Cours 1 : Networking Devices

Ceci est un cours pour le CCNA nous allons voir tous les sujets qui concernent le CCNA.
Ce cours est dédié pour :
- Les personnes qui veulent passer l'examen du CCNA
- Les personnes qui veulent comprendre comment fonctionne un réseau

Nous allons comprendre d'abord les bases du réseau.
Donc qu'est ce qu'un Réseau ou Network en Anglais ?
« un réseau d'ordinateur est un réseau de télécommunication digital qui permet à des nœud de partager des ressources. »

Qu'est ce qu'un nœud ?
Pour comprendre nous allons prendre l'exemple de différents matériaux et de leurs symbole.

Voici un routeur : 

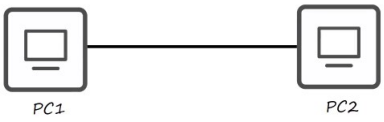
Ceci est un Switch ou Commutateur : 

Ceci est un Firewall ou Pare feu : 

Voici le serveur : 

Le poste client : 

Nous allons voir des exemples de différents types de réseaux.
Voici un premier exemple d'un réseau, cela peut sembler être un petit réseau mais à partir du moment ou deux ordinateurs sont connectés en même temps cela constitue un réseau, et cela correspond bien à la définition d'un réseau qui indique qu'un réseau d'ordinateur permet de partager des ressources.

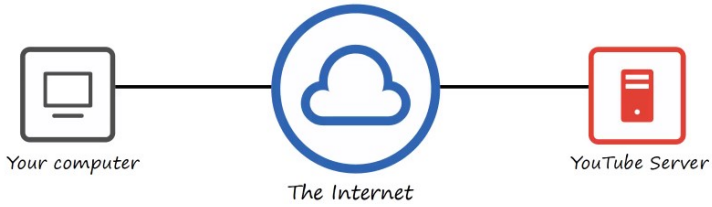


Un client peut être un téléphone, un ordinateur portable, un Mac, un ordinateur de bureau, etc..
Voici la définition d'un client :
« Un client est un appareil qui accède à un service rendu disponible par un serveur. »

Qu'est ce qu'un serveur ?
C'est tout simplement la définition inverse d'un client :
« Un appareil qui fournit des fonctions ou services pour des clients. »

Si l’on reprend l’exemple du réseau avec les deux PC on peut avoir le PC1 qui demande au PC2 de lui fournir des image jpg, le PC2 répond en fournissant ces images.
Ici le client est le PC1 et le PC2 est le serveur.

Voici un deuxième exemple d’un réseau avec un serveur et un client :



Le nuage est le symbole pour représenter Internet.
L’ordinateur demande la vidéo au serveur, le serveur Youtube envoie les données à travers le réseau.

Un exemple d’un réseau avec des Iphone :

L’Iphone qui fais la demande de vidéo est le client et l’autre est le serveur.

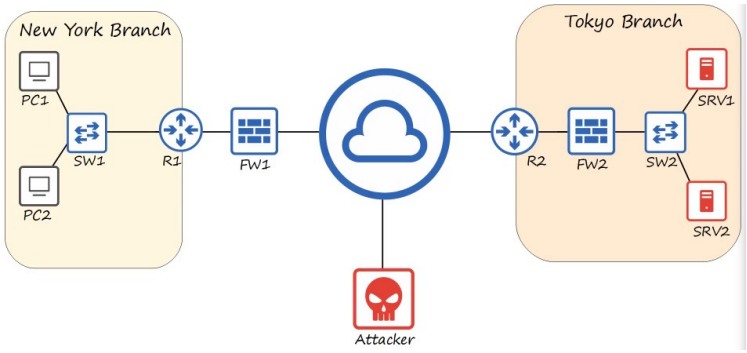
Il faut garder à l’esprit qu’un même appareil peut être un client dans certaines situation et un serveur dans d’autres situations.

Nous allons prendre un exemple plus large entre des clients se trouvant à New York et des serveurs se trouvant à Tokyo.
On ne connecte pas les clients directement entre eux la solution adapté est le Commutateur (ou Switch en Anglais) qui relie les appareils entre eux. Voici l’exemple d’un Switch qui permet de relier les clients et serveurs par ses interfaces. Voyons quelques caractéristiques de switchs :
- Les switchs ont plusieurs interfaces/ports réseau pour connecter les hôtes habituellement 24.
- Les switchs fournissent une connectivité pour les hôtes dans le même LAN (Local Area Network)
- Les switchs ne fournissent pas de connectivité entre des LAN sur Internet.

Tous ces périphériques font partis du même réseau aussi appelé LAN pour Local Area Network.
Les switchs ne communiquent pas directement avec Internet pour partager leurs ressources entre LAN, il est utilisé pour cela le routeur qui permet le partage de ressources à travers Internet.
Voyons quelques caractéristiques des Switchs :
- Les routeurs ont moins d’interfaces réseau que les switchs.
- Les routeurs fournissent de la connectivité entre les LANs
- Ils sont donc utilisés pour envoyer des données sur Internet.

Voici l’exemple du réseau schématisé :

Nous pouvons imaginer qu’il y ait un attaquant qui essaye de s’introduire dans notre réseau, la meilleure façon de se protéger contre cela est le Firewall.
Les Firewall sont spécialement conçus pour la sécurité du réseau et permettent de filtrer les entrées et sortis du réseau. Un Firewall peut être placé en dehors du réseau ou bien à l’intérieur du réseau.
Comme dans cette exemple :



L’essentiel est qu’ils protège les hôtes du dehors du réseau qui sont les appareils comme les ordinateurs.
Le Firewall est configuré avec des règles qui permettent d’autoriser quelle réseau sera permis et lequel sera renié. Il faut que les ordinateurs clients soient autorisés à passer le Firewall et puis celles externes qui pourraient être des attaquants soient bloqués en tentant de passer le Firewall.
Voici un exemple de Firewall :

Voici quelques caractéristiques des Firewalls :
- Il contrôlent et gèrent le trafique réseau basé sur les règles de configurés.
- Les Firewall peuvent être placés à l’intérieur et à l’extérieur du réseau
- Ils sont connus comme « Next Generation Firewall » lorsqu’ils incluent plus de capacités de filtrage plus modernes.

Nous avons vu des Firewall Hardware qui filtrent le trafique entre les réseaux. Ce sont les Network Firewall.
Il existe aussi les Host-Based Firewall qui sont des applications qui filtrent le trafique entrant et sortant d’une machine hôte comme un ordinateur.
C’est une protection supplémentaire pour le réseau.