Réseau : Ensemble de machines ou nœuds interconnectés entre eux à travers une infrastructure informatique dans l'objectif d'échanger les données.

Dimension d'un réseau :

--->Géographique :

-LAN (Local Area Network) : LAN signifie réseau local. Il s'agit d'un groupe de périphériques réseau qui permettent la communication entre divers périphériques connectés. LAN a un délai de propagation court que MAN ainsi que WAN. Il couvre les zones plus petites telles que les collèges, les écoles, les hôpitaux, etc.

Protocoles : Ethernet, Token Ring et FDDI

Dispositifs terminaux de communication : câbles Ethernet et WI-Fi

-MAN (Metropolitan Area Network) : signifie réseau métropolitain. Il couvre une zone plus vaste que le réseau local, comme les petites villes, les villes, etc.

Les MAN sont des réseaux de connexion à haut débit qui interconnectent plusieurs réseaux locaux en un seul réseau de grande taille avec un pont commun. Ce pont est appelé "backbone lines" qui est généralement établi par fibre optique pour augmenter la vitesse de transfert des données.

-WAN (Wide Area Network) : signifie réseau étendu. Il couvre une zone plus vaste que le LAN ainsi qu'un MAN tel qu'un pays/continent, etc.

Les dispositifs concernés sont plus diversifiés que ceux appliqués aux autres types, des routeurs aux commutateurs réseau, en passant par les modems, pare-feu, etc. Le WAN peut être virtuel via l'utilisation d'un VPN par exemple.

--->Hardware :

- Modem : Le modem établit la connexion entre votre réseau domestique (LAN) et le réseau Internet général (WAN).
- Switch : Aussi appelé commutateur réseau en français, c'est un équipement qui relie plusieurs segments dans un réseau informatique et qui permet de créer des circuits virtuels.
- Routeur : Le routeur est un appareil regroupant plusieurs fonctionnalités. Sa fonction de base est de permettre la communication entre un réseau local et Internet. Voici les fonctionnalités qu'on y retrouve : modem, switch, serveur DHCP, Firewall. On peut aussi y trouver un serveur VPN, la possibilité de lancer une VirtualMachine dessus…. En résumé c'est un organe réseau polyvalent.
- NAS : NAS Le NAS (Network Attached Storage) est un serveur de fichiers capable de fonctionner de façon autonome. Il permet de stocker les données de façon sécurisée. Il peut contenir une grande capacité de stockage.
- RAID La technologie RAID (Redundant Array of Independent Disks) permet de répartir les données sur plusieurs disques durs afin d'obtenir un stockage plus rapide, plus sécurisé ou les deux. Objectifs : Ne pas perdre les données + Stocker les données

Restreindre les utilisateurs :

- **Par-feu (IP TABLE):** est un système qui empêche un accès non autorisé depuis des réseaux externes et qui protège des attaques/intrusions sur un réseau local. Vous pouvez utiliser un pare-feu dans votre environnement réseau pour bloquer

l'accès depuis un réseau externe qui est considéré comme dangereux en restreignant les communications depuis l'adresse IP spécifiée d'un réseau externe (filtagre des addresses IP).

- **FAIL2BAN :** Une autre méthode pour restreindre un utilisateur à se connecter au réseau. A travers la configuration du fail2ban, on peut par exemple interdire une adresse IP à se connecter ou bloquer un utilisateur après un nombre de connexion.
- **Wireshark :** C'est un analyseur de paquets réseaux pour déterminer si une machine est infectée en analysant les connexions effectuées par les malwares.

Différence entre Cloud privé, public et hybride :

Un **cloud public** est un type de **cloud** computing dans lequel un fournisseur de services met des ressources de partage à la disposition du **public** via internet.

Les clouds privés sont généralement définis comme des environnements cloud spécifiques à un utilisateur final ou à un groupe, et sont habituellement exécutés derrière le pare-feu de l'utilisateur ou du groupe (accès entièrement isolé).

Cloud Hybride le Cloud hybride consiste à connecter un ou plusieurs Clouds publics à un Cloud privé .

C'est quoi un serveur : est un dispositif informatique qui fournit des ressources partagées aux utilisateurs à travers une communication entre eux (client/serveur).

Types des serveurs :

- **Serveurs des fichiers :** FTP pour le transfert des fichiers
- **Serveurs d'applications :** offre un contexte d'exécution aux ordinateurs clients pour leur éviter d'exécuter des applications localement
- **Serveurs DNS :** sont des serveurs d'applications utilisés pour résoudre les noms de domaines des ordinateurs clients, c'est-à-dire traduire des noms conçus pour être compris de l'homme en adresses IP exploitables par une machine.
- **Serveurs de messagerie : SMTP**
- **Serveurs WEB :** comme APACHE
- **Serveurs de BDD :**
- **Serveur de proxy :** il le rôle de passerelle entre la machine et l'Internet. C'est un serveur intermédiaire qui va filtrer les requêtes (joue le rôle d'un pare-feu), fournit des connexions réseau partagées et place les données en cache pour accélérer le traitement des requêtes les plus courantes
- **Serveurs DHCP :** est un serveur qui délivre des adresses IP aux équipements qui se connectent sur le réseau, délivre le bail DHCP (durée de temps pour laquelle les informations seront alloués pour la machine cad que l'adresse IP attribuée à une machine a une durée limitée), et fournit des paramètres réseaux (masquage de sous-réseau et adresse IP de la passerelle &DNS)

Communication Client/Serveur :

--->Couche 4 TCP/UDP : La couche 4 qui permet la communication réseau utilise 2 principaux protocoles, UDP et TCP

- **TCP :** Ce protocole permet d'envoyer une trame de données en s'assurant que les données ont bien été reçues, il y a une vérification de l'intégrité de la trame a la réception. Si la trame semble corrompue, elle est alors envoyée à nouveau. Ce protocole nécessite une validation et donc l'envoie et la réception de plusieurs signaux pour une même trame. De ce fait, ce protocole induit une certaine latence.

- **UDP :** Le protocole UDP est plus simple, les trames sont envoyées puis une fois reçu il y a deux possibilités : - la trame est valide, elle est alors utilisé - La trame est invalide, elle est ignorée Ce protocole étant plus rapide, il est utilisé pour tous les services ayant besoin d'une grande réactivité comme le streaming, le voip ….

➔ Ports :

Pour établir une connexion réseau, les protocoles UDP et TCP ont besoin de canaux de communication, ces canaux sont appelés ports. Les ports sont numérotés en continu, de 0 à 65 536. Y'en a certain qui sont déjà normalisé et définit comme le port 22 pour le SSH, 80 pour le protocole HTTP et le 443 pour le HTTPS…

➔ Sockets :

Le socket permet d'établir une connexion vers une IP à travers un port. Il est possible de déclarer plusieurs sockets sur le même port afin d'avoir plusieurs communications en parallèle.

L'intérêt d'utiliser une machine virtuelle : Pour optimiser vos équipements et la maintenance devient plus simple. Un matériel virtuel n'est pas sujet aux défaillances. Les ressources physiques sont mutualisées pour les machines virtuelles et un même serveur peut supporter plusieurs VM. Coté utilisateur, l'interaction avec une VM est la même que pour une machine physique. + flexibilité sans impacter le reste des machines et maitenance en cas de panne et inconv performance te coût

Trace route ➔ pc – routeur + dns +site

Vertualisation : La virtualisation est un mécanisme informatique qui consiste à faire fonctionner plusieurs systèmes, serveurs ou applications, sur un même serveur physique

Types des hyperviseurs : type 1 : directement connecté au hardware / type 2 : un logiciel installé dans l'os qui fait la communication alors il faut paser obligatoirement par l'os

Hyperviseur vs paravirtualisation : Para => la machine virtuelle a un accès directe au Hardware (carte réseaux) alors que dans l'hyperviseur la machine ets isolée du Hw

Dimensionner un réseau en fonction d'un besoin : Qualité des câbles et types des switchs

Augmenter la bande passante : dimensionner les switchs et qualité des câbles