Réalisé par : Karim maali

Principes Fondamentaux de la Mise en Réseau

Notions de base sur la mise en réseau :

Qu'est-ce que la mise en réseau ?

La mise en réseau est le processus de connexion d'appareils (ordinateurs, téléphones, serveurs) pour échanger

des données et partager des ressources. Considérez-le comme la construction d'une autoroute numérique pour la communication

Principaux composants du réseau :

1. **Nœuds :** appareils tels que les ordinateurs et les téléphones.
2. **Liens :** les voies (câbles, Wi-Fi) qui relient les appareils.
3. **Types de réseaux :**
   - **LAN :** réseau local (par exemple, à domicile ou au bureau).
   - **WAN :** réseau étendu (par exemple, Internet).
   - **MAN :** réseau métropolitain (réseaux à l'échelle de la ville).

Adressage IP :

Qu'est-ce qu'une adresse IP ?

Une adresse IP est un identifiant unique pour un appareil sur un réseau, comme l'adresse postale de votre domicile. Elle garantit que les données envoyées sur un réseau parviennent à la bonne destination.

Types of IP Addresses:

IPv4 : une adresse 32 bits, par exemple 192.168.1.1. Elle est simple mais limitée en nombre.

IPv6 : une adresse 128 bits, par exemple 2001:0db8:85a3::7334. Elle prend en charge un grand nombre d'appareils et comprend des fonctionnalités de sécurité intégrées.

IP publiques et privées :

Adresses IP publiques : Accessibles sur Internet et attribuées par les fournisseurs d'accès à Internet (FAI).

Adresses IP privées : Utilisées au sein des réseaux locaux (ex. : 192.168.x.x) et restent invisibles depuis Internet grâce à la traduction d'adresses réseau (NAT)

Principaux protocoles et ports réseau :

TCP (Transmission Control Protocol)

TCP garantit une livraison fiable des données en établissant une connexion avant l'envoi des données. C'est comme envoyer un colis avec un numéro de suivi.

7 ports TCP courants et exemples d'applications :

- **Port 80 :** HTTP (navigation Web).
- **Port 443 :** HTTPS (navigation Web sécurisée).
- **Port 21 :** FTP (protocole de transfert de fichiers).
- **Port 22 :** SSH (accès distant sécurisé).
- **Port 25 :** SMTP (envoi d'e-mails).
- **Port 3306** : MySQL (communication avec la base de données).
- **Port 3389** : RDP (protocole de bureau à distance).

UDP (User Datagram Protocol)

UDP est plus rapide mais moins fiable que TCP. Il ne confirme pas si les données sont reçues, ce qui le rend idéal pour les applications en temps réel

5 ports UDP courants et exemples d'applications :

Port 53 : DNS (traduit les noms de domaine en IP).

Port 123 : NTP (Network Time Protocol).

Port 161 : SNMP (surveillance des périphériques réseau).

Port 69 : TFTP (Trivial File Transfer Protocol).

Port 500 : IPsec (cryptage VPN).

20 protocoles réseau courants expliqués

Protocoles de la couche d'application

❖ HTTP (HyperText Transfer Protocol)

Fonction : Permet le transfert de pages web et de ressources.

Exemple : Accéder à un site comme http://example.com.

Note de cybersécurité : Vulnérable aux interceptions et attaques en l'absence de HTTPS.

❖ HTTPS (HTTP Secure)

Fonction : Sécurise les communications HTTP grâce au chiffrement SSL/TLS.

Exemple : Transactions sécurisées en ligne, par exemple https://bank.com.

Avantage en cybersécurité : Garantit le chiffrement des données en transit.

❖ FTP (File Transfer Protocol)

Fonction : Permet le transfert de fichiers entre systèmes.

Exemple : Téléverser des fichiers sur un serveur web.

Problème de cybersécurité : Les données sont transmises en clair sauf si FTP est sécurisé (ex. : SFTP).

❖ SFTP (Secure File Transfer Protocol)

Fonction : Transfert sécurisé des fichiers via SSH.

Exemple : Envoi de sauvegardes cryptées.

Avantage en cybersécurité : Protège contre l'interception des données

❖ SMTP (Simple Mail Transfer Protocol)

Fonction : Permet l'envoi d'emails depuis un client vers un serveur.

Exemple : Envoi d'emails via des services comme Gmail.

Préoccupation en cybersécurité : Vulnérable à l'usurpation d'identité sans SPF ou DKIM.

❖ IMAP (Internet Message Access Protocol)

Fonction : Permet d'accéder et de gérer les emails stockés sur un serveur.

Exemple : Synchroniser des emails sur plusieurs appareils.

Avantage en cybersécurité : Supporte le chiffrement via SSL/TLS pour un accès sécurisé.

❖ DNS (Domain Name System)

Fonction : Traduit les noms de domaine en adresses IP.

Exemple : Résolution de google.com en 142.250.190.14.

Risque en cybersécurité : Vulnérable au spoofing ou à l'empoisonnement de cache DNS.

❖ DHCP (Dynamic Host Configuration Protocol)

Fonction : Attribue automatiquement des adresses IP aux appareils sur un réseau.

Exemple : Un ordinateur se connecte au Wi-Fi et reçoit une adresse IP.

Préoccupation en cybersécurité : Des serveurs DHCP malveillants peuvent attribuer des configurations dangereuses.

❖ SNMP (Simple Network Management Protocol)

Fonction : Surveille et gère les équipements réseau tels que les routeurs et commutateurs.

Exemple : Gestion des performances des appareils réseau.

Problème de cybersécurité : Des identifiants SNMP faibles peuvent entraîner un accès non autorisé.

❖ Telnet

Fonction : Permet la gestion à distance des appareils (non sécurisé).

Exemple : Configurer un appareil réseau via Telnet.

Préoccupation en cybersécurité : Les identifiants sont transmis en clair, ce qui le rend non sécurisé.

❖ SSH (Secure Shell)

Fonction : Protocole sécurisé pour l'accès et la gestion à distance des appareils.

Exemple : ssh user@server.com pour se connecter à un serveur distant.

Avantages :

Chiffrement des communications.

Authentification sécurisée (mots de passe ou clés).

Protection contre les interceptions et attaques "man-in-the-middle".

Protocoles de la couche transport

TCP (Transmission Control Protocol) :

Objectif : Fournit une communication fiable.

Exemple : Navigation, téléchargement de fichiers.

Préoccupation en matière de cybersécurité : Les sessions TCP peuvent être piratées.

UDP (User Datagram Protocol) :

Objectif : Communication plus rapide sans vérification des erreurs.

Exemple : Jeux en ligne, streaming vidéo.

Préoccupation en matière de cybersécurité : Les attaques UDP peuvent provoquer des attaques DDoS.

Protocoles de la couche réseau

IP (Internet Protocol) :

Objectif : achemine les paquets de données entre les appareils.

Exemple : adresses IPv4, IPv6.

Préoccupation en matière de cybersécurité : attaques IP Spoong.

ICMP (Internet Control Message Protocol)

Objectif : envoie des messages d'erreur et de diagnostic.

Exemple : commande Ping.

Préoccupation en matière de cybersécurité : exploité dans les attaques DdoS.

- **Protocoles de la couche de liaison de données :**

ARP (Address Resolution Protocol) :

Objectif : Résout les adresses IP en adresses MAC.

Exemple : Assure un routage correct au sein d'un réseau local.

Préoccupation en matière de cybersécurité : Attaques ARP spoofing

Ethernet :

Purpose: Defines wired LAN communication.

Exemple : Réseaux de bureau.

Préoccupation en matière de cybersécurité : écoute clandestine du trafic Ethernet non chiffré.

- **Protocoles de sécurité :**

SSL/TLS (Secure Sockets Layer/Transport Layer Security)

Objectif : chiffrer les communications (par exemple, HTTPS, FTPS).

Exemple : sécuriser les transactions en ligne.

Avantage en matière de cybersécurité : empêcher les attaques MITM.

IPsec (Internet Protocol Security)

Objectif : sécurise le suivi IP (par exemple, les VPN).

Exemple : communication cryptée entre les sites.

Avantage en matière de cybersécurité : assure l'intégrité et la confidentialité des données.

- **Partage de fichiers et services d'annuaire**

NFS (Network File System)

Objectif : partage des fichiers sur un réseau.

Exemple : accès aux fichiers stockés sur un serveur distant.

Préoccupation en matière de cybersécurité : nécessite une authentification appropriée pour empêcher tout accès non autorisé

Samba

Fonction : Permet le partage de fichiers et d'imprimantes entre Linux/Unix et Windows via SMB/CIFS.

Exemple : Accéder à un dossier partagé Linux depuis un PC Windows.

Avantage : Intègre Linux dans des environnements Windows avec gestion des permissions et support Active Directory.

Préoccupation en matière de cybersécurité :Vulnérabilités dans les configurations de partage, exposant potentiellement des fichiers sensibles.

LDAP (Lightweight Directory Access Protocol)

Objectif : Fournit des services d'annuaire pour l'authentification.

Exemple : Systèmes de connexion centralisés dans les organisations.

Préoccupation en matière de cybersécurité : Un LDAP mal configuré peut permettre un accès non autorisé.

- **Traduction d'adresses réseau (NAT)**

La surcharge / pat permet à plusieurs appareils sur un réseau privé de partager une seule adresse IP publique pour l'accès à Internet

Exemple : votre routeur Wi-Fi domestique utilise NAT pour permettre à votre ordinateur portable, votre téléphone et votre téléviseur de se connecter à Internet à l'aide d'une adresse IP publique.

Pertinence en matière de cybersécurité : NAT masque les adresses IP internes, ajoutant ainsi une couche de sécurité

"Dans IPv6, NAT n'est généralement pas nécessaire car chaque appareil peut obtenir une adresse IP publique unique."

Principaux périphériques réseau :

Routeur :

But: Un routeur connecte différents réseaux et dirige les données entre eux en transférant des paquets en fonction des adresses IP.

Rôle de sécurité : Un routeur améliore la sécurité en filtrant le trafic, en bloquant les accès non autorisés, en utilisant NAT et en appliquant des listes de contrôle d'accès (ACL) pour gérer le trafic réseau.

Commutateur

Objectif : Connecter des appareils dans le même réseau local.

Fonctionnalité de sécurité : Prend en charge les VLAN pour isoler le trafic.

Pare-feu

Objectif : autorise ou bloque le trafic en fonction de règles.

Types : pare-feu de filtrage de paquets, avec état et de couche applicative.

Points d'accès (AP)

Objectif : fournit une connectivité sans fil à des appareils tels que des ordinateurs portables, des téléphones et des tablettes.

Problème de sécurité : des mots de passe faibles ou des configurations non sécurisées peuvent permettre un accès non autorisé au réseau. L'utilisation du cryptage WPA3 est recommandée pour une sécurité renforcée.

IDS/IPS (Système de détection d'intrusion / Système de prévention d'intrusion)

IDS : Détecte les intrusions et alerte sans bloquer.

IPS : Détecte et empêche les intrusions en bloquant le trafic malveillant.

Rôle de sécurité :Les deux systèmes améliorent la sécurité du réseau en détectant et en prévenant

les attaques telles que les logiciels malveillants, les tentatives d'accès non autorisées et les anomalies de trafic.

Attaques réseau courantes

DDoS (Distributed Denial of Service)

Description : Les attaquants saturent un réseau avec du trafic excessif, rendant un service ou serveur inaccessible.

Exemple : Un site web devient hors ligne à cause de demandes fictives.

Mitigation : Services de protection DDoS, filtrage du trafic, et limitation de débit.

MITM (Man-in-the-Middle)

Description : L'attaquant intercepte la communication entre deux parties pour voler des données ou injecter du contenu malveillant.

Exemple : Interception de trafic HTTP non chiffré pour voler des identifiants.

Mitigation : Utilisation de HTTPS, chiffrement, et VPNs sécurisés.

ARP Spoofing

Description : L'attaquant envoie de fausses messages ARP pour associer son adresse MAC à l'IP d'un autre appareil.

Exemple : Redirection du trafic réseau vers le système de l'attaquant.

Mitigation : Entrées ARP statiques et outils de surveillance réseau.

DNS Spoofing (DNS Poisoning)

Description : L'attaquant manipule les enregistrements DNS pour rediriger les utilisateurs vers des sites malveillants.

Exemple : Redirection vers un site frauduleux pour voler des informations de connexion.

Mitigation : DNSSEC et services DNS de confiance.

Phishing

Description : Attaque d'ingénierie sociale pour tromper les utilisateurs et leur faire révéler des informations sensibles.

Exemple : Un faux email d'une banque demandant des identifiants.

Mitigation : Éducation des utilisateurs, filtrage des emails, et authentification multi-facteurs (MFA).

Bonnes pratiques de cybersécurité pour les réseaux

Utiliser le chiffrement : Chiffrer les données sensibles en transit (ex. : HTTPS, IPsec, VPN) pour éviter l'interception.

Appliquer une authentification forte : Utiliser l'authentification multi-facteurs (MFA) pour renforcer la sécurité.

Surveiller le trafic réseau : Utiliser des outils comme Wireshark ou un système de surveillance pour détecter les anomalies.

Segmenter les réseaux : Utiliser des VLANs ou des sous-réseaux pour isoler les systèmes sensibles.

Mettre à jour régulièrement : Appliquer les patchs de sécurité pour corriger les vulnérabilités.

Utiliser des pare-feu et IDS/IPS : Installer des pare-feu et des systèmes IDS/IPS pour détecter et prévenir les activités malveillantes.

Implémenter un contrôle d'accès : Limiter l'accès aux systèmes en fonction des besoins, en appliquant le principe du moindre privilège.

Sauvegarder les données critiques : Sauvegarder régulièrement les données importantes pour éviter la perte en cas d'attaque.

Éduquer les utilisateurs : Former régulièrement les utilisateurs sur les risques de phishing et d'autres menaces.

Sécuriser les réseaux sans fil : Utiliser un chiffrement fort (ex. : WPA3) et éviter les identifiants par défaut pour protéger les réseaux Wi-Fi.

Qu'est-ce que le modèle OSI,

Le modèle OSI est un cadre conceptuel utilisé pour comprendre les interactions réseau, divisé en sept couches :

Physique : Gère la transmission physique des données (ex. : câbles, NICs).

Liaison de données : Détecte les erreurs et gère les adresses MAC (ex. : Ethernet).

Réseau : Routage des paquets via les adresses IP (ex. : routeurs).

Transport : Garantit la livraison fiable des données (ex. : TCP, UDP).

Session : Gère les sessions de communication entre applications (ex. : NetBIOS).

Présentation : S'occupe de la traduction, du chiffrement et de la compression des données (ex. : SSL/TLS).

Application : Permet l'interaction utilisateur avec des applications réseau (ex. : HTTP, FTP).

Scénario réel :

Lors de la navigation web, le navigateur utilise HTTP (couche Application), les données sont transférées via TCP (couche Transport), et les routeurs s'assurent que les données arrivent à destination (couche Réseau), avec un chiffrement pour la sécurité (couche Présentation).

Quelle est la différence entre IPv4 et IPv6 ?

Explication :
IPv4 utilise des adresses de 32 bits, offrant environ 4,3 milliards d'adresses uniques. IPv6, en revanche, utilise des adresses de 128 bits, offrant un nombre quasi infini d'adresses (340 undecillions). IPv6 a été conçu pour résoudre l'épuisement des adresses IPv4.

Scénario réel :
Avec l'augmentation du nombre d'appareils connectés à Internet (comme les appareils IoT, les smartphones), les adresses IPv4 sont en voie d'épuisement. IPv6 permet à des appareils comme les réfrigérateurs intelligents, les dispositifs portables et les capteurs d'avoir des adresses IP uniques.

- ### Quelle est la fonction d'un routeur et en quoi diffère-t-il d'un commutateur ?

Fonction d'un routeur :
Un routeur a pour fonction de diriger le trafic entre différents réseaux en utilisant les adresses IP. Il choisit le meilleur chemin pour transférer les paquets de données d'un réseau à un autre.

Différence avec un commutateur :
Un commutateur (switch) fonctionne au niveau de la couche de liaison de données (couche 2) et gère le trafic au sein d'un même réseau local en utilisant les adresses MAC, tandis qu'un routeur gère le trafic entre différents réseaux en utilisant les adresses IP.

- ### Pouvez-vous expliquer ce qu'est le NAT (Network Address Translation) et comment il fonctionne ?

NAT (Network Address Translation) :
Le NAT est une technique qui permet de modifier les adresses IP des paquets de données lorsqu'ils traversent un routeur ou un pare-feu. Il est utilisé pour masquer les adresses IP privées des dispositifs internes d'un réseau, en les remplaçant par une adresse IP publique lors de la communication avec l'extérieur.

Fonctionnement :
Lorsqu'un appareil sur un réseau interne envoie des données vers Internet, le routeur ou le pare-feu effectue une translation de l'adresse IP privée en une adresse IP publique. En retour, le NAT assure que les réponses sont envoyées vers l'appareil correct en utilisant une table de correspondance entre les adresses IP internes et l'adresse IP publique.

Scénario réel :
Imaginez une entreprise avec plusieurs ordinateurs sur un réseau interne utilisant des adresses IP privées (par exemple, 192.168.1.x). Lorsqu'un employé souhaite accéder à un site web, le routeur de l'entreprise utilise NAT pour convertir l'adresse IP privée de l'ordinateur en une adresse IP publique (par exemple, 203.0.113.5). Lorsque le serveur web répond, le routeur traduit à nouveau l'adresse pour rediriger la réponse vers l'ordinateur interne approprié. Cela

permet à de nombreux appareils d'utiliser une seule adresse IP publique pour accéder à Internet tout en maintenant la sécurité et la confidentialité du réseau interne.

Qu'est-ce que le DNS et comment fonctionne-t-il ?

DNS (Domain Name System) :
Le DNS est un système qui traduit les noms de domaine (comme www.karimmaali.com) en adresses IP (comme 192.168.1.1) afin que les navigateurs et autres applications puissent localiser les serveurs et ressources sur Internet.

Fonctionnement :
Lorsqu'un utilisateur entre un nom de domaine dans son navigateur, une requête DNS est envoyée à un serveur DNS qui recherche l'adresse IP correspondante. Si le serveur DNS ne connaît pas l'adresse, il transmet la demande à d'autres serveurs DNS jusqu'à ce qu'il trouve la réponse. Une fois l'adresse IP obtenue, le navigateur peut se connecter au serveur pour charger la page web.

Scénario en temps réel :
Lorsque vous tapez "www.google.com" dans votre navigateur, votre appareil envoie une requête DNS pour traduire ce nom de domaine en une adresse IP. Le serveur DNS interroge ses bases de données ou d'autres serveurs DNS pour trouver l'adresse IP associée (par exemple, 142.250.190.14). Une fois l'adresse trouvée, le navigateur se connecte à ce serveur pour charger la page de Google. Cela permet à l'utilisateur d'accéder à un site web en utilisant un nom facile à retenir plutôt qu'une adresse IP complexe.

Qu'est-ce que l'ARP et comment fonctionne l'usurpation d'identité ARP (ARP spoofing) ?

ARP (Address Resolution Protocol) :
ARP est un protocole utilisé pour mapper les adresses IP aux adresses MAC dans un réseau local (LAN). Lorsqu'un appareil souhaite communiquer avec un autre appareil sur le même réseau, il utilise ARP pour trouver l'adresse MAC associée à une adresse IP donnée.

Usurpation d'identité ARP (ARP Spoofing) :
L'ARP spoofing est une attaque où un attaquant envoie de fausses réponses ARP sur un réseau local. Cela permet à l'attaquant d'associer son adresse MAC à l'adresse IP d'un autre appareil (comme un routeur ou un autre utilisateur). L'attaquant peut alors intercepter, modifier ou rediriger le trafic réseau, permettant des attaques de type Man-in-the-Middle, où il peut voler des données sensibles ou perturber la communication du réseau.

Scénario en temps réel :
Supposons qu'un utilisateur envoie une requête ARP pour trouver l'adresse MAC du routeur sur un réseau local. Un attaquant sur le même réseau envoie une réponse ARP falsifiée, indiquant que son adresse MAC est celle du routeur. À partir de ce moment, l'utilisateur commence à envoyer son trafic au faux routeur (l'attaquant), ce qui permet à l'attaquant d'intercepter et de potentiellement modifier ou voler des informations sensibles, comme des mots de passe ou des données bancaires.

- **Qu'est-ce qu'un VLAN et comment améliore-t-il la sécurité du réseau ?**

VLAN (Virtual Local Area Network) :
Un VLAN est un réseau local virtuel qui permet de segmenter un réseau physique en plusieurs réseaux logiques, indépendants les uns des autres, même si les dispositifs sont connectés au même matériel physique (commutateur).

Amélioration de la sécurité :
Les VLANs isolent le trafic entre différents groupes d'utilisateurs ou services, ce qui limite la portée des attaques. Par exemple, un VLAN peut être dédié à la gestion du réseau, un autre à la production, et un autre aux invités. Cela empêche les utilisateurs d'un VLAN d'interagir directement avec ceux des autres VLANs, augmentant ainsi la sécurité en limitant les risques de propagation des menaces.

Qu'est-ce qu'un VPN et comment fonctionne-t-il ?

VPN (Virtual Private Network) :
Un VPN est une technologie qui permet de créer une connexion sécurisée et chiffrée entre un appareil et un réseau via Internet, comme si l'appareil était connecté directement au réseau local de l'entreprise ou d'un autre endroit sécurisé.

Fonctionnement :
Lorsqu'un utilisateur se connecte à un VPN, toutes ses communications passent par un tunnel sécurisé, qui chiffre les données envoyées et reçues. Cela protège les informations contre l'interception, même si l'utilisateur utilise un réseau public (comme le Wi-Fi d'un café). Le VPN permet également de masquer l'adresse IP de l'utilisateur et de contourner les restrictions géographiques ou les censures en lui attribuant une adresse IP d'un autre endroit.

Quelle est la différence entre TCP et UDP ?

TCP (Transmission Control Protocol) :
TCP est un protocole de transport fiable qui garantit que les données sont envoyées dans le bon ordre et sans erreur. Il établit une connexion entre l'expéditeur et le récepteur, en vérifiant que chaque segment de données est bien reçu. Cela assure une communication fiable, mais peut introduire une certaine latence.

UDP (User Datagram Protocol) :
UDP est un protocole plus rapide mais non fiable. Il n'établit pas de connexion et ne vérifie pas la réception des données. Les segments de données peuvent arriver dans n'importe quel ordre ou être perdus sans notification. UDP est souvent utilisé pour les applications nécessitant des transferts rapides et où la perte de quelques paquets n'est pas critique, comme la diffusion vidéo en temps réel.

Pouvez-vous expliquer la différence entre HTTP et HTTPS ?

Explication :
HTTP est un protocole de transfert de données non sécurisé, tandis que HTTPS (HTTP Secure) utilise un chiffrement SSL/TLS pour sécuriser la communication entre le navigateur et le serveur, assurant ainsi l'intégrité et la confidentialité des informations échangées.

Scénario en temps réel :
Lorsque vous accédez à votre compte bancaire en ligne, le HTTPS crypte la communication entre votre navigateur et le serveur bancaire. Cela protège vos informations sensibles, comme vos identifiants et mots de passe, contre toute interception ou tentative d'attaque par des tiers malveillants.

- Qu'est-ce qu'un pare-feu et comment protège-t-il un réseau ?

Explication :
Un pare-feu agit comme une barrière de sécurité entre un réseau interne et l'extérieur, en filtrant le trafic entrant et sortant selon des règles définies. Il empêche l'accès non autorisé et protège contre les menaces potentielles.

Scénario en temps réel :
Dans un réseau d'entreprise, le pare-feu empêche les attaquants externes d'accéder aux serveurs et systèmes internes. Il bloque également l'accès à des sites web non sécurisés ou à des ports susceptibles d'être utilisés par des logiciels malveillants, garantissant ainsi la sécurité du réseau contre les intrusions et attaques.

- Qu'est-ce que IPsec et comment est-il utilisé dans les réseaux ?

IPsec (Internet Protocol Security) :
IPsec est un ensemble de protocoles utilisés pour sécuriser les communications sur un réseau IP. Il fournit des mécanismes de chiffrement et d'authentification pour protéger les données transmises entre deux dispositifs, assurant ainsi la confidentialité, l'intégrité et l'authenticité des informations.

Utilisation dans les réseaux :
IPsec est couramment utilisé pour établir des connexions VPN sécurisées, en chiffrant le trafic entre un client et un serveur ou entre deux réseaux distants. Il protège les données contre l'interception et l'altération pendant le transfert, ce qui le rend essentiel dans les réseaux d'entreprise, en particulier pour les connexions entre sites distants ou les utilisateurs à distance accédant aux ressources internes via un VPN.

Quel est le but d'un serveur proxy ?

Un serveur proxy sert d'intermédiaire entre un utilisateur et un serveur. Il reçoit les requêtes des utilisateurs, les transmet au serveur cible, puis renvoie la réponse du serveur à l'utilisateur. Cela permet de filtrer le trafic, de cacher l'adresse IP réelle de l'utilisateur, et d'améliorer la sécurité, la performance et l'anonymat des communications.

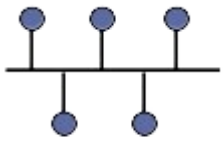
Applications courantes :

- **Sécurité** : Un proxy peut bloquer l'accès à certains sites Web ou filtrer les contenus malveillants.
- **Anonymat** : Il masque l'adresse IP de l'utilisateur, offrant ainsi une certaine confidentialité.
- **Optimisation de la bande passante** : En mettant en cache les réponses courantes, un proxy peut réduire la charge sur le réseau et accélérer l'accès à des ressources fréquemment demandées.

Types de Topologies de Réseau

Topologie en Bus :

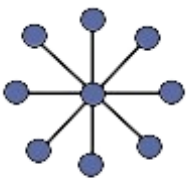
- Tous les appareils sont connectés à un seul câble central. Les données sont envoyées dans une direction et chaque appareil écoute pour déterminer si les données lui sont destinées.



Bus

Topologie en Étoile :

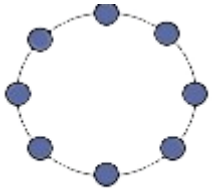
- Chaque appareil est connecté à un concentrateur central (hub ou switch). Si un appareil tombe en panne, le reste du réseau continue de fonctionner.



étoile

Topologie en Anneau :

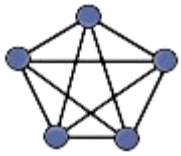
- Les appareils sont connectés en boucle fermée, chaque appareil est relié à deux autres. Les données circulent dans un sens jusqu'à atteindre leur destination.



anneau

Topologie en Maillage :

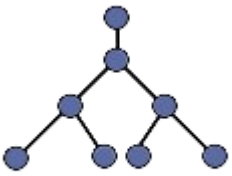
- Chaque appareil est connecté à tous les autres. Elle offre une redondance élevée et est souvent utilisée pour des réseaux de grande envergure ou critiques.



Maillage

Topologie en Arbre (ou Hiérarchique) :

- Combine les topologies en bus et en étoile. Les appareils sont organisés en une hiérarchie, avec des sous-réseaux connectés à un ou plusieurs concentrateurs centraux.



Hierarchical