peut être lu depuis n'importe quel ordinateur du réseau

Protocole	Description fonctionnelle	A	M
SMB, CIFS	Ce système intégré dans le S.E. Windows permet de partager un fichier, un répertoire ou un disque complet **dans le réseau local.** (voisinnage réseau)		
FTP	Permet la copie d'un fichier d'une machine à une autre **dans le réseau étendu**.		
HTTP	Permet la consultation de documents au format HTML **dans le réseau étendu.**		
POP, SMTP	Messagerie électronique; permet l'échange de fichiers dans un système de « boites aux lettres », c.a.d utilisant une machine tierce **dans le réseau étendu.**		
NFS	permet de partager un fichier, un répertoire ou un disque complet **dans le réseau étendu**		
WebDAV	(voir FTP). Spécialisé dans la mise à jour à distance des pages HTML (web)		

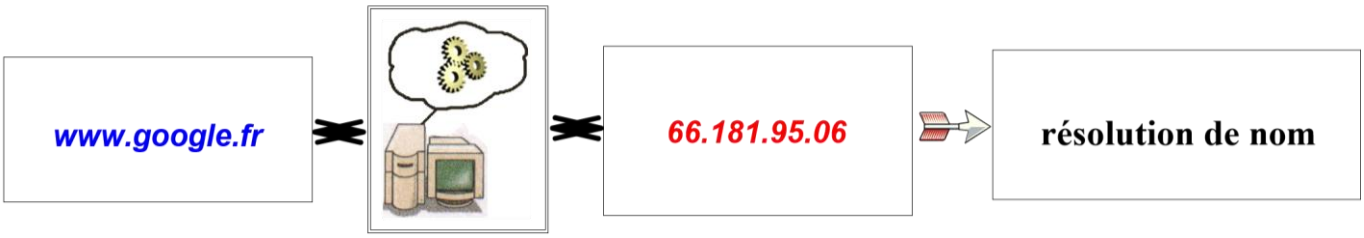
3. Les services d'authentification



L'utilisateur qui travaille sur un ordinateur du réseau est identifié. Cela permet de personnaliser son ENT (Environnement Numérique de Travail) et ses droits d'accès aux différents ressources du réseau. Cela suppose l'existence d'un annuaire (liste d'utilisateurs inscrits) sur le serveur.

Protocole	***description fonctionnelle***	***A***	***M***
LANMAN	Ce système intégré dans NT4 permet d'identifier l'utilisateur au sein d'un réseau local. Les utilisateurs sont déclarées dans le fichier ***SAM***		
YP	système d'annuaire pour les réseaux Unix.		
LDAP	Ce système d'annuaire standard convient aux réseaux étendus hétérogènes. Il comprend à la fois une base de donnée d'utilisateurs et un protocole pour la consulter. (*2000 Server AD* l'implémente de manière non-conventionnelle)		

4. Les services de résolution de nom



Les dénominations des ordinateurs peuvent varier en fonction du support physique emprunté pour véhiculer l'information. Il est nécessaire d'effectuer les traductions appropriées.

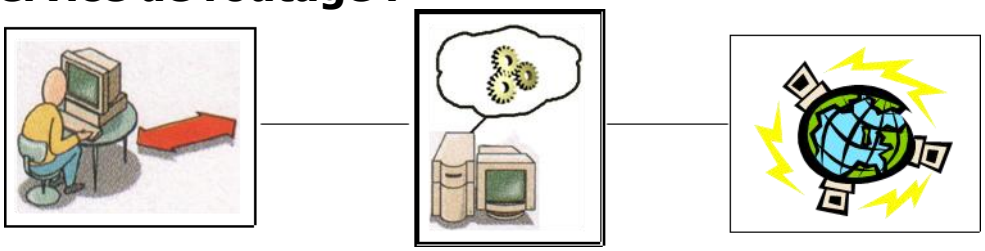
Protocole	***description fonctionnelle***	***A***	***M***
ARP / RARP	permet de traduire des adresses de liaison locale (ex : Ethernet) en adresse de réseau étendu (adresse IP) et inversement.		
NBNS	permet la traduction de nom NetBios en adresse réseau IP (broadcast)		
WINS	permet la traduction de nom NetBios en adresse réseau IP (unicast)		
DNS	permet la traduction de nom FDQN en adresse réseau IP		

4. Les services de contrôle et gestion du réseau

Ces services sont à la dispositions de l'administrateur du réseau; ils lui permettent 1) de vérifier le bon fonctionnement du réseau (monitoring) et 2) de modifier/corriger la configuration du réseau.

Protocole ou service	***description fonctionnelle***	***A***	***M***
ICMP	Implémenté dans la commande ping; permet de tester les liaisons réseaux		
SNMP	protocole pour configurer les actifs à distance.		
Telnet	Permet une connection à distance sur un serveur ou un actif.		
HTTPS	Interface WEB sécurisée pour configurer à distance un serveur ou un actif.		
DHCP	Configure dynamiquement les paramètres réseau des stations clientes.		

5. service de routage :



Il permet de relier les ordinateurs du réseau local à d'autres réseaux locaux en renseignant les routes existant entre ces réseaux et en aiguillant les paquets de donnés sur celles-ci. C'est la base de l'internet (routage IP).

Protocole	***description fonctionnelle***	***A***	***M***
statique	la couche réseau des S.E. serveurs permet un routage simplifié.		
iptables	ajoute des fonctionnalités de filtrage (firewall) et de NAT		
proxy	NAT, cache et filtrage de haut niveau (ex : Squid)		
RIP	détermine de manière dynamique des routes entre les réseaux.		

REMARQUES DIVERSES

- ✓ Les débutants font souvent l'erreur de regarder dans le *« voisinnage réseau »* pour vérifier le bon fonctionnement du réseau; Or le protocole *SMB* utilisé par *« voisinnage réseau »* n'est qu'un protocole parmi beaucoup d'autres. Le réseau peut donc très bien fonctionner sans *« voisinnage réseau ».* Il convient donc dans ce cas d'utiliser la commande ***ping*** qui implémente le protocole de contrôle *ICMP*.

- ✓ Dans ce document, nous avons utilisé de façon équivoque les notions de service et de protocole; cela se justifie, car ces notions sont techniquement imbriquées. Toutefois, il existe des protocoles qui ne sont pas liés à des services réseau; d'autres part, il est possible que deux services différents mais techniquement proches utilisent le même protocole (par exemple les protocoles *HTTP* et *HTTPS* sont utilisés par de nombreux services réseau).

- ✓ Certains services réseau n'ont pas d'interactions avec l'être humain; ce sont des services rendus par des machines pour d'autres machines! (ex : certains services de routage qui permettent la cooprération entre routeurs).

- ✓ Le mauvais fonctionnement voire l'arrêt d'un service réseau pénalise les utilisateurs et peut avoir des conséquences financières dramatiques pour l'entreprise. On doit donc veiller à la *tolérance de panne* (failover); c'est-à-dire que si un logiciel serveur ou la machine sur lequel il tourne a une défaillance, des mesures doivent être prises pour que, du point de vue de l'utilisateur, le service ne s'interrompe pas.

III. LES SERVICES RESEAU STANDARD :

Les services réseau standard jouent des rôles cruciaux dans le fonctionnement et la gestion des réseaux IP, allant de la résolution de noms à l'attribution d'adresses, en passant par la communication par e-mail et la gestion centralisée des informations de configuration. DHCP est aujourd'hui le protocole dominant pour la configuration dynamique des adresses IP, tandis que DNS est indispensable pour la navigation sur Internet. Les autres services ont une pertinence variable en fonction des environnements réseau spécifiques et de leur évolution technologique.

1. DNS (Domain Name System) :

- **Rôle :** Traduit les noms de domaine conviviaux (comme www.google.com) en adresses IP numériques (comme 172.217.160.142) que les ordinateurs peuvent comprendre et utiliser pour la communication.
- **Fonctionnement :** Utilise une structure hiérarchique distribuée de serveurs de noms. Lorsqu'un utilisateur entre un nom de domaine, une requête est envoyée à un serveur DNS qui, soit connaît l'adresse IP correspondante, soit interroge d'autres serveurs DNS jusqu'à ce qu'elle soit trouvée.
- **Importance :** Essentiel pour la navigation sur Internet et l'accès aux ressources réseau par des noms mémorables plutôt que par des adresses IP complexes.

2. WINS (Windows Internet Name Service) :

- **Rôle :** (Principalement utilisé dans les anciens réseaux Microsoft) Fournit un service de résolution de noms NetBIOS en adresses IP. NetBIOS est un protocole utilisé par les systèmes Windows pour le partage de fichiers et d'imprimantes sur des réseaux locaux.
- **Fonctionnement :** Un serveur WINS maintient une base de données des noms NetBIOS et de leurs adresses IP correspondantes. Les clients Windows enregistrent leurs noms NetBIOS auprès du serveur WINS au démarrage et interrogent le serveur pour résoudre les noms NetBIOS d'autres machines sur le réseau local.
- **Importance :** De moins en moins pertinent avec l'adoption généralisée du DNS dans les environnements Windows modernes.

3. NIS (Network Information Service) :

- **Rôle :** (Principalement utilisé dans les environnements Unix/Linux) Fournit un service d'annuaire centralisé pour la gestion des informations de configuration système telles que les noms d'utilisateurs, les mots de passe, les groupes, les hôtes et les informations de montage réseau.
- **Fonctionnement :** Utilise une architecture maître-esclave. Un serveur maître NIS maintient la base de données centrale, et des serveurs esclaves répliquent ces informations. Les clients NIS interrogent les serveurs NIS pour obtenir les informations de configuration.
- **Importance :** Simplifie l'administration des systèmes dans les grands environnements Unix/Linux en centralisant la gestion des informations de configuration.

4. DHCP (Dynamic Host Configuration Protocol) :

- **Rôle :** Automatise l'attribution des adresses IP et d'autres informations de configuration réseau (comme le masque de sous-réseau, la passerelle par défaut et les serveurs DNS) aux clients sur un réseau.
- **Fonctionnement :** Lorsqu'un client DHCP démarre, il envoie une requête de découverte (DHCP Discover). Un serveur DHCP répond avec une offre d'adresse IP et d'autres configurations (DHCP Offer). Le client accepte l'offre (DHCP Request), et le serveur confirme l'attribution (DHCP Acknowledge).
- **Importance :** Simplifie l'administration du réseau en évitant l'attribution manuelle des adresses IP, réduisant ainsi les risques de conflits d'adresses et facilitant la gestion des changements dans le réseau.

5. SMTP (Simple Mail Transfer Protocol) :

- **Rôle :** Protocole standard utilisé pour l'envoi d'e-mails entre les serveurs de messagerie.
- **Fonctionnement :** Un client de messagerie (ou un serveur de messagerie) établit une connexion TCP avec un serveur SMTP (port 25). Il envoie ensuite les informations de l'e-mail (expéditeur, destinataire, sujet, corps) en utilisant une série de commandes SMTP.
- **Importance :** Pilier de la communication par e-mail sur Internet.

6. POP (Post Office Protocol) :

- **Rôle :** Protocole utilisé par les clients de messagerie pour récupérer les e-mails stockés sur un serveur de messagerie.
- **Fonctionnement :** Un client POP se connecte à un serveur POP (généralement sur le port 110), s'authentifie, puis télécharge les e-mails. Après le téléchargement, les e-mails peuvent être supprimés du serveur (comportement par défaut de POP3) ou conservés (option configurable).
- **Importance :** Permet aux utilisateurs d'accéder à leurs e-mails à partir de différentes machines.

7. MIME (Multipurpose Internet Mail Extensions) :

- **Rôle :** Standard qui étend le format des e-mails pour prendre en charge le texte dans différents jeux de caractères, ainsi que les pièces jointes non textuelles (images, audio, vidéo, etc.).
- **Fonctionnement :** Ajoute des en-têtes aux messages e-mail pour indiquer le type de contenu du corps du message et des pièces jointes. Les clients de messagerie compatibles MIME peuvent interpréter et afficher correctement ces contenus.
- **Importance :** Essentiel pour l'échange de contenu multimédia par e-mail.

8. RARP (Reverse Address Resolution Protocol) :

- **Rôle :** (Obsolète dans la plupart des environnements modernes) Permettait à une machine sur un réseau local de découvrir son adresse IP à partir d'un serveur RARP, en connaissant uniquement son adresse MAC (adresse physique de la carte réseau).
- **Fonctionnement :** Un client RARP envoie une requête contenant son adresse MAC à un serveur RARP. Le serveur RARP répond avec l'adresse IP correspondante configurée pour cette adresse MAC.
- **Importance :** Principalement utilisé par les stations de travail sans disque au démarrage pour obtenir une adresse IP avant de pouvoir accéder à un serveur de fichiers. Remplacé par BOOTP et DHCP.

9. BOOTP (Bootstrap Protocol) :

- **Rôle :** Protocole qui permettait également aux clients de démarrer sans disque d'obtenir une adresse IP et d'autres informations de configuration réseau à partir d'un serveur BOOTP.
- **Fonctionnement :** Similaire à RARP, mais BOOTP permettait de fournir plus d'informations de configuration au client, comme l'adresse du serveur de démarrage et le nom du fichier de démarrage. Les configurations étaient généralement statiques et basées sur l'adresse MAC du client.
- **Importance :** Une amélioration par rapport à RARP, offrant plus de flexibilité pour le démarrage à distance. Précurseur de DHCP.

IV. LA METHODE DETERMINISTE (TOKEN RING - IEEE 802.5) ET LA METHODE ALEATOIRE CSMA/CD (ETHERNET - IEEE 802.3) :

1. METHODE D'ACCES DETERMINISTE : TOKEN RING (IEEE 802.5) :

- **Principe de fonctionnement :** Dans un réseau Token Ring, un jeton (token) circule de manière séquentielle entre les stations connectées en anneau logique. Une station ne peut transmettre des données que lorsqu'elle est en possession du jeton. Après avoir transmis ses données (et éventuellement reçu un accusé de réception), la station libère le jeton, qui passe à la station suivante dans l'anneau.
- **Caractérisation :**

- **Déterministe :** L'accès au médium de transmission est **déterministe**. Chaque station a une chance garantie de transmettre pendant un intervalle de temps maximal prédéfini. Il n'y a pas de collisions car une seule station est autorisée à transmettre à la fois.
- **Ordonné :** L'accès est séquentiel, suivant l'ordre physique ou logique de l'anneau.
- **Gestion du jeton :** Un mécanisme sophistiqué est nécessaire pour la gestion du jeton :
  - **Acquisition du jeton :** Une station doit capturer le jeton avant de pouvoir transmettre.
  - **Libération du jeton :** Après la transmission, le jeton est relâché pour la station suivante.
  - **Gestion de la perte du jeton :** Des procédures sont en place pour détecter et régénérer un jeton perdu.
  - **Gestion des doublons de jeton :** Des mécanismes existent pour résoudre les situations où plusieurs jetons circulent accidentellement.
- **Performance :** La performance est plus prévisible sous forte charge car l'accès est garanti. Le temps d'attente maximal pour une station est borné.
- **Complexité :** La mise en œuvre et la gestion du protocole sont plus complexes que les méthodes aléatoires en raison de la gestion du jeton.
- **Tolérance aux pannes :** La rupture de l'anneau physique peut impacter la communication. Des mécanismes comme les anneaux doubles peuvent améliorer la tolérance aux pannes.

- **Avantages principaux :**

- Bande passante garantie et prévisible.
- Performance stable sous forte charge.
- Pas de collisions.

- **Inconvénients principaux :**

- Plus complexe à mettre en œuvre et à gérer.
- Sensibilité aux pannes de l'anneau (si non redondant).
- Peut introduire une latence plus élevée sous faible charge par rapport aux méthodes aléatoires.

- **Utilisation historique :** Principalement utilisé dans les réseaux locaux d'IBM et dans certains environnements industriels nécessitant un accès déterministe. Moins courant aujourd'hui avec la prédominance d'Ethernet.

2. METHODE D'ACCES ALEATOIRE : CSMA/CD (CARRIER SENSE MULTIPLE ACCESS WITH COLLISION DETECTION) (IEEE 802.3 - ETHERNET) :

- **Principe de fonctionnement :** Dans un réseau utilisant CSMA/CD, chaque station écoute le médium de transmission (Carrier Sense) avant de tenter d'envoyer des données. Si le médium est libre, la station commence à transmettre (Multiple Access). Pendant la transmission, la station continue d'écouter le médium pour détecter d'éventuelles collisions (Collision Detection). Si une collision est détectée, toutes les stations impliquées cessent immédiatement de transmettre, envoient un signal de brouillage (jam signal) pour informer les autres stations de la collision, puis attendent un délai aléatoire (backoff) avant de tenter une nouvelle transmission.
- **Caractérisation :**

- **Aléatoire :** L'accès au médium est **aléatoire** et basé sur la disponibilité perçue du canal. Il n'y a pas de mécanisme d'ordonnancement centralisé ou de garantie d'accès.
- **Sensibilité à la charge :** La probabilité de collision augmente avec le nombre de stations et la charge du réseau.
- **Gestion des collisions :** La détection et la résolution des collisions sont des aspects clés du protocole :
  - **Détection précoce :** Les stations doivent être capables de détecter les collisions rapidement.
  - **Signal de brouillage :** Assure que toutes les stations sont informées de la collision.
  - **Algorithme de backoff :** Le délai d'attente aléatoire (souvent basé sur un algorithme d'exponentiation binaire) réduit la probabilité de collisions répétées.
- **Performance :** La performance est bonne sous faible charge car les stations peuvent transmettre immédiatement si le médium est libre. Cependant, sous forte charge, les collisions peuvent entraîner une dégradation significative des performances en raison des retransmissions.
- **Simplicité :** La mise en œuvre et la gestion du protocole sont relativement simples par rapport aux méthodes déterministes.
- **Topologie flexible :** Fonctionne bien avec différentes topologies physiques (bus, étoile).

- **Avantages principaux :**

- Simple à mettre en œuvre et à gérer.
- Efficace sous faible charge.
- Flexible en termes de topologie.

- **Inconvénients principaux :**

- Les collisions peuvent réduire considérablement les performances sous forte charge.
- L'accès n'est pas garanti, et il peut y avoir des délais importants en cas de congestion.
- Non adapté aux applications nécessitant un délai de transmission garanti.

- **Utilisation historique et actuelle :** La méthode d'accès CSMA/CD est la base de la norme Ethernet (IEEE 802.3), qui est de loin la technologie de réseau local la plus répandue au monde. Les améliorations ultérieures d'Ethernet (comme le passage au full-duplex et l'utilisation de commutateurs) ont considérablement réduit l'impact des collisions et amélioré les performances globales.

LEÇON N°06 : LA SECURITE RESEAU

Objectif de la leçon n°06 : A la fin de cette leçon, le stagiaire doit être capable d'applique les notions des protocoles de sécurités

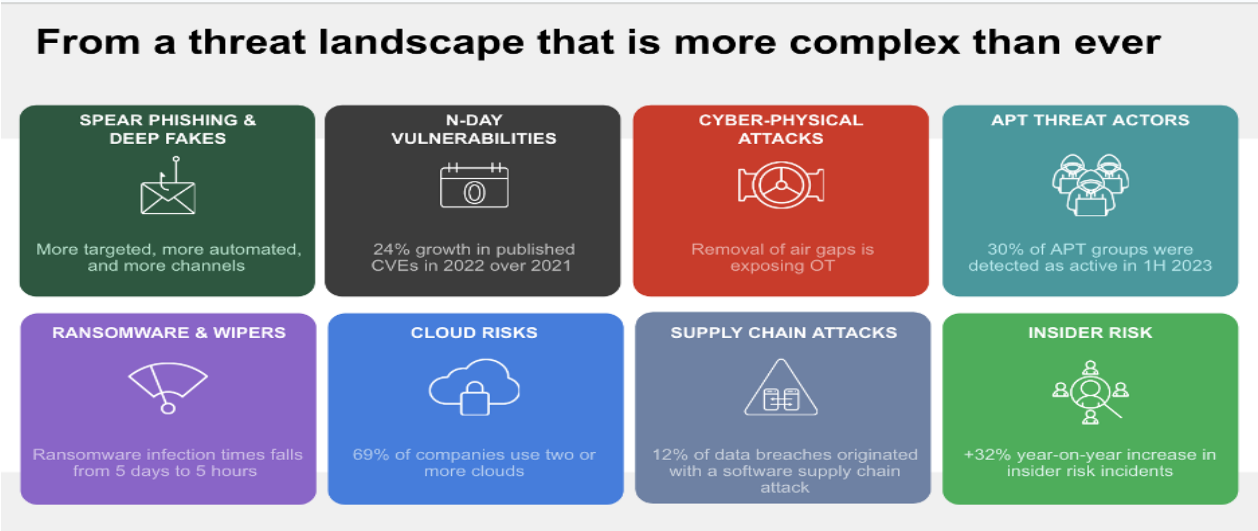
I. Définition : Qu'est-ce que la sécurité réseau ?

La sécurité réseau fait référence aux technologies, politiques, personnes et procédures qui défendent toute infrastructure de communication contre les cyberattaques, les accès non autorisés et la perte de données. En plus du réseau lui-même, ils sécurisent également le trafic et les ressources accessibles au réseau à la fois à la **périphérie du réseau** et à l'intérieur du périmètre.

II. Comment fonctionne la sécurité réseau ?

L'accélération numérique a ouvert la voie à l'efficacité commerciale, à la réduction des coûts et à l'amélioration de la productivité. Pourtant, cela a également conduit à une surface d'attaque étendue sur la périphérie du réseau en croissance. Des réseaux locaux (LAN) et des réseaux étendus (WAN) à l'Internet des objets (IoT) et au cloud computing, chaque nouveau déploiement entraîne une autre vulnérabilité potentielle.

Pire encore, les cybercriminels de plus en plus sophistiqués exploitent les vulnérabilités du réseau à un rythme alarmant. **Les logiciels malveillants**, les ransomwares, les attaques **par déni de service distribué** (DDoS) et d'innombrables autres menaces incitent les équipes informatiques à renforcer leurs défenses.



À leur tour, les entreprises ont beaucoup à gagner en renforçant leurs protections réseau :

- **Réduction des cyber-risques :** Des mesures de sécurité solides et robustes permettent de garantir que vos données restent toujours protégées.
- **Protection renforcée des données :** L'élimination des vecteurs de menace garantit que les informations sensibles sont protégées contre les accès non autorisés tout en traversant le réseau, protégeant ainsi les données des clients et assurant la conformité.
- **Amélioration de la continuité des activités :** Les réseaux protégés sont plus résilients face aux perturbations potentielles et subissent un temps d'arrêt minimal, ce qui permet une productivité optimale.
- **Meilleures performances réseau :** La sécurité empêche les acteurs malveillants de désactiver le réseau, garantissant ainsi que les ressources critiques sont toujours facilement disponibles.

III. Dispositifs essentiels pour sécuriser l'infrastructure réseau

Le matériel joue un rôle essentiel dans la sécurisation de l'infrastructure. Trois dispositifs, en particulier, sont pertinents pour la sécurité réseau :

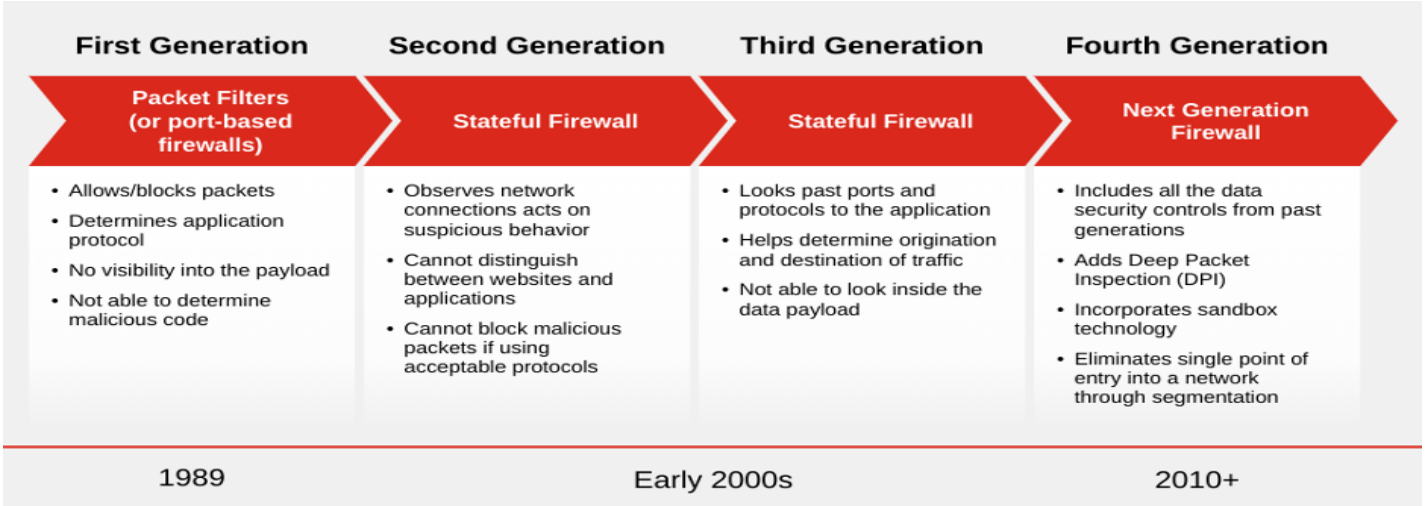
1. **Commutateurs Ethernet :** La commutation garantit une sécurité adéquate à la périphérie du réseau en facilitant le filtrage du trafic et le contrôle d'accès au niveau du port, ce qui permet aux administrateurs d'appliquer des politiques sur des segments de réseau granulaires.

2. **Points d'accès Wi-Fi (AP) :** Les points d'accès sans fil mettent en œuvre des protocoles de cryptage et des mécanismes d'authentification, protégeant les données en transit. Ils prennent également en charge les listes de contrôle d'accès (ACL), empêchant les appareils non autorisés de se connecter au réseau.

3. **Passerelles :** Les passerelles 5G et LTE sont essentielles aux liens redondants et primaires vers les succursales et les campus. Le fait de loger ces appareils sous le même dispositif de sécurité que le reste du réseau garantit une configuration commune, réduisant ainsi la surface d'attaque.

IV. TYPES DE SOLUTIONS DE SECURITE RESEAU

1. Les pare-feux



Un **pare-feu** est un dispositif qui surveille, filtre et contrôle le trafic réseau entrant et sortant en fonction de règles de sécurité prédéfinies. Agir comme une barrière entre les réseaux internes et externes de confiance, il fonctionne en inspectant les paquets de données et en choisissant de les bloquer ou de les autoriser.

Par exemple, une institution financière peut configurer son pare-feu pour bloquer le trafic provenant d'adresses IP non autorisées tout en autorisant le trafic légitime à passer. Cela atténue une violation potentielle sans interrompre les opérations principales.

Pare-feu nouvelle-génération (NGFW) est une itération moderne qui va au-delà des solutions traditionnelles, intégrant une inspection plus approfondie des paquets pour une protection plus robuste. Les NGFW regroupent souvent de nombreuses fonctionnalités essentielles de sécurité réseau en une seule offre complète, notamment la prévention des intrusions, l'antivirus et le sandboxing de fichiers, le filtrage Web et DNS, etc.

Avec une architecture maillée hybride, la prochaine évolution du pare-feu, les organisations peuvent centraliser le contrôle et la visibilité d'outils auparavant disparates. Cela facilite la coordination et le contrôle des politiques sur les pare-feux sur site et dans le cloud, sans parler de plusieurs succursales et sites de campus.

2. Systèmes de prévention des intrusions (IPS)

Les systèmes de prévention des intrusions détectent et bloquent les menaces connues et suspectées avant qu'elles n'impactent le cœur du réseau ou les appareils à sa périphérie. Outre l'inspection approfondie des paquets nord/sud et est/ouest, y compris l'inspection du trafic chiffré, ils peuvent également fournir des correctifs virtuels, ce qui atténue les vulnérabilités au niveau du réseau.

À l'aide d'un IPS, les organisations peuvent détecter rapidement les signatures d'attaque et les comportements anormaux. Le système prend automatiquement des mesures pour bloquer le trafic malveillant tout en alertant les administrateurs pour une enquête plus approfondie.

3. Antivirus et sandboxing

Les outils antivirus et de **sandboxing** sont essentiels pour déterminer si un fichier est malveillant. Alors que l'antivirus bloque les menaces de malware connues, le sandboxing fournit un environnement sûr pour analyser les fichiers suspects.

Imaginons qu'un utilisateur télécharge un fichier à partir d'une pièce jointe d'e-mail. Le logiciel antivirus l'analyse à la recherche de signatures et de comportements d'attaque connus. S'il s'agit d'une menace confirmée, le logiciel met le fichier en quarantaine ou le supprime. Pour un fichier inconnu, le sandboxing l'isole dans un espace protégé où il peut être testé pour déterminer s'il est malveillant.

Certains fournisseurs de sécurité tirent parti de ces fonctionnalités de concert avec l'IA, ce qui leur permet d'effectuer une analyse en moins d'une seconde des menaces inédites.

4. Filtrage Web et DNS

Le filtrage DNS (Domain Name System) permet aux organisations de stopper les attaques basées sur le domaine, telles que le détournement DNS, la tunnellisation, etc. De même, le filtrage des URL empêche les utilisateurs et les applications d'accéder aux URL suspectes, qui pourraient être liées à des sites Web malveillants. Ces **outils de sécurité Web** aident les entreprises à appliquer des règles d'utilisation acceptables tout en les protégeant contre les contenus nuisibles.

Par exemple, si un utilisateur tente d'accéder à un site Web malveillant, le filtre Web vérifie sa base de données de sites catégorisés. Si le domaine a été marqué, il bloquera entièrement l'accès.

5. Gestion de la surface d'attaque

Certaines solutions de pare-feu comprennent désormais des outils de **gestion de la surface d'attaque des cyber-actifs** qui peuvent aider les organisations à identifier automatiquement les actifs IT, OT et IoT du réseau, et à évaluer ces actifs à la recherche de risques potentiels. Les outils peuvent également évaluer l'infrastructure et les contrôles de sécurité existants pour détecter les erreurs de configuration et les paramètres moins optimaux qui peuvent ensuite être mis à jour pour renforcer la posture de sécurité d'une organisation.

6. VPN d’accès à distance

Les VPN d’accès à distance permettent aux utilisateurs d’accéder en toute sécurité au réseau de l’entreprise depuis l’extérieur du bureau de leur organisation. Ils créent une connexion privée et cryptée à partir d’un réseau Wi-Fi public, permettant aux employés d’utiliser en toute sécurité les ressources critiques de leurs appareils personnels, quel que soit l’emplacement.

Ces solutions sont particulièrement utiles dans les environnements de travail hybrides, ce qui permet aux télétravailleurs de rester productifs en s’assurant que leurs données sont protégées contre l’interception malveillante.

7. Contrôle d’accès réseau (NAC)

Le contrôle d’accès au réseau régit l’accès au réseau, garantissant que seuls les appareils autorisés et conformes sont autorisés à entrer. Les solutions NAC identifient et authentifient les appareils, en accordant l’accès uniquement s’ils répondent à des politiques de conformité prédéfinies.

Par exemple, les entreprises peuvent configurer leur NAC pour bloquer certains types d’appareils. Cela empêche les utilisateurs d’accéder au réseau sur des appareils personnels non protégés, mais peut également aider l’entreprise à gérer les déploiements IoT et de **technologie opérationnelle** (OT).

Le matériel qui ne répond pas aux critères peut être mis en quarantaine, redirigé vers un réseau de remédiation ou entièrement refusé.

V. TECHNOLOGIES DE SECURITE RESEAU ASSOCIEES :

Bien que ne prenant pas directement en charge le réseau, il existe des technologies de cyber sécurité connexes qui aident à protéger l’infrastructure :

1. Endpoint Detection and Response (EDR)

Les solutions de sécurité Endpoint **Detection and Response** (EDR) surveillent en permanence toutes les activités des utilisateurs et des endpoints pour les protéger contre les menaces et détecter les comportements suspects. Ils offrent également des capacités d’investigation et de réponse aux incidents, qui éradiquent la menace et isolent le système affecté de l’impact sur le reste du réseau.

2. Sécurité de l'email

La **sécurité des e**-mails protège les employés contre les cybermenaces et les attaques d’ingénierie sociale, y compris le phishing, le spear-phishing et d’autres tactiques basées sur les e-mails. Il fonctionne en examinant les e-mails entrants pour détecter les facteurs de risque potentiels. Par exemple, il peut identifier les communications qui contiennent des logiciels malveillants, des liens suspects, du contenu et des images douteux, et d’autres anomalies, empêchant l’e-mail d’atteindre la boîte de réception de l’utilisateur.

3. Prévention des pertes de données (DLP)

Les **solutions DLP** identifient les informations sensibles dans les systèmes cloud, atténuent le partage accidentel de données et préviennent l'exfiltration de données. Ils augmentent la visibilité sur les magasins de données, aidant les entreprises à suivre et à corriger les violations de politiques, améliorant ainsi la conformité interne.

4. Protection contre les attaques DDoS

La protection DDoS protège contre les attaques par déni de service, qui visent à submerger le réseau de l'entreprise et à perturber les opérations. **FortiDDoS**, par exemple, inspecte rapidement les paquets de données et empêche automatiquement le trafic illégitime d'inonder le réseau.

5. Sécurité applicative

Les outils de sécurité des applications permettent aux administrateurs de reconnaître le trafic généré par des applications connues et personnalisées. À l'aide de décodeurs de protocole IPS, il analyse le trafic pour identifier les applications, ce qui permet aux administrateurs de former rapidement des politiques pour autoriser, refuser ou restreindre l'accès à des applications spécifiques ou à des catégories entières d'applications. Cela optimise l'utilisation de la largeur de bande tout en atténuant les logiciels malveillants, les transferts de fichiers non autorisés et d'autres risques.

6. Cloud Access Security Broker (CASB)

Les **solutions CASB** offrent une sécurité aux applications SaaS (Software-as-a-Service), aux utilisateurs et aux données. Le CASB en ligne offre visibilité, conformité et protection contre les menaces pour les données en mouvement et au repos dans les applications cloud, mais crée également des rapports informatiques fantômes, des évaluations des risques, etc.

Les interfaces de programmation d'applications (API) permettent aux CASB à architecture ouverte de s'intégrer directement aux fournisseurs SaaS. Cela permet aux administrateurs d'analyser les configurations cloud, garantissant que leurs utilisateurs sont surveillés et protégés, quel que soit l'appareil qu'ils utilisent.

IV. SOLUTIONS DE SECURITE RESEAU D'ENTREPRISE

La sécurité réseau est intrinsèquement plus complexe dans des environnements informatiques plus vastes et plus complexes. Heureusement, il existe plusieurs solutions adaptées à la protection du réseau à grande échelle :

1. SIEM (Security Information and Event Management)

Les centres opérationnels de sécurité (SOC) modernes nécessitent une approche centralisée de la gestion des événements. Sans cela, ils ne disposent pas du contexte ou de la visibilité nécessaires pour protéger efficacement l'organisation.

Les **solutions SIEM** offrent une vue unifiée de la sécurité dans toute l'entreprise, en recueillant des informations à partir du réseau, des endpoints, du cloud et d'autres produits de sécurité. Ils offrent également une détection des menaces basée sur l'IA basée sur le comportement, une enquête, un reporting de conformité, etc. En bref, le SIEM réduit la complexité de la gestion des opérations réseau et de sécurité.

2. Détection et réponse au réseau (NDR)

Le NDR surveille le trafic réseau interne, en définissant les comportements normaux et en utilisant le machine learning (ML) et d'autres analyses pour détecter les logiciels malveillants, le trafic malveillant et les modèles anormaux qui peuvent indiquer un attaquant au sein du réseau. Il offre également une capacité robuste d'enquêter et de prendre des mesures immédiates sur les alertes vérifiées.

3. Extended Detection and Response (XDR)

XDR rationalise la détection et la réponse aux menaces dans l'écosystème de sécurité d'une entreprise. En consolidant les données des endpoints, des réseaux, des e-mails et du cloud, il identifie et relie les activités suspectes que des outils individuels peuvent manquer. Cette approche intégrée permet une investigation et une correction rapides des alertes ou des incidents en plusieurs étapes grâce à des actions automatisées et manuelles. En tirant parti des capacités de détection et de réponse aux endpoints (EDR), XDR fournit des agents de endpoints, des indicateurs et un blocage des endpoints pour gérer efficacement les défis tout en améliorant les capacités de détection et de réponse aux menaces.

IIV. SERVICES MANAGES DE SECURITE RESEAU

La progression de la détection et de la réponse aux endpoints (**EDR**) vers la détection et la réponse gérées (MDR) vers la détection et la réponse étendues (XDR) suit le chemin de l'accélération numérique avec des surfaces d'attaque en expansion constante et une main-d'œuvre hybride.

La différence entre EDR, MDR et XDR est essentiellement la suivante :

- **EDR** : **La détection et la réponse aux terminaux** agissent comme un système d'alarme pour une organisation. Lorsqu'il détecte une menace sur un endpoint, il alerte immédiatement l'entreprise.
- MDR : **la détection et la réponse gérées** sont une approche de sécurité qui se concentre sur les individus et leurs comportements. Il donne la priorité à la protection des endpoints.
- **XDR** : **la détection et la réponse étendues** font passer le MDR au niveau supérieur grâce à une pratique logicielle qui protège l'ensemble de l'infrastructure d'une entreprise.

Aujourd'hui, les périphéries du réseau sont là où l'utilisateur se connecte et les entreprises peuvent ne pas être en mesure d'étendre la sécurité partout où elle est nécessaire. Les fournisseurs de services de sécurité managés (MSSP) peuvent aider à combler le fossé avec l'expertise et l'infrastructure critiques requises immédiatement, à moindre coût.

Par exemple, un service **managé de détection et de réponse** (MDR) peut être un excellent choix pour les PME qui ont besoin d'une surveillance et d'une réponse aux menaces de niveau entreprise, mais qui estiment qu'il est trop coûteux de créer ou de doter en personnel en interne.

Les grandes organisations qui ont besoin d'une protection plus complète d'un environnement distribué et qui n'ont pas les ressources en interne peuvent choisir un **service XDR** pour la détection et la réponse multicouches. XDR collecte, normalise, puis met en corrélation les données sur une variété de couches de sécurité, y compris les endpoints, les pare-feux, la messagerie électronique, les serveurs, les charges de travail cloud et le réseau général.

1 - MDR + XDR

Le MDR est un service de détection et de réponse aux menaces entièrement géré, fourni par un MSSP externalisé. Avec les services MDR, les équipes de sécurité peuvent améliorer leur capacité à détecter, enquêter et répondre rapidement aux activités non autorisées et/ou suspectes. Certains services MDR offrent également une chasse aux menaces et des recommandations pour améliorer la posture de sécurité globale.

Certains MSSP étendent également le MDR avec XDR qui surveille, détecte et analyse les signaux de sécurité sur les endpoints, le réseau, le cloud, le SIEM et les systèmes de sécurité de messagerie. XDR est une nouvelle approche alternative à la détection traditionnelle et à la réponse aux incidents, intégrant des procédures de détection et de réponse dans plusieurs environnements afin de réduire le temps moyen de détection et de réparation des attaques.

XDR est une extension naturelle de l'EDR adaptée aux organisations qui ont des environnements informatiques complexes ou qui sont hautement vulnérables aux cyberattaques. XDR est hautement évolutif, prend en charge plusieurs sources de données et assure une protection de bout en bout des surfaces d'attaque d'une organisation.

2 - SOC-as-a-Service géré (SOCaaS)

Un centre d'opérations de sécurité (SOC) interne typique nécessite un personnel dédié d'ingénieurs et d'analystes de sécurité et les outils nécessaires pour soutenir leur travail. Le coût élevé de l'exécution d'un SOC en interne, aggravé par la pénurie de talents en cyber sécurité et le burnout qui souvent transpire, conduit de nombreuses organisations à choisir un **SOC-as-a-Service** (SOCaaS) géré. Cela leur permet d'externaliser la chasse aux menaces, la surveillance, la détection et la

correction à un fournisseur de services MDR ou MXDR avec l'expérience, l'infrastructure et les outils de cyber sécurité, afin de surveiller activement les surfaces de menaces des clients 24 h/24, 7 j/7.

3 - Service de pare-feu géré

La sécurité du cloud est une responsabilité partagée. En général, l'infrastructure de cloud public est sécurisée par le fournisseur de services, tel qu'AWS, Azure ou GCP, et les charges de travail exécutées sur l'infrastructure sont sécurisées par le client. Pour répondre à l'impératif commercial de la migration vers le cloud, les organisations ont besoin d'une solution de sécurité réseau dans le cloud qui offre une protection avancée, une flexibilité et des coûts prévisibles.

Cependant, les organisations qui accélèrent leur adoption du cloud peuvent ne pas avoir les **ressources, les compétences** ou le temps nécessaires pour créer, faire évoluer ou adapter leur sécurité cloud pour répondre au rythme de leur activité. Un service de pare-feu géré permet aux organisations de décharger la maintenance de l'infrastructure de sécurité cloud, d'obtenir une visibilité approfondie, d'appliquer des contrôles robustes et d'optimiser les dépenses de sécurité cloud.

Un service de pare-**feu géré**, natif du cloud, élimine le lourde charge des opérations de sécurité réseau et offre une expérience sans heurt pour aider les clients à déployer facilement une sécurité de niveau entreprise sur le cloud public.

La migration vers le cloud exige des organisations qu'elles sécurisent les services cloud clés. Un **service de pare-feu géré** de nouvelle génération ou un pare-feu en tant que service (FWaaS) réseausimplifie la gestion de la sécurité avec une visibilité complète sur les environnements et une protection étendue sur les charges de travail et les applications cloud.

Qu'il s'agisse d'un service de pare-feu géré ou d'un FWaaS réseau, il est essentiel que les organisations s'assurent que leurs charges de travail de cloud public sont protégées par des solutions de sécurité de nouvelle génération optimisées par une veille complète sur les menaces.